

А.М. Голиков

**СЕТИ И СИСТЕМЫ РАДИОСВЯЗИ И СРЕДСТВА ИХ
ИНФОРМАЦИОННОЙ ЗАЩИТЫ**

Учебное пособие

Томск

Федеральное агентство по образованию

Томский государственный университет
систем управления и радиоэлектроники

А.М. ГОЛИКОВ

**СЕТИ И СИСТЕМЫ РАДИОСВЯЗИ И СРЕДСТВА ИХ
ИНФОРМАЦИОННОЙ ЗАЩИТЫ**

Учебное пособие

2007

УДК 621.396.001.25(075.8)
ББК 32.884.1я73
Г60

Рецензенты:

Голиков А.М.

Сети и системы радиосвязи и средства их информационной защиты: учеб. пособие / А.М. Голиков. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 392 с.
ISBN 978-5-86889-393-3

Рассмотрены современные сети и системы радиосвязи, включая системы цифровой радиорелейной связи, аналоговые и цифровые системы транкинговой связи, системы сотовой связи стандарта GSM, сети и системы радиотелефонной связи, использующие стандарты IS-95 (CDMA) и DECT, стандарты кодирования информации в пейджинговых сетях, перспективные спутниковые системы связи, включая спутниковые системы персональной радиосвязи, стандарты беспроводных локальных сетей IEEE 802.11, персональные сети радиодоступа стандартов IEEE 802.15, стандарты городских сетей широкополосного радиодоступа IEEE 802.16 (WiMAX), а также средства информационной защиты сетей и систем радиосвязи, предусмотренные соответствующими стандартами.

Предназначено для изучения вопросов, предлагаемых Государственным образовательным стандартом по специальности 210403 – Защищенные системы связи.

УДК 621.396.001.25(075.8)
ББК 32.884.1я73

ISBN 978-5-86889-393-3

@ Голиков А.М., 2007
@ Томск. гос. ун-т систем упр.
и радиоэлектроники, 2007

СОДЕРЖАНИЕ

Предисловие	4
1. Системы цифровой радиорелейной связи	5
2. Транкинговые системы радиосвязи	26
3. Системы сотовой связи стандарта GSM	67
4. Системы подвижной связи в стандартах IS-95 (CDMA) и DECT	111
5. Стандарты кодирования в пейджинговой связи	142
6. Перспективные спутниковые системы связи	152
7. Беспроводные локальные сети на основе стандартов IEEE 802.11	193
8. Персональные сети радиодоступа. Стандарты IEEE 802.15, Bluetooth	212
9. Стандарты городских сетей широкополосного радиодоступа IEEE 802.16 (WiMAX)	240
Рекомендуемая литература	282
Интернет ссылки	283
ПРИЛОЖЕНИЯ	285

ПРЕДИСЛОВИЕ

Учебное пособие предназначено для изучения современных сетей и систем цифровой радиосвязи и средств их информационной защиты студентами специальности 210403 – Защищенные системы связи.

Цифровая радиосвязь это одна из наиболее динамично развивающихся областей телекоммуникаций. Ожидается, что в течение следующих десяти лет не менее половины всех устанавливаемых соединений станут частично или полностью беспроводными. Системы подвижной радиосвязи перешли из разряда дорогих игрушек для богатых пользователей в массовый сектор рынка. Быстрое развитие сети Интернет, ее приложений и новых услуг создало благоприятную почву для дальнейшего развития мобильных систем.

В настоящее время цифровая радиосвязь позволяет реализовать полный спектр информационных услуг: передачу телефонных сообщений, обмен данными, подключение к глобальным информационным сетям, получение и передачу видеоизображений, телевидения и т.д. Радиосвязь дополняет и расширяет возможности проводной связи, дает свободу передвижения. Применение средств радиосвязи реализует единое информационное пространство, позволяющее в любой точке планеты и в любое время получать необходимые информационные услуги.

В последние годы в мире наблюдается повышенный интерес к системам беспроводного доступа, а также лавинный рост производства оборудования. В результате оборудование от различных производителей появляется практически сразу после объявления о стандартизации технологии. Несмотря на недавнее происхождение, понятия BWA, WiFi, RLAN, WiMAX, FWA, WLAN и др. прочно вошли в обиход специалистов в области радиосвязи.

Сегодня все более ощущается потребность в качественных, надежных и емких каналах связи. Если в Европе на магистральных линиях основную роль играют волоконно-оптические линии связи, то на просторах России прокладка оптоволоконной линии связи может иметь слишком высокую стоимость. Применение цифровых радиорелейных систем (ЦРРС) позволит значительно снизить расходы на эксплуатацию такой линии связи.

В настоящее время профессиональная мобильная радиосвязь обеспечивается цифровыми транкинговыми системами связи. В России заказчиками систем профессиональной мобильной радиосвязи являются крупные ведомства и корпорации, такие как РАО ЕЭС, Минтранс, МПС, Сибнефть и другие, а также силовые структуры и правоохранительные органы.

Бурно развивающиеся сети сотовой связи сейчас предоставляют 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).

Спутниковая связь составляет относительно небольшой удельный вес в общем объеме телекоммуникационной индустрии, однако темпы развития спутниковой связи стремительно наращиваются в последние годы. В последнее десятилетие распространение получили малоапертурные наземные станции типа VSAT, обеспечившие возможность организации межрегиональных и корпоративных спутниковых телекоммуникаций с голосовой связью и цифровой передачей данных "из конца в конец" при достаточно низкой стоимости.

Беспроводные сети и системы связи является наиболее уязвимыми, с точки зрения защиты передаваемой информации, поэтому современные стандарты включают в себя особые требования к средствам их информационной защиты.

1. СИСТЕМЫ ЦИФРОВОЙ РАДИОРЕЛЕЙНОЙ СВЯЗИ

В России наиболее широкое распространение получили две технологии построения транспортной инфраструктуры оператора связи: на основе волоконно-оптических систем и на основе систем радиосвязи. Первые характеризуются очень высокой пропускной способностью, но при этом требуют серьезных изыскательских работ и времени на реализацию проекта. В связи с этим волоконная оптика нашла применение прежде всего у операторов междугородной и международной связи. Системы радиосвязи позволяют гибко и оперативно охватывать большие территории, но при этом имеют ограниченную пропускную способность, что во многом обусловлено количеством частотных назначений, выданных тому или иному оператору.

На протяжении уже многих лет одним из наиболее экономичных и быстрых способов организации радиопередачи информационно-транспортных потоков на большие расстояния остается радиорелейная связь. Причем, если раньше в основной своей массе магистральные линии, обеспечивающие такую связь, были аналоговыми, то сейчас им на смену пришли современные цифровые радиорелейные станции (ЦРРС), обладающие высокой пропускной способностью. Работают такие станции, как правило, в диапазоне частот 3,4-11,7 ГГц. Их пропускная способность составляет 155 Мбит/с и более, а передача сигналов ведется с использованием многопозиционных видов модуляции. Для ЦРРС магистральных и внутризональных линий характерно наличие системы телеобслуживания, программно поддерживающей уровень управления сетевыми элементами и сетью, а также обеспечивающей контроль, управление и техническое обслуживание оборудования. Со строительством высокоскоростных ЦРРС связано ведущееся в настоящее время интенсивное освоение районов Крайнего Севера, которое требует серьезных инвестиций не только в создание технологических объектов, но и в построение телекоммуникационной составляющей. Выбор технологии построения транспортной инфраструктуры этого региона во многом предопределили его климатические и природные особенности. В частности, низкие температуры в зимний период, требующие специальных технологий защиты волоконно-оптических кабелей при их подвешивании на опоры (например, линий электропередач), наличие огромного количества водных преград (особенно в Ямало-Ненецком округе) и вечная мерзлота грунта серьезно затрудняют использование волоконной оптики в северных округах Тюменской области.

В сети связи Томской области доля радиорелейной связи составляет 60-70%. Преобладание радиорелейных систем над проводными и спутниковыми основывается на следующих факторах:

- большая площадь территории области - 314,4 тыс. км²;
- особенности рельефа: степень заболоченности Томской области достигает 40%, на долю речных долин приходится 1/5 всей территории области, лесные массивы занимают 63% территории;
- большие расстояния между населёнными пунктами,
- развитая нефте- и газодобывающая отрасль, требующая обеспечения связи на больших расстояниях и в труднодоступных районах, а также на протяжении всей трассы трубопроводов.

Наиболее крупными владельцами радиорелейных систем передачи информации на территории Томской области являются следующие организации:

- ООО «СибПТУС», обеспечивающая технологическую связь вдоль нефтепроводов, проходящих через Томскую область;
- ООО «Томсктрансгаз», обеспечивающая технологическую связь вдоль газопроводов, проходящих через Томскую область;
- ОАО «Сибирьтелеком», являющаяся оператором дальней связи на территории Томской области;

- операторы сотовой связи ОАО «Вымпелком» и ОАО «МТС».

Перед разработкой любого проекта следует рассмотреть все возможные альтернативные варианты. В качестве таковых в нашем случае возможен только один – аренда потоков у других операторов, поскольку заболоченность местности, большие расстояния и тяжелые климатические условия не позволяют даже рассматривать построение оптоволоконной системы связи. Вариант с арендой каналов для организации ООО «Томсктрансгаз» является неприемлемым по следующим причинам: во-первых, точки доступа к другим операторам в некоторых местах расположены на значительном расстоянии от мест расположения аппаратуры «Томсктрансгаз», что приведет к необходимости проведения дополнительных строительных работ; во-вторых, не во всех пунктах доступа имеется достаточная пропускная способность, необходимая для «Томсктрансгаз»; в-третьих, аренда каналов в долгосрочной перспективе оказывается слишком дорогой по сравнению с модернизацией используемого сейчас оборудования «Трал 400/24».

Последним и наиболее важным условием необходимости проектирования собственной цифровой РРЛ становится независимость обеспечения технологической связи от внешних факторов.

Обзор радиорелейных линий связи

В состав любой радиорелейной станции входит следующее оборудование:

- 1) аппаратура уплотнения каналов;
- 2) аппаратура служебной связи,
- 3) телесигнализации и телеуправления;
- 4) приемопередающая аппаратура;
- 5) аппаратура систем автоматического резервирования стволов;
- 6) антенно-фидерные устройства;
- 7) оборудование систем гарантированного электропитания

Современный приемопередающий комплекс способен передавать от нескольких каналов тональной частоты до 34 Мбит/с при плезиохронной цифровой иерархии (ПЦИ), и от потока STM-0 до STM-16 при синхронной цифровой иерархии (СЦИ).

В тех случаях, когда радиорелейная система передачи (РРСП) предназначена для передачи большого числа сигналов, она образуется несколькими приемопередающими комплексами, работающими в одном направлении на различных частотах. Каждый из таких комплексов сверхвысокочастотных приемопередатчиков принято называть стволом.

По пропускной способности различают следующие РРЛ:

- а) многоканальные, с числом каналов ТЧ свыше 300;
- б) средней емкости – от 60 до 300 каналов ТЧ
- в) малоканальные – меньше 60 каналов ТЧ.

По области применения РРЛС делятся на магистральные, протяженностью более 2,5 тысяч км, внутризоновые – республиканского и областного значения протяженностью 250-1400 км, местные 50-200 км.

По способу деления каналов РРЛС могут быть с частотным и временным разделением каналов, а по диапазону используемых частот – дециметрового, сантиметрового и миллиметрового диапазонов.

Чтобы обеспечить радиорелейную связь в пределах прямой видимости, необходимо поднять антенны над уровнем земли на башнях или мачтах. Высоты антенных опор в зависимости от длины и профиля каждого пролета между соседними станциями могут

достигать 120 м, строительство более высоких антенных башен становится экономически невыгодным.

Длина пролета между соседними РРС обычно от 30 до 55 км. В диапазонах частот выше 11 ГГц это значение может уменьшаться с повышением частоты. В отдельных случаях длина может быть уменьшена до 20 или 30 км из-за необходимости размещения РРС в заданном пункте, а также когда на трассе РРЛ имеются препятствия.

Ограниченность расстояния прямой видимости не следует рассматривать как сугубо отрицательный фактор. Именно за счет невозможности свободного распространения радиоволн на большие расстояния устраняются взаимные помехи между РРС, а также возможно повторное использование частотного диапазона.

Основные проблемы организации связи

Физические процессы, происходящие в канале связи, определяют изменения, которые претерпевает сигнал на пути от передатчика к приемнику.

Во-первых, на сигнал действуют *аддитивные помехи*. Для НЧ и СЧ систем такими помехами являются сигналы соседних по частоте радиостанций, атмосферные и промышленные шумы. Для УВЧ и СВЧ радиорелейных систем решающее значение приобретают собственные внутренние шумы приемных устройств, а для систем космической радиосвязи к ним добавляются шумы космического происхождения (при нарушении правил электромагнитной совместимости возможно также влияние других радиосредств, работающих в совмещенном диапазоне частот).

Во-вторых, на сигнал в канале действуют *мультипликативные помехи*, обусловленные изменениями параметров канала как четырехполосника.

Совместное воздействие аддитивных и мультипликативных помех определяет искажения сигнала. Величина искажений зависит от интенсивности помех и помехоустойчивых свойств системы связи. Любой канал связи вносит те или иные искажения. Вместе с тем передача считается неискаженной, если вносимые системой связи искажения не превышают установленных норм.

Электрические характеристики систем связи, определяющие искажения передаваемой информации, определяются на внутренних линиях РФ нормами ЕАСС, на международных линиях - рекомендациями МСЭ и Т.

Немаловажна ещё одна проблема. Загрузка диапазона радиочастот до 11 ГГц в настоящее время такова, что средства самой радиосвязи вынуждены работать в совмещенных диапазонах частот, а ведь в этом диапазоне работают еще и средства радиолокации, радионавигации, радиотелеметрии. Возникает серьезная и сложная проблема электромагнитной совместимости различных радиосредств, требующая решения не только в национальном, но и в глобальном масштабе.

Плезиохронная цифровая иерархия

Плезиохронная цифровая иерархия была разработана в начале 80-х годов. Она делится на три различные иерархические цифровые наборы, или цифровые иерархии. В первой из них, принятой в США и Канаде, в качестве скорости сигнала первичного цифрового канала (ПЦК) -DS1 была выбрана скорость 1544 кбит/с (т.е. двадцать четыре цифровых телефонных канала 64 кбит/с). Во второй, принятой в Японии, использовалась та же скорость для DS1. В третьей, принятой в Европе и Южной Америке, в качестве первичной была выбрана скорость 2048 кбит/с (формально количество каналов - 32, но два канала используются для сигнализации и управления).

Первая иерархия, порожденная скоростью 1544 кбит/с, давала последовательность: DS1 -DS2 - DS3 - DS4 или последовательность вида: 1544 - 6312 - 44736 - 274176 кбит/с,

что, с учетом скорости DS0, соответствует ряду коэффициентов мультиплексирования $n=24$, $m=4$, $l=7$, $k=6$. Указанная иерархия позволяет передавать соответственно 24, 96, 672 и 4032 канала DS0.

Вторая иерархия, порожденная скоростью 1544 кбит/с, давала последовательность DS1 - DS2 - DS3 - DS4 или последовательность 1544 - 6312 - 32064 - 97728 кбит/с, что, с учетом скорости DS0, соответствует ряду коэффициентов мультиплексирования $n=24$, $m=4$, $l=5$, $k=3$. Указанная иерархия позволяет передавать соответственно 24, 96, 480 и 1440 каналов DS0.

Третья иерархия, порожденная скоростью 2048 кбит/с, давала последовательность E1 - E2 - E3 - E4 - E5 или последовательность 2048 - 8448 - 34368 - 139264 - 564992 - кбит/с, что соответствует ряду коэффициентов $n=30$ (32), $m=4$, $l=4$, $k=4$, $i=4$, (т.е. коэффициент мультиплексирования в этой иерархии выбирался постоянным и кратным 2). Указанная иерархия позволяет передавать соответственно 30, 120, 480, 1920 и 7680 каналов DS0, что отражается и в названии ИКМ систем: ИКМ-30, ИКМ-120, ИКМ-480 и т.д..

Указанные иерархии, известные под общим названием плезиохронная цифровая иерархия PDH, или ПЦИ, сведены в таблицу 1.1.

Таблица 1.1 - Схемы цифровых иерархий: американская (АС), японская (ЯС) и европейская (ЕС)

Уровень цифровой иерархии	Скорости передачи, соответствующие различным схемам цифровой иерархии		
	АС: 1 544 кбит/с	ЯС: 1544 кбит/с	ЕС: 2048 кбит/с
0	64	64	64
1	1544	1544	2048
2	6312	6312	8448
3	44736	32064	34368
4	—	97728	139264

Параллельное развитие трех различных иерархий не могло способствовать развитию глобальных телекоммуникаций в мире в целом, поэтому комитетом по стандартизации ИТУ-Т или МСЭ-Т были сделаны шаги по их унификации и возможному объединению. В результате был разработан стандарт, согласно которому были стандартизованы три первых уровня первой иерархии (DS1-DS2-DS3), четыре уровня второй иерархии (DS1-DS2-DSJ3-DSJ4) и четыре уровня третьей иерархии (E1-E2-E3-E4) в качестве основных. Также были указаны схемы кросс-мультиплексирования иерархий, например, из третьей в первую и обратно. На рисунке 1.1 схематично представлен результат, полученный после стандартизации.

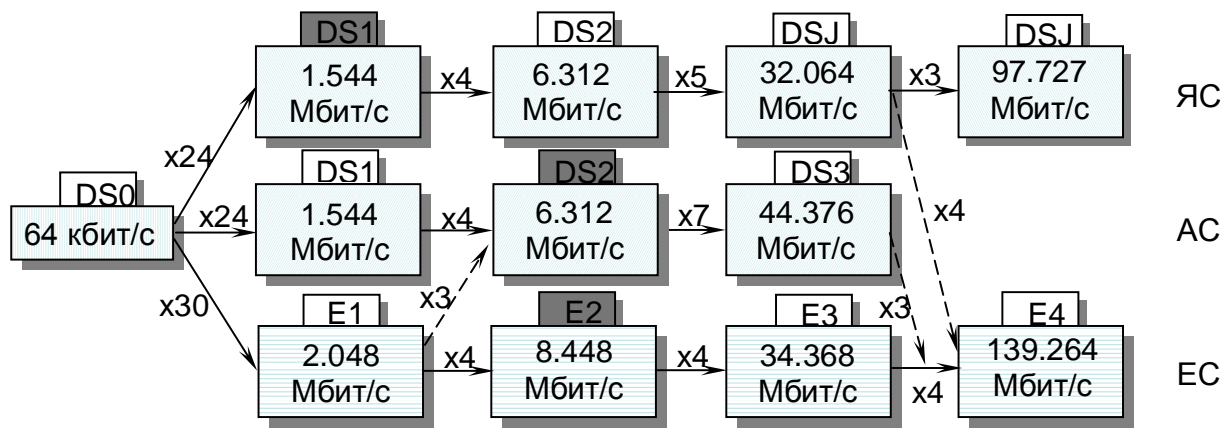


Рис. 1.1-Схема мультиплексирования и кросс-мультиплексирования в американской, японской и европейской цифровых иерархиях

Наличие стандартных скоростей передачи и фиксированных коэффициентов мультиплексирования позволило говорить о трех схемах мультиплексирования - американской, японской и европейской. При использовании жесткой синхронизации при приеме/передаче можно было бы применить метод мультиплексирования с чередованием октетов или байтов, как это делалось при формировании цифровых сигналов первого уровня, для того, чтобы иметь принципиальную возможность идентификации байтов или групп байтов каждого канала в общем потоке. Однако учитывая, что синхронизация входных последовательностей, подаваемых на мультиплексор от разных абонентов/пользователей, отсутствует, в схемах второго и более высокого уровней мультиплексирования был использован метод мультиплексирования с чередованием бит (а не байт). В этом методе мультиплексор, например, второго уровня формирует выходную цифровую последовательность скоростью 6 Мбит/с - АС, ЯС (или 8 Мбит/с - ЕС) путем чередования бит входных последовательностей от разных каналов (для АС и ЯС это каналы Т1, а для ЕС - каналы Е1).

Так как мультиплексор не формирует структуры, которая могла бы быть использована для определения позиции бита каждого канала, а входные скорости разных каналов могут не совпадать, то используется внутренняя побитовая синхронизация, при которой мультиплексор сам выравнивает скорости входных потоков путем добавления или удаления нужного числа выравнивающих бит в каналы с относительно меньшими скоростями передачи. Благодаря этому на выходе мультиплексора формируется синхронизированная цифровая последовательность. Информация о вставленных/изъятых битах передается по служебным каналам, формируемым отдельными битами в структуре фрейма. На последующих уровнях мультиплексирования эта схема повторяется, добавляя новые выравнивающие биты. Эти биты затем удаляются/добавляются при демультиплексировании на приемной стороне для восстановления исходной цифровой последовательности. Такой процесс передачи получил название плезиохронного (т.е. почти синхронного), а цифровые иерархии АС, ЯС и ЕС соответственно название плезиохронных цифровых иерархий - PDH.

Кроме синхронизации, на уровне мультиплексора второго порядка также происходит формирование фреймов и мультифреймов, которые позволяют структурировать последовательность в целом. Формирование фреймов и мультифреймов и их выравнивание особенно важно для локализации на приемной стороне каждого фрейма, что позволяет в свою очередь получить информацию о сигнализации и кодовых группах контролируемых избыточных кодов CRC и информацию служебного канала данных.

Общая схема канала передачи с использованием технологии PDH даже в самом простом варианте топологии сети "точка - точка" на скорости 140 Мбит/с должна

включать три уровня мультиплексирования на передающей стороне (для ЕС, например, 2→8, 8→34 и 34→140) и три уровня демультиплексирования на приемной стороне, что приводит к достаточно сложной аппаратурной реализации таких систем.

Еще одним недостатком систем передачи плездохронной цифровой иерархии является также то, что при нарушении синхронизации группового сигнала восстановление синхронизации первичных цифровых потоков происходит многоступенчатым путем, а это занимает довольно много времени.

Но самое главное, что заставило уже в середине 80-х годов XX в. искать новые походы к построению цифровых иерархий систем передачи, это почти полное отсутствие возможностей автоматически контролировать состояние сети связи и управлять ею. А без этого создать надежную сеть с высоким качеством обслуживания практически невозможно. Все эти факторы и побудили разработать еще одну цифровую иерархию.

Синхронная цифровая иерархия

Новая цифровая иерархия была задумана как скоростная информационная автострада для транспортирования цифровых потоков с разными скоростями. В этой иерархии объединяются и разъединяются потоки со скоростями 155,520 Мбит/с и выше. Поскольку способ объединения потоков был выбран синхронный, то данная иерархия получила название синхронной цифровой иерархии (Synchronous Digital Hierarchy — SDH).

Для транспортирования цифрового потока со скоростью 155 Мбит/с создается синхронный транспортный модуль (Synchronous Transport Module) STM-1. Его упрощенная структура дана на рисунок 1.1.. Модуль представляет собой фрейм (рамку) $9 \cdot 270 = 2430$ байт. Кроме передаваемой информации (называемой в литературе полезной нагрузкой), он содержит в 4-й строке указатель (Pointer, PTR), определяющий начало записи полезной нагрузки.



Рис. 1.2 – Структура модуля STM-1

Чтобы определить маршрут транспортного модуля, в левой части рамки записывается секционный заголовок (Section Over Head, SOH). Нижние $5 \cdot 9 = 45$ байтов (после указателя) отвечают за доставку информации в то место сети, к тому мультиплексору, где этот транспортный модуль будет переформировываться. Данная часть заголовка так и называется: секционный заголовок мультиплексора (MSOH). Верхние $3 \cdot 9 = 27$ байтов (до указателя) представляют собой секционный заголовок регенератора (RSOH), где будут осуществляться восстановление потока, "поврежденного" помехами, и исправление ошибок в нем.

Один цикл передачи включает в себя считывание в линию такой прямоугольной таблицы. Порядок передачи байтов — слева направо, сверху вниз (так же, как при чтении текста на странице). Продолжительность цикла передачи STM-1 составляет 125 мкс, т.е.

он повторяется с частотой 8 кГц. Каждая клеточка соответствует скорости передачи 8 бит•8 кГц = 64 кбит/с. Значит, если тратить на передачу в линию каждой прямоугольной рамки 125 мкс, то за секунду в линию будет передано $9 \cdot 270 \cdot 64$ Кбит/с = 155 520 Кбит/с, т.е. 155 Мбит/с.

Для создания более мощных цифровых потоков в SDH-системах формируется следующая скоростная иерархия: четыре модуля STM-1 объединяются путем побайтового мультиплексирования в модуль STM-4, передаваемый со скоростью 622,080 Мбит/с; затем четыре модуля STM-4 объединяются в модуль STM-16 со скоростью передачи 2488,320 Мбит/с; наконец четыре модуля STM-16 могут быть объединены в высокоскоростной модуль STM-64 (9953, 280 Мбит/с).

В сети SDH применены принципы контейнерных перевозок. Подлежащие транспортировке сигналы предварительно размещаются в стандартных контейнерах (Container — С). Все операции с контейнерами производятся независимо от их содержания, чем и достигается прозрачность сети SDH, т.е. способность транспортировать различные сигналы, в частности сигналы PDH.

Наиболее близким по скорости к первому уровню иерархии SDH (155, 520 Мбит/с) является цифровой поток со скоростью 139,264 Мбит/с, образуемый на выходе аппаратуры плезиохронной цифровой иерархии ИКМ-1920. Его проще всего разместить в модуле STM-1. Для этого поступающий цифровой сигнал сначала "упаковывают" в контейнер (т.е. размещают на определенных позициях его цикла), который обозначается С-4. Рамка контейнера С-4 содержит 9 строк и 260 однобайтовых столбцов. Добавлением слева еще одного столбца — маршрутного или трактового заголовка (Path Over Head, ПОН) — этот контейнер преобразуется в виртуальный контейнер VC-4.

Наконец, чтобы поместить виртуальный контейнер VC-4 в модуль STM-1, его снабжают указателем (PTR), образуя таким способом административный блок AU-4 (Administrative Unit), а последний помещают непосредственно в модуль STM-1 вместе с секционным заголовком SOH (Рисунок 1.3).

Синхронный транспортный модуль STM-1 можно загрузить и плезиохронными потоками со скоростями 2,048 Мбит/с. Такие потоки формируются аппаратурой ИКМ-30, они широко распространены в современных сетях. Для первоначальной "упаковки" используется контейнер С12. Цифровой сигнал размещается на определенных позициях этого контейнера. Путем добавления маршрутного, или транспортного, заголовка (ПОН) образуется виртуальный контейнер VC-12. Виртуальные контейнеры формируются и расформируются в точках окончаний трактов.

В модуле STM-1 можно разместить 63 виртуальных контейнера VC-12. При этом поступают следующим образом. Виртуальный контейнер VC-12 снабжают указателем (PTR) и образуют тем самым транспортный блок TU-12 (Tributary Unit). Теперь цифровые потоки разных транспортных блоков можно объединять в цифровой поток 155,520 Мбит/с. Сначала три транспортных блока TU-12 путем мультиплексирования объединяют в группу транспортных блоков TUG-2 (Tributary Unit Group), затем семь групп TUG-2 мультиплексируют в группы транспортных блоков TUG-3, а три группы TUG-3 объединяют вместе и помещают в виртуальный контейнер VC-4. Далее путь преобразования известен (Рисунок 1.3).

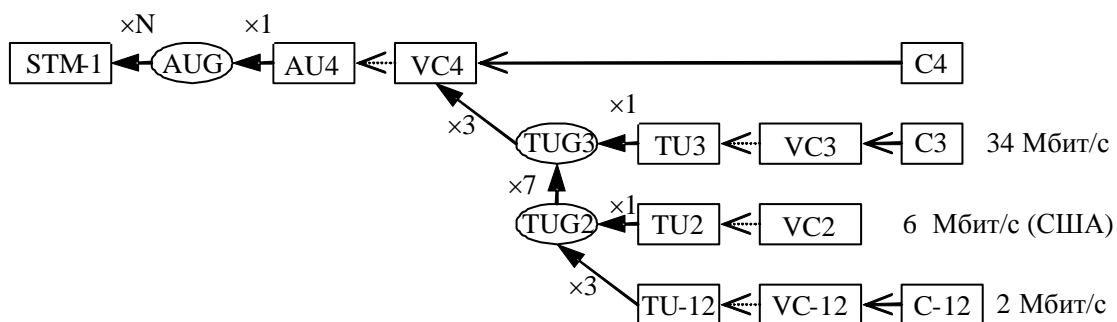


Рис. 1.3 -Упрощенная схема преобразования в SDH

Плезиохронные цифровые потоки всех уровней размещаются в контейнерах С с использованием процедуры выравнивания скоростей (положительного, отрицательного и двухстороннего).

Важной особенностью аппаратуры SDH является то, что в трактовых и сетевых заголовках помимо маршрутной информации создается много информации, позволяющей обеспечить наблюдение и управление всей сетью в целом, дистанционные переключения в мультиплексорах по требованию клиентов, осуществлять контроль и диагностику, своевременно обнаружить и устранять неисправности, реализовать эффективную эксплуатацию сети и сохранить высокое качество предоставляемых услуг.

К особенностям SDH можно отнести:

- синхронную передачу и мультиплексирование. Элементы сети используют один задающий генератор, поэтому вопросы построения системы синхронизации становятся особо важными;
- предусматривает прямой ввод/вывод потока E1;
- надёжность и самовосстанавливаемость сети, обусловленные тем, что, во-первых, сеть использует волоконно – оптические кабели, передача по которым не подвержена действию электромагнитных помех, во-вторых, архитектура и гибкое управление сетями позволяет использовать защищенный режим работы, допускающий два альтернативных пути распространения сигнала с почти мгновенным переключением в случае повреждения одного из них, а также обход поврежденного узла сети, что делает эти сети самовосстанавливающимися;
- выделение полосы пропускания по требованию – услуга, которая раньше могла быть осуществлена только по заранее спланированной договоренности, теперь может быть предоставлена в считанные секунды путем переключения на другой канал;
- прозрачность для передачи любого трафика, что обусловлено использованием виртуальных контейнеров для передачи трафика, сформированного другими технологиями (ATM, ISDN, Frame Relay);
- гибкость управления сетью, обусловленная наличием большого числа широкополосных каналов управления.

Подведем итоги рассмотренных нами систем цифровой иерархии:

Отличия SDH от PDH:

1. Единый для всех высокостабильный тактовый генератор;
2. Большое количество служебной информации, т.е. заголовков и указателей;
3. Универсальный интерфейс (имеется в виду взаимодействие) для всех национальных систем: США, Япония, Европа.

Достоинства SDH:

1. Упрощенный процесс мультиплексирования и демultipлексирования. Здесь не надо много распаковывать, как в ПЦИ, так как есть много заголовков.
2. Простота ввода компонентных сигналов - Заголовки + плавающий режим
3. Качественное управление сложными сетями:
 - управление конфигурацией;
 - управление неисправностями: выявление дистанционной неисправности и исправление ее;
 - управление качеством;
 - управление безопасностью.

Недостатки SDH:

1. Система очень дорогая;
2. Должна быть высочайшая стабильность частоты. А это сделать сложно.
3. Большое время вхождения в синхронизм;
4. Система чрезвычайно избыточна, т.к. много заголовков и пустых мест на будущее. Но это окупается высокой пропускной способностью.

Частотные диапазоны РРЛ

Диапазон 7 ГГц (7.25-7.55 ГГц)

Диапазон 7 ГГц освоен в настоящее время достаточно хорошо. В нем работает большое количество радиорелейных систем средней емкости (порядка 300-700 ТЛФ каналов в стволе для аналоговых систем и до 55 Мбит/с - для цифровых). Существует и аппаратура большой емкости, предназначенная для передачи потоков STM-1. В этом диапазоне на распространение сигнала начинают оказывать влияние гидрометеоры (дождь, снег, туман и пр.). Кроме того, влияет атмосферная рефракция, приводящая к закрытию трассы или к интерференции волн.

Средняя протяженность пролета РРЛ составляет 30-40 км. Антенны имеют высокий коэффициент усиления при диаметрах порядка 1.5 - 2.5 м.

Число радиосредств в России, использующих этот диапазон, пока относительно невелико, и, следовательно, электромагнитная обстановка благополучна. Однако необходимо учитывать помехи от соседних радиорелейных линий, работающих в данном диапазоне частот.

Диапазоны 11 и 13 ГГц (10.7-11.7, 12.7-13.2 ГГц)

Эти диапазоны перспективны с точки зрения эффективности систем РРЛ. При протяженности пролета 15-30 км, высокоэффективные антенны имеют небольшие габариты и вес, что обеспечивает относительную дешевизну антенных опор.

Доля влияния атмосферной рефракции на устойчивость работы систем уменьшается, но увеличивается влияние гидрометеоров. В этих диапазонах, в основном, строятся цифровые радиорелейные системы связи на скорости до 55 Мбит/с, хотя, есть примеры передачи цифровых потоков со скоростями до 155 Мбит/с.

Но эти диапазоны используют большое количество радиосредств. Спутниковые системы связи, различные радиолокаторы и пеленгаторы, охранные системы создают неблагоприятную электромагнитную обстановку, что затрудняет работу в данных диапазонах.

Диапазоны 15 и 18 ГГц (14.5-15.35, 17.7-19.7 ГГц)

Интенсивное развитие систем связи привело к бурному освоению этих диапазонов частот. Средняя протяженность пролетов достигает 20 км для зон с умеренным климатом. Аппаратура выполняется в виде моноблока. Типовые параболические антенны имеют диаметры 0.6, 1.2 или 1.8 м при коэффициентах усиления от 38 до 46 дБ. В ряде регионов России диапазон 15 ГГц уже перегружен радиосредствами. Диапазон 18 ГГц пока более свободен.

На распространение сигналов сильное влияние оказывают гидрометеоры и интерференция прямых и отраженных волн. Ослабление в дожде может составлять 1-12 дБ/км (при интенсивности дождей 20-160 мм/час). Некоторое влияние оказывает и сама атмосфера (атомы кислорода и молекулы воды), ослабление в которой достигает 0.1 дБ/км.

Диапазон 23 ГГц (21.2-23.6 ГГц)

Согласно рекомендациям МСЭ-Р в этом диапазоне разрешено строить системы аналоговой и цифровой связи любой емкости. Средняя протяженность пролетов меньше 20 км, так как на распространение сигналов сильное влияние оказывают гидрометеоры и ослабления в атмосфере. Желательно использовать вертикальную поляризацию радиоволн, хотя разрешено использование любой поляризации. Типовые параболические антенны имеют диаметры 0.3, 0.6 и 1.2 м.

Ослабление в дождях может быть от 2 до 18 дБ/км, а в атмосфере достигает 0.2 дБ/км. Диапазон разрешено использовать в спутниковых системах связи. Поэтому при расчетах необходимо учитывать возможность помех.

Таким образом, в соответствии с вышесказанным в нашем случае более предпочтительным является диапазон 7 ГГц, поскольку у ООО «Томсктрансгаз» используемая аналоговая РРЛ уже работает на этих частотах, следовательно получать разрешение ГРЧК не требуется, а нужно просто подать заявление на регистрацию нового оборудования и частотного плана. Кроме того, оборудование фирм, рассчитанное на пропускную способность в STM-1 для данного диапазона, значительно дешевле своих аналогов, работающих на более высоких частотах.

Виды станций РРЛ

На РРЛ имеется несколько видов станций:

1. **Оконечная станция (ОС)**, предназначаются для ввода в РРЛ многоканального и ТВ сигнала на стороне передачи и для выделения этих сигналов на стороне приема. ОС РРЛ связана соединительными линиями с МТС и ТЦ. Часто ОС совмещаются с ТЦ. Структурная схема ОС приведена на рисунке 1.4.

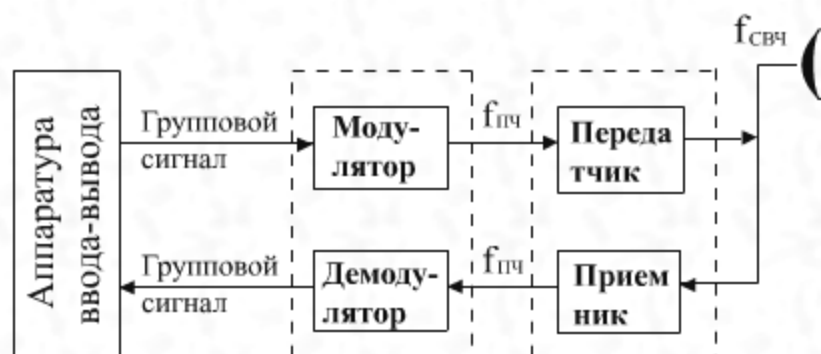


Рис. 1.4 – Структурная схема ОС

2. **Промежуточная станция (ПС)**, предназначена для приема сигналов от предыдущей станции, их усиления и передачи в направлении следующей станции. Соединение на ПС между передатчиком и приемником осуществляется по промежуточной частоте, т.е. без демодуляции сигналов в приемнике и без модуляции в передатчике. При необходимости может быть осуществлено выделение ТВ программы - для этого демодуляция сигнала промежуточной

частоты осуществляется путем его снятия с дополнительного выхода приемника, что не оказывает влияние на качественные показатели сквозных каналов.

В малоканальных РРЛ и особенно в РРЛ с временным разделением применяется построение аппаратуры ПС, при котором демодуляция и модуляция производится на каждой ПС. Это позволяет вводить и выводить ТЛФ каналы на любой ПС. Структурная схема станции приведена на рисунке 1.5.

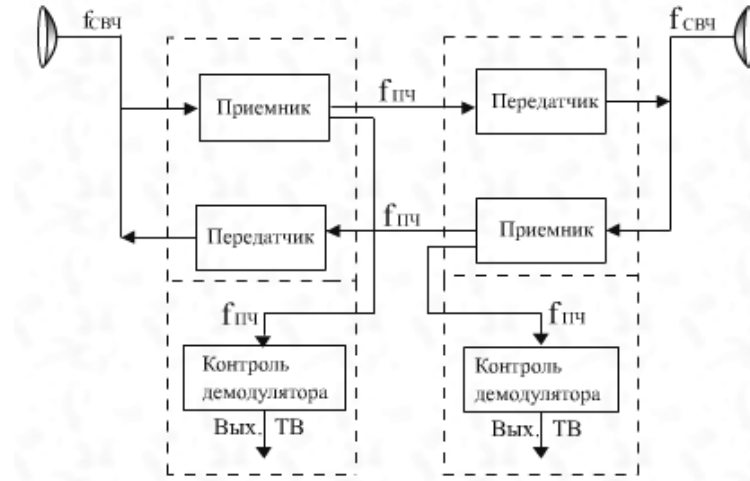


Рис. 1.5-Структурная схема ПС

3. **Узловые станции (УС)** предназначены для выделения части ТЛФ каналов и введения соответствующего количества новых каналов. От УС часто берут начало новые РРЛ (линии ответвления). В ТЛФ стволах на УС производится демодуляция сигналов со стороны приема и модуляция со стороны передачи. При необходимости эти преобразования производятся и в ТВ стволах. Структурная схема станции приведена на рисунке 1.6.

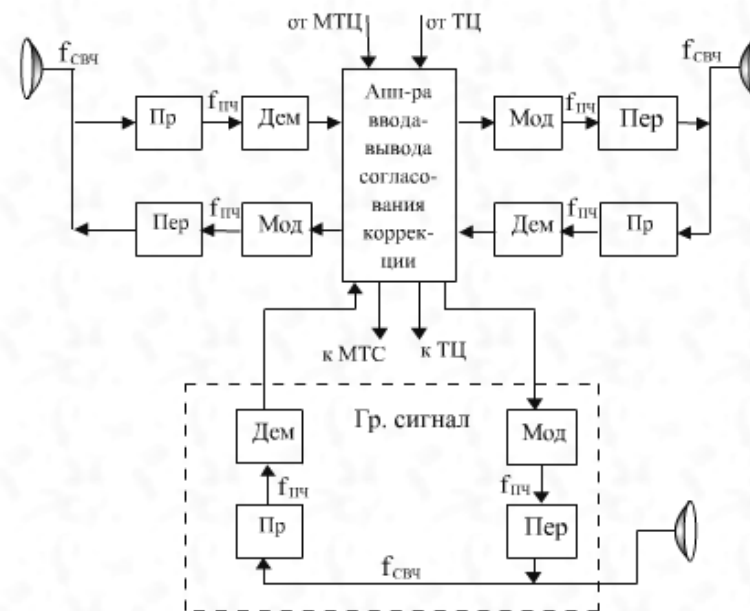


Рис. 1.6-Структурная схема УС

Основные требования, предъявляемые к антеннам РРЛ

В настоящее время на РРЛ прямой видимости применяются передатчики мощностью $2 \div 10$ Вт и в последнее время даже $0,5$ Вт. Расстояние между промежуточными пунктами составляет $40 \div 60$ км и высота мачт $50 \div 100$ м. При этом для устойчивой связи необходимо, чтобы коэффициент усиления антенны составляет $1000 \div 40000$ ($30 \div 46$ дБ). Обычно антенны дециметровых волн обладают коэффициентом усиления примерно 30 дБ и антенны сантиметровых волн $40 \div 46$ дБ.

На магистральных РРЛ большой емкости применяют, как правило, двухчастотную схему, которая, как известно, требует защитного действия антенн не менее $65 \div 70$ дБ.

Для увеличения переходного затухания между трактами приема и передачи, излучаемое и принимаемое антенной поля должны иметь взаимно перпендикулярные поляризации. Для этого линии питания и облучатель антенны должны быть выполнены так, чтобы было можно одновременно передавать и принимать волны с различными поляризациями, и диаграмма направленности антенны должна быть асимметричной.

Отраженные волны в тракте питания приводят к нелинейности фазовой характеристики последнего, что вызывает нелинейные искажения в сигнале. Допустимая величина коэффициента отражения, вызванного рассогласованием линии с антенной, для многоканальных систем не должна превышать 2% во всей рабочей полосе частот. Для этих систем полоса частот, удовлетворяющая данному требованию, должна составлять $10 \div 15\%$ от несущей частоты высокочастотного сигнала.

Конструкция антенны должна быть жесткой, чтобы при порывах ветра упругая деформация антенны не превышала допустимую величину. Атмосферные осадки не должны попадать в тракт питания антенны, т.к. это приводит к увеличению затухания в тракте и к рассогласованию. Антенна должна иметь возможность поворота в небольших пределах с целью точной установки направления максимального излучения на корреспондента.

План распределения частот

Под частотным планом системы РРЛ связи понимают распределение частот приема и передачи между стволами системы, а также распределение частот гетеродинов, т.е. распределение частот передачи и приема на одном стволе.

Так как особенностью построения аппаратуры РРЛ связи является то, что на ПС приемные и передающие антенны одного направления связи практически расположены рядом, то возникающие в этом случае взаимосвязи между антеннами не позволяют использовать одни и те же рабочие частоты при приеме и передачи сигналов в данном направлении. Поэтому на ПС возникает необходимость в изменении рабочих частот приема и передачи как при организации односторонней, так и двусторонней связи. Изменение частот производится на каждой станции в соответствии с принятой схемой построения аппаратуры.

Следовательно, ПС выполняет две функции:

1. Усиление сигнала;
2. Преобразование частоты СВЧ сигнала с целью устранения возможной связи между передатчиком и приемником данной станции.

Существуют три плана распределения частот в РРЛ прямой видимости, для ствола:

- двухчастотный план (рисунок 1.7);
- четырехчастотный план (рисунок 1.8);
- шестичастотный план (рисунок 1.9).

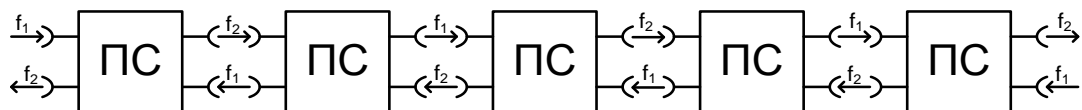


Рис. 1.7. Схема двухчастотного плана

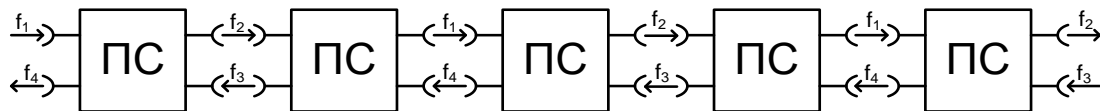


Рис. 1.8. Схема четырехчастотного плана

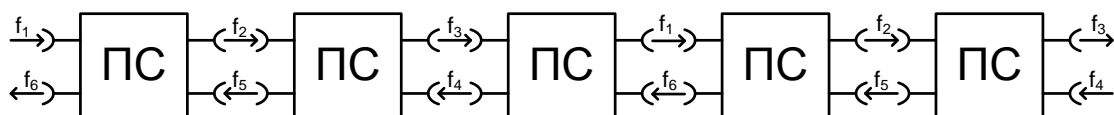


Рис. 1.9. Схема шестичастотного плана

Двухчастотная система экономична с точки зрения использования диапазона частот, но требует высоких защитных свойств антенн от приема сигналов с обратного направления. При двухчастотной системе используются РПА, параболические или другие антенны, имеющие защиту от приема сигналов с обратного направления порядка $60 \div 70$ дБ. Такая система применяется обычно на РРЛ большой и средней емкости.

Четырехчастотная система допускает использование более простых дешевых конструкций антенных систем, например перископических. Однако количество дуплексных радиостволов, которое может быть образовано в данной полосе частот при четырехчастотной системе в два раза меньше, чем при двухчастотной системе. Четырехчастотная система с более простыми антенными системами применяется на РРЛ средней и малой пропускной способности, предназначенных для внутризональных и низовых связей.

Частоты приема и передачи в одном стволе РРЛ чередуются от станции к станции. Станции, на которых прием осуществляется на более низкой частоте (f_1), а передача на более высокой (f_2), обозначаются индексом “НВ”, а станции, на которых прием производится на более высокой частоте (f_2), передача на более низкой (f_1) обозначается индексом “ВН”.

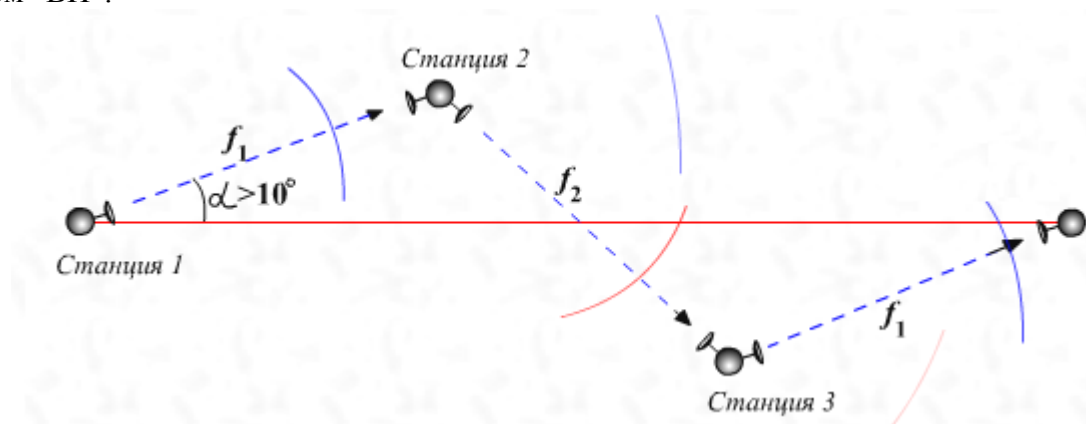


Рис. 1.10. Расположение станций РРЛ

Повторение через интервал одних и тех же частот допустимо потому, что в диапазонах дециметровых и сантиметровых волн при отсутствии прямой видимости

между антеннами ослабление сигнала достаточно велико. Однако при некоторых условиях распространения радиоволн, например при повышенной рефракции, возможен прием сигнала от станции, отстоящей на 3 интервала (минус 2 станции), что и приводит к значительным искажениям передаваемых сигналов. Во избежание этого станции РРЛ располагают на ломаной линии с тем, чтобы паразитный сигнал дополнительно сильно ослаблялся за счет направленных свойств антенн (рисунок 1.10).

Для того чтобы свести к минимуму интерференционные помехи в многоствольных РРЛ, возникающие при одновременной работе нескольких приемников и передатчиков на общий антенно-фидерный тракт, существуют определенные планы распределения частот.

Во всех современных РРЛ системах применяются планы с разнесенными частотами приема и передачи, т.е. частоты приема размещены в одной половине диапазона, а частоты передач – в другой половине диапазона. Такой план распределения частот приведен на рисунке 1.11.

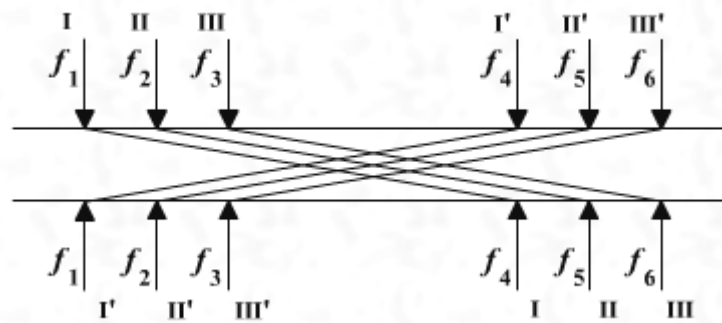


Рис. 1.11 - План с разнесенными частотами приема и передачи

При таком плане распределения частот разность между частотами передачи и приема одного ствола значительно и это облегчает требования к характеристикам приемных полосовых фильтров. При этом плане каждая антенна может быть использована одновременно как для передачи, так и приема сигналов.

Существует второй план распределения частот – при этом плане предусматривается чередование частот приема и передачи отдельных стволов (рисунок 1.12).

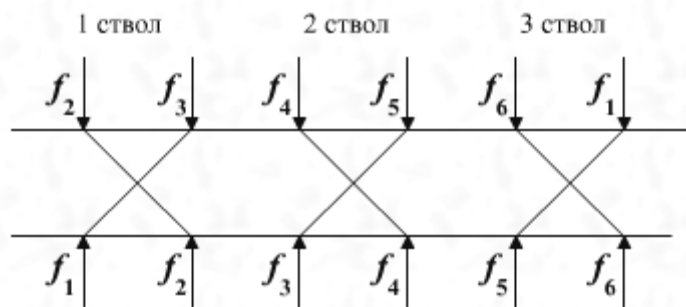


Рис. 1.12 – План с чередованием частот приема и передачи

В нашем случае выберем четырехчастотный план, поскольку двухчастотного будет недостаточно из-за почти прямолинейного расположения РРС. С другой стороны, использование шестичастотного плана неоправданно с точки зрения частотного ресурса, получение разрешения на использование которого в диапазоне 7 ГГц может быть проблематично из-за его занятости. Выбор частот приема и передачи осуществим по предоставленной производителем оборудования формуле:

$$F_H = 7400 - 164.5 + 28 \cdot n \quad (1.1)$$

$$F_B = 7400 - 3.5 + 28 \cdot n \quad (1.2)$$

Формула 1.1 позволяет рассчитать нижнюю рабочую частоту приемо-передатчика, а формула 1.2 – верхнюю, при условии, что шаг сетки частот составляет 28 МГц, а дуплексный разнос – 160 МГц. Полный частотный план проектируемой РРЛ приведен на структурной схеме РТФ ДП.464543.001 ЭЗ.

Оборудование РРЛ

Размещение оборудования радиорелейных систем производится по следующим принципам:

1. Антенны размещаются на мачте и с оборудованием их соединяют волноводы. Герметичность антенно-волноводного тракта (АВТ) обеспечивается установкой дегидраторов – устройств, обеспечивающих избыточное давление в волноводах. Оборудование находится на земле в помещении, где поддерживается необходимый микроклимат.
2. Размещение приемопередающего высокочастотного (ВЧ) оборудования возле антенны и остальное оборудование внизу в помещении. Соединение между модулятором и ВЧ трактом выполняется коаксиальным кабелем, по которому также подается питание на передатчики и приемники. При использовании разнесенного приема дополнительное оборудование также размещается на мачте возле приемной антенны.

Система электропитания ЦРРС обеспечивается соединением нескольких источников энергии – внешних источников электроснабжения, солнечных батарей, ветроэлектрогенераторов и аккумуляторных батарей, обеспечивающих работу оборудования при перерывах подачи электроэнергии от других источников. Все оборудование разделяется на классы энергопотребителей, в зависимости от этого обеспечивается та или иная система резервирования источников электропитания.

Существует и тенденция в размещении оборудования: если в недавнем прошлом все оборудование ЦРРС размещалось на земле, то в настоящее время с ростом миниатюризации элементов производители при производстве радиорелейных станций все больше проектируют радиооборудование с размещением возле антенны, как более дешевое. Номенклатура цифровых радиорелейных станций с размещением всего оборудования на земле становится все меньше, а то и вообще отсутствует. Как правило, современные производители стараются обеспечить возможность размещения оборудования как на земле, так и возле антенны, а заказчик уже сам выбирает, как ему удобно.

Исполнение с размещением оборудования возле антенны имеет свои достоинства и недостатки. К достоинствам следует отнести следующее:

- Отсутствует затухание в волноводном тракте, которое на высоких частотах достигает довольно больших величин. Например, на частоте 7 ГГц затухание в стандартном волноводе марки Е65 – 0,06дБ/м, что на 100метров длины волновода дает затухание на прием и на передачу на 6дБ. На более высоких частотах затухание будет еще больше. Компенсация потерь на затухание требует увеличения мощности передатчика и применения антенн большего диаметра для увеличения уровня принимаемого сигнала, что значительно удорожает систему.
- Стоимость соединительного коаксиального кабеля значительно ниже стоимости волновода.
- Отпадает проблема поддержания герметичности волноводного тракта.

Существуют и недостатки:

- При размещении СВЧ оборудования на мачте часто затруднен доступ к нему для настройки, обслуживания, профилактики или при неисправностях, что значительно

замедляет устранение повреждений – важное условие при эксплуатации магистральных линий связи.

- Оборудование должно работать в большом диапазоне температур наружного воздуха – от максимальной – летом до минимальной – в сильный мороз. При этом надо учитывать, что радиочастотный блок размещен в открытом пространстве, где солнце может дополнительно разогреть его.
- Необходимо применять дополнительные меры гроззащиты, предотвращающие выход из строя ВЧ оборудования в радиочастотном блоке.
- Затруднено, а то и невозможно наращивание количества стволов при использовании одной антенны.

При проектировании данной радиорелейной линии связи основными недостатками размещения оборудования возле антенны стали следующие факторы:

1. не все фирмы дают гарантии работы оборудования при крайне отрицательных температурах, таких как -50 и ниже, при этом зима 2006 года показала важность данного показателя;
2. подобное размещение затрудняет проведение профилактических работ, которые проводятся достаточно часто, так как деятельность ООО «Томсктрансгаз» связано с особо опасным производством.

Использование аппаратуры в благоприятных условиях аппаратной, позволяет увеличить срок ее эксплуатации, что немаловажно при необходимости обеспечения непрерывности технологической связи.

Фирмы производители РРЛ

Главными факторами, которые следует учитывать при выборе поставщика радиорелейного оборудования, являются:

- положительные отзывы ведущих операторов связи;
- опыт эксплуатации в неблагоприятных климатических условиях;
- наличие сервисных центров;
- перспективы производства оборудования на ближайшее десятилетие;
- экономическая целесообразность внедрения;
- стоимостные характеристики.

Анализ возможностей использования оборудования отечественных производителей показывает, что, несмотря на растущее число производителей отечественного оборудования ЦРПС уровня STM-1 (M-Link, «Пламя», Nateks Microlink SDH), оно не соответствует первым двум критериям.

Кроме того, в большинстве случаев данное оборудование собрано из отдельных узлов производства зарубежных производителей, в том числе малоизвестных на телекоммуникационном рынке, а используемое отечественное программное обеспечение часто конфликтует со старыми версиями. Опыта их использования на магистральных линиях практически нет. Сертификаты получены на использование во внутризоновых радиорелейных линиях.

Из зарубежного оборудования внимания заслуживает прежде всего продукция, имеющая положительные отзывы российских операторов и удовлетворяющая перечисленным ниже требованиям (таблица 1.2).

Таблица 1.2 – Радиорелейное оборудование зарубежных производителей

Тип ЦРР	Диапазон, ГГц	Производитель	Система
TRuepoint	6-38	Harris	SDH STM-1 (также может работать в PDH-сетях)
MegaStar	5,6,7,8, 11	Harris	SDH STM-1
Pasolink+	6-38	NEC	SDHSTM-1
DMR 3000S	4-11	NEC (сертифицирована в 2003 г.)	SDHSTM-1
Mini-Link High Capacity	18	Ericsson	SDH STM-1
Altium MX	6-38	Stratex Networks	SDHSTM-1
Eclipse	7, 15, 18	Stratex Networks	SDHSTM-1
SRT1F	4-13	Siemens (сертифицирована в 2003 г.)	SDHSTM-1
SRA4	6-38	Siemens (сертифицирована в 2003 г.)	SDHSTM-1
CityLink	5-38	NERA	SDH STM-1 (также может работать в PDH-сетях)
InterLink	5-38	NERA	SDHSTM-1

Среди них выделяются три производителя - NEC (ЦРР DMR 3000S), Nera (Interlink) и Harris (MegaStar) на их оборудовании остановили свой выбор наиболее крупные телекоммуникационные операторы, и это оборудование имеет длительный и положительный срок эксплуатации.

Произведя поиск в Internet, было обнаружено, что фирма Harris не имеет в России своего представительства и, соответственно, сервисного центра. В дополнении можно отметить, что в России очень малое количество дилеров работает с их продукцией. Таким образом, наш выбор останавливается на фирмах Nec и Nera, имеющих свои представительства как в России, так и в странах СНГ. В этом можно убедиться, посетив их сайты по следующим адресам: www.nera.com.ru и www.nec.ru. Кроме того, оборудование этих фирм более дешевое.

Для DMR 3000S и MegaStar характерно нижнее расположение радиомодулей с эффективной и надежной системой дегидратации волноводных трактов. По оценкам операторов связи, оборудование хорошо себя зарекомендовало в эксплуатации. В обеих станциях применены специальные схемы коррекции дисперсионных искажений, а также эквалайзеры для компенсации потерь и борьбы с замираниями сигналов. ЦРР DMR 3000S обеспечивает увеличение пропускной способности до 16 потоков по 155,52 Мбит/с, MegaStar - до 7 потоков уровня STM-1.

Поскольку мы проектируем внутризональную радиорелейную линию (ее протяженность – 275.5 км), то нам не нужно оборудование, способное передавать до нескольких потоков STM-1.

Для применения на внутризональных ЦРРЛ и линиях относительно небольшой протяженности представляют интерес ЦРР Pasolink+ (NEC), TRuepoint (Harris), InterLink и CityLink (NERA). Пропускная способность каналаобразующей аппаратуры составляет 155 Мбит/с синхронной цифровой иерархии уровня STM-1 с возможностью увеличения до 4 потоков 155,52 Мбит/с. Наличие встроенного мультиплексора и единой системы управления позволяет минимизировать затраты на создание транспортной инфраструктуры. Кроме того, оборудование допускает как нижнее, так и верхнее

расположение радиомодулей. Для компенсации дисперсионных искажений, возникающих вследствие замираний в волноводной части, используются высокоэффективные корректоры. Возможно пространственное разнесение антенн и радиомодулей на расстояние до 200 м.

В ходе поиска характеристик радиорелейного оборудования вышеуказанных фирм-производителей, столкнулся с основной проблемой. Ни один из официальных дилеров или представительств фирм не дает полную и подробную информацию о своем оборудовании и его применении в конкретных случаях.. В связи с этим фактом, дальнейшее проектирование было решено производить на оборудовании фирмы «Микран», хотя, по имеющимся сведениям, ни один из комплектов еще не был установлен, поэтому опыта эксплуатации данного радиорелейного оборудование нет.

Кроме того, оборудования фирмы «Микран» не позволяет нижнее размещения высокочастотного оборудования, что также является большим минусом при его эксплуатации. Тем не менее, определившись с производителями оборудования и представляемыми ими линейками, проведем сравнительный анализ и представим результаты в таблице 1.3.

Таблица 1.3 – Сравнительный анализ радиорелейного оборудования

№	Параметр	МИКРАН МИК- РЛ7...15С	Nera Interlink	Nec DMR 3000S	Nec Pasolink+
1	Диапазон частот, ГГц	7-15	3-11	4-11	6-38
2	Пропускная способность	STM-1	От STM-1 до 16 STM-1	От STM-1 до 16 STM-1	От STM-0 до 2 STM-1/OC3
3	Разнос каналов, МГц	28-56	30-40	30-40	28-56
4	Тип модуляции	16 QAM, 64 QAM, 128 QAM	64 QAM, 128 QAM	64 QAM, 128 QAM	32 QAM, 128 QAM
5	Выходная мощность передатчика, дБм	21-27	26-29	30-33	10.5-25
6	Порог приемника, BER 10^{-6} , дБм	-(65-76)	-(68-72)	-(67-77)	-(67-68)
7	Система резервирования	1+0; 1+1; 2+0; 2+1; 3+0; 3+1	от 1+0 до 8+0 без резерва, от 1+1 до 7+1 с резервом	до 11+1	1+0; 1+1; 2+0
9	Служебная связь	2 x 64 кбит/с	3 x 64 кбит/с	4 x 64 Кбит/с	2 x 64 кбит/с
10	Управление сетью	ПО «Магистраль»	Nera NMS/LCT	MS3201	PNMS / PNMT
11	Расположение аппаратуры	верхнее	Верхнее и нижнее	Верхнее и нижнее	Верхнее и нижнее

Радиорелейное оборудование фирмы «Микран»

Аппаратура цифровых радиорелейных станций SDH иерархии «МИК-РЛххС» работает в диапазоне частот от 4 до 40 ГГц со скоростью передачи информации 155.52 Мбит/с и позволяет в пределах пропускной способности передавать 1 поток STM-1 или 63

потока E1 или 42 потока E1 + трафик Ethernet (50 Мбит/с) или 21 поток E1 + трафик Ethernet (100 Мбит/с)].

Высокоскоростные ЦРРС «МИК-РЛ4...6С» предназначены для организации магистральных линий связи в диапазонах частот 4; 5 и 6 ГГц;

Высокоскоростные ЦРРС «МИК-РЛ7...15С» предназначены для организации внутризонавых, местных и технологических линий связи в диапазонах частот 7...15 ГГц;

Высокоскоростные ЦРРС «МИК-РЛ18...40С» предназначены для организации местных и технологических линий связи в диапазонах частот 18...40 ГГц;



Рис. 1.13 – Общий вид радиорелейной аппаратуры SDH иерархии «Микран»

Исполнение системы

Станции МИК-РЛ4...40С представляют собой функционально законченные системы передачи, позволяющие строить синхронные сети связи произвольной топологии. В состав РРС входят: приёмопередающая аппаратура, мультиплексоры уровня STM-1 (терминальные и ввода-вывода), источники гарантированного электропитания и система управления сетью.

В традиционном для систем МИК-РЛ раздельном исполнении возможна реализация конфигураций 1+0; 1+1 и 2+0. Станция в конфигурации 1+1 состоит из двух выносных приемопередатчиков и приемников канала пространственного разнесения, устанавливаемых непосредственно на антеннах, и оборудования внутреннего исполнения – модуля доступа МД1-6. При нижнем расположении приёмопередатчиков возможна реализация конфигураций 2+1, 3+0 или 3+1, в этом случае используется два модуля доступа МД1-6.

Особенности аппаратной реализации.

Архитектура модуля доступа МД1-6 позволяет в составе одного модуля простым добавлением необходимого количества блоков реализовать следующие варианты станций:

- терминальная станция 63xE1, одно направление по СВЧ, конфигурация 1+0 или 1+1;
- станция ввода/вывода 21xE1 или 42xE1, два направления по СВЧ, конфигурация 1+0 или 1+1;
- регенераторная станция без выделения потоков E1, два направления по СВЧ, конфигурация 1+0 или 1+1;
- регенераторная станция без выделения потоков E1, конфигурация 1+0 или 1+1, одно направление по СВЧ и одно направление по STM-1 (для работы с SDH-мультиплексорами других производителей).



Рис. 1.14 – Модуль доступа МД1-6

Модуль доступа МД1-6 имеет в своём составе мультиплексор STM-1 который обеспечивает мультиплексирование трибутарных цифровых потоков и сервисных каналов, вместо передачи потоков Е1 возможна организация передачи трафика Ethernet (n x 21Е1). Модемы формируют спектр радиосигнала на промежуточной частоте и имеют встроенную аппаратную поддержку пространственного разнесения, для реализации которого требуется только установка антенн и приёмников пространственного разнесения. В модуле доступа МД1-6 используется распределенная система электропитания, благодаря чему достигается общая надежность и независимость питания каждого блока от остальных. Модуль доступа МД1-6 выполнен в корпусе Евромеханика 19' высотой 6U.

В системе предусмотрены дополнительный канал передачи данных с программно выбираемым типом интерфейса RS-232/422/485 (скорость передачи от 110 до 57 600 бит/с) и 2 цифровых канала служебной связи РСМ-64 с двухпроводными окончаниями FXO/FXS с возможностью выхода в ТфОП. Для более эффективного использования каналов служебной связи на каждой станции предусмотрен встроенный коммутатор каналов. На всех промежуточных станциях возможен ввод/вывод сервисных каналов.

Контроль и управление сетью РРС

Система управления состоит из сетевых агентов, размещаемых на каждой станции и программного обеспечения верхнего уровня. На уровне сетевых агентов, размещаемых на каждой станции, решаются задачи как локального управления при помощи подключаемого терминала на базе Pocket-PC, так и сетевого управления при помощи менеджера сети - компьютера с установленным ПО «Магистраль». Система управления взаимодействует с сетью радиорелейных линий (РРЛ) посредством соединения TCP/IP (интерфейс - Ethernet 10Base-T) на основе протокола SNMP. Особенностью аппаратного исполнения агента сети является наличие подсистемы хранения «firmware» всех блоков, входящих в состав станции, предусмотрена процедура обновления «firmware». Ядром сетевого агента является операционная система реального времени (RTOS).

В аппаратуре реализована возможность удаленного конфигурирования рабочих параметров всех устройств, входящих в состав РРС. Из центра управления осуществляется необходимая оперативная поддержка по обслуживанию сети при ее эксплуатации, вносятся своевременные коррективы в работу устройств. Обновляемая библиотека файлов-описаний позволяет изменять методы представления/анализа данных и способы управления устройствами, что обеспечивает независимость ПО от оборудования.

Возможно создание нескольких центров управления сетью, благодаря чему нагрузка на канал управления распределяется более равномерно. При необходимости реализуется резервирование управления. ПО системы управления защищено от несанкционированного доступа. Используемый механизм предоставления привилегий позволяет вводить

несколько уровней взаимодействия с системой, ограничивая или расширяя права операторов.

Список условных сокращений

БС – базовая станция;

ГЭС – гипотетическое эталонное соединение;

ГЭЦЛ - гипотетическая эталонная цифровая линия;

ГЭЦТ - гипотетический эталонный цифровой тракт;

ИБЭП – источник бесперебойного электропитания;

ЗОЗ – зона ограничения застройки;

МСЭ – международный союз электросвязи;

ОЦК – основной цифровой канал;

ПЦИ – плезиохронная цифровая иерархия;

ПЦК – первичный цифровой канал;

СЦИ – синхронная цифровая иерархия;

ТфОП – телефонная сеть общего пользования;

УАТС – учрежденческая автоматическая телефонная станция;

ЦРРЛ – цифровая радиорелейная линия;

SESR – коэффициент секунд со значительным количеством ошибок;

SINAD – отношение сигнал/шум.

2. ТРАНКИНГОВЫЕ СИСТЕМЫ РАДИОСВЯЗИ

Под широко распространенным в настоящее время понятием "профессиональная мобильная радиосвязь" (ПМР) обычно понимают системы двусторонней сухопутной подвижной радиосвязи, использующие диапазон ультракоротких волн (УКВ).

Как правило, сети ПМР используются ограниченными группами пользователей, объединенными по профессиональному признаку. Это могут быть сети оперативного, диспетчерского, административно-хозяйственного, производственно-технологического и т. п. назначения. Они используются силовыми структурами и правоохранительными органами, аварийными и муниципальными службами, энергетическими, транспортными и производственными предприятиями и т. д. Именно поэтому сети ПМР часто называют ведомственными и корпоративными сетями радиосвязи.

Достаточно четко можно охарактеризовать сети профессиональной мобильной радиосвязи и по техническим признакам. По способам использования частотного ресурса системы двусторонней подвижной радиосвязи делятся на следующие классы:

- системы связи с закреплением за абонентами каналов связи (конвенциональные системы);
- системы связи с общим доступом абонентов к общему частотному ресурсу (транкинговые системы);
- системы связи с пространственно-разнесенным повторным использованием частот (сотовые системы).

Первые 2 класса и относятся к системам профессиональной мобильной радиосвязи.

Конвенциональные системы, являясь простейшим классом систем ПМР, используют принцип фиксированного закрепления каналов связи за определенной группой абонентов. По сравнению с другими классами систем подвижной радиосвязи для конвенциональных систем характерна, с одной стороны, наименьшая пропускная способность, определяемая достижимым количеством абонентов, работающих на одном канале, а с другой - наибольшая оперативность связи, характеризующаяся временем установления канала связи. Основным типом вызова в конвенциональных системах является групповой, при котором переговоры обеспечиваются по принципу "каждый со всеми". Вместе с тем, используемые в современных сетях конвенциональной радиосвязи системы избирательного вызова, основанные на различных методах сигнализации, позволяют разделять группы абонентов и осуществлять не только групповые, но и индивидуальные вызовы.

Транкинговые системы используют автоматическое распределение каналов связи между абонентами. Это означает, что все пользователи делят между собой общую группу радиоканалов, а выделение свободных каналов осуществляется по требованию абонентов. Основным элементом сетей транкинговой радиосвязи является базовая станция (БС), включающая несколько ретрансляторов с соответствующим антенным оборудованием и контроллер, который управляет работой БС, коммутирует каналы ретрансляторов, обеспечивает выход на телефонную сеть общего пользования или другую сеть фиксированной связи. По сравнению с конвенциональными сетями, сети транкинга обладают повышенной пропускной способностью, расширенными функциональными возможностями, разнообразными типами вызова (групповой, индивидуальный, широковещательный), большей зоной территориального охвата.

Целесообразность применения транкинговых систем при построении ведомственных и корпоративных сетей ПМР обуславливается двумя факторами: высокой плотностью абонентов и необходимостью централизованного управления системой.

Применение транкинговых систем при построении ведомственных и корпоративных сетей ПМР обуславливается как техническими, так и экономическими факторами.

Основная идея транкинга состоит в обеспечении равного доступа абонентов к общему частотному ресурсу. Такой доступ существенно повышает эффективность использования

спектра по сравнению с системами с закреплением за абонентами каналов связи (конвенциональными системами). Можно говорить, что либо при одном и том же количестве каналов связи транкинговая система позволяет обслужить значительно большее количество абонентов, чем конвенциональная система (при одинаковом качестве обслуживания), либо при одном и том же количестве абонентов для реализации транкинговой системы потребуется меньше каналов связи. Например, одна четырехканальная система транкинговой связи в 7,5 раз эффективнее конвенциональной системы с тем же количеством каналов. Эффективность использования частотного ресурса определяет экономическую эффективность применения транкинговых систем. Считается, что транкинговая система становится экономически эффективной при количестве абонентов более 50-100.

Архитектура транкинговых систем основана на сети соединенных друг с другом базовых станций, каждая из которых обслуживает определенную зону. Такая архитектура позволяет строить сети радиосвязи самого различного масштаба: от локальных однозоновых сетей до крупных региональных сетей с широким территориальным охватом. При этом сохраняется возможность централизованного управления сетью, что практически невозможно в конвенциональных сетях. Поэтому по сравнению с конвенциональными системами системы транкинговой радиосвязи обеспечивают гораздо более эффективное управление эксплуатацией и развитием сетей связи.

Совершенствование транкинговых систем позволяет говорить об их расширенных функциональных возможностях по сравнению с системами конвенциональной радиосвязи. Это касается разнообразных типов вызова (групповой, индивидуальный, широковещательный), возможности использования приоритетных и аварийных вызовов, передачи данных, взаимодействия с телефонными сетями общего пользования (ТфОП), возможности динамического создания, модификации и удаления групп абонентов и т.д. В целом можно говорить, что транкинговые системы представляют наиболее мощный и эффективный класс систем ПМР.

По сравнению с сотовыми системами подвижной связи (ССПС) транкинговые системы обеспечивают ряд возможностей, не реализуемых ССПС. К ним, прежде всего, относится возможность групповой связи, которая является основным видом взаимодействия в сетях ПМР. Кроме этого, в транкинговых сетях возможны приоритетные и аварийные вызовы, динамическая перегруппировка абонентов, что недоступно абонентам сотовых сетей. Важнейшим преимуществом является высокая скорость установления соединения. В транкинговых системах время установления канала связи, как правило, не более 0.5 с, тогда как сотовые системы не позволяют установить соединение быстрее, чем за 5 с.

Транкинговые системы радиосвязи (ТСР) являются развитием систем низовой полудуплексной радиосвязи и по ряду признаков могут быть соотнесены с сотовыми системами связи. В отличие от обычных систем с постоянно закрепленными частотными каналами в ТСР применяется динамическое распределение каналов. Термин «транкинг», принятый в сфере профессиональной радиосвязи, означает метод свободного доступа большого числа абонентов к ограниченному числу каналов (пучку, стволу или, по зарубежной терминологии, - транку). Поскольку в какой-либо момент времени не все абоненты активны, необходимое число каналов значительно меньше общего числа абонентов.

Когда радиоабонент транкинговой системы осуществляет вызов, система назначает ему один из имеющихся свободных каналов. При этом статистика активности обычно такова, что небольшого количества выделенных каналов достаточно для обслуживания значительного числа абонентов. Эту ситуацию иллюстрируют цифры, заимствованные из документации на систему ACCESSNET фирмы Rohde & Schwarz (табл. 2.1).

В отличие от обычных систем радиосвязи ТСР характеризуются следующими признаками:

- экономное использование радиоспектра;
- наличие одной или нескольких базовой радиостанций и системы управления;
- возможность выхода в другие сети, в частности в телефонную сеть общего пользования;
- увеличение зоны обслуживания путем создания многозоновой сети;

- передача данных и телеметрической информации;
- множество сервисных возможностей.

Таблица 2.1 – Зависимость числа абонентов от числа радиоканалов

Число каналов	Общее число абонентов
6	320
11	790
21	1760
25	2160

Перечисленные выше признаки характерны и для сотовых систем связи. Однако, в отличие от сотовых, транкинговые системы в первую очередь ориентированы на задачи, связанные с оперативным управлением. Список потребителей здесь чрезвычайно широк - подразделения железных и автомобильных дорог, предприятия энергетического комплекса, администрации всех уровней, учреждения городского хозяйства, правоохранительные органы, отряды министерства по чрезвычайным ситуациям (МЧС), коммерческие структуры и т.д.

В сравнении с сотовыми системами к преимуществам ТСП, позволяющим отдать им предпочтение при организации оперативной связи, следует отнести:

- гибкую систему вызовов - индивидуальный, групповой, вещательный, приоритетный, аварийный и др.;
- гибкую систему нумерации - от коротких двух- или трехзначных до полноценных городских номеров;
- малое время установления соединения - менее секунды, против нескольких секунд в сотовых системах;
- возможность работы в группе;
- наличие (в ряде систем) режима непосредственной связи между двумя абонентскими радиостанциями без участия базовой;
- экономичность - по стоимости оборудования и по эксплуатационным расходам ТСП в несколько раз экономичнее сотовых систем.

Сравнивая сотовые и транкинговые системы, необходимо отметить, что при внешней структурной схожести они существенно отличаются по ряду функциональных особенностей и системных возможностей. Если первые ориентированы на потребителей обычных телефонных услуг и окупаются в регионах с высокой плотностью населения (порядка тысячи и более абонентов в зоне), то вторые, прежде всего, являются средством оперативной и производственно-технологической связи и рентабельны при на порядок меньшем числе абонентов.

Следует заметить, что сами термины «сотовые» или «транкинговые системы» малоинформативны с точки зрения выявления их отличий. Так, в сотовых системах используется метод динамического распределения каналов, т.е. транкинг, и наоборот, современные многозоновые транкинговые системы содержат ряд «родовых» признаков сотовых систем. Эти термины сложились исторически и обозначают системы мобильной радиосвязи, которые развивались своими путями, решая разные задачи.

Транкинговыми системами называются радиально-зональные системы наземной подвижной радиосвязи, использующие автоматическое распределение каналов связи ретрансляторов между абонентами. Это достаточно общее определение, но оно выражает в себе совокупность признаков, объединяющих все транкинговые системы - от простейших SmarTrunk до сверхсовременных TETRA. Термин "транкинг" происходит от английского trunking, что можно перевести как "объединение в пучок". В отечественной литературе можно встретить также термин "транковые системы" - видимо, по аналогии с англоязычным термином trunked systems.

Однозоновые системы.

Основные архитектурные принципы транкинговых систем легко просматриваются на обобщенной структурной схеме однозональной транкинговой системы, представленной на рисунке 2.1. Инфраструктура транкинговой системы представлена базовой станцией (БС), в состав которой, помимо радиочастотного оборудования (ретрансляторы, устройство объединения радиосигналов, антенны) входят также коммутатор, устройство управления и интерфейсы различных внешних сетей.

Ретранслятор. Под ретранслятором в данном случае понимается набор приемопередающего оборудования, обслуживающего одну пару несущих частот. До последнего времени в подавляющем большинстве транкинговых систем одна пара несущих означала один канал трафика. Сегодня, с появлением систем стандарта TETRA и системы EDACS ProtoCALL, предусматривающих временное уплотнение, один ретранслятор может обеспечить два или четыре канала трафика.

Антенны. Важнейший принцип построения транкинговых систем заключается в том, чтобы создавать зоны радиопокрытия настолько большими, насколько это возможно. Поэтому антенны базовой станции, как правило, размещаются на высоких мачтах или сооружениях и имеют круговую диаграмму направленности. Разумеется, при расположении базовой станции на краю зоны применяются направленные антенны. Базовая станция может располагать как единой приемопередающей антенной, так и отдельными антеннами для приема и передачи. В некоторых случаях на одной мачте может размещаться несколько приемных антенн для борьбы с замираниями, вызванными многолучевым распространением.

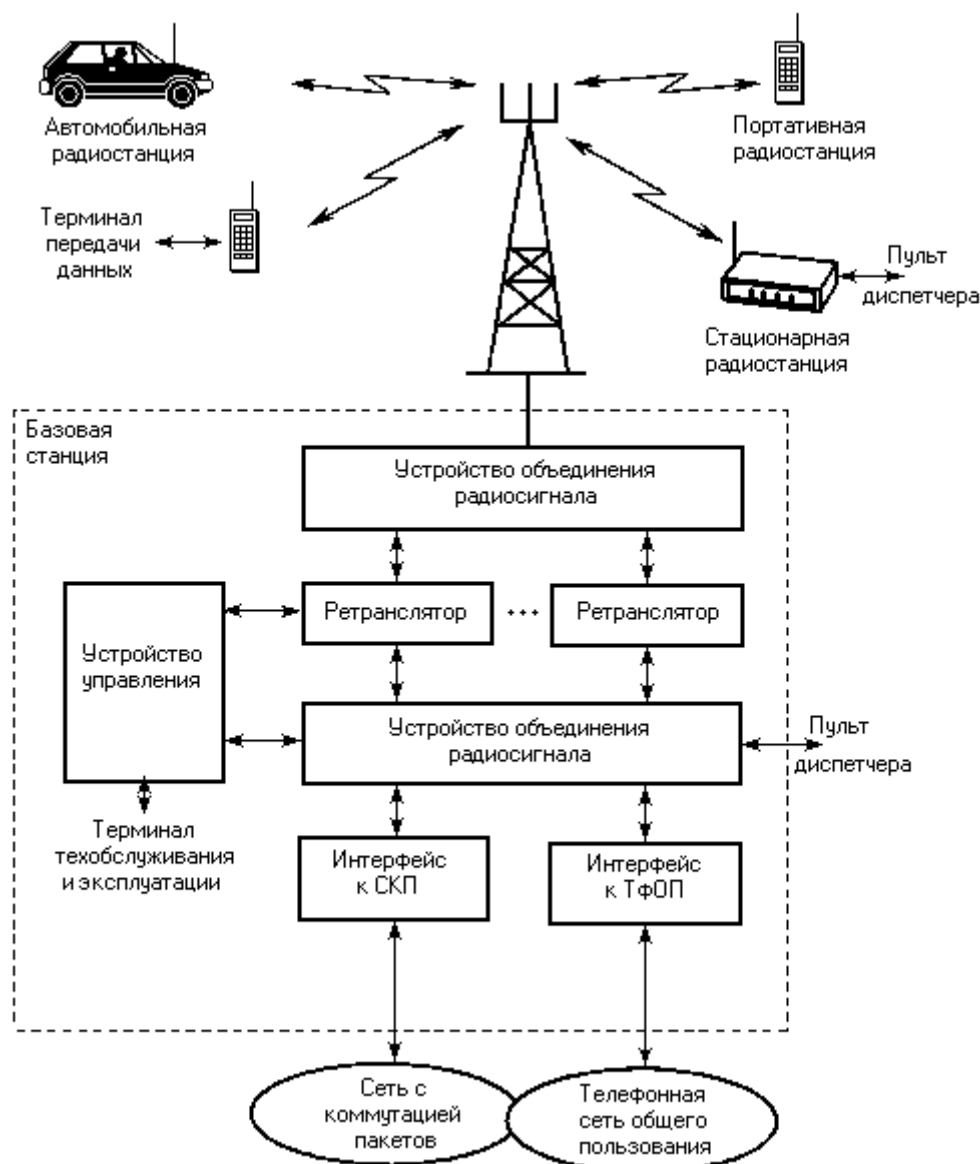


Рис. 2.1. Обобщенная структура однозонавой транкинговой системы

Устройство объединения радиосигналов позволяет использовать одно и то же антенное оборудование для одновременной работы приемников и передатчиков на нескольких частотных каналах. Ретрансляторы транкинговых систем работают только в дуплексном режиме.

Коммутатор в однозонавой транкинговой системе обслуживает весь ее трафик, включая соединение подвижных абонентов с ТФОП и все вызовы, связанные с передачей данных.

Устройство управления обеспечивает взаимодействие всех узлов базовой станции. Оно также обрабатывает вызовы, осуществляет аутентификацию вызывающих абонентов, ведение очередей вызовов, внесение записей в базы данных повременной оплаты. В некоторых системах управляющее устройство регулирует максимально допустимую продолжительность соединения с телефонной сетью. Как правило, используются два варианта регулировки: уменьшение продолжительности соединения в заранее заданные часы наибольшей нагрузки, или адаптивное изменение в зависимости от текущей нагрузки.

Интерфейс ТФОП реализуется в транкинговых системах различными способами. В недорогих системах (напр., SmarTrunk) подключение производится по двухпроводной коммутируемой линии. Более современные транкинговые системы имеют в составе интерфейса ТФОП аппаратуру прямого набора номера DID (Direct Inward Dialing), обеспечивающую доступ к абонентам транкинговой сети с использованием стандартной нумерации абонентской телефонной станции (АТС). Ряд транкинговых систем, претендующих на высокое качество обслуживания, использует цифровое ИКМ-соединение с аппаратурой АТС.

Соединение с ТфОП является традиционным для транкинговых систем, но в последнее время все более возрастает число приложений, предполагающих передачу данных, в связи с чем наличие интерфейса сети с коммутацией пакетов становится обязательным.

Терминал технического обслуживания и эксплуатации (терминал O&M) располагается, как правило, на базовой станции однозоновой сети. Терминал предназначен для контроля за состоянием системы, проведения диагностики неисправностей, учета тарификационной информации, внесения изменений в базу данных абонентов. Подавляющее большинство выпускаемых и разрабатываемых транкинговых систем имеют возможность удаленного подключения терминала O&M через ТфОП или сеть с коммутацией пакетов (СКП).

Диспетчерский пульт. Необязательными, но очень характерными элементами инфраструктуры транкинговой системы являются диспетчерские пульта. Дело в том, что транкинговые системы используются в первую очередь теми потребителями, чья работа не обходится без диспетчера - службы охраны правопорядка, скорая медицинская помощь, пожарная охрана, транспортные компании, муниципальные службы. Диспетчерские пульта могут включаться в систему по абонентским радиоканалам, или подключаться по выделенным линиям непосредственно к коммутатору базовой станции. Следует отметить, что в рамках одной транкинговой системы может быть организовано несколько независимых сетей связи. Пользователи каждой из таких сетей не будут замечать работу соседей, и что не менее важно, не смогут вмешиваться в работу других сетей. Поэтому, в одной транкинговой системе могут работать несколько диспетчерских пультов, различным образом подключенных к ней.

Абонентское оборудование транкинговых систем включает в себя широкий набор устройств. Как правило, наиболее многочисленными являются *полудуплексные радиостанции* - именно они в наибольшей степени подходят для работы в замкнутых группах. В большинстве своем это функционально ограниченные устройства, не имеющие цифровой клавиатуры. Их пользователи имеют возможность связываться лишь с абонентами внутри своей рабочей группы, а также посылать экстренные вызовы диспетчеру. Впрочем, этого вполне достаточно для большинства потребителей услуг связи транкинговых систем. Встречаются и полудуплексные радиостанции с широким набором функций и цифровой клавиатурой, но они, будучи заметно дороже, предназначены для более узкого привилегированного круга абонентов.

В транкинговых системах постепенно приживается новый класс абонентских устройств - *дуплексные радиостанции*, скорее напоминающие сотовые телефоны, но обладающие значительно большей функциональностью по сравнению с последними. Дуплексные радиостанции транкинговых систем обеспечивают пользователям не только полноценное соединение с ТфОП, но и возможность групповой работы в полудуплексном режиме. Эти радиостанции предназначены в первую очередь для персонала высшего звена управления компаний, использующих транкинговые системы для организации корпоративных сетей. Стоимость дуплексных транкинговых радиостанций значительно выше, чем сотовых телефонов: от \$ 1500 (аналоговая) до \$ 2500 (цифровая). Несмотря на высокую цену, применение дуплексных транкинговых радиостанций позволяет в большинстве случаев интегрировать все необходимые руководителю средства связи в одном устройстве.

Как полудуплексные, так и дуплексные транкинговые радиостанции выпускаются не только в портативном, но и в автомобильном исполнении. Как правило, выходная мощность передатчиков автомобильных радиостанций выше.

Относительно новым классом устройств для транкинговых систем являются *терминалы передачи данных*. В аналоговых транкинговых системах терминалы передачи данных - это специализированные радиомодемы, поддерживающие соответствующий протокол радиоинтерфейса. Для цифровых систем более характерно встраивание интерфейса передачи данных в абонентские радиостанции различных классов. Как правило, это асинхронный интерфейс типа RS-232. В состав автомобильного терминала передачи данных часто включают спутниковый навигационный приемник системы Global Position System (GPS), предназначенный для определения текущих координат и последующей передачи их диспетчеру на пульт.

В транкинговых системах используются также *стационарные радиостанции*, преимущественно для подключения диспетчерских пультов. Выходная мощность передатчиков стационарных радиостанций приблизительно такая же, как у автомобильных радиостанций.

Многозоновые системы.

Наиболее ранние стандарты транкинговых систем не предусматривали каких-либо механизмов взаимодействия различных зон обслуживания. Архитектура многозоновых транкинговых систем может строиться по двум различным принципам. В том случае, если определяющим фактором является стоимость оборудования, используется *распределенная межзональная коммутация*. Структура такой системы показана на рисунке 2.2. Каждая базовая станция в такой системе имеет свое собственное подключение к ТфОП. Этого уже вполне достаточно для организации многозоновой системы - при необходимости вызова из одной зоны в другую он производится через интерфейс ТфОП, включая процедуру набора телефонного номера. Кроме того, базовые станции могут быть непосредственно соединены с помощью физических выделенных линий связи (чаще всего используются малоканальные радиорелейные линии). Лишь в последнее время сети с коммутацией пакетов стали рассматриваться как средство объединения зон для транкинговых систем. Так, в новейшей цифровой системе DigiStar фирмы Digital Wireless Corporation в качестве опорной сети для объединения зон может использоваться любая сеть с коммутацией пакетов, поддерживающая протокол IP, в том числе глобальная сеть Интернет. Принимая во внимание тот факт, что стоимость доступа к Интернет намного ниже стоимости междугородной телефонной связи, и уж тем более ниже стоимости установки собственных выделенных физических линий, решение фирмы Digital Wireless Corporation нельзя не признать заслуживающим внимания.

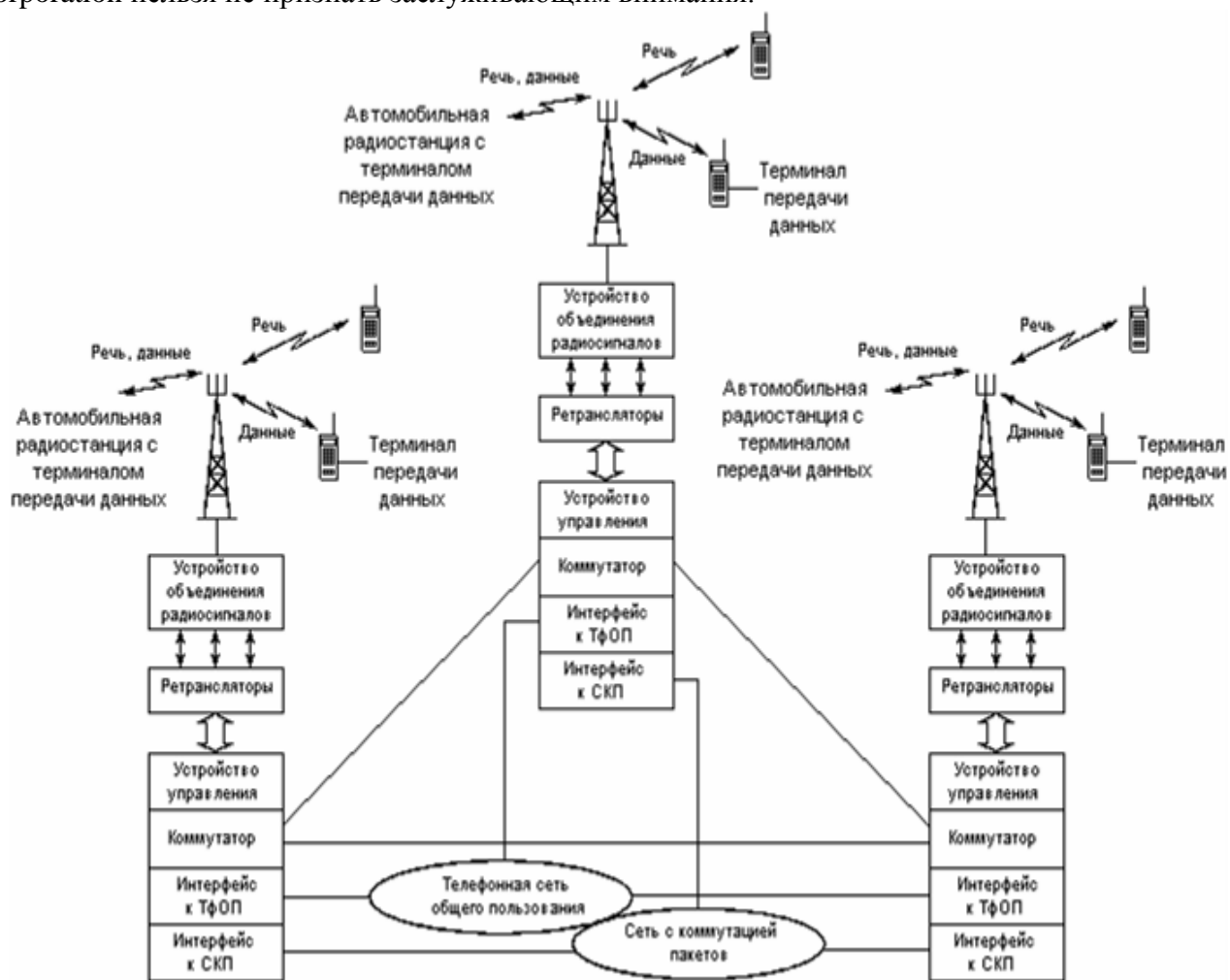


Рис. 2.2. Обобщенная структура транкинговой системы с распределенной межзональной коммутацией

Все же, использование распределенной межзональной коммутации пригодно лишь для систем с небольшим количеством зон и с невысокими требованиями к оперативности транзональных вызовов (особенно в случае соединения через коммутируемые каналы ТфОП). В системах с высоким качеством обслуживания используется другая архитектура многозоновых систем - архитектура с *централизованной коммутацией*. Структура многозоновой транкинговой системы с централизованной коммутацией показана на рисунке 2.3.

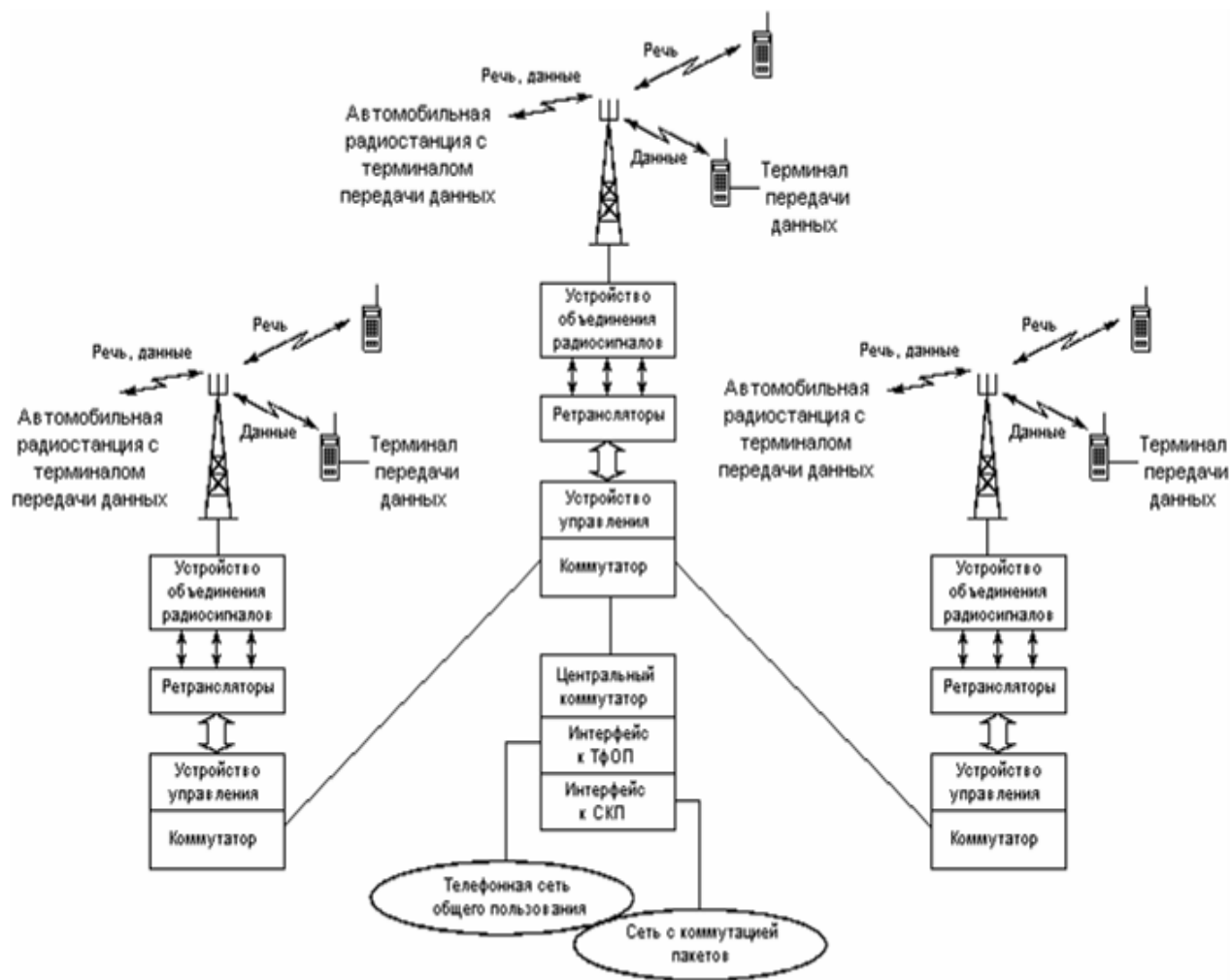


Рис. 2.3. Обобщенная структура транкинговой системы с централизованной межзональной коммутацией

Важнейший элемент этой схемы - межзональный коммутатор. Он обрабатывает все виды транзональных вызовов. Таким образом, весь межзональный трафик проходит через один коммутатор, соединенный с базовыми станциями по выделенным линиям. Это обеспечивает быструю обработку вызовов, возможность подключения централизованных диспетчерских пультов. Информация о местонахождении абонентов системы с централизованной коммутацией хранится в единственном месте, поэтому ее легче защитить. Кроме того, межзональный коммутатор осуществляет также функции централизованного интерфейса ТфОП и СКП, что позволяет при необходимости полностью контролировать как речевой трафик телефонной сети, так и трафик всех приложений передачи данных, связанный с внешними СКП, например Интернет. Таким образом, система с централизованной коммутацией обладает более высокой управляемостью. За все эти преимущества приходится дорого платить - стоимость одного только коммутатора составляет сотни тысяч долларов, а ведь нужно еще обеспечить его подключение к базовым станциям по выделенным линиям.

Итак, можно выделить несколько важнейших архитектурных признаков, присущих транкинговым системам. Во-первых, это ограниченная (а значит, дорогая) инфраструктура. В многозоновых транкинговых системах она более развита, но все равно не идет ни в какое сравнение с мощностью инфраструктуры сотовых сетей.

Во-вторых, это большой пространственный охват зон обслуживания базовых станций - объясняется необходимостью поддержания групповой работы на обширных территориях и требованиями минимизации стоимости системы. В сотовых сетях, где инвестиции в инфраструктуру быстро окупаются, а трафик растет, базовые станции размещаются все более плотно, с малым радиусом зон покрытия (сот). При развертывании транкинговых систем все обстоит несколько иначе - объем финансирования, как правило, ограничен, и для достижения высокой эффективности капиталовложений нужно обслужить с помощью одного комплекта оборудования базовой станции возможно более обширную территорию.

В-третьих, широкий набор абонентского оборудования позволяет транкинговым системам охватить практически весь спектр потребностей корпоративного потребителя в подвижной связи. Возможность обслуживания разнородных по функциональному назначению устройств в единой системе - еще один путь к минимизации расходов.

В-четвертых, транкинговые системы позволяют на базе своих каналов организовать независимые выделенные сети связи (или, как принято говорить в последнее время, частные виртуальные сети). Это означает, что несколько организаций могут совместными усилиями развернуть единую систему, вместо установки отдельных систем. Таким образом, достигается ощутимая экономия радиочастотного ресурса, а также снижение стоимости инфраструктуры.

Таким образом, все архитектурные признаки транкинговых систем свидетельствуют о прочности позиций последних в корпоративном секторе рынка систем и средств подвижной связи.

Службы транкинговых систем

Транкинговые системы связи характеризуются широким разнообразием служб, обеспечивающих работу различного оборудования, а также поддержку сетей связи внутри этих систем. Наиболее важной и наиболее часто используемой службой транкинговых систем является служба внутренних вызовов.

Внутренние вызовы.

Транкинговые сети предоставляют абонентам возможность производить различные типы вызовов внутри системы: индивидуальный (персональный) и групповой (диспетчерский). В первом случае вызов направляется только одному абоненту, во втором - нескольким абонентам.

Основным типом вызова в транкинговых системах является групповой вызов в рамках одной группы (см. рис.2.4). Групповой вызов принципиально может быть произведен только в полудуплексном режиме - пока вызывающий абонент говорит и его радиостанция находится в режиме передачи, все остальные члены группы принимают речь вызывающего абонента. Таким образом, реплика любого члена группы автоматически становится слышимой всеми участниками группы. Групповой вызов может производиться с самой простой (а следовательно, недорогой) полудуплексной радиостанции - для этого пользователю достаточно, как правило, лишь нажать на кнопку "Передача". Вхождение в связь с ретранслятором и группой абонентов производится в этом случае автоматически. Этот тип вызова обеспечивают все известные транкинговые системы.

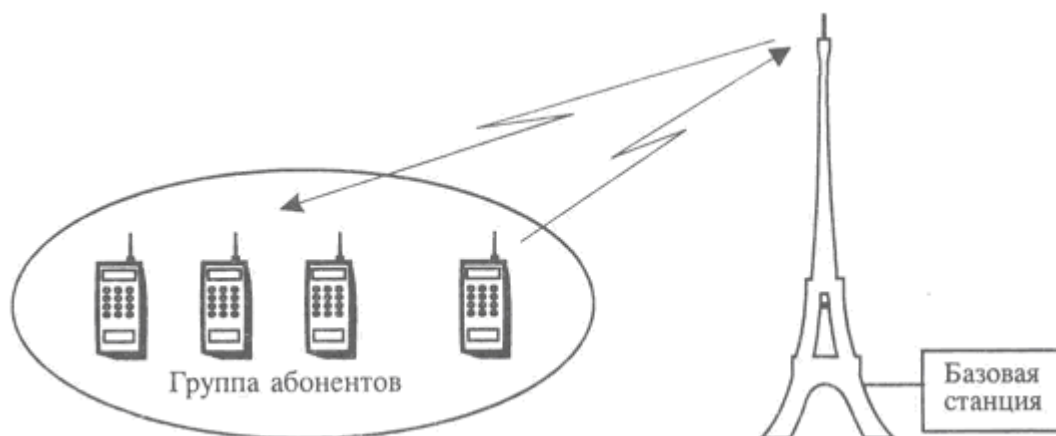


Рис. 2.4. Групповой вызов

В большинстве существующих транкинговых систем предусмотрена возможность одновременного вызова абонентов нескольких групп. К числу таких вызовов относятся общий вызов (all call), экстренный вызов (от диспетчера). В некоторых системах используется иерархическое вложение групп и предусматриваются соответствующие типы вызовов: многоуровневый, многогрупповой и т.д. Как правило, право производить столь сложные вызовы предоставляется только диспетчеру. Некоторые системы обеспечивают возможность соединения с произвольно выбранной группой, причем не только для абонента транкинговой системы (см. рис.2.5), но и для абонента телефонной сети общего пользования (см. рис.2.6).

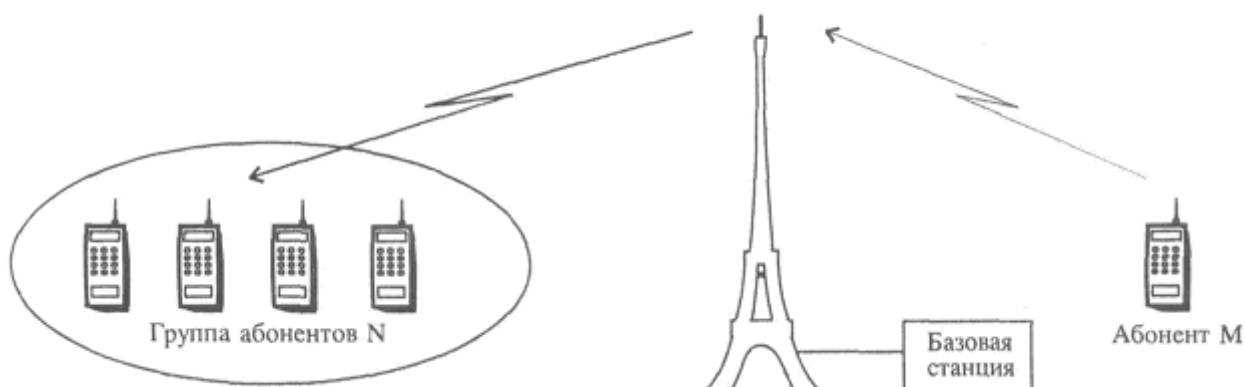


Рис. 2.5. Вызов произвольно выбранной группы

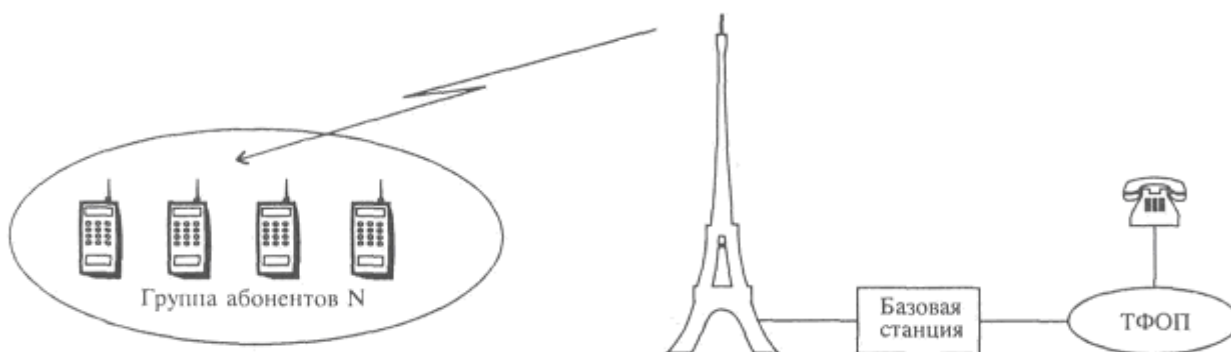


Рис. 2.6. Вызов группы из ТфОП

Персональный внутренний вызов (см. рис. 2.7) является более привилегированным типом вызова. Для его посылки пользователь должен использовать радиостанцию с цифровой клавиатурой. Персональный внутренний вызов может быть произведен не только в полудуплексном, но и в дуплексном режиме (разумеется, если абонентские радиостанции также являются дуплексными).

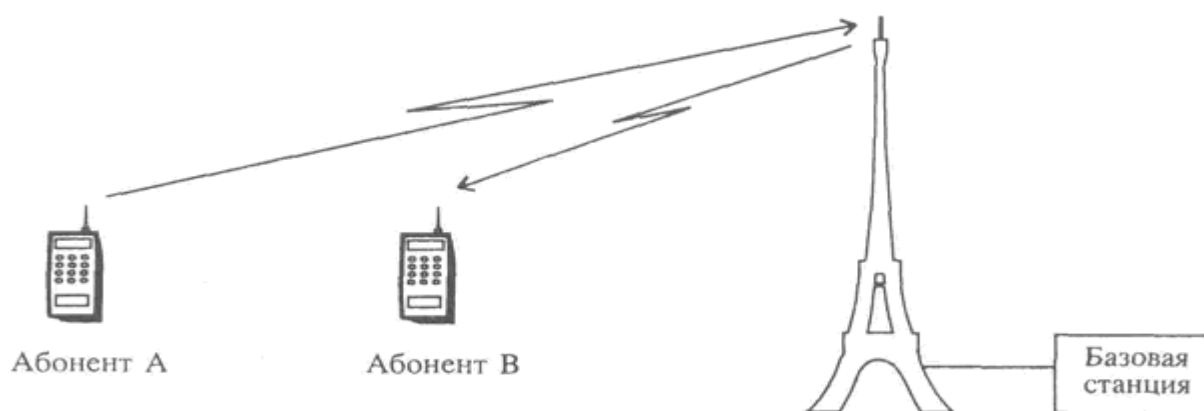


Рис. 2.7. Персональный вызов

Существует еще одна специфическая разновидность внутренних вызовов - статусные вызовы. Они служат заменой тривиальным репликам, таким как "вас понял", "повторите" и т.п. Вместо речевого ответа абонент может нажать соответствующую функциональную кнопку, что вызовет передачу короткого цифрового сообщения. Применение статусных вызовов позволяет существенно уменьшить загрузку системы, т.к. в условиях диспетчерской связи и групповой работы такие реплики употребляются очень часто.

Приоритетные вызовы.

Многие транкинговые системы предусматривают обработку вызовов с несколькими уровнями приоритета. Так, в системе DigiStar предусмотрено 10 уровней приоритета, в системе EDACS - 8 уровней. Разграничение приоритетов может использоваться в различных целях: предоставление привилегий отдельным абонентам или группам, а также оптимизация обработки трафика. В любом случае, влияние приоритетной обработки вызовов начинает сказываться только при высокой загрузке системы.

Оптимизация обработки трафика заключается в том, что вызовам абонентов, уже начавших и продолжающих разговор, присваивается более высокий приоритет, чем вызовам абонентов, только устанавливающих соединение. Таким образом, ценой некоторого увеличения времени на первое установление соединения минимизируется продолжительность пауз в разговоре абонентов, что в конечном счете ведет к улучшению комфортности радиопереговоров.

Некоторые системы предусматривают наделение ряда абонентов правом вызова сверхвысокого приоритета, или так называемого вытесняющего вызова. При поступлении такого вызова в ситуации, когда все ретрансляционные ресурсы заняты (т.е. в ситуации блокирования), одно из текущих соединений прерывается, а освободившийся ресурс отводится для обслуживания поступившего вызова со сверхвысоким приоритетом.

Существует еще один тип приоритетной обработки вызовов - предоставление так называемого открытого канала, заключающееся во временном переключении одного из каналов в монопольное владение одной группы абонентов. Это позволяет группе получить гарантированный и быстрый доступ к ретранслятору. Предоставление открытого канала является средством, используемым лишь в исключительных ситуациях и доступным для крайне ограниченного круга пользователей. Включение режима открытого канала приносит заметные неудобства остальным абонентам системы - за счет уменьшения числа разделяемых каналов ухудшается качество обслуживания, особенно в ситуации тяжелой нагрузки.

Доступ к ТфОП

Как правило, доступ к ТфОП имеют лишь немногие абоненты транкинговых систем. Вызов абонента ТфОП может быть произведен только с радиостанции, имеющей цифровую клавиатуру. Для доступа к ТфОП лучше всего использовать дуплексную радиостанцию, поскольку сама ТфОП работает в дуплексном режиме. Вместе с тем, практически все известные транкинговые системы предоставляют возможность доступа к ТфОП с помощью полудуплексных радиостанций. Следует заметить, что в России для вновь устанавливаемых систем допускается только дуплексное соединение.

Абонент ТфОП может вызывать не только отдельного абонента транкинговой системы, но и группу абонентов. Процедура вызова для абонентов ТфОП может быть двухступенчатой (в том случае, если интерфейс ТфОП подключен к телефонной сети с помощью двухпроводной коммутируемой линии), или одноступенчатой (при подключении интерфейса ТфОП по методу Direct ID). При двухступенчатой процедуре абонент ТфОП должен сначала набрать номер телефона, к которому подключен интерфейс ТфОП, а затем - номер абонента внутри транкинговой системы. Поскольку в этом случае набор номера абонента транкинговой системы происходит в условиях установленного соединения через ТфОП, часто (особенно в России) сопровождающегося импульсными и другими помехами, вероятность ошибочного соединения или обрыва связи относительно высока. Поэтому, все вновь разрабатываемые системы и стандарты предполагают использование метода Direct ID, позволяющего организовать доступ из ТфОП с использованием единой системы нумерации абонентов. Абоненту ТфОП для вызова абонента транкинговой системы, оснащенной аппаратурой Direct ID, достаточно набрать обычный городской телефонный номер, также как и в сотовой сети.

Роуминг.

В многозоновых транкинговых системах осуществляется отслеживание текущего расположения абонентов. При перемещении абонента из одной зоны в другую обеспечивается регистрация и назначение новых каналов доступа. В системах с распределенной коммутацией каждая базовая станция самостоятельно осуществляет коммутацию поступающих вызовов. В системах с централизованной коммутацией роуминг более надежен, а скорость обработки межзональных вызовов выше.

Для большинства транкинговых систем характерно прерывание связи при перемещении абонента из одной зоны обслуживания в другую (hard hand-over), связанное с отсутствием механизма эстафетной передачи. Для продолжения разговора абонент вынужден повторять вызов. Вместе с тем, при полудуплексном режиме работы, когда каждая новая реплика передается с помощью отдельного вызова, межзональный переход практически незаметен. Все же, требования пользователей транкинговых систем растут, и в новейших цифровых системах TETRA и EDACS ProtoCALL обеспечивается эстафетная передача.

Особый аспект роуминга в транкинговых системах - обслуживание многозональных групповых вызовов. Отслеживая перемещения абонентов, система при поступлении группового вызова обеспечивает его доведение до всех членов группы, в какой бы зоне они не находились.

Передача данных.

В транкинговых системах передача данных является дополнительной службой, поэтому до последнего времени не получила развитых средств поддержки. Скорость передачи данных во всех аналоговых системах лежит в пределах 0,6 - 4,8 кбит/с. Как правило, аналоговые транкинговые системы лишь предоставляют каналы для передачи данных, не обеспечивая сетевую маршрутизацию. В то же время для цифровых транкинговых систем передача данных является значительно более родственной службой. Цифровые транкинговые системы предоставляют сервис не только канального, но и сетевого уровня, а в ряде случаев - и транспортного. Возможна поддержка наложенных сетей, например IP-сетей. Пользовательская скорость передачи данных для цифровых систем может варьироваться в широких пределах. Так, новейший стандарт TETRA предусматривает скорость до 28,8 кбит/с. При проектировании собственных сетей передачи данных на базе цифровых транкинговых систем пользователю

предоставляется, как правило, возможность выбора параметров протокола канального и транспортного уровня, а также возможность использования датаграмм.

Оборудование базовых станций или центрального коммутатора цифровых транкинговых систем осуществляет также функции шлюза с внешними сетями передачи данных, т.е. сетями с коммутацией пакетов. В функции шлюза входит конвертирование протоколов, включая взаимное преобразование адресов внутренней и внешней сетей, а также поддержание наложенной сети.

Важнейшая область применения служб передачи данных - организация в рамках транкинговых систем сетей дистанционного мониторинга и контроля местоположения подвижных объектов.

Режим непосредственной связи.

В некоторых транкинговых системах предусмотрена возможность непосредственной связи абонентов без участия ретранслятора. Этот режим, называемый также talk around или direct mode operation, используется в том случае, если один или несколько абонентов вышли из зоны действия всех ретрансляторов системы (см. рис. 2.8).



Рис. 2.8. Режим непосредственной связи

Тарификация (биллинг).

Оборудование транкинговых систем позволяет вести учет и тарификацию соединений с получением подробной информации по каждому соединению. В данные по учету и тарификации могут входить следующие параметры: идентификаторы вызывающего и вызываемого абонентов, время и дата начала установления соединения, длительность соединения, тип вызова (индивидуальный, групповой и др.), категория приоритета (обычный или высокий и др.).

В транкинговых системах могут задаваться несколько тарифных периодов для разных дней недели и времени суток.

Данные биллинга могут использоваться для документирования связи и предоставления счетов абонентам, а также для выявления попыток несанкционированного доступа.

Удаленное управление абонентскими радиостанциями.

Ряд транкинговых систем предоставляет оператору возможность оперативного изменения параметров доступа абонентских радиостанций. Так, в системе EDACS можно дистанционно перепрограммировать сетевой идентификатор (ID), частоты каналов, а также переконфигурировать группы абонентов. Удаленное управление используется также в целях борьбы с попытками несанкционированного доступа, что особенно важно в случае хищения абонентского оборудования. В системах стандарта SmartTrunk II имеется так называемый радиокиллер: при посылке специальной команды в абонентской радиостанции происходят необратимые изменения, превращающие ее в бесполезную игрушку.

Классификация транкинговых систем

Для классифицирования транкинговых систем связи можно использовать следующие признаки.

Метод передачи речевой информации.

По методу передачи речевой информации транкинговые системы подразделяются на аналоговые и цифровые. Передача речи в радиоканале аналоговых систем осуществляется с использованием частотной модуляции, а шаг сетки частот обычно составляет 12,5 кГц или 25 кГц. Для передачи речи в цифровых системах используются различные типы вокодеров, преобразующих аналоговый речевой сигнал в цифровой поток со скоростью не более 4,8 кбит/с.

Количество зон.

В зависимости от количества базовых станций и общей архитектуры различают однозоновые или многозоновые системы. Первые располагают лишь одной базовой станцией, вторые - несколькими БС с возможностью роуминга.

Метод объединения базовых станций в многозоновых системах.

Базовые станции в транкинговых системах могут объединяться с помощью единого коммутатора (системы с централизованной коммутацией), либо соединяться друг с другом непосредственно или через сети общего пользования (системы с распределенной коммутацией).

Тип многостанционного доступа.

В подавляющем большинстве транкинговых систем используется многостанционный доступ с частотным разделением (МДЧР), включая цифровые системы. Для систем МДЧР справедливо соотношение "одна несущая - один канал". Комбинация МДЧР и многостанционного доступа с временным разделением (МДВР) используется в системах стандарта TETRA, а также является факультативной возможностью системы EDACS ProtoCALL.

Способ поиска и назначения канала.

По способу поиска и назначения канала различают системы с децентрализованным и централизованным управлением. В первых процедуру поиска свободного канала выполняют абонентские радиостанции. В этих системах ретрансляторы базовой станции обычно не связаны друг с другом и работают независимо. Особенностью систем с децентрализованным управлением является относительно большое время установления соединения между абонентами, растущее с увеличением числа ретрансляторов. Такая зависимость вызвана тем, что абонентские радиостанции вынуждены непрерывно последовательно сканировать каналы в поисках вызывного сигнала (последний может поступить от любого ретранслятора) или свободного канала (если абонент сам посылает вызов). Наиболее характерными представителями данного класса являются системы стандарта SmartTrunk.

В системах с централизованным управлением поиск и назначение свободного канала производится на базовой станции. Для обеспечения нормального функционирования таких систем организуются каналы двух типов: рабочие (traffic channel) и управления (control channel). Все запросы на предоставление связи направляются по каналу управления, по этому же каналу базовая станция извещает абонентские устройства о назначении канала, отклонении запроса, либо о постановке запроса в очередь.

Тип канала управления.

Во всех транкинговых системах каналы управления являются цифровыми. Различают системы с выделенным частотным каналом управления и системы с распределенным каналом управления. В системах первого типа передача данных в канале управления производится со скоростью до 9,6 кбит/с, а для разрешения конфликтов используются протоколы типа ALOHA.

Выделенный канал управления имеют транкинговые системы фирмы Motorola: StartSite, SmartNet, SmartZone, система EDACS фирмы Ericsson и некоторые другие. В системах с распределенным каналом управления информация о состоянии системы и поступающих вызовах распределена между низкоскоростными субканалами передачи данных, совмещенными со всеми рабочими каналами. Таким образом, в каждом частотном канале системы передается не только речь, но и данные канала управления. Для организации парциального канала в

аналоговых системах обычно используется субтональный диапазон частот 0 - 300 Гц. Наиболее характерными представителями данного класса являются системы LTR и Multi-Net фирмы E.F.Johnson.

Способ удержания канала.

Транкинговые системы позволяют абонентам удерживать канал связи на протяжении всего разговора, или только на время передачи. Первый способ, называемый также транкингом сообщений (message trunking), наиболее традиционен для систем связи, и обязательно используется во всех случаях применения дуплексной связи или соединения с ТфОП.

Второй способ может быть реализован только при использовании полудуплексных радиостанций. В последних передатчик включается только на время произнесения абонентом фраз разговора. В паузах между окончанием фраз одного абонента и началом ответных фраз другого передатчики обеих радиостанций выключены. Значительная часть транкинговых систем эффективно использует такие паузы, освобождая канал немедленно после окончания работы передатчика абонентской радиостанции. Реплики одного и того же разговора могут передаваться по разным каналам. Такой метод обслуживания, предусматривающий удержание канала только на время передачи, называется транкингом передачи (transmission trunking). Платой за высокую эффективность данного метода служит снижение комфортности переговоров - в состоянии высокой нагрузки канал предоставляется с некоторой задержкой, что приводит к фрагментарности и раздробленности разговора.

Транкинговые системы, при всем своем универсализме, занимают вполне определенную нишу на рынке систем подвижной связи. Это отчетливо заметно при сопоставлении параметров различных типов систем, доминирующих на рынке (см. табл. 2.2). К таковым относятся обычные¹ (неавтоматизированные), транкинговые и сотовые системы.

До появления транкинговых систем корпоративный сектор рынка практически полностью был занят обычными системами. Поскольку транкинговые системы ориентированы на тот же сектор, можно найти много общих черт между ними и обычными системами. Так, в частности, радиус зон обслуживания как в транкинговых, так и в обычных системах делается максимально возможным и зависит в основном от высоты подвеса антенн базовых станций. В сотовых системах, напротив, по мере роста числа абонентов приходится уменьшать радиусы зон, с тем чтобы увеличить количество доступных каналов связи на обслуживаемой территории. Таким образом, использование технологии МДВР/МДЧР, предусматривающей уменьшение зон по сравнению с МДЧР, в наибольшей степени отвечает принципам создания именно сотовых систем. Нижнее значение радиуса зон в транкинговых системах, равное приблизительно 5 км, дают системы МДВР/МДЧР, такие как TETRA и EDACS ProtoCALL. Для остальных транкинговых систем, использующих только МДЧР, характерны значительно большие радиусы зон.

В обычных системах возможен только один тип вызова - групповой. Сотовые системы, наоборот, поддерживают лишь индивидуальные вызовы. Спецификации некоторых стандартов сотовых систем (к ним относится GSM, являющийся федеральным стандартом России) и соответствующая аппаратура поддерживают режим телеконференций, но он не является прямым аналогом группового вызова, к тому же региональные операторы редко разрешают его использование. Транкинговые системы, как уже было показано в предыдущем разделе, предусматривают обслуживание групповых и индивидуальных вызовов, а также множества их разновидностей.

Таблица 2.2

Параметры системы	обычная	транкинговая	сотовая
Конфигурация	однозоновая	однозоновая, многозоновая	многозоновая
Радиус зоны, км	20-80	5-80	0,3-10

Тип вызова	групповой	индивидуальный, групповой	индивидуальный
Метод посылки вызова	Нажатие кнопки "Передача"	нажатие кнопки "Передача", набор номера	набор номера
Режим радиосвязи	Полудуплекс	Полудуплекс, дуплекс	Дуплекс
Внутрисистемный трафик	100%	50% - 95%	3% - 15%
Роуминг	-	есть	есть
Режим переключения каналов при смене зоны	-	жесткий, мягкий	мягкий
Среднее число абонентов на канал	до 30	50-100	до 30

Наиболее удобным способом посылки группового вызова является нажатие на кнопку "Передача". Для обычных систем этот способ является также и единственным. В транкинговых системах нажатие на кнопку "Передача" приводит к запуску процедуры установления соединения с базовой станцией, в ходе которой устройству управления БС сообщается идентификатор вызываемой группы. Базовая станция назначает канал связи и уведомляет об этом как радиостанцию вызывающего абонента, так и радиостанции остальных абонентов группы. После этого радиостанция вызывающего абонента переходит в режим передачи речи на назначенном канале. Процесс вхождения в связь и установления соединения проходит в течение 0,2 - 0,3 сек., т.е. незаметно для абонента. Для вызова произвольно выбранной группы, посылки индивидуального вызова, а также при соединении с ТфОП в транкинговых системах используется набор номера. Таким образом, транкинговые системы позволяют использовать в каждом случае тот метод посылки вызова, который в наибольшей степени отвечает ситуации. В сотовых системах, являющихся расширением ТфОП, единственным средством посылки вызова является набор номера.

В то время как доля внутрисистемного трафика в сотовых системах всегда незначительна и лишь в исключительных случаях поднимается до уровня в 15%, для транкинговых систем этот показатель сильно различается от одной сети к другой. Если транкинговая система используется преимущественно в целях внутрикорпоративной и ведомственной связи, а право доступа к ТфОП предоставлено лишь отдельным абонентам, внутрисистемный трафик может достигать 95%, и проблема перегрузки интерфейса ТфОП не будет доставлять хлопот оператору. В случае, если оператор предоставляет услугу доступа к ТфОП частным потребителям, конкурируя с сотовой сетью или (за неимением) заменяя ее, что является обычной практикой в России, внутрисистемный трафик может упасть до 50% и даже ниже. При этом количество каналов интерфейса ТфОП должно соответствовать количеству радиоканалов и соотношению внутреннего и полного трафика.

Роуминг используется как в сотовых, так и в транкинговых системах, но его реализации существенно различаются. Если в сотовых системах изначально закладывалась возможность организации глобальных сетей с автоматическим роумингом, то разработчики транкинговых систем до недавних пор ограничивали роуминг пределами одной системы. Лишь в последних системах и стандартах транкинговой связи – EDACS ProtoCALL, APCO25 и TETRA - обеспечивается возможность межсистемного роуминга. То же относится и к поддержке эстафетной передачи абонента от одной базовой станции к другой. Большинство транкинговых систем не имеют такой возможности. Среднее число абонентов на канал является важнейшей интегральной характеристикой любой системы подвижной связи. Несмотря на то, что характер нагрузки в обычных и транкинговых системах почти совпадает, отсутствие механизма автоматического доступа к свободному каналу у первых не позволяет достичь им значения в 100 абонентов на канал. Что касается сотовых систем, невысокое значение этого параметра объясняется большим уровнем трафика, создаваемым абонентами при телефонных переговорах.

Стандарты транкинговых систем

Выбор базового варианта и стандарта должен основываться, прежде всего, на соответствии технических возможностей проектируемой системы требуемым: максимальная емкость системы, возможное количество зон обслуживания и каналов, набор сервисных функций, подключение к телефонной сети общего пользования и т.д.

Известно, что по методу передачи речевой информации транкинговые системы подразделяются на аналоговые и цифровые. Сразу же следует оговориться, что будем рассматривать только открытые стандарты, так как открытость технологии, в первую очередь указывает на то, что спецификации стандарта доступны всем желающим, и любой производитель может наладить выпуск такого оборудования. А это означает адекватный уровень цен и независимость заказчика от позиции конкретного производителя. Кроме того, открытость предусматривает совместимость и взаимодействие оборудования разных производителей

Рассмотрим сначала аналоговые стандарты.

В настоящее время и в мире, и в России достаточно широко распространены появившиеся ранее аналоговые транкинговые системы радиосвязи, такие как SmarTrunk, системы протокола MPT1327 (ACCESSNET, ACTIONET и др.), системы фирмы Motorola (Startsite, Smartnet, Smartzone), системы с распределенным каналом управления (LTR и Multi-Net фирмы E.F.Johnson Co и ESAS фирмы Uniden). Наибольшее распространение получили системы MPT1327, что объясняется значительными преимуществами данного стандарта по сравнению с другими аналоговыми системами.

Аналоговая транкинговая система MPT1327

Транкинговая система MPT1327 является оптимальным решением для построения ведомственных и коммерческих систем радиотелефонной связи, работающих в небольшом географическом районе и имеющих не более 5000 абонентов (система поддерживает до 5000 индивидуальных идентификаторов и до 2000 групповых). Система может быть построена в как в однозональном варианте (до 24 каналов в базовой станции), так и в многозональном (до 12 базовых станций). Основными потребителями системы являются предприятия нефтегазового комплекса, крупные индустриальные предприятия, такие ведомства как РЕЧФЛОТ, МОРФЛОТ (наземное обслуживание), коммунальные и аварийные службы, подразделения Скорой помощи и служб общественной безопасности, операторы системы «АЛТАЙ».

Идеология предлагаемой системы строится на четырех основных принципах:

- Использование открытого стандарта MPT1327.
- Устойчивость системы. Ни один из модулей системы не может быть причиной выхода ее из строя. Потеря одного из контроллеров или ретранслятора лишь снижает количество рабочих каналов системы.
- Экономическая эффективность. При построении системы не требуется применение центрального коммутатора, что особенно важно для небольших систем.
- Модульность и расширяемость. Простое добавление каналов системы (контроллеров и ретрансляторов) позволяет постепенно расширять систему.

Система полностью соответствует протоколам MPT1327/1343, поэтому к основным возможностям системы можно отнести основные возможности этого стандарта:

- полная совместимость с абонентским оборудованием, работающим в протоколе MPT1327;
- поддержка всех видов вызовов MPT1327 и их приоритетности (индивидуальный и групповой вызовы, вызов для оповещения, обычный, приоритетный, аварийные вызовы и пр.);
- передача статусных сообщений;
- передача коротких блоков данных (до 184 бит);

- передача данных произвольного размера по протоколу MAP27;
- подключение к телефонной сети в каждой зоне обслуживания;
- регистрация и полная проверка электронного серийного номера (ESN) абонента;
- постановка в очередь при занятости системы, телефонной линии или вызываемого абонента;
- переадресация вызовов, роуминг;
- защита от несанкционированного доступа;

К особенностям системы можно отнести следующее:

- распределенная архитектура системы;
- все радиоканалы имеют равный доступ ко всем телефонным интерфейсам системы;
- широкие возможности программирования и настройки телефонных интерфейсов;
- дистанционный контроль и управление через встроенный модем;
- объединение в одном блоке контроллера радиоканала, базы данных абонентов системы, телефонного интерфейса или интерфейса межбазовых соединений;
- поддержка дуплексных абонентских станций;
- цифровая обработка речевого сигнала;
- возможность подключения к системе обычных конвенциональных сетей;
- возможность построения различных конфигураций в многозоновом варианте системы (типа "звезда", "круг", "линия", соединение каждой базовой станции со всеми базовыми станциями).

Основными преимуществами предлагаемой транкинговой системы является ее простота, надежность, а также эффективность и доступность. Существующее на рынке представление о том, что любая система, работающая в протоколе MPT1327, является очень дорогостоящей и сложной, уже не актуально. Модульная конструкция системы, позволяющая наращивать количество каналов в базовой станции (до 24), а также отсутствие центрального коммутатора системы, которое компенсируется распределением его функций между контроллерами системы, соединенными цифровой шиной, позволяет существенно снизить затраты и упростить систему. Доступность системы определяется прежде всего тем, что отсутствует центральный коммутатор, а также тем, что цены на абонентские станции MPT1327 существенно снизились за последнее время. Удельная стоимость в расчете на одного абонента (с учетом стоимости полного комплекта базового оборудования и абонентских станций) гораздо ниже, чем аналогичный стартовый показатель для других сетей протокола MPT1327. Как уже было отмечено выше, применение транкинговой системы MPT1327 оптимально при построении однозоновых и небольших многозоновых систем.

Перспектива перехода на цифровые технологии при построении систем связи практически не окажет влияние в ближайшие пять лет на сегмент небольших систем протокола MPT1327, так как активно разрабатываемые сегодня и внедряемые в Западной Европе решения на базе протокола TETRA предназначены для организации систем национального масштаба, с большими зонами действия и большим количеством абонентов. Наиболее корректным экономическим параметром оценки стоимости таких систем является оценка затрат на покрытие единицы площади с определенной пропускной способностью. На сегодняшний день этот параметр для небольших систем с невысокой плотностью абонентов, реализованных на базе протокола MPT1327 и TETRA, отличается в несколько раз. Необходимо учитывать, что зона действия одной базовой станции TETRA существенно меньше (в силу того, что используется временное разделение каналов), чем зона действия базовой станции MPT1327, а затраты на построение качественных межзоновых соединений с требуемой пропускной способностью очень высоки. Это означает, что реальный переход на цифровые технологии профессиональной мобильной связи в России начнется при формировании соответствующих экономических условий.

МРТ1327 и SmarTrunk

Ближайшим конкурентом небольших систем протокола МРТ1327 является система SmarTrunk, исторически завоевавшая в России большую популярность. Реально, эта конкуренция является скорее формальной, так как ряд особенностей системы SmarTrunk не позволяют ей полноценно решать задачи технологической связи. Во-первых, система принципиально предназначена для осуществления индивидуальных вызовов и вызовов в ТФОП, а не для оперативной (групповой), технологической связи. Во-вторых, в многоканальных системах SmarTrunk время установления связи столь велико, в силу особенностей технологии, что не удовлетворяет профессионального потребителя. Существенным фактором, также влияющим на выбор потребителя, является цена. Разница между удельной стоимостью одного абонента в системе SmarTrunk и в транкинговой системе МРТ1327 составляет около 15% при порядковой разнице в функциональных возможностях системы. Нужно учитывать, что корректное сравнение любых систем (в том числе SmarTrunk и МРТ1327) возможно при условии использования аналогичных (по качеству) ретрансляторов, антенн и оборудования ВЧ-тракта.

Следует сказать, что и в России большинство крупных транкинговых сетей построено на базе оборудования стандарта МРТ1327. Руководители компаний, занимающихся поставками оборудования и системной интеграцией в области профессиональной радиосвязи, отмечают, что большинство стоящих перед их заказчиками задач оперативной речевой связи достаточно эффективно решается с помощью аналоговых систем стандарта МРТ1327.

Цифровые стандарты транкинговой радиосвязи

Цифровые стандарты транкинговой радиосвязи пока не получили широкого распространения в России, но уже сейчас можно говорить об их активном и успешном внедрении.

Вместе с тем, круг пользователей цифровых транкинговых систем постоянно расширяется. В России также появляются крупные заказчики систем профессиональной радиосвязи, требования которых обуславливают переход к цифровым технологиям. В первую очередь, это крупные ведомства и корпорации, такие как РАО ЕЭС, Минтранс, МПС, Сибнефть и другие, а также силовые структуры и правоохранительные органы.

Необходимость перехода объясняется рядом преимуществ цифрового транкинга перед аналоговыми системами, такими как большая спектральная эффективность за счет применения сложных видов модуляции сигнала и низкоскоростных алгоритмов речепреобразования, повышенная емкость систем связи, выравнивание качества речевого обмена по всей зоне обслуживания базовой станции за счет применения цифровых сигналов в сочетании с помехоустойчивым кодированием. Развитие мирового рынка систем транкинговой радиосвязи сегодня характеризуется широким внедрением цифровых технологий. Ведущие мировые производители оборудования транкинговых систем объявляют о переходе к цифровым стандартам радиосвязи, предусматривая при этом либо выпуск принципиально нового оборудования, либо адаптацию аналоговых систем к цифровой связи.

Цифровые транкинговые системы по сравнению с аналоговыми имеют ряд преимуществ за счет реализации требований по повышенной оперативности и безопасности связи, предоставления широких возможностей по передаче данных, более широкого спектра услуг связи (включая специфические услуги связи для реализации специальных требований служб общественной безопасности), возможностей организации взаимодействия абонентов различных сетей.

1. Высокая оперативность связи. Прежде всего, это требование означает минимально возможное время установления канала связи (время доступа) при различных видах соединений (индивидуальных, групповых, с абонентами телефонных сетей и пр.). В конвенциональных системах связи при передаче цифровой информации, требующей временной синхронизации передатчика и приемника, для установления канала связи требуется большее время, чем аналоговой системе. Однако для транкинговых систем радиосвязи, где информационный обмен,

в основном, производится через базовые станции, цифровой режим сравним по времени доступа с аналоговым (и в аналоговых, и в цифровых системах радиосвязи, как правило, канал управления реализуется на основе цифровых сигналов).

Кроме этого, в системах цифровой транкинговой радиосвязи более просто реализуются различные режимы связи, повышающие ее оперативность, такие как режим непосредственной (прямой) связи между подвижными абонентами (без использования базовой станции), режим открытого канала (выделения и закрепления частотных ресурсов сети за определенной группой абонентов для ведения ими в дальнейшем переговоров без выполнения какой-либо установочной процедуры, в т. ч. без задержки), режимы аварийных и приоритетных вызовов и др.

Цифровые системы транкинговой радиосвязи лучше приспособлены к различным режимам передачи данных, что предоставляет, например, сотрудникам правоохранительных органов и служб общественной безопасности широкие возможности оперативного получения сведений из централизованных баз данных, передачи необходимой информации, включая изображения с мест происшествий, организации централизованных диспетчерских систем местоопределения подвижных объектов на основе спутниковых радионавигационных систем. Данные системы позволяют потребителям нефтегазового комплекса использовать их как транспорт не только для передачи голосовой связи, но и для передачи телеметрии и телеуправления.

2. Передача данных. Цифровые системы транкинговой радиосвязи лучше приспособлены к различным режимам передачи данных, что предоставляет абонентам цифровых сетей широкие возможности оперативного получения сведений из централизованных баз данных, передачи необходимой информации, включая изображения, организации централизованных диспетчерских систем местоопределения подвижных объектов на основе спутниковых радионавигационных систем. Скорость передачи данных в цифровых системах значительно выше, чем в аналоговых.

В большинстве систем радиосвязи на основе цифровых стандартов реализуются услуги передачи коротких и статусных сообщений, персонального радиовызова, факсимильной связи, доступа к фиксированным сетям связи (в т. ч. работающим на основе протоколов ТСП/Р).

3. Безопасность связи. Включает в себя требования по обеспечению секретности переговоров (исключение возможности извлечения информации из каналов связи кому-либо, кроме санкционированного получателя) и защиты от несанкционированного доступа к системе (исключение возможности захвата управления системой и попыток вывести ее из строя, защита от «двойников» и т. п.). Как правило, основными механизмами обеспечения безопасности связи является шифрование и аутентификация абонентов.

Естественно, что в системах цифровой радиосвязи по сравнению с аналоговыми системами гораздо легче обеспечить безопасность связи. Даже без принятия специальных мер по закрытию информации цифровые системы обеспечивают повышенный уровень защиты переговоров (аналоговые сканирующие приемники непригодны для прослушивания переговоров в системах цифровой радиосвязи). Кроме того, некоторые стандарты цифровой радиосвязи предусматривают возможность сквозного шифрования информации, что позволяет использовать оригинальные (т. е. разработанные самим пользователем) алгоритмы закрытия речи.

Цифровые системы транкинговой радиосвязи позволяют использовать разнообразные механизмы аутентификации абонентов: различные идентификационные ключи и SIM-карты, сложные алгоритмы аутентификации, использующие шифрование, и т. п.

4. Услуги связи. Цифровые транкинговые системы реализуют современный уровень сервисного обслуживания абонентов сетей связи, предоставляя возможности автоматической регистрации абонентов, роуминга, управления потоком данных, различных режимов приоритетного вызова, переадресации вызова и т. д.

Наряду со стандартными функциями сетевого обслуживания по заявкам правоохранительных органов в стандарты цифровой транкинговой радиосвязи часто включают требования по наличию специфических услуг связи: режиму вызова, поступающему только с санкции диспетчера системы; режиму динамической модификации групп пользователей;

режиму дистанционного включения радиостанций для акустического прослушивания обстановки и т. д.

5. Возможность взаимодействия. Цифровые системы радиосвязи, имеющие гибкую структуру адресации абонентов, предоставляют широкие возможности как для создания различных виртуальных сетей в рамках одной системы, так и для организации при необходимости взаимодействия абонентов различных сетей связи. Для служб общественной безопасности особенно актуальным является требование по обеспечению возможности взаимодействия подразделений различных ведомств для координации совместных действий при чрезвычайных ситуациях: стихийных бедствиях, террористических актах и т. п.

К наиболее популярным, заслужившим международное признание стандартам цифровой транкинговой радиосвязи, на основе которых во многих странах развернуты системы связи, относятся:

- EDACS, разработанный фирмой Ericsson;
- TETRA, разработанный Европейским институтом стандартов связи;
- APCO 25, разработанный Ассоциацией официальных представителей служб связи органов общественной безопасности;
- Tetrapol, разработанный фирмой Matra Communication (Франция);
- IDEN, разработанный фирмой Motorola (США).

Все эти стандарты отвечают современным требованиям к системам транкинговой радиосвязи. Они позволяют создавать различные конфигурации сетей связи: от простейших локальных однозоновых систем до сложных многозоновых систем регионального или национального уровня. Системы на основе данных стандартов обеспечивают различные режимы передачи речи (индивидуальная связь, групповая связь, широковещательный вызов и т. п.) и данных (коммутируемые пакеты, передача данных с коммутацией цепей, короткие сообщения и т. п.) и возможность организации связи с различными системами по стандартным интерфейсам (с цифровой сетью с интеграцией услуг, с телефонной сетью общего пользования, с учрежденческими АТС и т. д.).

Система EDACS

Одним из первых стандартов цифровой транкинговой радиосвязи был стандарт EDACS (Enhanced Digital Access Communication System), разработанный фирмой Ericsson (Швеция). Первоначально он предусматривал только аналоговую передачу речи, однако позднее была разработана специальная цифровая модификация системы EDACS Aegis.

Система EDACS работает в соответствии с закрытым фирменным протоколом, отвечающим требованиям по безопасности пользования системами транкинговой радиосвязи, которые были разработаны рядом фирм-производителей оборудования подвижной связи совместно с правоохранительными органами.

Цифровые системы EDACS выпускались на диапазоны частот 138-174 МГц, 403-423, 450-470 МГц и 806-870 МГц с разносом частот 30; 25; и 12,5 кГц.

Представьте, что Вы пришли на обычный железнодорожный вокзал за билетами. Окинув взглядом очереди желающих уехать, Вы безошибочно выбираете нужную Вам кассу. Но Вы же не знаете, сколько времени кассир будет обслуживать каждого стоящего перед Вами... И другая ситуация: вы приходите в "Экспресс-кассy". Общий принцип такого обслуживания сводится к тому, что очередь здесь всего одна, и ожидающий обслуживается первой освободившейся кассой. И как раз эта схема описывает то, как обслуживаются заявки в транкинговой связи (рис. 2.9).

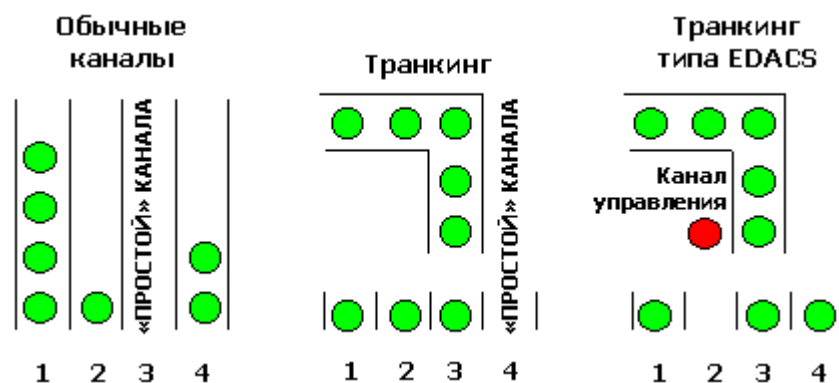


Рис. 2.9. Организация очередей

Речевое кодирование в системе производится путем компрессии импульсно-кодовой последовательности со скоростью 64 Кбит/с, полученной с помощью аналого-цифрового преобразования сигнала с тактовой частотой 8 кГц и разрядностью 8 бит. Алгоритм компрессии, реализующий метод адаптивного многоуровневого кодирования (разработка фирмы Ericsson), обеспечивает динамическую адаптацию к индивидуальным характеристикам речи абонента и формирует низкоскоростную цифровую последовательность, которая подвергается помехоустойчивому кодированию, доводящему скорость цифрового потока до 9,2 Кбит/с. Далее сформированная последовательность делится на пакеты, в каждый из которых включаются сигналы синхронизации и управления. Результирующая последовательность передается в канал связи со скоростью 9600 бит/с.

В системах EDACS применяется частотное разделение каналов связи с использованием высокоскоростного выделенного канала управления, который предназначается для обмена цифровой информацией между радиостанциями и устройствами управления работой системы. Это обеспечивает высокую оперативность связи в системе (время установления канала связи в однозоновой системе не превышает 0,25 с). Скорость передачи информации в рабочем канале как и в канале управления равна 9600 бит/с.

Основными функциями стандарта EDACS, обеспечивающими специфику служб общественной безопасности, являются различные режимы вызова (групповой, индивидуальный, экстренный, статусный), динамическое управление приоритетностью вызовов (в системе может использоваться до 8 уровней приоритета), динамическая модификация групп абонентов (перегруппировка), дистанционное выключение радиостанций (при утере или краже радиосредств).

Системы стандарта EDACS обеспечивают возможность работы радиосредств как в цифровом, так и в аналоговом режиме, что позволяет пользователям на определенном этапе использовать старый парк технических средств радиосвязи.

Одной из основных задач разработки системы было достижение высокой надежности и отказоустойчивости сетей связи на основе данного стандарта. Эта цель была достигнута, что подтверждается надежной и устойчивой работой систем связи в различных регионах мира. Высокая отказоустойчивость обеспечивается реализацией в аппаратуре системы EDACS распределенной архитектуры и заложенным принципом распределенной обработки данных. Базовая станция сети связи сохраняет работоспособность даже в случае отказа всех ретрансляторов, кроме одного. Последний работоспособный ретранслятор в этом случае в исходном состоянии работает как ретранслятор канала управления, при поступлении вызовов обрабатывает их, назначая свой собственный частотный канал, после чего переходит в режим ретранслятора рабочего канала. При выходе из строя контроллера базовой станции система переходит в аварийный режим, при котором теряются некоторые функции сети, однако сохраняется частичная работоспособность (ретрансляторы работают автономно).

В системе EDACS возможно сквозное шифрование информации, однако в связи с закрытым протоколом приходится применять либо стандартный алгоритм защиты,

предлагаемый фирмой Ericsson, либо согласовывать с ней возможность использования собственных программно-аппаратных модулей, реализующих оригинальные алгоритмы, которые должны быть совместимы с системным протоколом EDACS.

На сегодняшний день в мире развернуто большое количество сетей стандарта EDACS, в числе которых есть многозоновые сети связи, используемые службами общественной безопасности различных стран. В России функционирует около десяти сетей данного стандарта, наиболее крупной является сеть связи в г. Москве, включающая 9 базовых станций. Вместе с тем, в настоящее время фирма Ericsson не проводит работ по совершенствованию системы EDACS, прекратила поставки оборудования для развертывания новых сетей данного стандарта и только поддерживает функционирование действующих сетей.

Система TETRA

TETRA представляет собой стандарт цифровой транкинговой радиосвязи, состоящий из ряда спецификаций, разработанных Европейским институтом телекоммуникационных стандартов ETSI (European Telecommunications Standards Institute). Стандарт TETRA создавался как единый общеевропейский цифровой стандарт. Поэтому до апреля 1997 г. аббревиатура TETRA означала Трансьевропейское транкинговое радио (Trans-European Trunked RAdio). Однако в связи с большим интересом, проявленным к стандарту в других регионах, территория его действия не ограничивается только Европой. В настоящее время TETRA расшифровывается как Наземное транкинговое радио (TErrestrial Trunked RAdio).

TETRA - открытый стандарт, т. е. предполагается, что оборудование различных производителей будет совместимо. Доступ к спецификациям TETRA свободен для всех заинтересованных сторон, вступивших в ассоциацию «Меморандум о взаимопонимании и содействии стандарту TETRA» (MoU TETRA). Ассоциация, в которую в конце 2001 г. входило более 80 участников, объединяет разработчиков, производителей, испытательные лаборатории и пользователей различных стран.

Стандарт TETRA состоит из двух частей: TETRA V+D (TETRA Voice+Data) - стандарта на интегрированную систему передачи речи и данных, и TETRA PDO (TETRA Packet Data Optimized) - стандарта, описывающего специальный вариант транкинговой системы, ориентированный только на передачу данных.

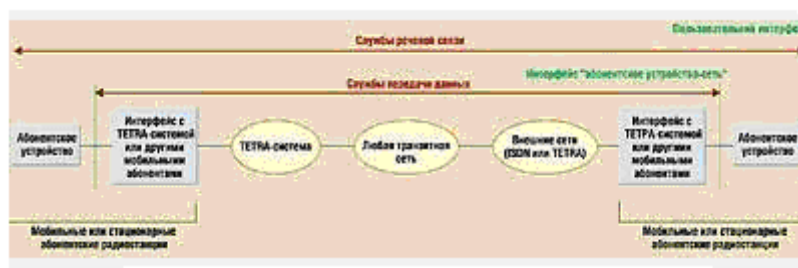


Рис. 2.10. Структура служб системы TETRA

В стандарт TETRA входят спецификации беспроводного интерфейса, интерфейсов между сетью TETRA и цифровой сетью с интеграцией услуг (ISDN), телефонной сетью общего пользования, сетью передачи данных, учрежденческими АТС и т. п. В стандарт включено описание всех основных и дополнительных услуг, предоставляемых сетями TETRA. Специфицированы также интерфейсы локального и внешнего централизованного управления сетью.

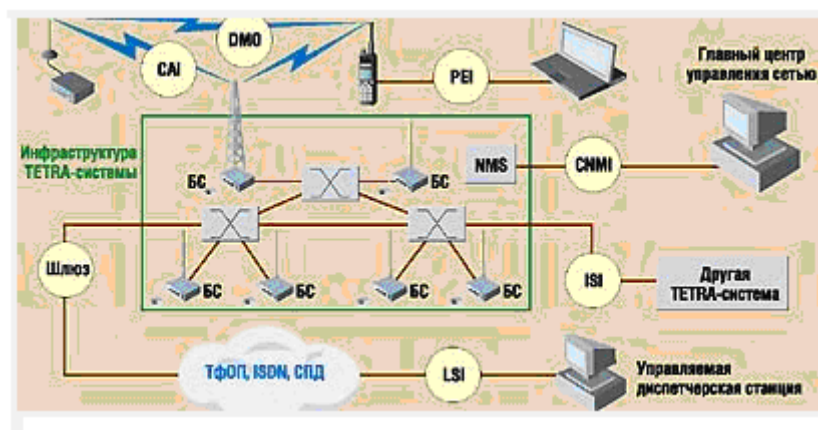


Рис. 2.11. Стандартные интерфейсы TETRA-систем

Радиоинтерфейс стандарта TETRA предполагает работу в стандартной сетке частот с шагом 25 кГц. Необходимый минимальный дуплексный разнос радиоканалов - 10 МГц. Для систем стандарта TETRA могут использоваться некоторые поддиапазоны частот. В странах Европы за службами безопасности закреплены диапазоны 380-385/390-395 МГц, а для коммерческих организаций предусмотрены диапазоны 410-430/450-470 МГц. В Азии для систем TETRA используется диапазон 806-870 МГц.

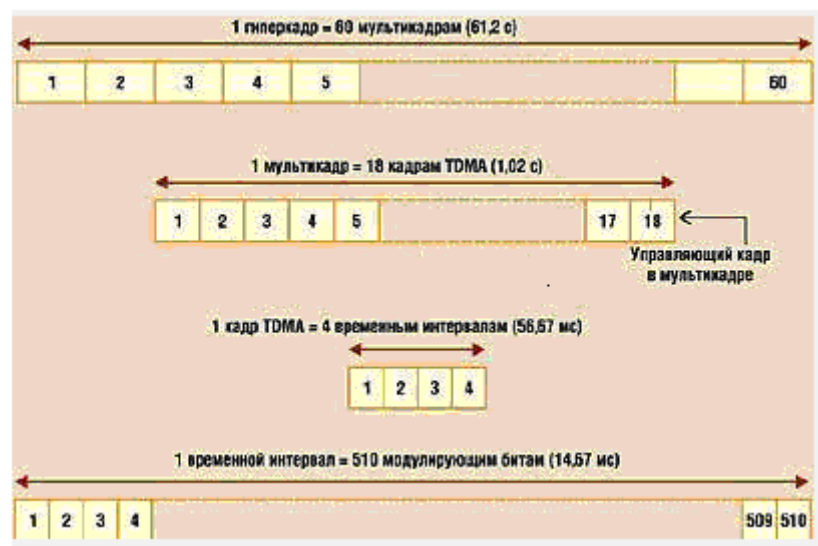


Рис. 2.12. Структура кадра TETRA

В системах стандарта TETRA V+D используется метод многостанционного доступа с временным разделением (МДВР) каналов связи. На одной физической частоте может быть организовано до 4 независимых информационных каналов.

Сообщения передаются мультикадрами длительностью 1,02 с. Мультикадр содержит 18 кадров, один из которых является контрольным. Кадр имеет длительность 56,67 мс и содержит 4 временных интервала (time slots). В каждом из временных интервалов передается информация своего временного канала. Временной интервал имеет длину 510 бит, из которых 432 являются информационными (2 блока по 216 бит).

Пропускная способность одного информационного канала составляет 7,2 Кбит/с, а скорость цифрового информационного потока данных - 28,8 Кбит/с. (При этом общая скорость передачи символов в радиоканале за счет дополнительной служебной информации и контрольного кадра в мультикадре соответствует скорости модуляции и равна 36 Кбит/с.)

Системы стандарта TETRA могут функционировать в следующих режимах:

- транкинговой связи;
- с открытым каналом;

- непосредственной связи.

В режиме транкинговой связи обслуживаемая территория перекрывается зонами действия базовых приемопередающих станций. Стандарт TETRA позволяет как использовать в системах только распределенный канал управления, так и организовывать его сочетание с выделенным частотным каналом управления. При работе сети с распределенным каналом управления служебная информация передается либо только в контрольном кадре мультикадра (одном из 18), либо еще в специально выделенном временном канале (одном из 4-х каналов, организуемых на одной частоте). В дополнение к распределенному каналу связи может использоваться выделенный частотный канал управления, специально предназначенный для обмена служебной информацией (при этом реализуются максимальные услуги связи).

В режиме с открытым каналом группа пользователей имеет возможность устанавливать соединение «один пункт - несколько пунктов» без какой-либо установочной процедуры. Любой абонент, присоединившись к группе, может в любой момент использовать этот канал. В режиме с открытым каналом радиостанции работают в двухчастотном симплексе.

В режиме непосредственной (прямой) связи между терминалами устанавливаются двух- и многоточечные соединения по радиоканалам, не связанным с каналом управления сетью, без передачи сигналов через базовые приемопередающие станции.

Для увеличения зон обслуживания в стандарте TETRA предусматривается возможность использования абонентских радиостанций в качестве ретрансляторов.

TETRA предоставляет пользователям ряд услуг, которые включены в стандарт по заявке Ассоциации европейской полиции (Schengen Group), сотрудничающей с техническим комитетом ETSI:

- вызов, санкционированный диспетчером (режим, при котором вызовы поступают только с санкции диспетчера);
- приоритетный доступ (в случае перегруженности сети доступные ресурсы присваиваются в соответствии со схемой приоритетов);
- приоритетный вызов (присвоение вызовов в соответствии со схемой приоритетов);
- приоритетное прерывание обслуживания вызовов (прерывание обслуживания вызовов с низким приоритетом, если ресурсы системы исчерпаны);
- избирательное прослушивание (перехват поступающего вызова без влияния на работу других абонентов);
- дистанционное прослушивание (дистанционное включение абонентской радиостанции на передачу для прослушивания обстановки у абонента);
- динамическая перегруппировка (динамическое создание, модификация и удаление групп пользователей);
- идентификация вызывающей стороны.

Средства защиты радиоинтерфейса стандарта TETRA включают механизмы аутентификации абонента и инфраструктуры, обеспечения конфиденциальности трафика за счет потока псевдоимен и специфицированного шифрования информации. Определенная дополнительная защита информации обеспечивается возможностью переключения информационных каналов и каналов управления в процессе ведения сеанса связи.

Следует также отметить, что в стандарте TETRA в связи с использованием метода временного разделения каналов (МДВР) связи во всех абонентских терминалах имеется возможность организации связи в режиме полного дуплекса.

Сети TETRA развернуты в Европе, Северной и Южной Америке, Китае, Юго-Восточной Азии, Австралии, Африке.

В настоящее время завершается разработка второй стадии стандарта (TETRA Release 2 (R2)), направленной на интеграцию с мобильными сетями 3-го поколения, кардинальное увеличение скорости передачи данных, переход от специализированных SIM-карт к универсальным, дальнейшее увеличение эффективности сетей связи и расширение возможных зон обслуживания.

В России оборудование TETRA предлагается рядом компаний – системных интеграторов. Реализовано несколько пилотных проектов сетей TETRA. Под эгидой Минсвязи проводится разработка системного проекта «Федеральная сеть подвижной радиосвязи TETRA», получившего название «Тетрарус». В 2001 г. был создан Российский TETRA Форум, в задачи которого входят продвижение технологии TETRA в России, организация обмена информацией, содействие развитию национального производства, участие в работе по гармонизации радиочастотного спектра и т. д. В соответствии с решением ГКЭС от 02.07.2003 г. использование стандарта TETRA признано перспективным «...в целях обеспечения связью органов государственного управления всех уровней, обороны, безопасности, охраны правопорядка, потребностей ведомств и крупных корпораций».

Система APCO 25

Стандарт APCO 25 разработан Ассоциацией официальных представителей служб связи органов общественной безопасности (Association of Public safety Communications Officials-international – APCO), которая объединяет пользователей систем связи, работающих в службах общественной безопасности. APCO является международной организацией и объединяет представителей правоохранительных органов около 70 стран. Штаб-квартира APCO находится в городе Южная Дейтона (штат Флорида, США), кроме этого, эта организация имеет представительства в Канаде, Карибском регионе и в Австралии.

Первые спецификации стандартов транкинговой радиосвязи, на основе которых были созданы системы EDACS (Ericsson), SmartNet (Motorola), LTR (E.F.Johnson), были разработаны APCO еще в конце 70-х годов. Однако эти спецификации не позволяли обеспечить совместимость и возможность взаимодействия различных систем, что послужило причиной начала нового проекта по разработке стандарта цифровой транкинговой радиосвязи, получившего название APCO 25.

Работы по созданию стандарта были начаты в конце 1989 г., а последние документы по установлению стандарта были утверждены и подписаны в августе 1995 г. на международной конференции и выставке APCO в Детройте. В настоящее время стандарт включает все основные документы, определяющие принципы построения радиointерфейса и других системных интерфейсов, протоколы шифрования, методы речевого кодирования и т.д.

В 1996 г. было принято решение о разделении всех спецификаций стандарта на два этапа реализации, которые были обозначены как Фаза I и Фаза II. В середине 1998 г. были сформулированы функциональные и технические требования к каждой из фаз стандарта, подчеркивающие новые возможности Фазы II и ее отличия от Фазы I.

Основополагающими принципами разработки стандарта APCO 25, сформулированными его разработчиками, были требования:

- по обеспечению плавного перехода к средствам цифровой радиосвязи (т.е. возможности совместной работы на начальном этапе базовых станций стандарта с абонентскими аналоговыми радиостанциями, используемыми в настоящее время);
- по созданию открытой системной архитектуры для стимулирования конкуренции среди производителей оборудования;
- по обеспечению возможности взаимодействия различных подразделений служб общественной безопасности при проведении совместных мероприятий.

Если стандарты TETRA и Tetrapol не поддерживают работу в своих системах аналоговых станций, то стандарт APCO 25 специально ориентирован на совместную работу цифровых и аналоговых радиосредств. При этом разработчики стандарта декларируют, что системы на основе APCO 25 позволяют, с одной стороны, жестко разграничить используемые частотные ресурсы (на аналоговые и цифровые), а с другой стороны – допускают и гибкое

конфигурирование каналов, т.е. совместное использование общего частотного ресурса цифровыми и аналоговыми абонентскими станциями.

В том случае, если указанная возможность действительно удобно реализуется на практике (причем не только для систем производства компании Motorola), то она обеспечит серьезное преимущество APCO 25 перед другими стандартами, т.к. позволит производить плавный переход к цифровой радиосвязи путем поэтапного переоснащения подразделений служб общественной безопасности цифровыми радиостанциями. В особенности это актуально для России, где правоохранительные органы и службы общественной безопасности пока еще используют достаточно большой парк устаревших аналоговых радиосредств.

Системная архитектура стандарта поддерживает как транкинговые, так и обычные (конвенциональные) системы радиосвязи, в которых абоненты взаимодействуют между собой либо в режиме непосредственной связи, либо через ретранслятор. Основным функциональным блоком системы стандарта APCO 25 является радиоподсистема, определяемая как сеть связи, которая строится на основе одной или нескольких базовых станций. При этом каждая базовая станция должна поддерживать Общий радиointерфейс (CAI - Common Radio Interface) и другие стандартизованные интерфейсы (межсистемный, с ТФОП, с портом передачи данных, с сетью передачи данных и сетевым управлением). При транкинговой системе используется выделенный канал управления.

Сильной стороной стандарта APCO 25 является то, что он предусматривает возможность работы в любом из стандартных диапазонов частот используемых системами подвижной радиосвязи: 138 – 174, 406 – 512 или 746 – 869 МГц.

Основной метод доступа к каналам связи – частотный (МДЧР), вместе с тем по заявке фирмы Ericsson в Фазу II включена возможность использования в системах стандарта APCO 25 множественного доступа с временным разделением каналов (МДВР).

В Фазе I стандартный шаг сетки частот составляет 12,5 кГц, для Фазы II - 6,25 кГц. При этом при полосе 12,5 кГц осуществляется четырехпозиционная частотная модуляция по методу S4FM со скоростью 4800 символов в секунду, а при полосе 6,25 кГц – четырехпозиционная фазовая модуляция со сглаживанием фазы по методу CQPSK. Сочетание указанных методов модуляции позволяет использовать на разных Фазах одинаковые приемники, дополняемые различными усилителями мощности (для Фазы I - простые усилители с высоким КПД, для Фазы II - усилители с высокой линейностью и ограниченной шириной излучаемого спектра). При этом демодулятор может осуществлять обработку сигналов по любому из методов.

Для речевого кодирования в стандарте используется кодек IMBE (Improved MultiBand Excitation), который применяется также в системе спутниковой связи Inmarsat. Скорость кодирования – 4400 бит/с. После помехоустойчивого кодирования речевой информации скорость информационного потока увеличивается до 7200 бит/с, а после формирования речевых кадров путем добавления служебной информации – до 9600 бит/с.

Речевая информация в радиоканале передается кадрами по 180 мс, которые носят название логических блоков данных (LDU – Logical Data Unit). Группа из 2 кадров образует суперкадр длительностью 360 мс. Любая передача речевой информации предваряется преамбулой, имеющей продолжительность 82,5 мс, а заканчивается маркером конца сообщения (сигналом отбоя). Структура речевого сообщения показана на рис.2.13.

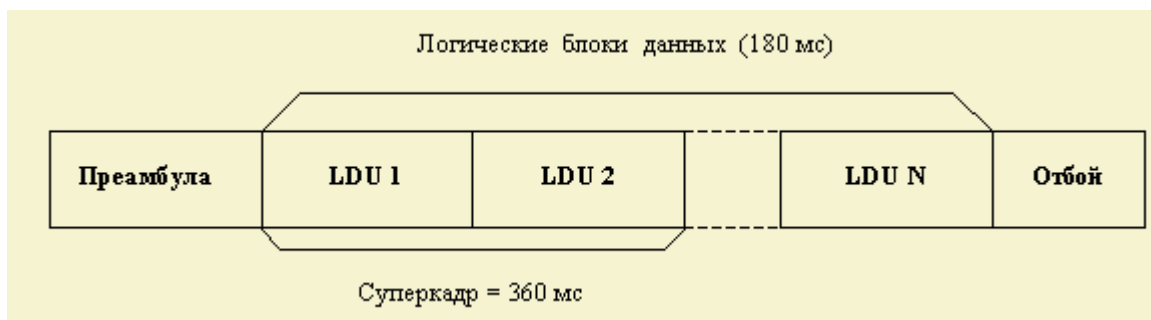


Рис. 2.13. Структура речевого сообщения в стандарте APCO 25

Речевая преамбула предназначена для начальной синхронизации передающей и приемной радиостанции, инициализации всех функций шифрования и передачи адресной информации. Основу преамбулы составляет кодовое слово заголовка, в которое входят:

- индикатор сообщения (MI – Message Indicator), характеризующий начальные условия для алгоритма шифрования (72 бита);
- идентификатор изготовителя (8 бит);
- идентификатор типа используемого алгоритма шифрования (8 бит);
- идентификатор ключа шифрования (16 бит);
- идентификатор разговорной группы (16 бит).

Кодовое слово длиной 120 бит подвергается помехоустойчивому кодированию с помощью кодов Рида-Соломона и Голея, в результате чего его размерность увеличивается до 648 бит. После этого, в начало преамбулы помещается:

- начальный синхропакет (FS – Frame Synchronization) длиной 48 бит;
- идентификатор сети (NID – Network Identifier), передаваемый для предотвращения конфликтов между радиостанциями различных сетей, работающими на одной частоте (64 бита), а в конец – 10 нулевых бит.

Окончательное формирование структуры преамбулы производится путем вставки 2 бит статусной информации после каждых 70 бит пакета данных преамбулы (770 бит), получившегося после добавления синхропакета, идентификатора сети и нулевых бит (всего добавляется 22 статусных бита). Окончательная длина преамбулы составляет 792 бита, так что при скорости информации в канале 9600 бит/с передача преамбулы производится в течение 82,5 мс.

Каждый логический блок данных состоит из 9 речевых фреймов длиной 144 бита, образованных 88 информационными битами, полученными преобразованием с помощью кодека IMBE 20 мс отрезка речевого сигнала, и 56 битами корректирующего кода контроля четности. Кроме этого, в состав LDU входят дополнительные служебные сообщения. В первом логическом блоке суперкадра передается информация управления связью (LC – Link Control), состоящая 72 битов информации и 168 бит корректирующего кода) и информация низкоскоростного канала сигнализации (LSD – Low Speed Data), включающая 16 бит данных и 16 бит корректирующего кода. Второй логический блок суперкадра также содержит информацию низкоскоростного канала сигнализации LSD, и кроме этого, информацию алгоритма шифрования (ES – Encryption Sync), включающую 96 информационных бит и 144 бит корректирующего кода. Структура суперкадра речевой информации показана на рис.2.14.



Рис. 2.14. Структура речевого суперкадра в стандарте APCO 25

Информация управления каналом связи включает индикатор сообщения, идентификатор производителя, признак экстренного вызова, резервное поле, идентификаторы разговорной группы (для индивидуального вызова – вызываемого абонента) и передающего абонента. Встроенные в общий информационный поток кадры управления каналом связи позволяют повысить надежность связи за счет возможности восстановления соединения после кратковременного разрушения канала связи.

Информация алгоритма шифрования содержит индикатор сообщения, идентификатор типа используемого алгоритма шифрования и идентификатор ключа шифрования.

Канал низкоскоростной сигнализации может быть использован для различных применений, в частности для передачи сигналов местоположения подвижных объектов. Заложенная в стандарте APCO 25 система идентификации абонентов позволяет адресовать в одной сети не менее 2 миллионов радиостанций и до 65 тысяч групп. При этом задержка при установлении канала связи в подсистеме, в соответствии с функциональными и техническими требованиями к стандарту APCO 25, не должна превышать 500 мс (в режиме прямой связи – 250 мс, при связи через ретранслятор 0 350 мс).

В системах стандарта APCO 25 предусмотрены 2 варианта *передачи данных*: с подтверждением приема и без подтверждения. При передаче данных для исправления ошибок используется избыточное решетчатое кодирование и межблочное перемежение.

Исходные массивы данных разбиваются на фрагменты длиной не более 512 байт. При передаче с подтверждением приема фрагменты делят на блоки по 16 байт, при этом каждый блок имеет свой номер для возможности повтора. При передаче без подтверждения приема блоки, на которые разбиваются фрагменты массивов данных, содержат 12 байт.

Передача каждого пакета данных начинается с преамбулы, содержащей синхропакет, номер фрагмента, количество блоков в пакете, а также идентификаторы сети, производителя, точки доступа и логический идентификатор связи.

Данные передаются по тем же каналам, что и речевые сообщения, и с той же скоростью 9600 бит/с. Радиосистемы стандарта APCO 25 обеспечивают связь с сетями фиксированной связи с протоколами X.25, SNA, TCP/IP. Следует отметить, что протокол IP поддерживается как специальная IP-служба, которая с помощью специального сетевого шлюза обеспечивает возможность связи мобильных терминалов и проводной инфраструктуры с приложениями, использующими IP.

Разработчики стандарта при рассмотрении модели гипотетического противника выделили следующие угрозы безопасности связи: перехват сообщений, повтор сообщений с задержкой и с искажением информации, создание преднамеренной помехи, анализ трафика абонентов, создание дубликатов абонентов, внедрение противника в качестве легитимного пользователя

системы. Противодействие большинству этих угроз в стандарте APCO 25 обеспечивается с помощью 3-х основных механизмов:

- **конфиденциальности** связи, т.е. защиты информации от любых видов несанкционированного доступа;
- **аутентификации** абонентов и сообщений;
- **системы управления ключевой информацией.**

В основе всех указанных механизмов обеспечения безопасности связи лежит криптографическое шифрование информации. Системы APCO 25, в соответствии с функциональными и техническими требованиями, должны быть рассчитаны на обеспечение, как минимум, двух из 4-х уровней криптозащиты в зависимости от типа системы связи:

Тип 1 – связь с гарантированным засекречиванием информации на уровне национального правительства;

Тип 2 – несекретная связь национального уровня, требующая защиты коммуникаций;

Тип 3 – несекретная правительственная связь, требующая ограничений по доступу;

Тип 4 – для коммерческих и других применений (включая экспортируемые модификации систем).

Общая модель криптопреобразования (шифрования/дешифрования) информации в системе связи представлена на рис.2.15.

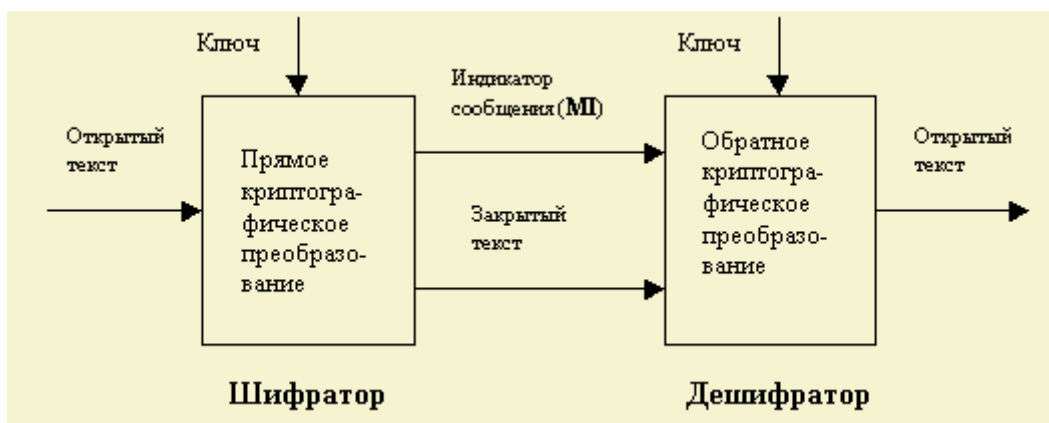


Рис. 2.15. Модель криптопреобразования информации в стандарте APCO 25

На передающей стороне открытый текст сообщения поступает на шифратор, где на основе ключа и определенного криптографического алгоритма преобразуется в шифрованный текст той же длины, после чего передается по радиоканалу. Вместе с шифрованным текстом передается индикатор сообщения MI, который предназначен для синхронизации работы шифратора и дешифратора. На приемной стороне после выполнения процедуры синхронизации с помощью аналогичных криптоалгоритмов и криптографического ключа шифрованный текст преобразуется в открытый.

В различных режимах используются различные модификации общей модели криптозащиты информации, показанные на рис.2.16.:

а) ECB – Electronic Code Book;

б) OFB – Output Feed Back;

в) CFB – Cipher Feed Back.

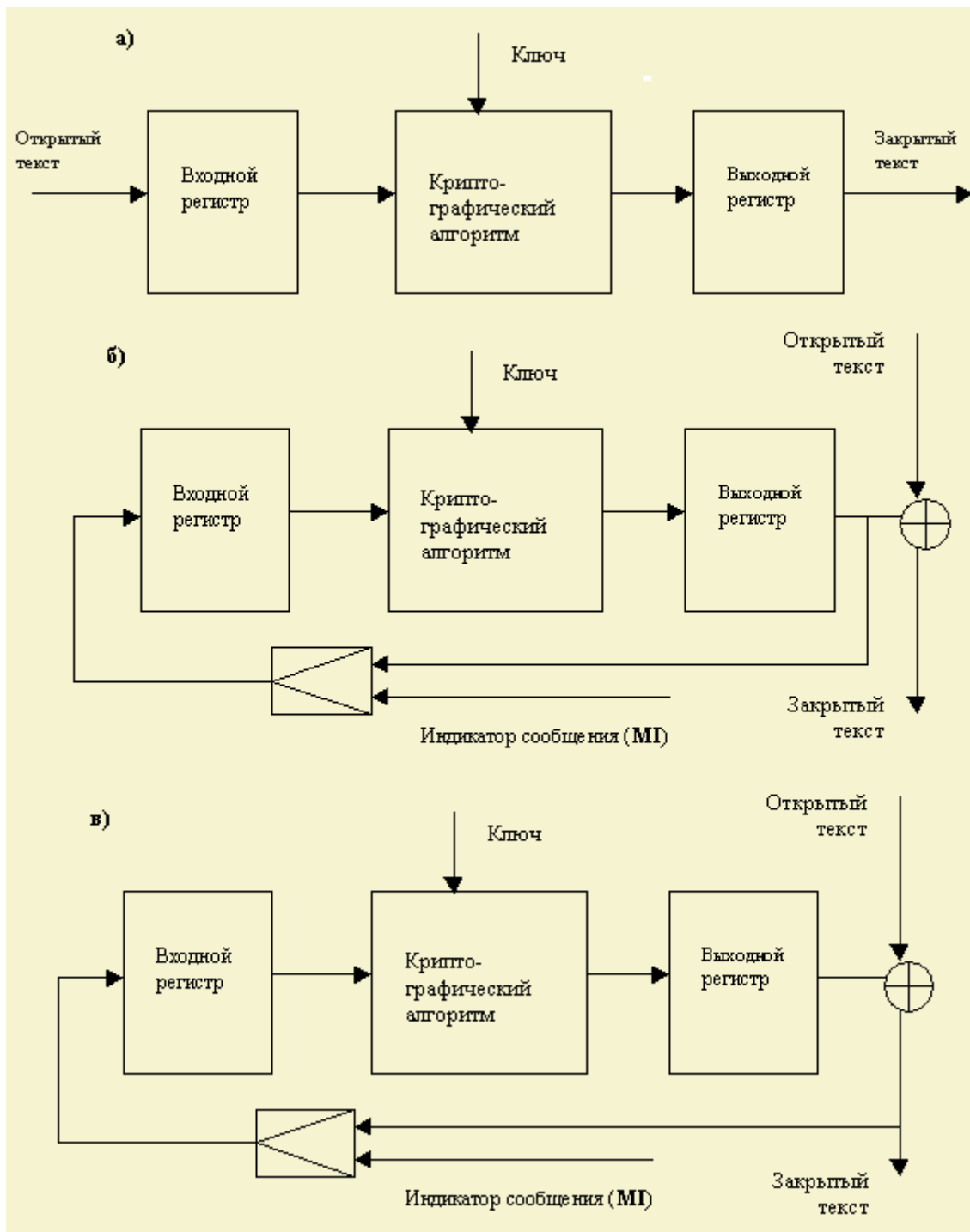


Рис. 2.16. Разновидности криптографических преобразований информации

Конфиденциальность связи достигается шифрованием трафика речи и данных, которое осуществляется по методу OFB (рис. 2.16б).

Аутентификация, предназначенная для удостоверения подлинности сообщений и абонентов, а также обеспечения секретности абонентов (т.е. защиты сведений о том, кому адресовано и от кого исходит передаваемое сообщение), осуществляется путем передачи номеров сообщений, которые подвергаются шифрации по варианту OFB (рис. 2.16б) и добавления к сообщению специального аутентификационного кода (MAC – Message Authentication Code), который генерируется по варианту CFB (рис. 2.16в). Код номера сообщения и его идентификационный код носят временный характер и изменяются от сообщения к сообщению.

Система управления ключевой информацией предназначена для генерации, хранения, ввода, распределения, архивирования и удаления криптографических ключей. Ввод ключей в абонентское оборудование производится с помощью специальной аппаратуры КМФ (Key Management Facility). Кроме этого, в системах стандарта APCO 25 стандартизован специальный режим распространения ключей по радиоканалу OTAR (Over-the-air-rekeying). Информация о ключах, пересылаемых по радиоканалу защищается по варианту ECB (рис.4а).

Несмотря на то, что APCO является международной организацией, представительства которой находятся в ряде регионов, основную роль в продвижении этого стандарта играют американские фирмы, поддерживаемые правительством США. К числу участников общественного сектора Ассоциации относятся ФБР, Министерство обороны США, Федеральный комитет связи, полиции ряда штатов США, Секретная служба и многие другие государственные организации. В качестве производителей оборудования стандарта APCO 25 уже заявили себя такие ведущие фирмы, как Motorola (основной разработчик стандарта), E.F.Johnson, Transcrypt, Stanlite Electronics и др. Фирма Motorola уже представила свою первую систему, основанную на стандарте APCO 25, имеющую название ASTRO.

В составе сетей радиосвязи ASTRO может использоваться широкий набор абонентского оборудования, удовлетворяющего запросам различных пользователей.

Первые полнофункциональные цифровые портативные радиостанции, выпущенные компанией Motorola, получили название **ASTRO Saber**. Они могут работать как в цифровом, так и в аналоговом режиме в конвенциональных и транкинговых сетях радиосвязи в любом из диапазонов частот, выделенных для систем сухопутной подвижной связи (138-174, 406-512, 746-869 МГц). Шаг сетки частот может иметь значения – 12,5; 25 и 30 кГц. Выпускаются различные модификации станций, отличающиеся друг от друга числом рабочих каналов, вариантами реализации органов управления и индикации, а также некоторыми функциональными возможностями.

Новейшая разработка компании Motorola – **семейство портативных радиостанций XTS 3000**. Эти радиостанции поддерживают тот же набор функций, что ASTRO Saber, но выполнены в другом конструктиве и имеют меньшие габариты и вес. Благодаря унификации конструктивных решений с серией станций MTS 2000, работающих в системе SmartNet, станции XTS 3000 могут использовать те же аксессуары: головные телефоны, гарнитуру скрытного ношения, выносные микрофон и динамик, зарядное устройство, антенны.

Мобильные радиостанции ASTRO Spectra выпускаются в двух модификациях: для автомашин и мотоциклов. Motorola предлагает пять вариантов исполнения станций, отличающихся некоторыми функциональными возможностями, числом рабочих каналов и размерами индикационного табло.

В качестве стационарной радиостанции в системе используется станция **ASTRO CONSOLETTE**. Кроме поддержки протокола стандарта APCO 25, стационарная радиостанция может работать с аналоговыми системами сигнализации MDC-1200 и PL/PDL. Станция ASTRO CONSOLETTE имеет два варианта исполнения: для местного и дистанционного управления по телефонной линии.

Для организации передачи данных компания Motorola выпускает **беспроводной портативный терминал передачи данных FORTE**. Он представляет карманный персональный компьютер с сенсорным дисплеем и пером, оснащенный средствами для поддержания радиосвязи.

Пока в России системы стандарта APCO 25 не развернуты, однако специалисты проявляют большой интерес к данному стандарту, привлекательность которого заключается в его преимуществах по отношению к существующим аналоговым системам радиосвязи, большом количестве производителей оборудования и возможности построения сетей связи во всех стандартных диапазонах частот. Активную политику продвижения систем данного стандарта в России проводят представительства фирм Motorola и ADI Limited (Австралия).

Система Tetrapol

Работы по созданию стандарта цифровой транкинговой радиосвязи Tetrapol были начаты в 1987 г., когда фирма Matra Communications заключила контракт с французской жандармерией на разработку и ввод в эксплуатацию сети цифровой радиосвязи Rubis. Сеть связи была введена в эксплуатацию в 1994 г. По данным фирмы Matra на сегодняшний день сеть французской жандармерии охватывает более половины территории Франции и обслуживает более 15 тыс. абонентов. В том же 1994 г. фирма Matra создала свой форум Tetrapol, под эгидой которого были разработаны спецификации Tetrapol PAS (Publicly Available Specifications), определяющие стандарт цифровой транкинговой радиосвязи.

Стандарт Tetrapol описывает цифровую транкинговую систему радиосвязи с выделенным каналом управления и частотным методом разделения каналов связи. Стандарт позволяет создавать как однозоновые, так и многозоновые сети связи различной конфигурации, обеспечивая также возможность прямой связи между подвижными абонентами без использования инфраструктуры сети и ретрансляции сигналов на фиксированных каналах.

Системы связи стандарта Tetrapol имеют возможность работы в диапазоне частот от 70 до 520 МГц, который в соответствии со стандартом определяется как совокупность двух поддиапазонов: ниже 150 МГц (VHF) и выше 150 МГц (UHF). Большая часть радиointерфейсов для систем этих поддиапазонов является общей, различие заключается в использовании различных методов помехоустойчивого кодирования и кодового перемежения. В поддиапазоне UHF рекомендуемый дуплексный разнос каналов приема и передачи составляет 10 МГц.

Частотный разнос между соседними каналами связи может составлять 12,5 или 10 кГц. В дальнейшем предполагается переход к разносу между каналами в 6,25 кГц. В системах стандарта Tetrapol поддерживается ширина полосы до 5 МГц, что обеспечивает возможность использования в сети 400 (при разносе 12,5 кГц) или 500 (при разносе 10 кГц) радиоканалов. При этом в каждой зоне может использоваться от 1 до 24 каналов.

В стандарте определяются три основных режима связи: транкинговый, режим прямой связи и режим ретрансляции.

В сетевом режиме (или режиме транкинговой связи) взаимодействие абонентов осуществляется с помощью базовых станций (БС), которые распределяют каналы связи между абонентами. При этом сигналы управления передаются на отдельном, специально выделенном для каждой БС частотном канале. В режиме прямой связи обмен информацией между подвижными абонентами производится напрямую без участия базовой станции. В режиме ретрансляции связь между абонентами осуществляется через ретранслятор, который имеет фиксированные каналы передачи и приема информации.

В системах стандарта Tetrapol поддерживается 2 основных вида информационного обмена: передача речи и передача данных.

Службы речевой связи позволяют осуществлять следующие виды вызовов: широковещательный вызов, вызов установки открытого канала, групповой вызов, индивидуальный вызов, множественный вызов с использованием списка абонентов, аварийный вызов.

Службы передачи данных предоставляют ряд услуг прикладного уровня, поддерживаемых заложенными в радиотерминалах функциями, таких как межабонентский обмен сообщениями в соответствии с протоколом X.400, доступ к централизованным базам данных, доступ к фиксированным сетям в соответствии с протоколом TCP/IP, передача факсимильных сообщений, пересылка файлов, передача сигналов персонального вызова, передача коротких сообщений, передача статусных вызовов, поддержка режима передачи получаемых с помощью приемников GPS данных о местоположении объекта, передача видеоизображений.

В стандарте Tetrapol предусмотрены стандартные сетевые процедуры, обеспечивающие современный уровень обслуживания абонентов: динамическая перегруппировка, аутентификация абонента, роуминг, приоритетный вызов, управление передатчиком абонента, управление «профилем» абонента (дистанционное изменение параметров абонентского радиотерминала, заложенных в него при программировании) и др.

В связи с тем, что с самого начала стандарт Tetrapol был ориентирован на обеспечение требований правоохранительных органов, в нем предусмотрены различные механизмы обеспечения безопасности связи, направленные на предотвращение таких угроз, как несанкционированный доступ в систему, прослушивание ведущихся переговоров, создание преднамеренных помех, анализ трафика конкретных абонентов и т. п. К числу таких механизмов относятся:

- автоматическая реконфигурация сети (периодическое перераспределение ресурсов сети связи (изменение конфигурации) за счет установки и отмены открытых каналов, динамической перегруппировки, переназначения каналов связи диспетчером сети и т. п.);
- управление доступом в систему (контроль доступа к оборудованию сети связи посредством смарт-карт и системы паролей);
- сквозное шифрование информации (обеспечение возможности защиты передаваемой информации в любой точке линии связи между абонентами);
- аутентификация абонентов (автоматическое или проводимое по запросу диспетчера сети удостоверение подлинности абонентов);
- использование временных идентификаторов абонентов (замена уникальных идентификационных номеров абонентов на псевдонимы, сменяемые при каждом новом сеансе связи);
- имитация активности радиоабонентов (режим поддержки постоянного трафика при перерыве в ведении переговоров путем посылки БС по каналам связи сигналов, которые трудно отличить от информационных);
- дистанционное отключение радиотерминала (возможность отключения абонентского радиотерминала диспетчером сети);
- распространение ключей по радиоканалу (возможность передачи диспетчером сети секретных ключей абонентам по радиоканалу).

Системы стандарта Tetrapol широко используются во Франции. Видимо, не без поддержки правительством отечественного производителя, кроме сети связи Rubis национальной жандармерии, системы Tetrapol эксплуатируются французской полицией (система Ascropole) и службой железных дорог (система Iris).

Стандарт Tetrapol пользуется популярностью и в некоторых других странах Европы. На основе данного стандарта развернуты сети связи полиции Мадрида и Каталонии, подразделений безопасности Чешской Республики, службы аэропорта во Франкфурте. Специальная сеть связи Matracom 9600 разворачивается в интересах Берлинского транспортного предприятия. Радиостанции сети связи будут установлены на более чем 2000 автобусах предприятия. Кроме радиосвязи, в сети задействуется функция определения местоположения транспортных средств.

В 1997 г. фирма Matra Communications выиграла тендер по созданию системы цифровой радиосвязи для королевской тайландской полиции. Контракт является частью заказа по модернизации полицейской радиосети, которая объединит 70 полицейских участков. Предполагается использование самых современных возможностей системы, включая доступ к централизованной базе данных, электронную почту, сквозное шифрование информации, местоопределение. Имеются также сведения о развертывании нескольких систем в двух других странах юго-восточной Азии, а также в интересах полиции Мехико.

В нашей стране системы стандарта Tetrapol пока не используются. В настоящее время ФАПСИ предполагает развертывание в России опытного района транкинговой радиосвязи данного стандарта.

Система IDEN

Технология IDEN (Integrated Digital Enhanced Network) была разработана компанией Motorola в начале 90-х годов. Первая коммерческая система на базе этой технологии была развернута в США компанией NEXTEL в 1994 г.

С точки зрения статуса стандарта IDEN можно охарактеризовать как корпоративный стандарт с открытой архитектурой. Это означает, что компания Motorola, сохраняя за собой все

права по модификации системного протокола, предоставляет вместе с тем лицензии на производство компонентов системы различным производителям.

Данный стандарт разрабатывался для реализации интегрированных систем, обеспечивающих все виды подвижной радиосвязи: диспетчерской связи, мобильной телефонной связи, передачи текстовых сообщений и пакетов данных. Технология IDEN ориентирована на создание корпоративных сетей крупных организаций или коммерческих систем, предоставляющих услуги как организациям, так и частным лицам.

При реализации диспетчерских сетей подвижной радиосвязи IDEN предоставляет возможности группового и индивидуального вызова, а также режима сигнализации вызова, при котором в случае недоступности абонента вызов запоминается в системе, а затем передается абоненту, когда тот становится доступным. Число возможных групп в IDEN составляет 65535. Время установления связи при групповом вызове в полудуплексном режиме не превышает 0,5 с.

Системы IDEN предоставляют возможности организации телефонной связи по любым направлениям: мобильный абонент – мобильный абонент, мобильный абонент – абонент ТФОП. Телефонная связь полностью дуплексная.

Абоненты систем IDEN имеют возможность передавать и получать на свои терминалы текстовые сообщения, а также передавать данные (в коммутационном режиме со скоростью 9,6 Кбит/с, а в пакетном – до 32 Кбит/с), что обеспечивает возможность организации факсимильной связи и электронной почты, а также взаимодействия с фиксированными сетями, в частности с Internet. Пакетный режим передачи данных поддерживает протокол TCP/IP.

Система IDEN выполнена на базе технологии МДВР. В каждом частотном канале шириной 25 кГц передается 6 речевых каналов. Это достигается путем разбиения кадра длительностью 90 мс на временные интервалы по 15 мс, в каждом из которых передается информация своего канала.

В стандарте используется стандартный для Америки и Азии частотный диапазон 805-821/855-866 МГц. IDEN имеет самую высокую спектральную эффективность среди рассматриваемых стандартов цифровой транкинговой связи, он позволяет разместить в 1 МГц до 240 информационных каналов. Вместе с тем, размеры зон покрытия базовых станций (ячеек) в системах IDEN меньше, чем в системах других стандартов, что объясняется малой мощностью абонентских терминалов (0,6 Вт – для портативных станций и 3 Вт – для мобильных).

Первая коммерческая система, развернутая в 1994 г. компанией NEXTEL, в настоящее время является общенациональной и насчитывает около 5500 сайтов и 2,7 млн. абонентов. В США имеется другая сеть, оператором которой является компания Southern Co. Сети IDEN развернуты также в Канаде, Бразилии, Мексике, Колумбии, Аргентине, Японии, Сингапуре, Китае, Израиле и других странах. Общее число абонентов IDEN в мире на сегодня превышает 3 млн. человек.

В России системы IDEN не развернуты и нет сведений о разработках проектов сетей данного стандарта.

Сравнительный анализ стандартов цифровой радиосвязи

Обобщенные сведения о системах стандартов EDACS, TETRA, APCO 25, Tetrapol, iDEN и их технические характеристики представлены в таблице 2.4.

Таблица 2.4. Основные сведения и технические характеристики стандартов EDACS, TETRA, APCO 25, Tetrapol, iDEN

№	Характеристика стандарта (системы) связи	EDACS	TETRA	APCO25	Tetrapol	IDEN
1	Разработчик стандарта	Ericsson	ETSI	APCO	Matra Comm.	Motorola
2	Статус стандарта	корпорат.	открытый	открытый	корпорат.	корпорат.

3	Основные производители радиосредств	Ericsson	Nokia, Motorola, OTE, Rohde & Schwarz	Motorola, Tait Electr., E.F.Johnson Inc., Transcrypt	Matra, Nortel, CS Telecom	Motorola
4	Возможный диапазон рабочих частот, МГц	138-174; 403-423; 450-470; 806-870	138-174; 403-423; 450-470; 806-870	138-174; 406-512; 746-869	70-520	805-821/ 855-866
5	Разнос между частотными каналами, кГц	25; 12,5	8	12,5; 6,25	12,5; 10	25
6	Эффективная полоса частот на один речевой канал, кГц	25	6,25	12,5; 6,25	12,5; 10	4,167
7	Время установления канала связи, с	0,25	0,2 с	0,5	не более 0,5	не более 0,5
8	Метод разделения каналов связи	МДЧР	МДВР (с МДЧР в многозон. системах)	МДЧР	МДЧР	МДВР

Функциональные возможности, предоставляемые системами стандартов цифровой транкинговой радиосвязи, представлены в таблице 2.5.

Таблица 2.5. Функциональные возможности стандартов

№	Функциональные возможности системы связи	EDACS	TETRA	APCO 25	Tetrapol	IDEN
1	Поддержка основных видов вызова (индивид., групповой, широковещ.)	+	+	+	+	+
2	Выход на ТФОП	+	+	+	+	+
3	Полнодуплексные абонентские терминалы	+	+	-	-	+
4	Передача данных и доступ к централизованным базам данных	+	+	+	+	+
5	Режим прямой связи	+	+	+	+	н/с
6	Автоматическая регистрация мобильных абонентов	+	+	+	+	+
7	Персональный вызов	-	+	+	+	+
8	Доступ к фиксированным сетям IP	+	+	+	+	+
9	Передача статусных сообщений	+	+	+	+	+
10	Передача коротких сообщений	-	+	+	+	+
11	Поддержка режима передачи данных о местоположении от системы GPS	+	+	н/с	+	н/с
12	Факсимильная связь	-	+	+	+	+

13	Возможность установки открытого канала	-	+	н/с	+	-
14	Множественный доступ с использованием списка абонентов	-	+	+	+	+
15	Наличие стандартного режима ретрансляции сигналов	н/с	+	+	+	н/с

Примечание: (н/с - нет сведений)

Таблица 2.6. Услуги связи, предоставляемые представителям служб общественной безопасности

№	Специальные услуги связи	EDACS	TETRA	APCO 25	Tetrapol
1	Приоритет доступа	+	+	+	+
2	Система приоритетных вызовов	+	+	+	+
3	Динамическая перегруппировка	+	+	+	+
4	Избирательное прослушивание	+	+	+	+
5	Дистанционное прослушивание	-	+	н/с	+
6	Идентификация вызывающей стороны	+	+	+	+
7	Вызов, санкционированный диспетчером	+	+	+	+
8	Передача ключей по радиоканалу (OTAR)	-	+	+	+
9	Дистанционное отключение абонента	н/с	+	+	+
10	Аутентификация абонентов	н/с	+	+	+

Ресурсы радиочастотного спектра

Наличие ресурсов радиочастотного спектра для развертывания системы радиосвязи является важнейшим критерием выбора той или иной системы. В данном случае наиболее перспективны стандарты, которые обеспечивают возможность построения сетей связи в наиболее широком диапазоне.

Системы EDACS реализуются в диапазонах 138-174, 403-423, 450-470 и 806-870 МГц, причем есть сведения о действующих сетях радиосвязи во всех диапазонах.

Системы TETRA предполагают использование следующих диапазонов: 380-385/390-395, 410-430/450-470 МГц и 806-870 МГц.

Системы APCO25 в соответствии с функциональными и техническими требованиями обеспечивают возможность работы в любом из диапазонов, отведенных для подвижной радиосвязи.

Стандарт Tetrapol ограничивает верхнюю частоту своих систем на уровне 520 МГц.

Системы стандарта iDEN функционируют только в диапазоне 800 МГц, что ограничивает их использование для построения определенного круга систем.

Следует отметить, что выделение ресурсов радиочастотного спектра для построения систем цифровой транкинговой радиосвязи наиболее реально в диапазоне 400 МГц.

При выборе стандарта радиосвязи обязательно необходимо учитывать информацию о том, является ли стандарт открытым или корпоративным (закрытым).

Корпоративные стандарты (EDACS и Tetrapol) являются собственностью их разработчиков. Приобретение оборудования возможно только у ограниченного круга производителей.

Открытые стандарты, к которым относятся TETRA и APCO25, обеспечивают создание конкурентной среды, привлечение большого количества производителей базового оборудования, абонентских радиостанций, тестовой аппаратуры для выпуска совместимых радиосредств, что способствует снижению их стоимости. Доступ к спецификациям стандартов предоставляется любым организациям и фирмам, вступившим в соответствующую ассоциацию. Пользователи, выбирающие открытый стандарт радиосвязи, не попадают в зависимость от единственного производителя и могут менять поставщиков оборудования. Открытые стандарты пользуются поддержкой со стороны государственных и правоохранительных структур, крупных компаний многих стран мира, а также поддержаны ведущими мировыми производителями элементной и узловой базы.

Под дальностью связи обычно понимают максимальное расстояние между двумя радиостанциями, на котором обеспечивается устойчивая связь с требуемым качеством. При этом устойчивой связью считается тогда, когда отношение проведенных сеансов связи к общему числу попыток выхода на связь превышает заданное. Под требуемым качеством понимают качество приема речевого сигнала, при котором сохраняется заданная разборчивость.

Дальность связи зависит от большого количества факторов, которые можно разделить на 3 основные группы:

- факторы, определяемые условиями применения средств связи (высота установки антенн, рельеф местности, помеховая обстановка и т.д.);
- факторы, определяемые техническими параметрами, реализованными в аппаратуре связи (мощность передатчиков, чувствительность приемного тракта, коэффициент усиления антенны и т.д.);
- факторы, определяемые непосредственно заложенными в стандарте принципами построения каналов связи (ширина полосы канала связи, скорость информации в канале, способ модуляции сигнала, алгоритм речевого кодирования, методы помехоустойчивого кодирования).

Естественно, что корректно сравнивать стандарты цифровой транкинговой радиосвязи можно только по последней группе факторов, т.к. другие группы зависят или от условий эксплуатации, или определяются качеством производства радиосредств.

Следует понимать, что принципиально системы с FDMA (МДЧР) обеспечивают большую дальность связи (при прочих равных параметрах) по сравнению с системами с TDMA (МДВР). Это объясняется меньшей энергией сигнала на один бит информации. Известно, что энергия сигнала E_c определяется как

$$E_c = P_c \cdot T_c,$$

где P_c – мощность, а T_c – длительность сигнала. Понятно, что при уменьшении длительности сигнала (времени передачи одного информационного бита для цифровой системы) пропорционально уменьшается энергия. Например, для систем TETRA, с четырьмя информационными каналами на одной физической частоте эквивалентная мощность на бит информации в 4 раза меньше, чем в системах с FDMA, что равносильно снижению дальности связи ориентировочно на 40 %.

Другим фактором, влияющим на снижение дальности связи в системах с TDMA по сравнению с FDMA-системами, является устойчивость канала связи при многолучевом распространении сигнала, возникающем в условиях плотной городской застройки или холмистой местности из-за отражения сигнала от зданий и других преград и приводящем к появлению радиозаха. Отраженный сигнал оказывает тем большее влияние, чем больше его отношение к длительности сигнала. Поэтому уменьшение длительности информационного бита в системах с TDMA ухудшает качество приема в условиях многолучевости. (Принципиально можно добиться компенсации задержки сигнала, однако это требует применения различных типов приемников для различных условий распространения сигнала.)

Во многих источниках приводятся данные о приблизительно двукратном снижении дальности связи в системах с TDMA по сравнению с системами с частотным разделением каналов связи.

На сегодняшний день оборудование систем цифровой радиосвязи стоит значительно дороже по сравнению с аналоговыми системами. Как правило, стоимости заключенных контрактов являются коммерческой тайной, однако следует понимать, что при развертывании системы любого из представленных стандартов цифровой радиосвязи, обслуживающей несколько сотен абонентов, речь идет не о тысячах, а о миллионах долларов. Судя по рекламной информации зарубежных фирм, стоимость абонентских радиостанций, работающих в цифровых стандартах, может колебаться в пределах от 800 до 4 тыс. долларов, причем существенная доля стоимости может определяться наличием модулей или программных средств защиты информации.

Сравнение экономической эффективности систем различных стандартов нельзя рассматривать в отрыве от категории системы подвижной радиосвязи. Для создания сетей связи с небольшой нагрузкой, широким территориальным охватом и числом каналов в пределах 10 более оптимальным вариантом (в т.ч. и по стоимости) является использование систем МДЧР, к которым относятся APCO 25 (Фаза I) и Tetrapol. Это объясняется большим радиусом зон обслуживания систем МДЧР по сравнению с МДВР системами. По оценкам, приведенным в техническом отчете стандарта Tetrapol PAS, стоимость базового оборудования многозоновой сети радиосвязи, реализованной на основе МДВР, по отношению к системе с частотным разделением каналов (при одинаковой стоимости единицы оборудования) будет на 30-50 % выше.

Однако, для сетей связи с интенсивным трафиком и числом каналов в одной зоне более 15 предпочтительно использование систем с временным разделением каналов, к которым относится TETRA.

Следует отметить, что стандарт APCO25 (Фаза II) будет обладать универсальностью, обеспечивая возможность строить системы как с частотным, так и с временным разделением каналов.

Нет никаких сомнений в преимуществах цифровых систем по сравнению с аналоговыми. К ним относятся и повышение конфиденциальности переговоров, и наличие усовершенствованной системы идентификации абонентов, и более эффективное использование радиочастот (в отведенной полосе можно организовать больше телефонных каналов за счет компрессии речевого потока и применения современных схем модуляции), и выравнивание качества передачи по всей зоне обслуживания, и возможность дистанционного управления абонентской радиостанцией вплоть до ее включения/выключения, и определение местоположения абонента, и выполнение ряда других специфических задач. Немаловажно, что одно и то же абонентское устройство допускается использовать для передачи и приема речи, данных, факсимильных сообщений, сигналов персонального радиовызова и др. (фактически можно создавать цифровые сети с интеграцией служб).

Осознав богатство возможностей цифрового транкинга, согласимся с тем, что он нужен в России. Пройдет еще несколько лет, и основные поставщики прекратят выпуск аналогового транкингового оборудования. И тогда проблема высокой стоимости услуг еще более обострится: когда производство перестает быть массовым, это, как известно, снижению цен не способствует.

Краткий сравнительный анализ данных стандартов цифровой транкинговой радиосвязи по основным рассмотренным критериям позволяет сделать определенные выводы о перспективности их развития как в мире, так и в России.

Стандарт EDACS практически не имеет перспектив развития. По сравнению с другими стандартами, он имеет меньшую спектральную эффективность и менее широкие функциональные возможности. Компания Ericsson не планирует расширять возможности стандарта и практически свернула производство оборудования.

Стандарт iDEN не предусматривает многих специальных требований, а также, несмотря на высокую спектральную эффективность, ограничен необходимостью использования диапазона 800 МГц. Вероятно, что системы данного стандарта имеют определенный потенциал и будут еще разворачиваться и эксплуатироваться, в особенности в Северной и Южной Америке. В других регионах перспективы разворачивания систем данного стандарта выглядят сомнительными.

Стандарт Tetrapol имеет хорошие технические показатели и достаточные функциональные возможности, однако так же, как и стандарты EDACS и iDEN, не обладает статусом открытого стандарта, что может существенно сдерживать его развитие в техническом плане, а также в части стоимости абонентского и стационарного оборудования.

Стандарты TETRA и APCO25 обладают высокими техническими характеристиками и широкими функциональными возможностями, включая выполнение специальных требований силовых структур, имеют достаточную спектральную эффективность. Самым главным доводом в пользу этих систем является наличие статуса открытых стандартов. Однако неоспоримым преимуществом стандарта APCO25 по сравнению с TETRA является большая дальность связи и большая экономическая эффективность.

Список условных сокращений

APCO25 – стандарт цифровой транкинговой радиосвязи, разработанный Ассоциацией официальных представителей служб связи органов общественной безопасности (Association of Public Safety Communications Officials-international)

CAI – Common Radio Interface – Общий радиоинтерфейс

CEPT – Conference of European Posts and Telecommunications - Конференция европейских организаций связи

DID – Direct Inward Dialing – Аппаратура прямого набора номера

EDACS – Enhanced Digital Access Communication System – Стандарт цифровой транкинговой радиосвязи, разработанный фирмой Ericsson (Швеция)

EIA – Electronic Industries Alliance – Ассоциация электронной промышленности

ETSI – European Telecommunications Standards Institute – Европейский институт телекоммуникационных стандартов

GPS – Global Position System – Глобальная спутниковая навигационная система

iDEN – integrated Digital Enhanced Network

ITU – International Telecommunications Union - Международный Союз Электросвязи (МСЭ)

MoU TETRA – Ассоциация «Меморандум о взаимопонимании и содействии стандарту TETRA»

O&M – терминал технического обслуживания и эксплуатации

RS-232C – Стандарт интерфейса физического уровня, который поддерживает несбалансированных схем на скорости до 64кбит/с

SINAD – Отношение уровня сигнала к сумме уровней сигнала к сумме уровней сигнала, шумов и продуктов искажения сигнала

TETRA – Terrestrial Trunked Radio (Наземное транкинговое радио) – стандарт цифровой транкинговой радиосвязи, разработанный институтом ETSI

TETRA V+D – TETRA Voice + Data – стандарт на интегрированную систему передачи речи и данных

TETRA PDO – TETRA Packet Data Optimized – Стандарт, описывающий специальный вариант транкинговой системы, ориентированной только на передачу данных

АС – абонентская станция

БС – базовая станция

МДВР (TDMA) – Многостанционный доступ с временным разделением

МДЧР (FDMA) – Многостанционный доступ с частотным разделением

ПМП – Профессиональная мобильная радиосвязь

СКП – Сеть с коммутацией пакетов

ТСР – Транкинговые системы радиосвязи
ТфОП – Телефонная сеть общего пользования

3. СИСТЕМЫ СОТОВОЙ СВЯЗИ СТАНДАРТА GSM

В 1982 году Conference of European Posts and Telegraphs сформировала группу (Group Special Mobile) по изучению и разработке Общеввропейской наземной мобильной системы общественного пользования (pan-European public land mobile system). Предложенная система должна была удовлетворять следующим требованиям:

- Относительно хорошее качество речи
- Невысокая стоимость услуг и терминального оборудования
- Поддержка перемещения пользователей системы внутри страны и за ее пределами
- Возможность использования компактного терминального оборудования
- Поддержание широкого спектра услуг и возможностей
- Эффективное использование радио спектра
- Совместимость с ISDN

В 1989 году группа перешла в ведение ETSI (European Telecommunication Standards Institute), и в 1990 году была опубликована первая серия спецификаций GSM. Коммерческое использование GSM началось в середине 1991 года, и к 1993 году уже существовало 36 сетей GSM в 22 странах, и еще около 25 стран принимали GSM в качестве стандарта. Будучи стандартизованным в Европе, GSM не является только европейским стандартом: сети GSM (включая DCS1800 и PCS1900) функционируют в более чем 80 странах мира. К началу 1994 года более 1.3 миллиона человек являлись пользователями GSM. Только в Европе за 1995 год число пользователей GSM выросло с 5 миллионов человек в начале года, до более чем 10 миллионов человек в конце. С некоторым опозданием к стандарту присоединилась и Северная Америка (ответвление GSM - PCS1900). И в настоящее время GSM расшифровывается как Global System for Mobile Communications.

Разработчики GSM выбрали не опробованную (на тот момент) цифровую систему как альтернативу аналоговым сотовым системам, таким как AMPS в Соединенных Штатах или TACS в Великобритании. Они поверили в то, что при помощи алгоритмов упаковки и цифровых сигнальных устройств управления коммуникациями облегчатся задачи обеспечения качества и понижения стоимости связи и услуг.

С одной стороны, рекомендации GSM составляются так, чтобы предоставить производителям максимальную свободу в развитии системы, а, с другой, - гарантировать корректное взаимодействие между различными компонентами системы. Это достигается предоставлением описаний интерфейсов и функций каждой функциональной сущности, определенной в системе.

Попытаемся в двух словах сформулировать основные преимущества GSM перед аналоговыми системами:

Всеобщая мобильность: Абонент имеет возможность использовать все преимущества пан-европейской системы (Pan-European System), позволяющей ему звонить откуда угодно и куда угодно (в рамках областей, находящихся в сфере услуг сотовых GSM сетей), используя один и тот же телефонный номер, даже находясь вне области проживания. Его собеседник не обязан быть информирован о местонахождении абонента, поскольку сама сеть GSM отвечает за корректное нахождение абонента. С помощью своей персональной карточки абонент может использовать и другие мобильные средства связи (например, телефон в арендованной машине), даже во время путешествий за пределы своего места проживания.

Высокое качество передачи и оптимальное выделение спектра: В старых аналоговых сотовых сетях нередко возникали проблемы качества передачи, в особенности в городских районах. Посредством более эффективного использования выделенной для радиопередач частотной полосы и уменьшенных размеров сот, система GSM в состоянии обслуживать значительно большее число абонентов. Оптимальное использование доступного спектра

достигается посредством применения методов разделения времени и частоты (Frequency Division Multiple Access - FDMA, Time Division Multiple Access - TDMA), эффективного полно скоростного (full-rate) и полу скоростного(half-rate) кодирования речи и с помощью используемой схемы модуляции, так называемой Гауссовой Минимальной Манипуляции (GMSK - Gaussian Minimum Shift Keyng).

Секретность: Методы обеспечения секретности, стандартизованные для GSM систем, позволяют сказать, что системы GSM в данный момент являются наиболее секретными из всех доступных сотовых телекоммуникационных систем. Хотя конфиденциальность разговоров и анонимность абонента GSM гарантируется только в пределах радио соединения, это несомненно огромный шаг в сторону достижения “полной” (по всему пути прохождения информации) секретности. Анонимность абонента обеспечивается использованием временных идентификационных номеров. Собственно конфиденциальность связи по радио соединению обеспечивается применением алгоритмов шифрования и переходов по частотам (Frequency Hopping), которые могут применяться только в цифровых системах.

Услуги: Список услуг, предоставляемых абонентам GSM обычно включает в себя собственно разговор, факсимильные услуги, голосовую почту, передачу коротких сообщений, передачу данных и дополнительные услуги, такие как, например, переадресация вызова.

Общие характеристики стандарта GSM

Используемый спектр частот в диапазоне 862-960 МГц, разбит на два диапазона: 890-915 МГц (для передатчиков подвижных станций - MS), 935-960 МГц (для передатчиков базовых станций - BTS).

В стандарте GSM используется узкополосный многостанционный доступ с временным разделением каналов (NB TDMA). В структуре TDMA кадра содержится 8 временных позиций на каждой из 124 несущих.

Для защиты от ошибок в радиоканалах при передаче информационных сообщений применяется блочное и сверточное кодирование с перемежением. Повышение эффективности кодирования и перемежения при малой скорости перемещения подвижных станций достигается медленным переключением рабочих частот (SFH) 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 рассчитана на компенсацию абсолютного времени задержки сигналов до 233 мкс, что соответствует максимальной дальности связи или максимальному радиусу ячейки (соты) 35 км.

В стандарте GSM выбрана гауссовская частотная манипуляция с минимальным частотным сдвигом (GMSK). Обработка речи осуществляется в рамках принятой системы прерывистой передачи речи (DTX), которая обеспечивает включение передатчика только при наличии речевого сигнала и отключение передатчика в паузах и в конце разговора. В качестве речепреобразующего устройства выбран речевой кодек с регулярным импульсным возбуждением/долговременным предсказанием и линейным предикативным кодированием с предсказанием (RPE/LTR-LTP-кодек). Общая скорость преобразования речевого сигнала - 13 кбит/с.

В стандарте GSM достигается высокая степень безопасности передачи сообщений; 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).

Таблица 3.1 Основные характеристики стандарта GSM

Частоты передачи подвижной станции и приема базовой станции, МГц	890-915
Частоты приема подвижной станции и передачи базовой станции, МГц	935-960
Дуплексный разнос частот приема и передачи, МГц	45
Скорость передачи сообщений в радиоканале, кбит/с	270, 833
Скорость преобразования речевого кодека, кбит/с	13
Ширина полосы канала связи, кГц	200
Максимальное количество каналов связи	124
Максимальное количество каналов, организуемых в базовой станции	16-20
Вид модуляции	GMSK
Индекс модуляции	BT 0,3
Ширина полосы предмодуляционного гауссовского фильтра, кГц	81,2
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, км	до 35
Схема организации каналов	TDMA/FDMA

Структурная схема и состав оборудования сетей связи

Функциональное построение и интерфейсы, принятые в стандарте GSM, иллюстрируются структурной схемой (рис.3.1), на которой MSC (Mobile Switching Centre) - центр коммутации подвижной связи; BSS (Base Station System) - оборудование базовой станции; OMC (Operations and Maintenance Centre) - центр управления и обслуживания; MS (Mobile Stations) - подвижные станции.

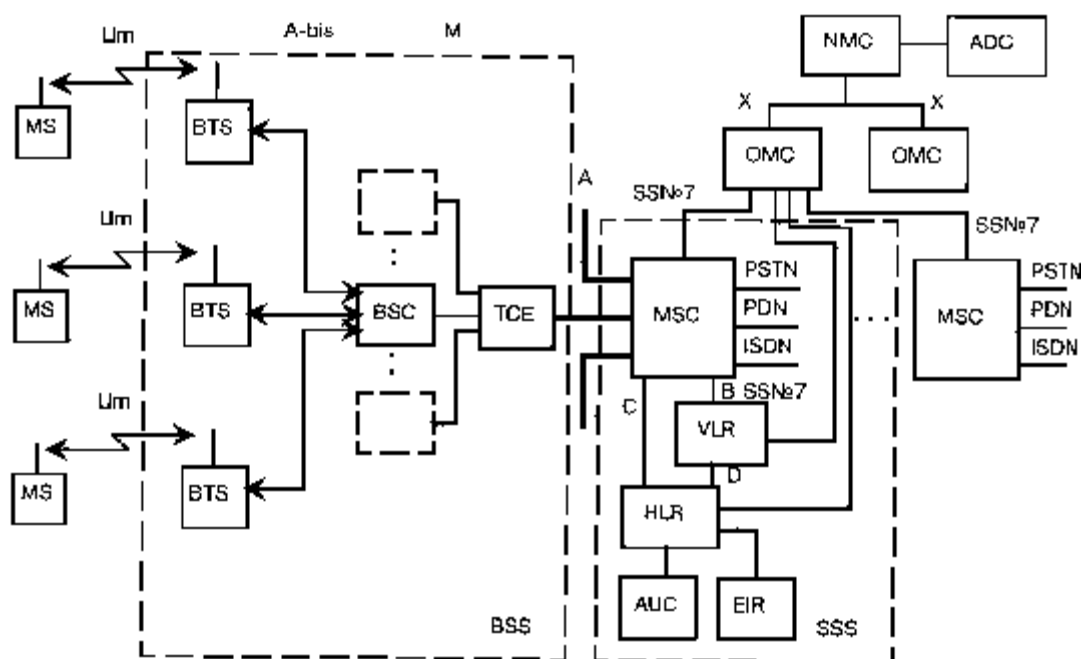


Рис. 3.1. Функциональное построение и интерфейсы стандарта GSM .

Функциональное сопряжение элементов системы осуществляется рядом интерфейсов. Все сетевые функциональные компоненты в стандарте GSM взаимодействуют в соответствии с системой сигнализации МСЭ-Т (ранее МККТТ) SS N 7 (ССИТSS.N7)).

Центр коммутации подвижной связи обслуживает группу сот и обеспечивает все виды соединений, в которых нуждается в процессе работы подвижная станция. MSC аналогичен коммутационной станции ISDN и представляет собой 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 коммутационной станции ISDN, 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. MSC управляет процедурами установления вызова и маршрутизации. Для телефонной сети общего пользования (PSTN) MSC обеспечивает функции сигнализации по протоколу SS N 7, передачи вызова или другие виды 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.

MSC поддерживает также 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 осуществляется 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 регистры положения (HLR) и перемещения (VLR). В HLR хранится та часть информации о местоположении какой-либо подвижной станции, которая позволяет центру коммутации доставить вызов станции. Регистр HLR содержит международный идентификационный номер подвижного абонента (IMSI). Он используется для опознавания подвижной станции в центре аутентификации (AUC).

Практически HLR представляет собой справочную базу данных о постоянно прописанных 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 о роуминге (блуждании) абонента, включая данные о временном идентификационном номере подвижного абонента (TMSI) и соответствующем VLR.

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 или MSISDN (номеру подвижного абонента в сети ISDN). К базе данных могут получить доступ MSC или VLR, относящиеся к другим сетям, в рамках обеспечения межсетевых роумингов абонентов.

Второе основное устройство, обеспечивающее контроль за передвижением подвижной станции из зоны в зону, - регистр перемещения 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 сбоя предусмотрена защита устройств памяти этих регистров.

VLR содержит 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), которым присваивается свой идентификационный номер (LAC). Каждый VLR содержит данные об абонентах 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 "блуждающей" подвижной станции (MSRN). 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.

VLR также распределяет номера передачи управления при передаче соединений от одного MSC к другому. Кроме того, VLR управляет распределением новых TMSI и передает их в HLR. Он также управляет процедурами установления подлинности во время обработки вызова. По решению оператора TMSI может периодически изменяться для усложнения процедуры идентификации абонентов. Доступ к базе данных VLR может обеспечиваться через IMSI, TMSI или MSRN. В целом VLR представляет собой

локальную базу данных о подвижном абоненте для той зоны, где находится абонент, что позволяет исключить постоянные запросы в HLR и сократить время на обслуживание вызовов.

Для исключения несанкционированного использования ресурсов системы связи вводятся механизмы аутентификации - удостоверения подлинности абонента. Центр аутентификации состоит из нескольких блоков и формирует ключи и алгоритмы аутентификации. С его помощью проверяются полномочия абонента и осуществляется его доступ к сети связи. AUC принимает решения о параметрах процесса аутентификации и определяет ключи шифрования абонентских станций на основе базы данных, сосредоточенной в регистре идентификации оборудования (EIR - Equipment Identification Register).

Каждый подвижный абонент на время пользования системой связи получает стандартный модуль подлинности абонента (SIM), который содержит: международный идентификационный номер (IMSI), свой индивидуальный ключ аутентификации (Ki), алгоритм аутентификации (A3).

С помощью записанной 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. На ней с помощью Ki и алгоритма аутентификации A3 определяется значение отклика (SRES), т.е. $SRES = Ki * [RAND]$.

Подвижная станция посылает вычисленное значение SRES в сеть, которая сверяет значение принятого SRES со значением SRES, вычисленным сетью. Если оба значения совпадают, подвижная станция приступает к передаче сообщений. В противном случае связь прерывается, и индикатор подвижной станции показывает, что опознавание не состоялось. Для обеспечения секретности вычисление SRES происходит в рамках SIM. Несекретная информация (например, Ki) не подвергается обработке в модуле SIM.

EIR - регистр идентификации оборудования, содержит централизованную базу данных для подтверждения подлинности международного идентификационного номера оборудования подвижной станции (IMEI). Эта база данных относится исключительно к оборудованию подвижной станции. База данных EIR состоит из списков номеров IMEI, организованных следующим образом:

БЕЛЫЙ СПИСОК - содержит номера IMEI, о которых есть сведения, что они закреплены за санкционированными подвижными станциями.

ЧЕРНЫЙ СПИСОК - содержит номера IMEI подвижных станций, которые украдены или которым отказано в обслуживании по другой причине.

СЕРЫЙ СПИСОК - содержит номера IMEI подвижных станций, у которых существуют проблемы, выявленные по данным программного обеспечения, что не является основанием для внесения в "черный список".

К базе данных EIR получают дистанционный доступ MSC данной сети, а также MSC других подвижных сетей.

Как и в случае с HLR, сеть может иметь более одного EIR, при этом каждый EIR управляет определенными группами IMEI. В состав MSC входит транслятор, который при получении номера IMEI возвращает адрес EIR, управляющий соответствующей частью базы данных об оборудовании.

IWF - межсетевой функциональный стык, является одной из составных частей MSC. Он обеспечивает абонентам доступ к средствам преобразования протокола и скорости передачи данных так, чтобы можно было передавать их между его терминальным оборудованием (DIE) сети GSM и обычным терминальным оборудованием фиксированной сети. Межсетевой функциональный стык также "выделяет" модем из своего банка оборудования для сопряжения с соответствующим модемом фиксированной

сети. IWF также обеспечивает интерфейсы типа прямого соединения для оборудования, поставляемого клиентам, например, для пакетной передачи данных PAD по протоколу X25.

ЕС - эхоподавитель, используется в MSC со стороны PSTN для всех телефонных каналов (независимо от их протяженности) из-за физических задержек в трактах распространения, включая радиоканал, сетей GSM. Типовой эхоподавитель может обеспечивать подавление в интервале 68 миллисекунд на участке между выходом ЕС и телефоном фиксированной телефонной сети. Общая задержка в канале GSM при распространении в прямом и обратном направлениях, вызванная обработкой сигнала, кодированием/декодированием речи, канальным кодированием и т.д., составляет около 180 мс. Эта задержка была бы незаметна подвижному абоненту, если бы в телефонный канал не была включена дифсистема с преобразованием тракта с двухпроводного на четырехпроводный режим, установка которого необходима в MSC, так как стандартное соединение с PSTN является двухпроводным. При соединении двух абонентов фиксированной сети эхо-сигналы отсутствуют. Без включения ЕС задержка от распространения сигналов в тракте GSM будет вызывать раздражение у абонентов, прерывать речь и отвлекать внимание.

ОМС - центр эксплуатации и технического обслуживания, является центральным элементом сети GSM, который обеспечивает контроль и управление другими компонентами сети и контроль качества ее работы. ОМС соединяется с другими компонентами сети GSM по каналам пакетной передачи протокола X.25. ОМС обеспечивает функции обработки аварийных сигналов, предназначенных для оповещения обслуживающего персонала, и регистрирует сведения об аварийных ситуациях в других компонентах сети. В зависимости от характера неисправности ОМС позволяет обеспечить ее устранение автоматически или при активном вмешательстве персонала. ОМС может обеспечить проверку состояния оборудования сети и прохождения вызова подвижной станции. ОМС позволяет производить управление нагрузкой в сети. Функция эффективного управления включает сбор статистических данных о нагрузке от компонентов сети GSM, записи их в дисковые файлы и вывод на дисплей для визуального анализа. ОМС обеспечивает управление изменениями программного обеспечения и базами данных о конфигурации элементов сети. Загрузка программного обеспечения в память может производиться из ОМС в другие элементы сети или из них в ОМС.

NMC - центр управления сетью, позволяет обеспечивать рациональное иерархическое управление сетью GSM. Он обеспечивает эксплуатацию и техническое обслуживание на уровне всей сети, поддерживаемой центрами ОМС, которые отвечают за управление региональными сетями. NMC обеспечивает управление графиком во всей сети и обеспечивает диспетчерское управление сетью при сложных аварийных ситуациях, как например, выход из строя или перегрузка узлов. Кроме того, он контролирует состояние устройств автоматического управления, задействованных в оборудовании сети, и отражает на дисплее состояние сети для операторов NMC. Это позволяет операторам контролировать региональные проблемы и, при необходимости, оказывать помощь ОМС, ответственному за конкретный регион. Таким образом, персонал NMC знает состояние всей сети и может дать указание персоналу ОМС изменить стратегию решения региональной проблемы.

NMC концентрирует внимание на маршрутах сигнализации и соединениях между узлами с тем, чтобы не допускать условий для возникновения перегрузки в сети. Контролируются также маршруты соединений между сетью GSM и PSTN во избежание распространения условий перегрузки между сетями. При этом персонал NMC координирует вопросы управления сетью с персоналом других NMC. NMC обеспечивает также возможность управления графиком для сетевого оборудования подсистемы базовых станций (BSS). Операторы NMC в экстремальных ситуациях могут задействовать такие

процедуры управления, как "приоритетный доступ", когда только абоненты с высоким приоритетом (экстренные службы) могут получить доступ к системе.

NMC может брать на себя ответственность в каком-либо регионе, когда местный ОМС является необслуживаемым, при этом ОМС действует в качестве транзитного пункта между NMC и оборудованием сети. NMC обеспечивает операторов функциями, аналогичными функциям ОМС.

NMC является также важным инструментом планирования сети, так как NMC контролирует сеть и ее работу на сетевом уровне, а, следовательно, обеспечивает планировщиков сети данными, определяющими ее оптимальное развитие.

BSS - оборудование базовой станции, состоит из контроллера базовой станции (BSC) и приемопередающих базовых станций (BTS). Контроллер базовой станции может управлять несколькими приемо-передающими блоками. BSS управляет распределением радиоканалов, контролирует соединения, регулирует их очередность, обеспечивает режим работы с прыгающей частотой, модуляцию и демодуляцию сигналов, кодирование и декодирование сообщений, кодирование речи, адаптацию скорости передачи для речи, данных и вызова, определяет очередность передачи сообщений персонального вызова.

BSS совместно с MSC, HLR, VLR выполняет некоторые функции, например: освобождение канала, главным образом, под контролем MSC, но MSC может запросить базовую станцию обеспечить освобождение канала, если вызов не проходит из-за радиопомех. BSS и MSC совместно осуществляют приоритетную передачу информации для некоторых категорий подвижных станций.

TCE - транскодер, обеспечивает преобразование выходных сигналов канала передачи речи и данных MSC (64 кбит/с ИКМ) к виду, соответствующему рекомендациям GSM по радиоинтерфейсу (Рек. GSM 04.08). В соответствии с этими требованиями скорость передачи речи, представленной в цифровой форме, составляет 13 кбит/с. Этот канал передачи цифровых речевых сигналов называется "полноскоростным". Стандартом предусматривается в перспективе использование полускоростного речевого канала (скорость передачи 6,5 кбит/с).

Снижение скорости передачи обеспечивается применением специального речепреобразующего устройства, использующего линейное предикативное кодирование (LPC), долговременное предсказание (LTP), остаточное импульсное возбуждение (RPE - иногда называется RELP).

Транскодер обычно располагается вместе с MSC, тогда передача цифровых сообщений в направлении к контроллеру базовых станций - BSC ведется с добавлением к потоку со скоростью передачи 13 кбит/с, дополнительных битов (стаффинг) до скорости передачи данных 16 кбит/с. Затем осуществляется уплотнение с кратностью 4 в стандартный канал 64 кбит/с. Так формируется определенная Рекомендациями GSM 30-канальная ИКМ линия, обеспечивающая передачу 120 речевых каналов. Шестнадцатый канал (64 кбит/с), "канальный интервал", выделяется отдельно для передачи информации сигнализации и часто содержит трафик SS N7 или LAPD. В другом канале (64 кбит/с) могут передаваться также пакеты данных, согласующиеся с протоколом X.25 МСЭ-Т.

Таким образом, результирующая скорость передачи по указанному интерфейсу составляет $30 \times 64 \text{ кбит/с} + 64 \text{ кбит/с} + 64 \text{ кбит/с} = 2048 \text{ кбит/с}$.

MS - подвижная станция, состоит из оборудования, которое служит для организации доступа абонентов сетей GSM к существующим фиксированным сетям электросвязи. В рамках стандарта GSM приняты пять классов подвижных станций от модели 1-го класса с выходной мощностью 20 Вт, устанавливаемой на транспортном средстве, до портативной модели 5-го класса, максимальной мощностью 0,8 Вт (таблица 2). При передаче сообщений предусматривается адаптивная регулировка мощности передатчика, обеспечивающая требуемое качество связи.

Подвижный абонент и станция независимы друг от друга. Как уже отмечалось, каждый абонент имеет свой международный идентификационный номер (IMSI),

записанный на его интеллектуальную карточку. Такой подход позволяет устанавливать радиотелефоны, например, в такси и автомобилях, сдаваемых на прокат. Каждой подвижной станции также присваивается свой международный идентификационный номер (IMEI). Этот номер используется для предотвращения доступа к сетям GSM похищенной станции или станции без полномочий.

Таблица 3.2

Класс мощности	Максимальный уровень мощности передатчика	Допустимые отклонения
1	20 Вт	1.5 дБ
2	8 Вт	1.5 дБ
3	5 Вт	1.5 дБ
4	2 Вт	1.5 дБ
5	0.8 Вт	1.5 дБ

Структура TDMA кадров и формирование сигналов в стандарте GSM

В результате анализа различных вариантов построения цифровых сотовых систем подвижной связи (ССПС) в стандарте GSM принят многостанционный доступ с временным разделением каналов (TDMA). Общая структура временных кадров показана на рис. 3.2

1 Гиперкадр = 2048 Суперкадрам = 2715648 TDMA кадрам

$T = 3ч\ 28мин\ 53с\ 760мс = 125336,76с$

0	1	...	2046	2047
---	---	-----	------	------

1 Суперкадр = 1326 TDMA кадрам = 51 мультикадру

(по 26 кадров) или 26 мультикадрам (по 51 кадру)

$T = 6,12с$

0	1	2	3	...	47	48	49	50
---	---	---	---	-----	----	----	----	----

0	1	...	24	25
---	---	-----	----	----

1 Мультикадр = 26 TDMA кадрам

$T_m = 120мс$

0	1	...	24	25
---	---	-----	----	----

1 TDMA кадр = 8 временным позициям (окнам)

$T_m = 4,615мс$

0	1	...	7	8
---	---	-----	---	---

1 временной интервал = 156,25 битам ($15/26 = 0,577мс$)

Длительность 1 бита = $48/13 = 3,69мс$

TB - Tail Bits - концевая комбинация

GP - Guard Period - защитный интервал

TB 3 бита	Зашифрованные биты 57	1	Обучающая послед. 26	1	Зашифрованные биты 57	TB 3 бита	GP 8,25
--------------	-----------------------	---	-------------------------	---	-----------------------	--------------	------------

ТВ 3 бита	Нулевые биты 142			ТВ 3 бита	GP 8,25
ТВ 3 бита	Зашифрованные биты 39	Синхропоследовательность 41	Зашифрованные биты 39	ТВ 3 бита	GP 8,25
ТВ 8 бит	Синхропоследовательность 41		Зашифрованные биты 36	ТВ 3 бита	GP 8,25

Рис 3.2. Общая структура временных кадров.

Длина периода последовательности в этой структуре, которая называется гиперкадром, равна $T_g = 3 \text{ ч } 28 \text{ мин } 53 \text{ с } 760 \text{ мс}$ (12533,76 с). Гиперкадр делится на 2048 суперкадров, каждый из которых имеет длительность $T_s = 12533,76/2048 = 6,12 \text{ с}$.

Суперкадр состоит из мультикадров. Для организации различных каналов связи и управления в стандарте GSM используются два вида мультикадров:

- 1) 26-позиционные TDMA кадры мультикадра;
- 2) 51-позиционные TDMA кадры мультикадра.

Суперкадр может содержать в себе 51 мультикадр первого типа или 26 мультикадров второго типа. Длительности мультикадров соответственно:

- 1) $T_m = 6120/51 = 120 \text{ мс}$;
- 2) $T_m = 6120/26 = 235,385 \text{ мс}$ (3060/13 мс).

Длительность каждого TDMA кадра

$$T_k = 120/26 = 235,385/51 = 4,615 \text{ мс} \text{ (60/13 мс)}.$$

В периоде последовательности каждый TDMA кадр имеет свой порядковый номер (NF) от 0 до NF_{\max} , где

$$NF_{\max} = (26 \times 51 \times 2048) - 1 = 2715647.$$

Таким образом, гиперкадр состоит из 2715647 TDMA кадров. Необходимость такого большого периода гиперкадра объясняется требованиями применяемого процесса криптографической защиты, в котором номер кадра NF используется как входной параметр.

TDMA кадр делится на восемь временных позиций с периодом $T_o = 60/13:8 = 576,9 \text{ мкс}$ (15/26 мс)

Каждая временная позиция обозначается TN с номером от 0 до 7. Физический смысл временных позиций, которые иначе называются окнами, - время, в течение которого осуществляется модуляция несущей цифровым информационным потоком, соответствующим речевому сообщению или данным.

Цифровой информационный поток представляет собой последовательность пакетов, размещаемых в этих временных интервалах (окнах). Пакеты формируются немного короче, чем интервалы, их длительность составляет 0,546 мс, что необходимо для приема сообщения при наличии временной дисперсии в канале распространения.

Информационное сообщение передается по радиоканалу со скоростью 270,833 кбит/с. Это означает, что временной интервал TDMA кадра содержит 156,25 бит. Длительность одного информационного бита $576,9 \text{ мкс}/156,25 = 3,69 \text{ мкс}$.

Каждый временной интервал, соответствующий длительности бита, обозначается VN с номером от 0 до 155; последнему интервалу длительностью 1/4 бита присвоен номер 156.

Для передачи информации по каналам связи и управления, подстройки несущих частот, обеспечения временной синхронизации и доступа к каналу связи в структуре TDMA кадра используются пять видов временных интервалов (окон):

Таблица 3.3

1	NB (Normal Burst)	Нормальный временной интервал
2	FB (Frequency Correction Burst)	Временной интервал подстройки частоты
3	SB (Synchronization Burst)	Интервал временной синхронизации
4	DB (Dummy Burst)	Установочный интервал
5	AB (Access Burst)	Интервал доступа

NB используется для передачи информации по каналам связи и управления, за исключением канала доступа RACH. Он состоит из 114 бит зашифрованного сообщения и включает защитный интервал (GP) в 8,25 бит длительностью 30,46 мкс. Информационный блок 114 бит разбит на два самостоятельных блока по 57 бит, разделенных между собой обучающей последовательностью в 26 бит, которая используется для установки эквалайзера в приемнике в соответствии с характеристиками канала связи в данный момент времени.

В состав NB включены два контрольных бита (Stealing Flag), которые служат признаком того, содержит ли передаваемая группа речевую информацию или информацию сигнализации. В последнем случае информационный канал (Traffic Channel) "украден" для обеспечения сигнализации.

Между двумя группами зашифрованных бит в составе NB находится обучающая последовательность из 26 бит, известная в приемнике.

С помощью этой последовательности обеспечивается:

- оценка частоты появления ошибок в двоичных разрядах по результатам сравнения принятой и эталонной последовательностей. В процессе сравнения вычисляется параметр RXQUAL, принятый для оценки качества связи. Конечно, речь идет только об оценке связи, а не о точных измерениях, так как проверяется только часть передаваемой информации. Параметр RXQUAL используется при вхождении в связь, при выполнении процедуры "эстафетной передачи" (Handover) и при оценке зоны покрытия радиосвязью;
- оценка импульсной характеристики радиоканала на интервале передачи NB для последующей коррекции тракта приема сигнала за счет использования адаптивного эквалайзера в тракте приема;
- определение задержек распространения сигнала между базовой и подвижной станциями для оценки дальности связи. Эта информация необходима для того, чтобы пакеты данных от разных подвижных станций не накладывались при приеме на базовой станции. Поэтому удаленные на большее расстояние подвижные станции должны передавать свои пакеты раньше станций, находящихся в непосредственной близости от базовой станции

FB предназначен для синхронизации по частоте подвижной станции. Все 142 бита в этом временном интервале - нулевые, что соответствует немодулированной несущей со сдвигом $1625/24$ кГц выше номинального значения частоты несущей. Это необходимо для проверки работы своего передатчика и приемника при небольшом частотном разносе каналов (200 кГц), что составляет около 0,022% от номинального значения полосы частот 900 МГц. FB содержит защитный интервал 8,25 бит так же, как и нормальный временной интервал. Повторяющиеся временные интервалы подстройки частоты (FB) образуют канал установки частоты (FSSN).

SB используется для синхронизации по времени базовой и подвижной станций. Он состоит из синхропоследовательности длительностью 64 бита, несет информацию о номере TDMA кадра и идентификационный код базовой станции. Этот интервал

передается вместе с интервалом установки частоты. Повторяющиеся интервалы синхронизации образуют так называемый канал синхронизации (SCH).

DB обеспечивает установление и тестирование канала связи. По своей структуре DB совпадает с NB и содержит установочную последовательность длиной 26 бит. В DB отсутствуют контрольные биты и не передается никакой информации. DB лишь информирует о том, что передатчик функционирует.

AB обеспечивает разрешение доступа подвижной станции к новой базовой станции. AB передается подвижной станцией при запросе канала сигнализации. Это первый передаваемый подвижной станцией пакет, следовательно, время прохождения сигнала еще не измерено. Поэтому пакет имеет специфическую структуру. Сначала передается концевая комбинация 8 бит, затем - последовательность синхронизации для базовой станции (41 бит), что позволяет базовой станции обеспечить правильный прием последующих 36 зашифрованных бит. Интервал содержит большой защитный интервал (68,25 бит, длительностью 252 мкс), что обеспечивает (независимо от времени прохождения сигнала) достаточное временное разнесение от пакетов других подвижных станций.

Этот защитный интервал соответствует двойному значению наибольшей возможной задержки сигнала в рамках одной соты и тем самым устанавливает максимально допустимые размеры соты. Особенность стандарта GSM - возможность обеспечения связью подвижных абонентов в сотах с радиусом около 35 км. Время распространения радиосигнала в прямом и обратном направлениях составляет при этом 233,3 мкс.

В структуре GSM строго определены временные характеристики огибающей сигнала, излучаемого пакетами на канальном временном интервале TDMA кадра, и спектральная характеристика сигнала. Различные формы огибающих излучаемых сигналов соответствуют разным длительностям интервала AB (88 бит) по отношению к другим указанным интервалам полного TDMA кадра (148 бит).

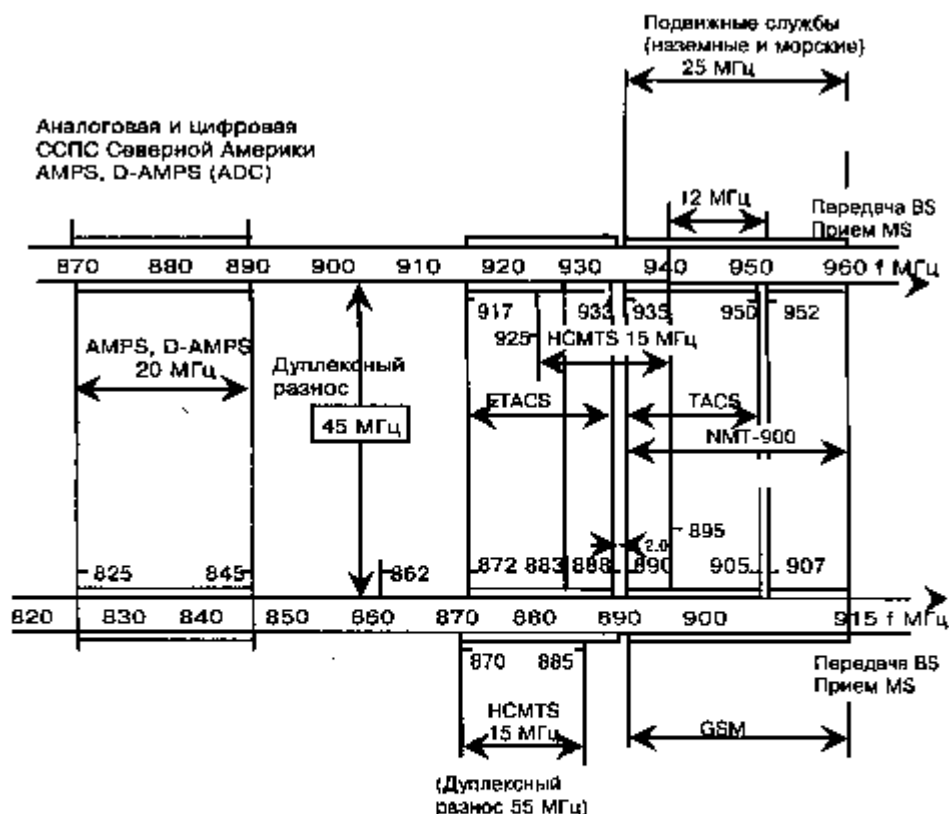
Одна из особенностей формирования сигналов в стандарте GSM - использование медленных скачков по частоте в процессе сеанса связи. Главное назначение таких скачков (SFH - Slow Frequency Hopping) - обеспечение частотного разнесения в радиоканалах, функционирующих в условиях многолучевого распространения радиоволн. SFH используется во всех подвижных сетях, что повышает эффективность кодирования и перемежения при медленном движении абонентских станций. Принцип формирования медленных скачков по частоте состоит в том, что сообщение, передаваемое в выделенном абоненту временном интервале TDMA кадра (577 мкс), в каждом последующем кадре передается (принимается) на новой фиксированной частоте. В соответствии со структурой кадров время для перестройки частоты составляет около 1 мс.

В процессе скачков по частоте постоянно сохраняется дуплексный разнос 45 МГц между каналами приема и передачи. Всем активным абонентам, находящимся в одной соте, ставятся в соответствие ортогональные формирующие последовательности, что исключает взаимные помехи при приеме сообщений абонентами в соте. Параметры последовательности переключения частот (частотно-временная матрица и начальная частота) назначаются каждой подвижной станции в процессе установления канала. Ортогональность последовательностей переключения частот в соте обеспечивается начальным частотным сдвигом одной и той же (по алгоритму формирования) последовательности. В смежных сотах используются различные формирующие последовательности.

ОРГАНИЗАЦИЯ ФИЗИЧЕСКИХ И ЛОГИЧЕСКИХ КАНАЛОВ В СТАНДАРТЕ GSM

Частотный план стандарта GSM

Стандарт GSM разработан для создания сотовых систем подвижной связи (СПС) в следующих полосах частот: 890-915 МГц - для передачи подвижными станциями (линия "вверх"); 935-960 МГц - для передачи базовыми станциями (линия "вниз"). Сети GSM функционируют параллельно с существующими европейскими национальными сетями аналоговых СПС стандартов NMT-900, TACS, ETACS. Частотные планы СПС, включая стандарт GSM, показаны на рис. 3.3.



- | | |
|--------------|---|
| GSM | - общеевропейский стандарт на цифровые СПС. |
| AMPS | - стандарт на аналоговые СПС Северной Америки. |
| D-AMPS (ADC) | - стандарт на цифровые СПС Северной Америки |
| TACS (ETACS) | - стандарт Великобритании на аналоговую СПС. |
| NMT-900 | - стандарт скандинавских стран на аналоговую СПС. |
| HCMTS | - стандарт на аналоговые СПС Японии. |

Рис.3.3. Частотные планы СПС.

Каждая из полос, выделенных для сетей GSM, разделяется на частотные каналы. Разнос каналов составляет 200 кГц, что позволяет организовать в сетях GSM 124 частотных канала. Частоты, выделенные для передачи сообщений подвижной станцией на базовую и в обратном направлении, группируются парами, организуя дуплексный канал с разномом 45 МГц. Эти пары частот сохраняются и при перескоках частоты. Каждая сота характеризуется фиксированным присвоением определенного количества пар частот.

Если обозначить $F_1(n)$ - номер несущей частоты в полосе 890-915 МГц, $F_u(n)$ - номер несущей частоты в полосе 935-960 МГц, то частоты каналов определяются по

следующим формулам:

$$F_I(n) = 890,2 + 0,2(n-1), \text{ МГц};$$

$$F_u(n) = F_I(n) + 45, \text{ МГц};$$

$$1 < n < 124.$$

Каждая частотная несущая содержит 8 физических каналов, размещенных в 8 временных окнах в пределах TDMA кадра и в последовательности кадров. Каждый физический канал использует одно и то же временное окно в каждом временном TDMA кадре. До формирования физического канала сообщения и данные, представленные в цифровой форме, группируются и объединяются в логические каналы двух типов: каналы связи - для передачи кодированной речи или данных (TCH); каналы управления - для передачи сигналов управления и синхронизации (CCH).

Более чем один тип логического канала может быть размещен на одном и том же физическом канале, но только при их соответствующей комбинации.

Структура логических каналов связи

В стандарте GSM различают логические каналы связи двух основных видов:

- TCH/F (Full Rate Traffic Channel) - канал передачи сообщений с полной скоростью 22,8 кбит/с (другое обозначение V_m);
- TCH/H (Half Rate Traffic Channel) - канал передачи сообщений с половинной скоростью 11,4 кбит/с (другое обозначение L_m).

Один физический канал может представлять собой канал передачи сообщений с полной скоростью или два канала с половинной скоростью передачи. В первом случае канал связи занимает одно временное окно; во втором - два канала связи занимают то же самое временное окно, но с перемежением в соседних кадрах (т.е. каждый канал - через кадр).

Для передачи кодированной речи и данных предназначены каналы связи следующих типов:

- TCH/FS (Full Rate Traffic Channel for Speech)
- канал для передачи речи с полной скоростью;
- TCH/HS (Half Rate Traffic Channel for Speech) :
- канал для передачи речи с половинной скоростью;
- TCH/F 9,6 (Full Rate Traffic Channel for 9,6 kbit/s User Data)
- канал передачи данных с полной скоростью 9,6 кбит/с;
- TCH/F 4,8 (Full Rate Traffic Channel for 4,8 kbit/s User Data)
- канал передачи данных с полной скоростью 4,8 кбит/с;
- TCH/F 2,4 (Full Rate Traffic Channel for 2,4 kbit/s User Data)
- канал передачи данных с полной скоростью 2,4 кбит/с;
- TCH/H 4,8 (Half Rate Traffic Channel for 9,6 kbit/s User Data)
- канал передачи данных с половинной скоростью 4,8 кбит/с;
- CH/H 2,4 (Half Rate Traffic Channel for 9,6 kbit/s User Data)
- канал передачи данных с половинной скоростью 2,4 кбит/с.

Скорость передачи цифрового речевого сигнала в канале TCH/FS равна 13 кбит/с (за счет кодирования увеличивается до 22,8 кбит/с в канале TCH/F).

Каналы связи могут передавать широкий набор информационных сообщений, но они не используются для передачи сигналов управления. Кроме того, для передачи данных по каналам связи могут использоваться разные протоколы, например, МСЭ-Т X.25.

Структура логических каналов управления

Каналы управления (CCH) обеспечивают передачу сигналов управления и синхронизации.

Различают четыре вида каналов управления:

- BCCH (Broadcast Control Channels)
- каналы передачи сигналов управления;
- CCCH (Common Control Channels)
- общие каналы управления;
- SDCCCH (Stand-alone Dedicated Control Channels)
- индивидуальные каналы управления;
- ACCH (Associated Control Channels)
- совмещенные каналы управления.

Каналы передачи сигналов управления используются только в направлении с базовой станции на все подвижные станции. Они несут информацию, которая необходима подвижным станциям для работы в системе. Различают три вида каналов передачи сигналов управления BCCH:

- FCCH (Frequency Correction Channel)
- канал подстройки частоты, который используется синхронизации несущей в подвижной станции. По этому каналу передается немодулированная несущая с фиксированным частотным сдвигом относительно номинального значения частоты канала связи;
- SCH (Synchronization Channel)
- канал синхронизации, по которому передается информация на подвижную станцию о кадровой (временной) синхронизации;
- BCCH (Broadcast Control Channel)
- канал управления передачей, обеспечивает передачу основных команд по управлению передачей (номер общих каналов управления тех из них, которые объединяются с другими каналами, в том числе и с физическими и т.д.).

Используются три типа общих каналов управления CCCH:

- PCH (Paging Channel)
- канал вызова, используется только в направлении от базовой станции к подвижной для ее вызова;
- RACH (Random Access Channel)
- канал параллельного доступа, используется только в направлении от подвижной станции к базовой для запроса о назначении индивидуального канала управления;
- AGCH (Access Grant Channel) - канал разрешенного доступа, используется только для передачи с базовой станции на подвижную (для выделения специального канала управления, обеспечивающего прямой доступ к каналу связи).

Выделенные индивидуальные каналы управления используются в двух направлениях для связи между базовой и подвижной станциями. Различают два вида таких каналов:

- SDCCCH/4 (Stand-alone Dedicated Control Channel)
- индивидуальный канал управления, состоит из четырех подканалов;
- SDCCCH/8 (Stand-alone Dedicated Control Channel)
- индивидуальный канал управления, состоит из восьми подканалов.

Эти каналы предназначены для установки требуемого пользователем вида обслуживания. По ним обеспечивается запрос подвижной станции о требуемом виде обслуживания, контроль правильного ответа базовой станции и выделение свободного канала связи, если это возможно.

Совмещенные каналы управления также используются в двух направлениях между базовой и подвижной станциями. По направлению "вниз" они передают команду управления с базовой станции, а по направлению "вверх" - информацию о статусе подвижной станции. Различают два вида ACCH:

- FАССН (Fast Associated Control Channel) - быстрый совмещенный канал управления, служит для передачи команд при переходе подвижной станции из соты в соту, т.е. при "эстафетной передаче" подвижной станции;
- SАССН (Slow Associated Control Channel) - медленный совмещенный канал управления, по направлению "вниз" передает команды для установки выходного уровня мощности передатчика подвижной станции. По направлению "вверх" подвижная станция посылает данные, касающиеся уровня установленной выходной мощности, измеренного приемником уровня радиосигнала и его качества.

В совмещенном канале управления всегда содержится один из двух каналов: канал связи или индивидуальный канал управления.

Совмещенные каналы управления всегда объединяются вместе с каналами связи или с индивидуальными каналами управления. При этом различают шесть видов объединенных каналов управления:

- FАССН/F, объединенный с ТСН/F;
- FАССН/H, объединенный с ТСН/H;
- SАССН/TF, объединенный с ТСН/F;
- SАССН/ТН, объединенный с ТСН/H;
- SАССН/C4, объединенный с SDCСН/4;
- SАССН/C8, объединенный с SDCСН/8.

Организация физических каналов

Для передачи каналов связи ТСН и совмещенных каналов управления FАССН и SАССН используется 26-кадровый мультикадр. В полноскоростном канале связи в каждом 13-м TDMA кадре мультикадра передается пакет информации канала SSАССН; каждый 26-й TDMA кадр мультикадра свободен. В полускоростном канале связи пакет информации канала SАССН передается в каждом 13-м и 26-м TDMA кадрах мультикадра.

Для одного физического канала в каждом TDMA кадре используется 114 бит. Так как в мультикадре для передачи канала связи ТСН используется 24 TDMA кадра из 26 и длительность мультикадра составляет 120 мс, общая скорость передачи информационных сообщений по ТСН каналу составляет 22,8 кбит/с. Канал SАССН занимает в полноскоростном канале связи только один TDMA кадр, то есть 114 бит, когда скорость передачи по SАССН каналу составит 950 бит/с. Полная скорость передачи в объединенном ТСН/SАССН канале с учетом пустого (свободного) 26-го TDMA кадра составит $22,8 + 0,950 + 0,950 = 24,7$ кбит/с.

За время 26-кадрового мультикадра (в одном физическом канале) может передаваться два полускоростных ТСН канала, каждый по 12 TDMA кадров (Т и t). Пустой 26-й TDMA кадр в полноскоростном канале ТСН отводится для канала SАССН во втором полускоростном канале ТСН. Для каждого полускоростного канала ТСН скорость передачи составляет 11,4 кбит/с; полная скорость передачи в объединенном полускоростном канале ТСН/SАССН остается прежней - 24,7 кбит/с.

Быстрый совмещенный канал управления FАССН передается половиной информационных бит временного интервала TDMA кадра в канале ТСН, с которым он совмещается в восьми последовательных Т или t кадрах.

Для передачи каналов управления (за исключением FАССН и SАССН) используется 51-кадровый мультикадр.

Объединение ВССН/СССН каналов

В отличие от структуры объединенного канала ТСН/SАССН, где физический канал выделяется для одного или двух абонентов, объединенный канал ВССН/СССН предназначен для всех подвижных станций, которые в одно и то же время находятся в одной соте. Более того, все подканалы, передаваемые в этой структуре, являются симплексными.

В канале передачи сигналов управления (BCCH, "сеть - подвижная станция") передается общая информация о сети (соте), в которой подвижная станция находится в данный момент, и о смежных сотах.

В канале синхронизации (SCH, "сеть - подвижная станция") передается информация о временной (цикловой) синхронизации и опознавании приемопередатчика базовой станции.

В канале подстройки частоты (FCCH, "сеть - подвижная станция") передается информация для синхронизации несущей.

Канал параллельного доступа (RACH, "подвижная станция - сеть") используется подвижной станцией в режиме пакетной передачи ALOHA для доступа к сети в случае, если надо пройти регистрацию при включении или сделать вызов.

Канал разрешенного доступа (AGCH, "сеть - подвижная станция") используется для занятия специальных видов обслуживания (SDCCH или TCH) подвижной станцией, которая ранее запрашивала их через канал RACH.

Канал вызова (PCH, "сеть - подвижная станция") используется для вызова подвижной станции в случае, когда инициатором вызова является сеть (абонент сети).

Линия "вверх" BCCH/CCCH каналов используется только для передачи канала параллельного доступа RACH, который является единственным каналом управления от подвижной станции к сети. Подвижная станция может использовать нулевой временной интервал в любом из кадров для осуществления доступа к сети.

На линии "вниз" 51 кадр группируется в 5 групп по 10 кадров, при этом один кадр остается свободным, каждая из этих групп начинается с канала FCCH, за которым следует канал SCH. Остальные 8 кадров в каждой группе образуют два блока из четырех кадров. Первый блок первой группы предназначен для канала CCH, тогда как другие 9 блоков (они называются блоками передачи сигнала вызова) используются для передачи каналов PCH и AGCH общего канала управления CCCH. Таким образом, в рассматриваемом случае: 4 кадра используются для канала BCCH, 5 - для FCCH, 5 - для SCH и 36 либо для AGCH, либо для PCH (9 блоков вызова).

Каждая подвижная станция может занимать один из девяти блоков вызова, но каждый вызывной блок может использоваться для вызова более одной станции.

Полная скорость передачи для канала BCCH, а также для канала AGCH/PCH составляет 1,94 кбит/с (4х114 бит за 235 мс).

Существуют и другие переменные структуры, которые могут использоваться в 51-кадровом мультикадре. "Переменными" их называют потому, что их структура изменяется в зависимости от нагрузки в соте. В одном случае может рассматриваться индивидуальный канал управления 8SDCCH/8 в одном физическом канале. Однако, если нагрузка в соте мала, структуру BCCH/CCCH можно объединить с индивидуальным каналом управления SDCCH/4 в одном физическом канале. Если сота испытывает большую нагрузку, одного физического канала может быть недостаточно для всего трафика BCCH/CCCH. В этом случае временные интервалы 2, 4 и 6 в структуре BCCH также используют для этой цели, однако в этом случае передаются пустые интервалы вместо SCH и FCCH.

Отображение логических каналов на физические каналы осуществляется через процессы кодирования и шифрования передаваемых сообщений.

Для защиты логических каналов от ошибок, которые имеют место в процессе передачи, используют три вида кодирования: блочное - для быстрого обнаружения ошибок при приеме; сверхточное - для исправления одиночных ошибок; перемежение - для преобразования пакетов ошибок в одиночные.

Для защиты каналов от подслушивания в каналах связи и управления применяется шифрование.

Для передачи сообщений по физическим каналам используется гауссовская частотная манипуляция с минимальным частотным сдвигом (GMSK).

Модуляция радиосигнала

В стандарте GSM применяется спектрально-эффективная гауссовская частотная манипуляция с минимальным частотным сдвигом (GMSK). Манипуляция называется "гауссовской" потому, что последовательность информационных бит до модулятора проходит через фильтр нижних частот (ФНЧ) с характеристикой Гаусса, что дает значительное уменьшение полосы частот излучаемого радиосигнала. Формирование GMSK радиосигнала осуществляется таким образом, что на интервале одного информационного бита фаза несущей изменяется на 90° . Это наименьшее возможное изменение фазы, распознаваемое при данном типе модуляции. Непрерывное изменение фазы синусоидального сигнала дает в результате частотную модуляцию с дискретным изменением частоты. Применение фильтра Гаусса позволяет при дискретном изменении частоты получить "гладкие переходы". В стандарте GSM применяется GMSK-модуляция с величиной нормированной полосы ВТ - 0,3, где В - ширина полосы фильтра по уровню минус 3 дБ, Т - длительность одного бита цифрового сообщения. Основой формирователя GMSK-сигнала является квадратурный (1/Q) модулятор. Схема состоит из двух умножителей и одного сумматора. Задача этой схемы заключается в том, чтобы обеспечить непрерывную, очень точную фазовую модуляцию. Один умножитель изменяет амплитуду синусоидального, а второй косинусоидального колебания. Входной сигнал до умножителя разбивается на две квадратурные составляющие. Разложение происходит в двух обозначенных "sin" и "cos" блоках.

Модуляцию GMSK отличают следующие свойства, которые предпочтительны для подвижной связи:

- постоянная по уровню огибающая, которая позволяет использовать эффективные передающие устройства с усилителями мощности в режиме класса С;
- компактный спектр на выходе усилителя мощности передающего устройства, обеспечивающий низкий уровень внеполосного излучения;
- хорошие характеристики помехоустойчивости канала связи.

КОДИРОВАНИЕ И ПЕРЕМЕЖЕНИЕ В КАНАЛАХ СВЯЗИ И УПРАВЛЕНИЯ СТАНДАРТА GSM

Общая структурная схема кодирования и перемежения в стандарте GSM

Для защиты от ошибок в радиоканалах подвижной связи GSM PLMN используются сверточное и блочное кодирование с перемежением. Перемежение обеспечивает преобразование пакетов ошибок в одиночные. Сверточное кодирование является мощным средством борьбы с одиночными ошибками. Блочное кодирование, главным образом, используется для обнаружения нескорректированных ошибок.

Блочный код (n, k, t) преобразует k информационных символов в n символов путем добавления символов четности (n-k), а также может корректировать t ошибок символов.

Сверточные коды (СК) относятся к классу непрерывных помехоустойчивых кодов. Одной из основных характеристик СК является величина K, которая называется длиной кодового ограничения, и показывает, на какое максимальное число выходных символов влияет данный информационный символ. Так как сложность декодирования СК по наиболее выгодному, с точки зрения реализации, алгоритму Витерби возрастает экспоненциально с увеличением длины кодового ограничения, то типовые значения K малы и лежат в интервале 3-10. Другой недостаток СК заключается в том, что они не могут обнаруживать ошибки. Поэтому в стандарте GSM для внешнего обнаружения ошибок используется блочный код на основе сверточного кода (2, 1, 5) со скоростью $r=1/2$. Наибольший выигрыш СК обеспечивает только при одиночных (случайных) ошибках в канале.

В каналах с замираниями, что имеет место в GSM PLMN, необходимо использовать СК совместно с перемежением.

В GSM PLMN основные свойства речевых каналов и каналов управления значительно отличаются друг от друга. Для речевых каналов необходима связь в реальном масштабе времени с короткими задержками при сравнительно низких требованиях к вероятности ошибки в канале. Для каналов управления требуется абсолютная целостность данных и обнаружения ошибок, но допускается более длительное время передачи и задержки.

В соответствии с общей структурой кадров в стандарте GSM передача информационных сообщений и сигналов управления осуществляется в нормальном временном интервале (NB) TDMA кадра. Структура NB (два пакета по 57 информационных бит каждый) требует, чтобы количество кодированных бит m , соответствующих n - некодированным битам в общей схеме кодирования и перемежения, равнялась бы целому числу, кратному 19. Затем эти биты зашифровываются и объединяются в I групп. Количество бит в этих группах также должно равняться 19, I групп переходят в I временных интервалов. Номер I называется степенью перемежения.

В различных логических каналах используются различные сверточные коды, поскольку скорости передачи и требования по защите от ошибок также различны. Для упрощения механизмов кодирования и декодирования для формирования кодов используются только несколько полиномов. Это позволяет использовать сверточный код с одной скоростью $\gamma=1/2$. Однако, чтобы выполнить требования формирования полноскоростного канала связи, а также привести в соответствие структуру размещения бит со структурой кадров необходима скорость $\gamma=244/456=0,535$. Для выравнивания скорости в речевом канале до $\gamma=1/2$ применяют прореживание, то есть периодический пропуск некоторых кодированных символов. Такая операция называется перфорированием, а формируемые таким образом коды называются перфорированными. При приеме декодер, зная алгоритм прореживания, интерполирует принимаемые данные.

При передаче логического быстрого совмещенного канала управления FASCH перфорирование не используется.

Кодирование и перемежение в полноскоростном канале передачи данных

Для повышения эффективности применения сверточного кодирования в полноскоростных каналах передачи данных необходим длительный период перемежения. В этих каналах внутрикадровое перемежение (IBI/B) реализуется для степени перемежения $I=19$, что приводит к задержке передачи данных на $19 \times 116 = 2204$ бит. Если биты I -го пакета (временного интервала) до перемежения обозначить как $C(K, m)$, $m=1 \dots 116$, то схема перемежения, то есть позиции бит после перемежения, определяются следующей формулой:

$I(K + j, j + 19t) = C(K, t)$ для всех K

$j = m \bmod 19, t = m \bmod 6$.

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

- 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 зашифрованному;

второй - для обратного перехода от зашифрованного 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. 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 открытым ключом был назван RSA (первые буквы фамилий авторов Rivest, Shamir, Adleman). 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 E_x и секретный D_x .

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

- зашифровать сообщение M ;
- подписать сообщение M ;

- зашифровать и подписать M .

В первом случае: A обеспечивает преобразование M , используя открытый ключ $C = EB(M)$ и посылает его абоненту B . B принимает C и вычисляет $DB(C) = DB(EB(M)) = M$.

Во втором случае: A подписывает M посредством вычисления $F = DA(M)$ и посылает F абоненту B (эти операции может осуществлять только пользователь A , которому известен секретный ключ DA). B получает F и вычисляет $EA(F) = EA(DA(M)) = M$.

В теперь известно, что сообщение M действительно послано пользователем A . В этом случае секретность сообщения M не гарантируется, так как все могут осуществить такую же операцию с использованием общего ключа EA .

В третьем случае: A вычисляет

$$F = DA(M) \text{ и } C = EB(F) = EB(DA(M));$$

A посылает C к B . B получает C и вычисляет $DB(C) = DB(EB(F)) = DA(M)$;

B может теперь легко получить M , вычислив $EA(DA(M)) = M$.

До операции шифрования и подписи каждое сообщение M 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.

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 :

- 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 ниже.

Таблица 3.4

GSM 02.09	Аспекты секретности	Определяет характеристики безопасности, применяемые в сетях GSM. Регламентируется их применение в подвижных станциях и сетях
GSM 03.20	Секретность, связанная с функциями сети	Определяет функции сети, необходимые для обеспечения характеристик безопасности, рассматриваемых в рекомендациях GSM 02.09
GSM 03.21	Алгоритмы секретности	Определяет криптографические алгоритмы в системе связи
GSM 02.17	Модули подлинности абонентов (SIM)	Определяет основные характеристики модуля SIM

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 (K_i);
- 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, K_i и алгоритм A3:
$$SRES = K_i [RAND].$$

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 K_i) не подвергается обработке в модуле SIM.

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 (K_c), используя RAND, K_i и алгоритм A8 : $K_c = K_i [RAND]$.

Ключ шифрования K_c не передается по радиоканалу. Как подвижная станция, так и сеть вычисляют ключ шифрования, который используется другими подвижными абонентами. По причине секретности вычисление K_c 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 K_c 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 СМС (Ciphering Mode Command) на переход в режим шифрования. После получения команды СМС 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 K_c .

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. При этом по каналу связи передается как зашифрованный информационный текст с прерыванием сообщения в процессе "эстафетной передачи" на 100-150 мс.

Процедура корректировки местоположения, включающая характеристики секретности, показаны на рис. 3.4.

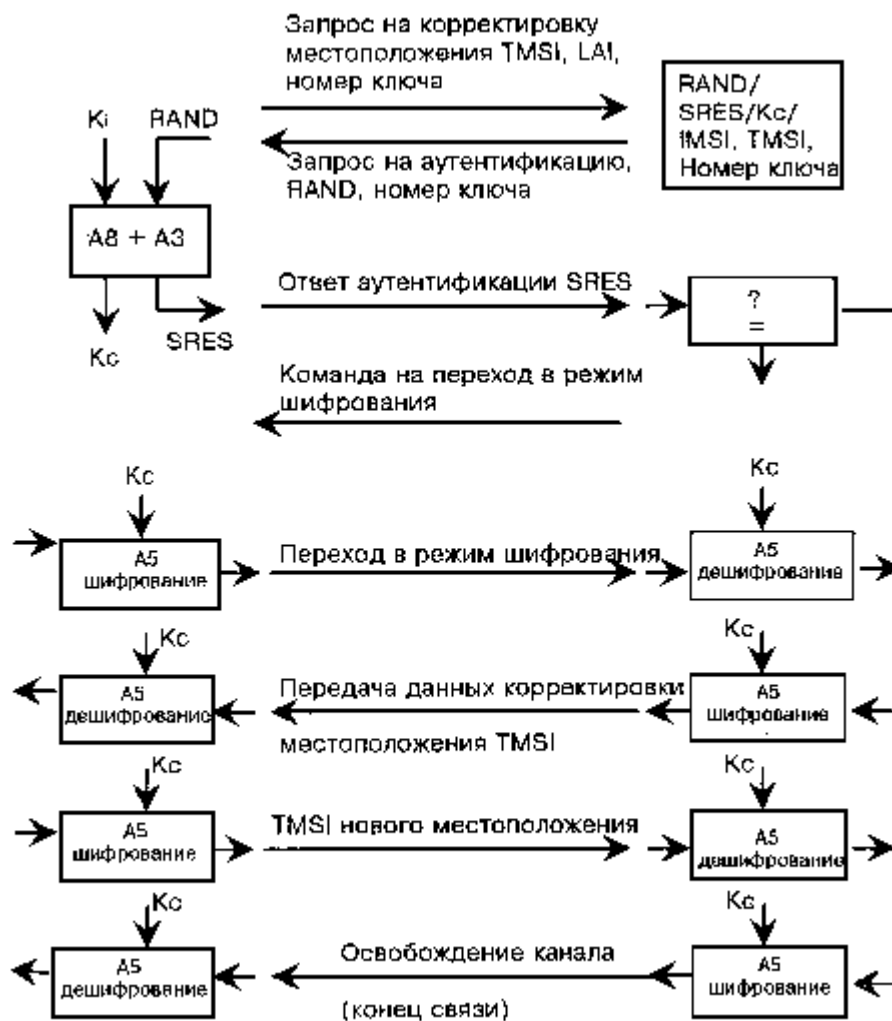


Рис 3.4. Процедура корректировки местоположения.

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;
- SRES - значение отклика - ответ подвижной станции на полученное случайное число;
- Ki - индивидуальный ключ аутентификации пользователя, используемый для вычисления, значения отклика и ключа шифрования;
- Kc - ключ шифрования, используемый для шифрования/дешифрования сообщений, сигналов управления и данных пользователя в радиоканале;
- A3 - алгоритм аутентификации, используемый для вычисления значения отклика из случайного числа с использованием ключа Ki;
- A8 - алгоритм формирования ключа шифрования, используемый для вычисления ключа Kc из случайного числа с использованием ключа Ki;
- A5 - алгоритм шифрования/дешифрования сообщений, сигналов управления и данных пользователя с использованием ключа Kc;
- CKSN - номер ключевой последовательности шифрования, указывает на действительное число Kc, чтобы избежать использования разных ключей на передающей и приемной сторонах;
- TMSI - временный международный идентификационный номер пользователя.

Таблица 3.5

Номер	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 номер TMSI с наименованием зоны расположения LAI. Новый VLR запрашивает прежний VLR для отправки 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.

Эволюция стандарта GSM

Когда в 1991 г. появились первые сети GSM главное внимание уделялось обеспечению ими услуг речевой связи на достойном уровне по сравнению с существовавшими тогда аналоговыми сотовыми системами. Однако уже с самого начала технология GSM была способна предложить несколько новых видов услуг, которые незамедлительно привлекли внимание определенной категории пользователей. Наиболее существенными нововведениями стали возможности шифрования передаваемой информации и роуминга по всей Европе.

Следующим шагом развития GSM было введение услуг пересылки коротких сообщений (Short Message Service SMS) и передачи данных. Сначала возможности услуг SMS ограничивались уведомлением о поступлении сообщения в ящик голосовой почты. С 1995 г., сервис SMS стал расширяться. Сегодня пользователи систем GSM имеют возможность посылать друг другу короткие сообщения непосредственно с телефонной трубки или через компьютерные сети. Период с конца 1994 г. до начала 1995 г. время бурного развития услуг передачи данных. Это было обусловлено появлением привлекательных радиотелефонов и тем, что значительное число сетей GSM стали способны поддерживать такие услуги. Широкое распространение портативных ПК позволяет абонентам сетей GSM получать доступ к компьютерным системам их офисов, а также посылать и принимать сообщения электронной почты через сети GSM.

Изначально развитие GSM планировалось таким образом, что любая новая услуга или техническое новшество должны были вводиться одновременно во всех сетях GSM. Это привело к так называемому поэтапному развитию GSM. Введение в строй сетей GSM в 1991 г. было, фактически, первым этапом. Второй этап развития GSM обеспечил такие дополнительные услуги, как, определение номера вызывающего абонента, удержание линии, групповой вызов, определение закрытой группы абонентов, выдача информации о плате за разговор. Другое важное новшество, которое было реализовано вскоре после завершения второго этапа, кодирование речи с половинной скоростью. Этот шаг направлен на увеличение пропускной способности систем GSM.

На третьем этапе упор был сделан на улучшение полноскоростного кодирования речи; высокоскоростной передачи данных по коммутируемым каналам (High Speed Circuit Switched Data - HSCSD); пакетной передачи данных (General Packet Radio Service - GPRS); сжатие данных; групповые и широковещательные вызовы; взаимодействие между системами GSM и DECT.

SMS

Структура взаимодействия центра SMS с коммутаторами мобильной связи и внешними сетями

Базовой функцией технологии SMS является предоставление абоненту возможности передавать и принимать алфавитноцифровые сообщения на дисплей мобильного телефона. При этом процессы обмена речевыми и текстовыми сообщениями в общем случае являются независимыми. На рис. “Структура взаимодействия центра SMS с коммутаторами мобильной связи и внешними сетями” схематично показаны основные элементы систем сетей мобильной связи и других информационных сетей, взаимодействующих с центром SMS в процессе обмена сообщениями.

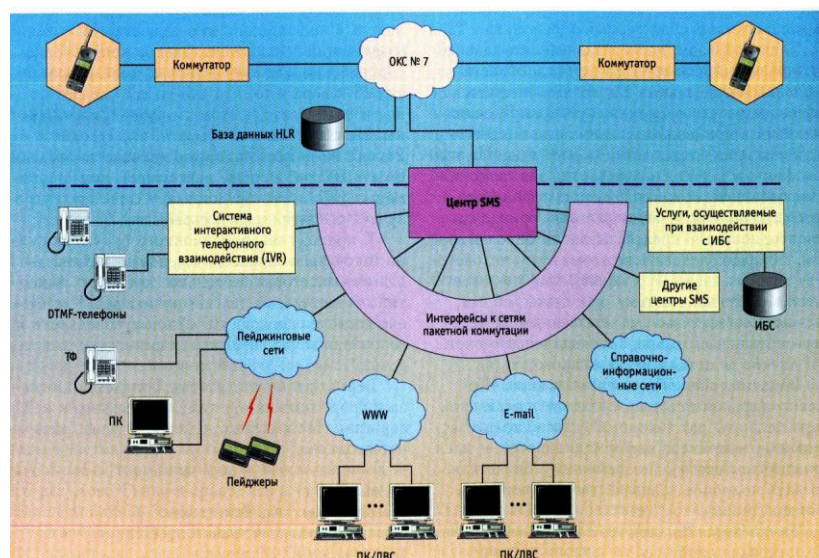


Рис. 3.5 Структура взаимодействия центра SMS с коммутаторами мобильной связи и внешними сетями

Верхняя часть рисунка иллюстрирует работу мобильной сети в минимальной конфигурации - обмен осуществляется короткими сообщениями между двумя абонентами. При этом технология обеспечивает следующие возможности:

- Доставка сообщения без занятия речевого канала. Такая доставка не только является более экономичным способом обмена информацией, так как не требует задействования дорогостоящих канальных коммутационных ресурсов, но и увеличивает скорость доставки срочной информации, поскольку сообщение поступает даже в том случае, если речевой канал занят.
- Подтверждение отправителю факта доставки информации (нотификация).
- Независимость процесса обмена сообщениями от места нахождения абонента (при роуминге) и, как следствие, отсутствие дополнительных расходов за междугородный/международный трафик. Так, один абонент может послать другому сообщение из другой страны и оплачивать его по обычному внутреннему тарифу.

Поступающие в центр SMS короткие сообщения фиксируются в базе данных системы и отправляются адресатам в соответствии с прописанной схемой доставки. Доставленное сообщение удаляется из базы данных (схема удаления тоже является настраиваемой). Для организации маршрута доставки сообщения центр SMS взаимодействует с базой данных HLR (Home Location Register - база данных с информацией о клиентах оператора мобильной связи). В случае невозможности доставить сообщение в данный момент времени (абонент находится вне зоны обслуживания, в метро или терминал выключен) центр SMS периодически возобновляет попытки передачи (после активизации терминала). Длина сообщения для технологии SMS определяется соответствующими стандартами и может достигать до 160 символов.

Несмотря на очевидную привлекательность и удобство перечисленных выше возможностей, следует тем не менее выделить главное достоинство технологии SMS - ее способность интегрироваться с другими сетевыми информационными технологиями и предоставлять абоненту мобильной сотовой сети универсальное средство эффективного доступа ко всему многообразию типов и видов передачи текстовой информации. Иными словами, технология SMS обеспечивает возможность взаимодействия и обмена информацией между абонентами различных сетей (см. нижнюю часть рисунка).

Работа с системой интерактивного речевого взаимодействия

Взаимодействие центра SMS с системой IVR (Interactive Voice Response - интерактивное речевое взаимодействие) позволяет посылать на мобильный телефон короткие сообщения с телефона как фиксированной, так и любой другой телефонной сети. Единственное условие здесь - наличие у телефонного аппарата возможностей тонового набора. В рамках сеанса взаимодействия с системой IVR отправитель имеет возможность либо выбрать и отправить predetermined сообщение из имеющейся библиотеки (например, “С добрым утром”, “С Новым годом”), либо самостоятельно набрать сообщение с клавиатуры телефона (в последнем случае желательно, чтобы на аппарате отправителя имелся дисплей).

Взаимодействие со службой Web

Интеграция центра SMS со службой Web позволяет любому пользователю ПЭВМ, подключенному к сети Интернет, обмениваться короткими сообщениями с абонентом сотовой сети. При этом возможны следующие варианты обмена сообщениями:

- Отправка сообщения с ПЭВМ на “трубку” - отправитель из Web-интерфейса вводит идентификатор интересующего его абонента (в общем случае номер телефона), текст сообщения и нажимает кнопку, инициирующую отправку этого сообщения абоненту.

- Прием посланного с трубки сообщения через Web-сервер. Такую возможность технология SMS предоставляет посредством размещения посланных сообщений на сайте оператора. Абонент сети сотовой связи (подписчик услуги SMS) может открыть соответствующую страницу и прочитать оставленные ему сообщения с любого подключенного к Интернет компьютера с Web-браузером, независимо от своего местонахождения. Такая возможность особенно важна в тех случаях, когда абонент, перемещаясь, выходит из зоны охвата сотовой сети, но имеет доступ к Интернет. В результате абонент оказывается доступным и за пределами зоны охвата. Следует упомянуть, что рассмотренный доступ удобен и сам по себе, особенно при прочтении большого объема накопившихся сообщений.

Естественно, что возможность получения абонентом информации предполагает процедуру идентификации обращающегося. Вопрос о том, размещать или не размещать адресованную ему информацию на Web-сервере (иными словами, дублировать ее или нет) решает сам абонент путем выполнения индивидуальных настроек, которые также могут осуществляться в режиме интерактивного обмена короткими сообщениями.

Работа с электронной почтой

Взаимодействие центра SMS и электронной почты позволяет абоненту мобильной сети динамично отслеживать поступление новых сообщений и вести обмен сообщениями. Технология обеспечивает следующие варианты обмена:

- Отправка сообщения E-mail с “трубки”. Абонент набирает на дисплее трубки адрес и текст сообщения и передает эту информацию центру SMS, который обеспечивает отправку сообщения по заданному адресу.

- Получение сообщения E-mail абонентом мобильной сети на “трубку”. Каждому абоненту сотовой сети ставится в соответствие некий электронный адрес, идентифицирующий его в пространстве электронных адресов данного оператора (например, абонент с номером 9876543 может иметь электронный адрес 9876543@mail.mobil.com). Поступающая на этот адрес электронная почта направляется центром SMS на мобильный телефон абонента. В зависимости от объема письма будет посылаться либо все сообщение, либо его часть. Получение абонентом мобильной сети

уведомлений о поступлении электронной почты. В этом случае абонент будет оперативно принимать на трубку сообщения о поступлении новых электронных писем. Настройки данного сервиса позволяют получать либо просто информацию о количестве новых писем (например, “5 new E-mail”), либо краткую информацию о письме - отправитель, дата отправки, тема и др. Оперативная информированность позволит абоненту в удобном ему месте принять весь объем почты с помощью ПЭВМ.

Взаимодействие с ИБС и управление услугами

Технология SMS предоставляет оператору мощный инструмент в части организации предоставления абонентам сотовых сетей широкого спектра услуг, связанных с функционированием информационно-биллинговой системы (ИБС).

Как известно, большинство услуг, предоставляемых абоненту сети мобильной связи, платные. Тарифы на них и динамику их использования отслеживает ИБС. С одной стороны, возможность оперативного включения и отключения определенных услуг и управления ими позволила бы абоненту оптимизировать эксплуатацию “трубки”, т. е. получить максимальный сервис при минимуме затрат. С другой стороны, уверенность в том, что он не переплачивает, снижает для абонента психологический порог при подписке на новые, предлагаемые оператором услуги. Для операторов же этот процесс означает упрощение введения новых сервисов, увеличение графика и рост общего дохода. Именно такую возможность оперативного и динамического управления услугами и предоставляет технология SMS.

Сервис коротких текстовых сообщений реализует для абонента интерактивный режим взаимодействия с ИБС и компонентами активизации услуг мобильной связи. Рассмотрим некоторые типовые примеры такого взаимодействия:

- Запрос об остатке на счете. Позволяет абоненту сети получить данные о состоянии своего счета, сделав стандартный запрос.
- Информирование о приближении к порогу отключения. Заблаговременно уведомляет абонента о приближении к порогу отключения и о тех действиях, которые оператор предпримет при достижении известного минимального значения баланса. Это, как правило, постепенное, пошаговое отключение услуг, а затем и собственно связи.
- Информирование абонента о скорости расходования средств в процессе разговора. Позволяет абоненту посредством стандартного запроса контролировать динамику расходования средств.
- Прием платежей по картам авансовых платежей. Абонент формирует сообщение по активации карты (информация о номере карты, ее номинале или величине оприходуемой суммы при частичной активации) и отправляет его. В ответ поступает сообщение, подтверждающее увеличение баланса на соответствующую сумму. Данный способ выгодно отличается от активизации карт в системе IVR, так как при этом не только не занимается речевой канал, но и все происходит наглядно, одной итерацией, без возможных при речевых итерациях ошибок и необходимости их исправления.
- Подключение и отключение услуг. Абонент короткой командной строкой может включать или отключать практически любые из предоставляемых ему оператором услуг:
 - включение/отключение роуминга при пересечении границы государства;
 - включение/отключение услуги постоянного информирования о чем-либо (например, о поступлении E-mail);
 - включение/отключение услуг речевой почты, получения рекламной информации и т. п.

Работа со справочно-информационными сетями

Взаимодействие со справочно-информационными общественными и коммерческими сетями - а их число непрерывно растет - позволяет абоненту иметь на

экране дисплея самую разнообразную оперативную информацию, спектр которой в перспективе ограничен только фантазией поставщиков такой информации.

Говоря о получении на дисплей мобильного телефона информации, следует различать два возможных режима ее поступления:

- Режим “пассивного” получения циркулярно рассылаемой информации, подписчиком на которую является данный абонент. Такой информацией уже сегодня могут быть курс основных валют, прогноз погоды, новости и т. п., Периодичность получения данных в таком режиме задается самим абонентом.

- Режим интерактивного взаимодействия с информационными базами данных посредством коротких сообщений. Такой режим обеспечивает гибкое перемещение по базе данных и позволяет абоненту проникнуть на любой уровень глубины и детализации информации. Примерами такого применения могут быть телебанкинг, получение кросскурсов валют, котировок на бирже, расписания движения транспорта, информации о товарах и услугах и пр.

Концепция технологии SMS

В рамках возможностей сигнализации ОКС № 7 технология SMS для своего воплощения подразумевает программно-аппаратную реализацию трех уровней подсистемы передачи сообщений (MTP1, MTP2 и MTP3), уровня управления соединениями SCCP и уровня подсистемы поддержки транзакций TCAP (см. рисунок).

Уровень SCCP в данном случае отвечает за передачу блоков данных сигнализации (собственно сообщений) в рамках процедур услуг, не ориентированных на соединение.

Уровень TCAP (взаимодействуя с SCCP и MTP) в технологии SMS обеспечивает корректность передачи сообщений через сеть (подуровень транзакций TSL) и результативность этих передач (компонентный подуровень CSL). На рисунке показаны все эти реализуемые технологией SMS компоненты, а также компоненты, отвечающие за организацию мобильной связи для стандартов GSM (подсистема MAP) и NMT (подсистема MUP).

При проектировании современного центра SMS учитываются основополагающие принципы модели взаимодействия открытых систем (OSI), что позволяет интегрировать решения технологии SMS в единую аппаратно-программную масштабируемую платформу для всего многообразия внедряемых служб сети. Такая концепция архитектуры позволяет операторам минимизировать затраты на внедрение новых технологий, таких, как IVR (интерактивное речевое взаимодействие), Prepaid (предоплаченные телефонные карты), VMS (речевая почта), и осуществлять их на базе универсального контроллера, реализующего все необходимые компоненты передачи и управления соединениями, причем как для подуровней сервисов, ориентированных на соединение, так и для сервисов с коммутацией пакетов, а также для их комбинаций. Подсистемы ISUP и INAP наряду с рассмотренными выше позволяют внедрять весь комплекс современных услуг связи.

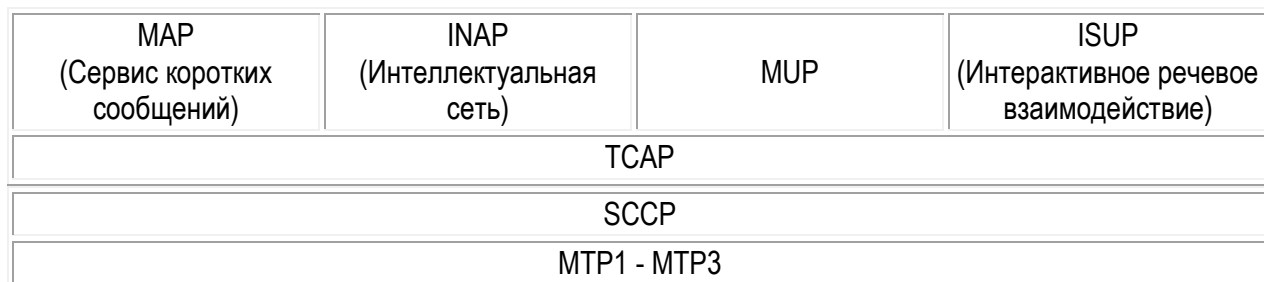


Рис. 3.6 Место сервиса SMS в структуре протоколов ОКС N 7

В ходе внедрения технологии SMS оператор сети мобильной связи попутно решает две важные задачи:

- повышение информативной плотности имеющихся канальных ресурсов за счет использования возможностей сигнализации ОКС № 7 для передачи данных;
- углубление интеграции ресурсов и служб сети.

General Packet Radio Service

Протокол GPRS (пакетный радио-сервис общего назначения) используется для передачи данных, обеспечивая мобильным сетям совместимость с сетью Интернет. GPRS использует пакетную технологию для эффективной передачи неравномерного (burst) трафика. Протокол поддерживает скорость передачи от 9,6 Кбайт/с до более чем 150 Кбайт/с на одного пользователя.

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, мы можем изучать содержимое столько, сколько нам необходимо, поскольку платим только за принятую информацию и не платим за время нахождения в сети Интернет (не передавая данные, мы не занимаем 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 - браузером, 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 появится 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.

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 (Gateway GPRS Support Node). Он обеспечивает связь системы GPRS с пакетными сетями передачи

данных: Internet, 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.

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 В - 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 С – терминал работает только в режиме 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.

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, 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 во время веб-браузинга он включается редко, что снижает мощность излучения до нескольких милливатт.

Основными характеристиками протокола GPRS являются эффективное использование радио- и сетевых ресурсов, а также полностью прозрачная поддержка протокола IP. GPRS оптимизирует использование сетевых и радиоресурсов. Протокол GPRS использует радиоресурсы только в тех случаях, когда реально требуется принять или передать данные. Используя пакетную технологию, этот протокол позволяет приложениям использовать сетевые ресурсы только тогда, когда пользовательские приложения имеют данные для передачи через сеть. Таким образом, протокол адаптирован к неравномерному характеру графика пользовательских приложений. Еще одной важной характеристикой GPRS является обеспечение немедленного соединения и высокая пропускная способность. Поддерживаются приложения, базирующиеся на стандартных протоколах передачи данных, таких, как IP и X.25. В GPRS обесточиваются 4 различных уровня качества обслуживания. Для поддержки приложений передачи данных Протокол GPRS использует несколько новых сетевых узлов, в дополнение к сетевым узлам, применяемым в GSM PLMN. Эти узлы отвечают за маршрутизацию трафика и реализацию других функций обмена с внешними сетями коммутации пакетов, поиск абонентов, выбор ячеек, роуминг и многие другие функции, требуемые для обеспечения работы сотовой сети. Кроме того, GPRS использует протоколы GSM SMS и GSM MM (последний в GPRS называется GMM).

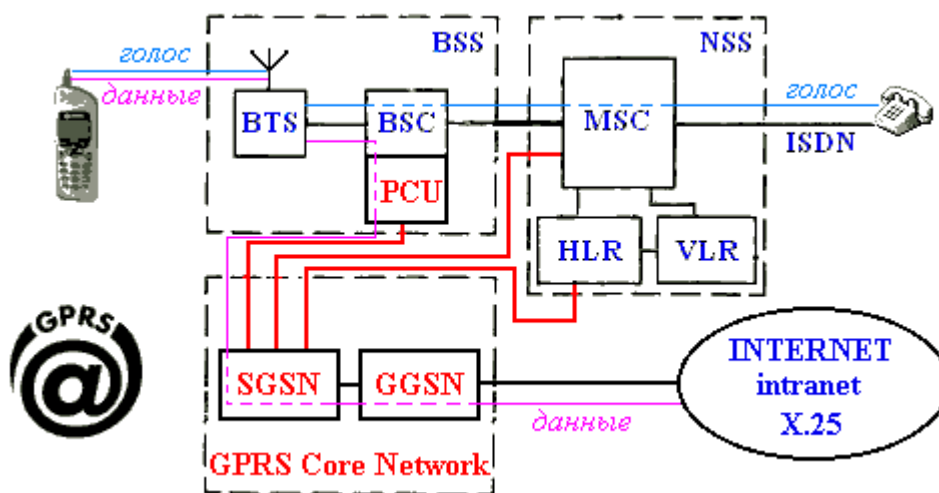


Рис. 3.7 Маршрут передачи GPRS

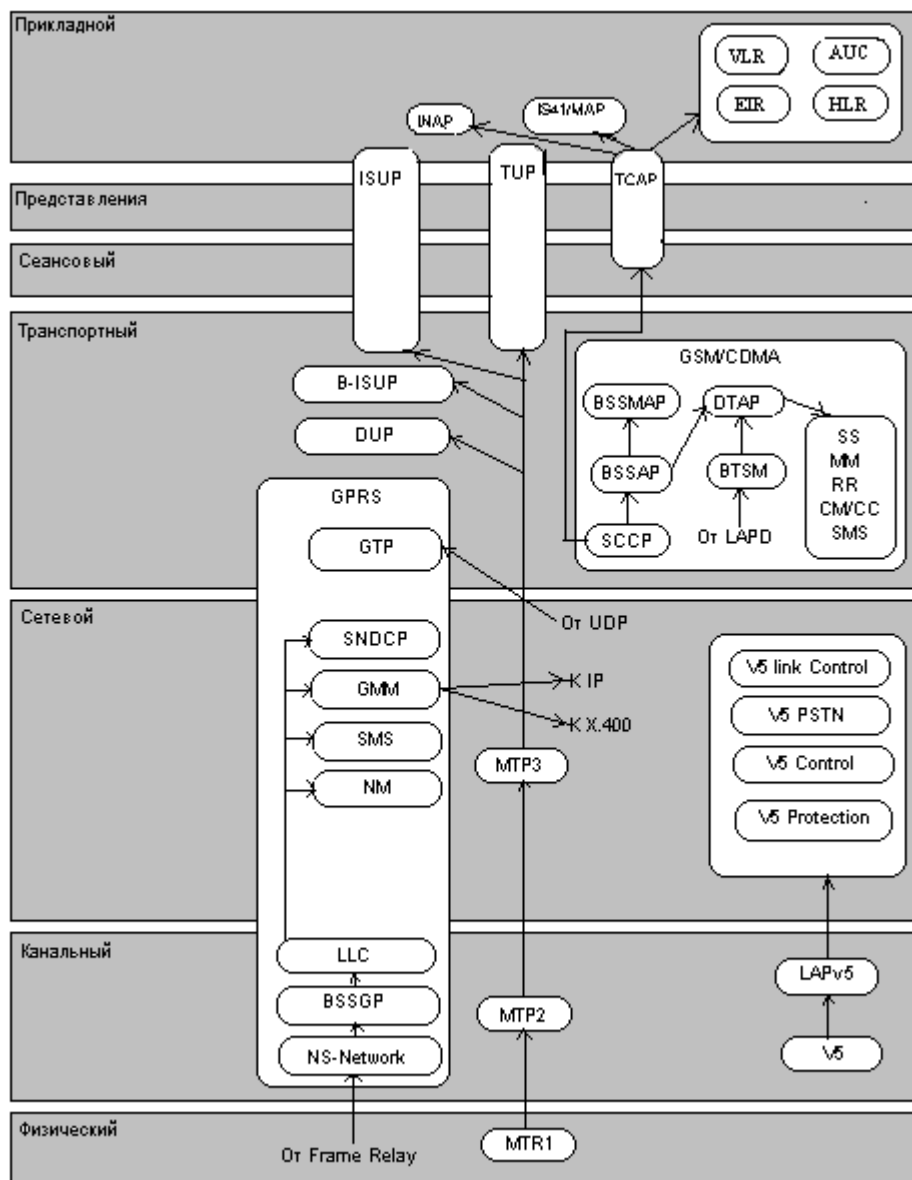


Рис. 3.8 Расположение стека протокола GPRS в эталонной модели OSI

Протокол сетевого сервиса NS (Network Service) обеспечивает транспортировку пакетов NS SOU между обслуживающими узлами поддержки GPRS (SGSN) и системой базовой станции (BSS). Сервис, обеспечиваемый пользователю NS, включает в себя:

- *Передачу пакетов сетевого сервиса.* NS поддерживает примитивы сетевого сервиса- позволяющие осуществлять передачу и прием пакетов данных протоколов вышележащего уровня между BSS и SGSN. Пакеты сетевого сервиса передаются в порядке, который обеспечивается протоколом NS, однако в экстремальных случаях порядок передачи пакетов может изменяться.
- *Индикацию сетевой перегрузки.* Механизм восстановления может реализоваться на уровне протокола более низкого уровня (например, Frame Relay). Механизм индикации перегрузки такого уровня будет использоваться сетевым сервисом для индикации перегрузки.
- *Индикацию состояния,* используемую для информирования пользователя сетевого уровня о событиях, оказывающих воздействие на работу сетевого уровня (например, изменение доступной полосы пропускания).

Структура пакета (PDU) Сетевого Уровня показана на следующем рисунке:

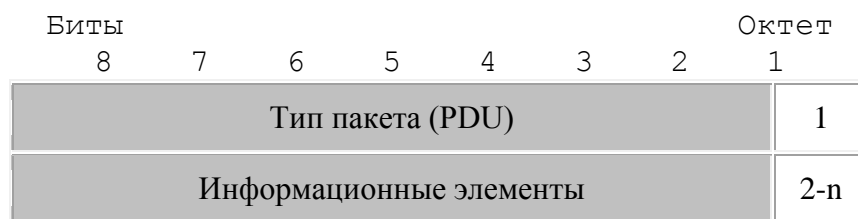


Рис. 3.9. Структура заголовка NS

Типы пакетов

Пакеты могут быть следующих типов

NS-ALIVE
 NS-ALIVE-ACK
 NS-BLOCK
 NS-BLOCK-ACK
 NS-RESET
 NS-RESET-ACK
 NS-STATUS
 NS-UNBLOCK
 NS-UNBLOCK-ACK
 NS-UNITDATA

Информационные элементы

В зависимости от типа пакета в него могут быть включены различные информационные элементы (IE). Структура информационного элемента показана на следующем рисунке:

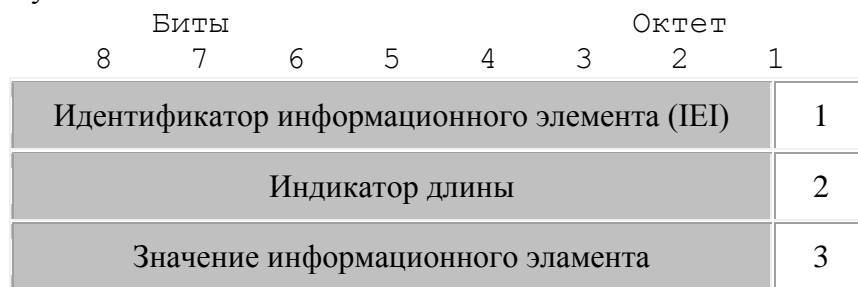


Рис. 3.10 Структура информационного элемента

Первый октет IE имеет формат TLV и содержит идентификатор информационного элемента (IEI). Если этот октет не соответствует ни одному из известных типов информационных пакетов, получатель предполагает, что следующий октет является первым октетом индикатора длины. Это правило позволяет получателю пакета пропускать информационные пакеты неизвестных типов и переходить к анализу следующих информационных элементов.

В зависимости от типа пакета в нем могут содержаться следующие информационные элементы:

Cause
 NC-VCI
 NS PDU

BVCI
NCEI.

Информационные элементы могут иметь различный размер. Индикатор длины - это поле размером 1 или 2 октета (второй октет может отсутствовать). Поле содержит бит расширения, а также размер информационного поля, следующего за полем индикатора длины. Бит расширения позволяет увеличить поле индикатора длины до двух октетов. Бит 8 первого октета зарезервирован для использования в качестве бита расширения. Если бит расширения имеет нулевое значение, это говорит о присутствии второго октета в поле индикатора длины. Если бит расширения имеет значение 1, поле индикатора длины состоит из одного октета.

BSSGP

Протокол сетевого сервиса NS обеспечивает транспортировку пакетов BSS GPRS между базовыми станциями BSS и узлами SGSN (обслуживающий узлом поддержки GPRS). Основные функции протокола BSSGP обеспечивают решение следующих задач:

- узлы обслуживания SGSN (Serving GPRS Support Node) обеспечивают для BSS радиоинформацию, используемую функцией RLC/MAC (в нисходящем канале).
- базовые станции BSS (Base Station Subsystem) обеспечивает для SGSN радиоинформацию, полученную от функции RLC/MAC (в восходящем канале).
- физически различные узлы SGSN и BSS могут поддерживать функции управления узлом.

Структура пакета BSSGP показана на рисунке.

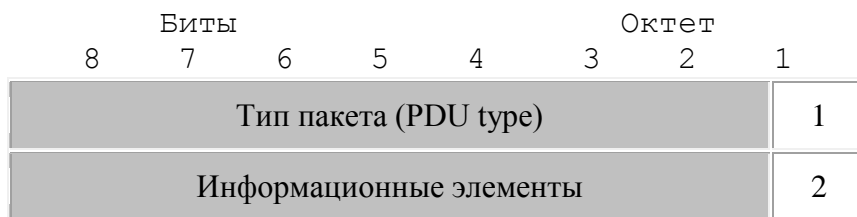


Рис. 3.11. Структура заголовка BSSGP

Типы пакетов

Пакеты BSSGP могут быть следующих типов:

UL-UNITDATA
RA-CAPABILITY
PTM-UNIYDATA
PAGING PS
PAGING CS
RA-CAPABILITY-UPDATE
RA-CAPABILITY-UPDATE-ACK
RADIO-STATUS
SUSPEND
SUSPEND-ACK
SUSPEND-NACK
RESUME
RESUME-ACK
RESUME-NACK
FLUSH-LL

FLUSH-LL-ACK
LLC-DISCARDED
FLOW-CONTROL-BVC
FLOW-CONTROL-BVC-ACK
FLOW-CONTROLMS
FLOW-CONTROLMS-ACK
BVC-BLOCK
BVC-BLOCK-ACK
BVC-UNBLOCK
BVC-UNBLOCK-ACK
BVC-RESET
BVC-RESET-ACK
STATUS
SGSN-INVOKE-TRACE.

Информационные элементы

В поле информационных элементов могут присутствовать перечисленные ниже значения (левая колонка списка).

0x00 Октеты выравнивания.
0x01 Bmax default MS
0x02 Индикация области BSS
0x03 Скорость передачи блоков (Bucket Leak Rate)
0x04 BVCI
0x05 Размер блока BVC
0x06 Измерение BVC (BVC Measurement)
0x07 Причина (Cause)
0x08 Идентификатор ячейки
0x09 Необходимость в канале (Channel needed)
0x0a Параметры DRX
0x0b Приоритет eMLPP
0x0c Действие подавления (Flush Action)
0x0d IMSI
0x0e LLC-SDU
0x0f Игнорированы пакеты LLC
0x10 Область местонахождения (Location Area)
0x11 Идентификатор пользователя (Mobile Id)
0x12 Размер блока MS
0x13 Мощность радиодоступа MS (MS Radio Access Capability)
0x14 Идентификатор OMC (OMC Id)
0x15 Ошибка входящего пакета (PDU In Error)
0x16 Время жизни пакета (PDU Lifetime)
0x17 Приоритет
0x18 Профиль QoS
0x19 Причина передачи радиосигнала (Radio Cause)
0x1a RA-Cap-UPD-Cause
0x1b Область маршрутизации
0x1c R-default_MS
0x1d Ссылка на приостановленный номер (Suspend Reference Number)
0x1e Ter
0x1f TLLI
0x20 TMSI
0x21 Ссылка на трассировку (Trace Reference)

- 0x22 Тип трассировки (Trace Type)
- 0x23 Идентификатор транзакции
- 0x24 Идентификатор триггера
- 0x25 Количество обработанных октетов

Те из перечисленных значений, которые не имеют точного определения, зарезервированы для будущего использования и трактуются получателем как неизвестный тип информационного элемента.

GPRS Tunneling Protocol

Протокол GTP (GPRS Tunneling Protocol) это протокол туннелирования GPRS. GTP описывает передачу данных между узлами GSN в магистральной сети GPRS. GTP определяется как для интерфейса Gn (т. е. интерфейса между GSN внутри одной PLMN), так и для интерфейса Gp (т. е. интерфейса между GSN в различных PLMN). Пакеты GTP инкапсулируются UDP.

GTP позволяет использовать туннелирование для передачи через магистраль GPRS между узлами GSN пакетов различных протоколов. С точки зрения сигнализации GTP определяет механизмы контроля и управления, позволяющие протоколу SGSN обеспечивать для MS доступ в сеть GPRS. Сигнализация служит для создания, модификации и уничтожения туннелей, С точки зрения передачи GTP использует механизм туннелирования для того, чтобы передавать пользовательские пакеты данных. Выбор маршрута зависит от того, требуют ли передаваемые по туннелю данные повышенной надежности соединения или нет.

Протокол GTP поддерживается только узлами обслуживания SGSN (Serving GPRS Support Node) и шлюзами GGSN (GPRS Gateway Support Node). Другие системы не обязаны знать что-либо о работе этого протокола. При подключении GPRS MS к узлам обслуживания SGSN работа с протоколом GTP не требуется. Предполагается, что при работе сети будут устанавливаться множественные соединения с узлами SGSN и GGSN. Один узел обслуживания SGSN может обеспечивать сервис для множества шлюзов GGSN. Один шлюз GGSN может иметь связь со многими узлами обслуживания SGSN для распределения графика между множеством территориально распределенных мобильных станций.

Заголовок пакета GTP используется для всех типов сообщений GTP и имеет фиксированную длину 16 октетов.

Биты				Октет				
8	7	6	5	4	3	2	1	
Версия			Зарезервировано			LFN		
Информационные элементы								1
Длина								2
Порядковый номер								3
Метка потока								4
Номер пакета LLC								5
x	X	x	x	x	x	x	FN	6
Резервировано								
TID								

Рис. 3.12 Структура заголовка BSSGP

Версия - Устанавливается в 0, показывая первую версию протокола GTP.

Зарезервировано - Биты, зарезервированные для будущего использования, имеют значение 1.

LFN - данный флаг показывает, включен ли в сообщение номер кадра LLC. Для сигнальных сообщений LFN=0.

Тип сообщения - указывает тип сообщения GTP- Для сигнальных сообщений это поле имеет значение, уникальное для каждого используемого типа сообщений.

Длина - содержит длину GTP-сообщения (G-POU) в октетах. Для сигнальных сообщений это поле включает размер сигнального сообщения и заголовка GTP.

Порядковый номер - идентификатор транзакции для сигнальных сообщений или порядковый номер для туннелированных сообщений T-PDU.

Метка потока - идентифицирует GTP-поток. В сигнальных сообщениях Path Management и Location Management метка потока не используется и данное поле имеет значение 0.

Номер пакета LLC - используется для координации передачи данных на канальном (link layer) уровне между MS и SGSN в процедурах обновления маршрутной информации внутри SGSN. Для сигнальных сообщений это поле не используется (отправитель устанавливает значение 255, а получатель игнорирует это поле).

TID - идентификатор туннеля, указывающий контекст MM и PDP в принимающем узле GSN. В сигнальных сообщениях это поле имеет значение 0 для всех сообщений V Management, Location Management и Mobility Management. Поле TID использует следующий формат:

Биты				Октет			
8	7	6	5	4	3	2	1
2-я цифра MCC			1-я цифра MCC			1	
1-я цифра MNC			3-я цифра MCC			2	
1-я цифра MSIN			2-я цифра MNC			3	
3-я цифра MSIN			2-я цифра MSIN			4	

5-я цифра MSIN	4-я цифра MSIN	5
7-я цифра MSIN	6-я цифра MSIN	6
9-я цифра MSIN	8-я цифра MSIN	7
NSAPI	10-я цифра MSIN	8

Рис. 3.13 Структура TID

Фрагменты IMSI (определены в GMS 04.08)

NSAPI - Идентификатор точки доступа к сетевому сервису.

LLC

Протокол LLC определяет управление логическим каналом связи (logical link control) и используется при передаче данных между мобильной станцией (MS-mobile station) и обслуживающим ее узлом обслуживания GPRS (SGSN -serving GPRS support node). Протокол LLC обеспечивает передачу данных от MS до SGSN и предназначен как для передачи данных с подтверждением приема, так и для передачи без подтверждений.

Формат кадров LLC основан на формате кадров LAPD и RLP. Однако существуют важные различия между LLC и другими протоколами существуют большие отличия в части методов обозначения границ кадров и механизмов прозрачности- Эти отличия диктуются требованиями независимости от конкретного радиомаршрута.

LLC поддерживает два режима передачи данных:

- операции точка-точка без подтверждения приема данных;
- операции точка-точка с подтверждением приема данных.

Весь обмен информацией между объектами одного уровня протокола LLC осуществляется при помощи кадров, имеющих следующий формат:

Биты				Октет				
8	7	6	5	4	3	2	1	
Адрес								1
Управление								2
Информация								
FCS								

Рис. 3.14 Структура заголовка LLC

Поле адреса обозначает DLCI, для которого предназначен передающийся кадр и DLCI для встречного потока кадров. Поле адреса имеет размер 1 байт и использует следующий формат:



Рис. 3.15 Структура поля адреса LLC

PD - идентификатор протокола указывает тип данного кадра - LLC или другой протокол. Для протокола LLC значение данного поля должно быть равно 0. Если в полученном кадре PD = 1, такой кадр трактуется как ошибочный.

C/R - поле указывает тип содержимого кадра - команда или отклик. MS передает кадры команд с полем C/R = 0, а в кадрах отклика устанавливается значение C/R = 1. Узлы обслуживания SGSN используют обратный порядок, т. е. для командных кадров C/R = 1, а для откликов C/R = 0.

Тип кадра Направление Значение C/R

- Команда От SGSN к MS 1
- Команда От MS к SGSN 0
- Отклик От SGSN к MS 0
- Отклик От MS к SGSN 1
- XX = Зарезервировано (2 бита)

SAPI - Идентификатор точки доступа к сервису (Service Access Point Identifier) обозначает точку доступа, через которую LLE обеспечивает для протокола LLC доступ к процессу вышележащего уровня (layer 3).

Управление Идентифицирует тип кадра. Протокол LLC использует 4 типа кадров:

- передача подтверждаемой информации (формат I);
- функции контроля (supervisory) (формат S);
- передача информации без подтверждения (формат UI)
- функции управления (формат U)

Информация -содержит различные команды и отклики на них.

FCS - Контрольная сумма, содержащая 24-битовый CRC-код, который служит для обнаружения ошибок в заголовке и информационном поле кадра.

SNDCP

Протокол SNDCP (Sub-Network Dependant Convergence Protocol) использует сервис, предоставляемый уровнями LLC (Logical Link Control - управление логическим каналом) и подуровнем SM (Session Management - управление сеансом). Существует SNDCP для протоколов IP и X.25.

Основными функциями протокола SNDCP являются:

- мультиплексирование нескольких пакетных протоколов PDP (packet data protocol);
- компрессия/декомпрессия пользовательских данных;
- компрессия/декомпрессия управляющей информации для протокола;
- сегментация пакетов сетевого уровня (N-PDU) в пакеты уровня логического канала (LL-PDU), а также обратный процесс сборки LL-PDU в N-PDU.

Пакеты SN-DATA используются для передачи данных с подтверждением приема. Эти пакеты имеют следующий формат:

Биты						Октет
8	7	6	5	4	3 2 1	
X	C	T	M		NSAPI	1
DCOMP					PCOMP	2
Данные						3-n

Рис. 3.16 Структура пакета SN-DATA

Пакеты SN-UNITDATA используются для передачи данных без подтверждения приема. Формат пакетов показан на рисунке.

Биты						Октет
8	7	6	5	4	3 2 1	
X	C	T	M		NSAPI	1
DCOMP					PCOMP	2
Смещение сегмента			Номер N-PDU			3
E	Номер N-PDU (продолжение)					4
Номер N-PDU (расширение)						5
Данные						6-n

Рис. 3.17 Структура пакета SN-UNITDATA

NSAPI - идентификатор точки доступа к сетевому сервису. Это поле может принимать следующие значения:

0 Механизм отмены, зарезервированный для использования в будущем.

1 Групповая передача "один ко многим" (PTM-M - point-to-multipoint multicast),

M - флаг наличия дополнительных сегментов.

0 Последний сегмент N-PDU

1 Данный сегмент N-PDU не является последним.

T - тип SN-PDU. Определяет тип пакета -SN-DATA (0) или SN-UNITDATA (1).

C - индикатор компрессии. Значение 0 показывает, что поля компрессии DCOMP и PCOMP не включены в пакет, 1 говорит о наличии этих полей в пакете.

X - запасной (spare) бит, устанавливаемый в 0.

DCOMP - идентификатор компрессии данных, включаемый в пакет при установке бита C. DCOMP может принимать следующие значения:

1. Компрессия не используется.

1-14 Указывает на динамически согласуемые идентификаторы компрессии данных.

15. Зарезервировано для будущего использования.

PCOMP - кодирование компрессии управляющей информации протокола, включаемое в пакеты при установленном бите C. PCOMP может принимать следующие значения:

0 Компрессия не используется.

1-14 Указатели на идентификаторы компрессии управляющей информации, согласуемые динамически.

15 Зарезервировано для будущего использования.

Смещение сегмента - смещение сегмента от начала N-PDU. Задается в единицах по 128 октетов.

Номер N-PDU - 0-2047 при нулевом значении бита расширения.

2048-524287 в тех случаях, когда бит расширения имеет значение 1.

E - бит расширения для номера N-PDU:

0 Следующий октет содержит данные.

1 Следующий октет используется для расширения номера N-PDU.

High Speed Circuit Switched Data

High Speed Circuit Switched Data (HSCSD) - Высокоскоростная передача данных по сетям с коммутацией каналов - многоканальная платформа для передачи данных в сетях GSM. Она преодолевает ограничения беспроводных сетей связи по скорости, позволяя абонентам GSM передавать данные со скоростями сравнимыми, и даже превышающими скорости передачи в проводных сетях. При использовании технологии HSCSD максимальная скорость может составить 57.6 кбит/с. HSCSD специально разработана для развития существующей инфраструктуры GSM путем модернизации программного обеспечения, поэтому внедрение этого решения производится быстро и экономично.

HSCSD должно было стать промежуточным этапом при внедрении более мощных технологий радиопередачи, таких как GPRS.

Для конечных пользователей HSCSD открывает возможность использования целого ряда новых приложений беспроводной связи. HSCSD позволяет просматривать с мобильного терминала WEB-страницы с более насыщенным графическим содержанием. Кроме того, пользователи получают возможность высокоскоростного доступа к ЛВС и корпоративным сетям.

HSCSD позволяет даже организовать дистанционное видеонаблюдение в тех местах, где прокладка кабеля нецелесообразна или невозможна. Необходимо упомянуть и возможность организации видеоконференций по беспроводному интерфейсу. Сегодня видео и аудиоконференции организуются в фиксированных сетях со скоростями 28.8 кбит/с: это более чем достижимо для HSCSD.

В отличие от GPRS, HSCSD занимает голосовые каналы в течение всего времени соединения (не зависимо от активности пользователя).

Телефоны поддерживающие HSCSD.

Самые распространенные марки телефонов, поддерживающие технологию HSCSD:

NOKIA 6210, 6310, 6500, 6510, 7650, 8310, 8855, 9210/9210i, Nokia Card Phone

MOTOROLA V120, V66, V70

ERICSSON – SONYERICSSON R520, T36, T39, T65, T68, T68i, T200, T300, T600, R600

SIEMENS S40

К сожалению данный стандарт не смог завоевать большой популярности, в России его внедрили «North-West GSM» в Санкт-Петербурге и «Мегафон». МТС и Beeline отказались от введения стандарта HSCSD и перешел к внедрению GPRS.

Данная глава посвящена рассмотрению систем подвижной связи стандарта GSM. Стандарту уже более 15 лет однако, он не теряет своей актуальности, идет непрерывное совершенствование. Новые компоненты вводятся поэтапно обеспечивая расширение спектра оказываемых услуг. В 1995 активно развивался сервис коротких сообщений (SMS), пользователи получили возможность обмениваться сообщениями, следить за состоянием счета, отключать и подключать дополнительные услуги. В последние годы усилия разработчиков были направлены на повышение скорости передачи данных. И в свет вышли два стандарта передачи данных HSCSD и GPRS, полноценной конкуренции между ними не получилось так как HSCSD обладал серьезным недостатком, он занимал голосовые каналы в течении всего времени соединения (пользователи вынуждены были оплачивать время проведенное в сети а не объем переданных данных).

В 1992 году GSM в нашей стране принят в качестве федерального стандарта. Долгое время у GSM не было конкурентов в России, однако сейчас на рынке появились системы сотовой связи стандарта CDMA.

4. СИСТЕМЫ ПОДВИЖНОЙ СВЯЗИ В СТАНДАРТАХ IS-95 (CDMA) И DECT

Мобильная связь развивается в мире стремительными темпами, непрерывно расширяя объем и качество предоставляемых услуг. Этому способствуют постоянный рост спроса на услуги связи и информацию, а также достижения научно-технического прогресса в области электроники, волоконной оптики и вычислительной техники.

В настоящее время во многих странах ведется интенсивное внедрение сотовых сетей подвижной связи, сетей персонального радиовызова и систем спутниковой связи. Передача данных подвижному абоненту резко расширяет его возможности поскольку кроме телефонных, он может принимать телекстные и факсимильные сообщения, различного рода графическую информацию и многое другое. Увеличение объема информации требует сокращения времени ее передачи и получения.

На темпы развития и качественные параметры систем радиотелефонной связи влияют следующие факторы – ограничение частотного ресурса и максимально развитие возможностей систем связи, т.е. увеличение объема передаваемой информации при постоянной или увеличиваемой скорости передачи, причем в условиях сохранения конфиденциальности, а также увеличение абонентской базы системы при увеличенном радиусе действия.

Эти факторы побуждают к развитию телекоммуникационной отрасли и породили множество стандартов систем связи, которые частично сочетают в себе эти противоречивые требования к параметрам систем.

Рассмотрим два стандарта связи, один из которых, имеет большую абонентскую емкость при малом радиусе действия и другую имеющую в своем активе большей радиус действия при меньшей вместительности и повышенный уровень конфиденциальности. Перечисленные свойства этих двух стандартов составляют лишь неполный список их достоинств, и различия между собой.

Стандарт сотовой связи CDMAone или IS-95.

Сотовая система подвижной радиосвязи общего пользования стандарта IS-95 с кодовым разделением каналов (CDMA) впервые была разработана фирмой Qualcomm (США). Основная цель разработки состояла в том, чтобы увеличить емкость системы сотовой связи по сравнению с аналоговой не менее чем на порядок и соответственно увеличить эффективность использования выделенного спектра частот.

Технические требования к системе CDMA сформированы в ряде стандартов Ассоциации промышленности связи (TIA):

- IS-95 - CDMA-радиоинтерфейс
- IS-96 - CDMA-речевые службы
- IS-97 - CDMA-подвижная станция
- IS-98 - CDMA-базовая станция
- IS-99 - CDMA-службы передачи данных.

Система CDMA IS-95 фирмы Qualcomm рассчитана на работу в диапазоне частот 800 МГц, выделенном для сотовых систем стандартов AMPS, N-AMPS и D-AMPS. (Стандарты TIA IS-19, IS-20; IS-54; IS-55, IS-56, IS-88, IS-89, IS-90, (S-553).

Система CDMA IS-95 даёт возможность каждому пользователю внутри соты использовать тот же самый радиоканал и всю выделенную полосу частот. Пользователь в смежной соте использует эту же полосу частот. Вместо деления спектра или

временных слотов (как в других технологиях ССПС), каждому пользователю назначается фрагмент шумоподобной несущей. Поскольку её фрагменты являются квазиортогональными, возникает возможность отвести всю ширину выделенного канала для каждого пользователя. Благодаря решению проблемы «ближней – дальней» зоны и динамическому управлению мощностью вся полоса частот 1,25 МГц используется каждым пользователем и она же вновь используется в смежной соте. Емкость на одну соту определяется балансом между требуемым отношением сигнал/шум для каждого пользователя и фактором сжатия кодовой последовательности. Таким образом, система абсолютно не нуждается в частотном планировании. Для уменьшения затрат операторов подвижной связи и облегчения перехода от AMPS к CDMA в системе CDMA предусмотрена ширина канала (1,25 МГц), такая же, как и у AMPS. В отличие от других сотовых систем, трафик одного канала не является постоянной величиной и зависит от голосовой активности и требований, предъявляемых к сети.

Безопасность или конфиденциальность является свойством технологии CDMA, поэтому во многих случаях операторам сотовых сетей не потребуется специального оборудования шифрования сообщений.

Система CDMA Qualcomm построена по методу прямого расширения спектра частот на основе использования последовательностей 64 видов, сформированных по закону функций Уолша. Для передачи речевых сообщений выбрано речепреобразующее устройство с алгоритмом CELP со скоростью преобразования 8000 бит/с (9600 бит/с в канале). Возможны режимы работы на скоростях 4800, 2400 и 1200 бит/с.

В каналах системы CDMA применяется сверточное кодирование со скоростью 1/2 (в каналах от базовой станции) и 1/3 (в каналах от подвижной станции), декодер Витерби с мягким решением, перемежение передаваемых сообщений. Общая полоса канала связи составляет 1,25 МГц. Основные характеристики стандарта CDMA Qualcomm и технические параметры оборудования сетей приведены в таблице 4.1.

Таблица 4.1

Характеристики	
Диапазон частот передачи MS	824,040 - 848,860 МГц
Диапазон частот передачи BTS	869,040 - 893,970 МГц
Относительная нестабильность несущей частоты BTS	$\pm 5 \cdot 10^{-8}$
Относительная нестабильность несущей частоты MS	$\pm 2,5 \cdot 10^{-6}$
Вид модуляции несущей частоты	QPSK (BTS), 0-QPSK (MS)
Ширина спектра излучаемого сигнала: по уровню минус 3 дБ по уровню минус 40 дБ	1,25 МГц 1,50 МГц
Метод расширения спектра	DSSS-CDMA
Тактовая частота ПСП	1,2288 МГц
Количество элементов в ПСП для: BTS MS	32768 бит 242- 1 бит
Количество каналов BTS на 1 несущей частоте	1 пилот-канал, 1 канал сигнализации, 7 каналов перс. вызова, 55 каналов связи
Количество каналов MS	1 канал доступа, 1 канал связи
Скорость передачи данных: в канале синхронизации, в канале перс. вызова и	1200 бит/с 9600, 4800 бит/с 9600, 4800, 2400, 1200 бит/с

На рис.4.2 приведена обобщенная структурная схема сети сотовой подвижной радиосвязи CDMA IS-95, основные элементы которой (BTS, BSC, MSC, OMC) аналогичны используемым в сотовых сетях с частотным (NMT-450/900, AMPS, TACS) и временным разделением каналов (GSM, DCS-1800, PCS-1900, D-AMPS, JDC). Основное отличие заключается в том, что в состав сети CDMA IS-95 включены устройства оценки качества и выбора кадров (SU). Кроме того, для реализации процедуры мягкого переключения между базовыми станциями, управляемыми разными контроллерами (BSC), вводятся линии передачи между SU и BSC (Inter BSC Soft handoff).

Протоколы установления связи в CDMA IS-95, также как в стандартах AMPS и N-AMPS, основаны на использовании логических каналов.

В CDMA каналы для передачи с базовой станции называются прямыми (Forward), для приема базовой станцией - обратными (Reverse). Для обратного канала IS-95 определяет полосу частот от 824 до 849 МГц. Для прямого канала — 869–894 МГц. Прямой и обратный каналы разделены интервалом в 45 МГц. Пользовательские данные упакованы и передаются в канале с пропускной способностью 1,2288 Мбит/с. Нагрузочная способность канала — 128 телефонных соединений со скоростью трафика 9,6 кбод. Структура каналов в CDMA в стандарте IS-95 показана на рис.3. В IS-95 используются различные типы модуляции для прямого и обратного каналов. В прямом канале базовая станция передаёт одновременно данные для всех пользователей, находящихся в соте, используя для разделения каналов различные коды для каждого пользователя. Также передается пилотный сигнал, он имеет больший уровень мощности, обеспечивая пользователям возможность синхронизировать частоты. В обратном направлении подвижные трубки отвечают асинхронно, при этом уровень мощности, приходящий к базовой станции от каждой подвижной станции, одинаков. Такой режим возможен благодаря контролю мощности и управлению мощностью подвижных трубок по служебному каналу.

- Прямые каналы в CDMA IS-95:

Данные в прямом канале трафика группируются во фрейм длительностью 20 мс. Пользовательские данные после предварительного кодирования и форматирования перемежаются с целью регулирования текущей скорости передачи данных, которая может изменяться. Затем спектр сигнала расширяется перемножением с одной из 64 псевдослучайных последовательностей (на основе функций Уолша) до значения 1,2288 Мбит/с. Каждому мобильному абоненту назначается фрагмент ПСП, с помощью которого его данные будут отделены от данных других абонентов. Ортогональность фрагментов ПСП обеспечивается одновременной синхронной кодировкой всех каналов в соте (т.е. используемые в каждый момент времени фрагменты являются ортогональными). Как уже упоминалось, в системе передается пилотный сигнал (код) для того, чтобы мобильный терминал мог управлять характеристиками канала, принимать временные метки, обеспечивая фазовую синхронизацию для когерентного детектирования. Для глобальной синхронизации сети в системе используются ещё радиометки от GPS-спутников.

Состав:

- Ведущий канал - используется подвижной станцией для начальной синхронизации с сетью и контроля за сигналами базовой станции по времени, частоте и фазе.

- Канал синхронизации - обеспечивает идентификацию базовой станции, определение уровня излучения пилотного сигнала, а также фазу псевдослучайной последовательности базовой станции. После завершения указанных этапов синхронизации начинаются процессы установления соединения. Канал синхронизации передаёт синхросигналы мобильным терминалам со скоростью 1200 бод.

- Канал вызова (пэйджинговый) - используется для вызова подвижной станции. Кол-во каналов: до 7 шт. После приема сигнала вызова подвижная станция передает сигнал подтверждения на базовую станцию, после чего по каналу вызова на подвижную станцию передается информация об установлении соединения и назначении канала связи. Канал персонального вызова начинает работать после того, как подвижная станция получит всю системную информацию (частота несущей, тактовая частота, задержка сигнала по каналу синхронизации). Работает со скоростью 9600, 4800, 2400 бод. Прямой канал трафика (КПД) передаёт любые пользовательские данные со скоростью 9600, 4800, 2400, 1200 бод.

- Канал прямого доступа - предназначен для передачи речевых сообщений и данных, а также управляющей информации с базовой станции на подвижную. Кол-во: до 63

Базовая скорость передачи данных в канале составляет 9,6 Кбит/с, что достигается добавлением дополнительных корректирующих двоичных символов к цифровому потоку вокодера 8,55 Кбит/с. Для реализации на приемной стороне прямой коррекции ошибок (без повторного запроса и передачи сообщения) в канале используется избыточное кодирование. Для этого базовый цифровой поток разбивается на пакеты длительностью по 20 мс и подается на сверточный кодер с половинной скоростью. На его выходе число битов удваивается. Затем данные перемежаются, т. е. перемешиваются во временном интервале 20 мс, это делается для того, чтобы равномерно распределить в потоке данных потерянные во время передачи биты. Известно, что ошибочно принятые символы обычно формируют группы. В то же время, схема прямой коррекции ошибок работает наилучшим образом, когда ошибки распределены равномерно во времени. Это происходит после осуществления на приемной стороне процедуры, обратной перемежению при передаче. После перемежения цифровой поток преобразуется с помощью длинного кода и логической операции "исключающее ИЛИ" (сложение по модулю два). По определению, длинными кодами (кодами максимальной длины) являются коды, которые могут быть получены с помощью регистра сдвига или элемента задержки заданной длины. Максимальная длина двоичной последовательности, которая может быть получена с помощью генератора, построенного на основе регистра сдвига, равна $2^n - 1$ двоичных символов, где n — число разрядов регистра сдвига. В аппаратуре стандарта IS-95 длинный код формируется в результате нескольких последовательных логических операций с псевдослучайной двоичной последовательностью, генерируемой в 42-разрядном регистре сдвига, и двоичной 32-битовой маской, которая определяется индивидуально имя каждого абонента. Такой регистр сдвига применяется во всех базовых станциях этого стандарта для обеспечения режима синхронизации всей сети, Так как информационный поток имеет

скорость 19,2 Кбит/с, то в прямом канале используется только каждый 64-й символ длинного кода. Следующий этап преобразования сообщения — кодирование с помощью кодов Уолша. Один ряд матрицы Уолша ставится в соответствие каналу связи между абонентом и базовой станцией. Если на входе кодера «0», то посылается соответствующий ряд матрицы (кода Уолша), если «1» — посылается последовательность, сформированная путем логического отрицания соответствующего ряда матрицы (кода Уолша). Это повышает скорость информационного потока с 19,2 Кбит/с до 1,2296 Мбит/с. Соответственно расширяется и спектр сигнала. На заключительном этапе двоичный поток разделяется между синфазным и квадратурным каналами (I- и Q-каналами) для последующей передачи с использованием квадратурной фазовой манипуляции (QPSK). До подачи на смесители цифровой поток в каждом из каналов преобразуется с помощью короткого кода и логической операции «исключающее ИЛИ».

Короткий код представляет собой псевдослучайную двоичную последовательность длиной 32768 двоичных символов, генерируемую со скоростью 1,2288 Мбит/с. Эта последовательность является общей для всех базовых и подвижных станций в сети. Короткий код формируется в 15-разрядном регистре сдвига с линейной обратной связью. Результирующий двоичный поток в каждом канале проходит через цифровой фильтр с конечной импульсной характеристикой (КИХ-фильтр), что позволяет ограничить полосу излучаемого сигнала. Частота среза фильтра составляет около 615 кГц. Полученные аналоговые сигналы поступают на соответствующие входы I/Q-модулятора. Ряд информационных сигналов образуется путем слияния I- и Q-каналов.

Поскольку все пользователи получают объединенный сигнал, то для выделения информации необходимо передавать опорный сигнал (по пилотному каналу). В этом канале передается нулевой информационный сигнал. Код Уолша для пилотного канала формируется из нулевого ряда матрицы Уолша. Другими словами, в пилотном канале передается только короткий код. Обычно на нем излучается около 20%, общей мощности. Опорный сигнал необходим для последующей фазовой демодуляции. Короткий код позволяет многократно использовать в каждой ячейке один и тот же набор кодов Уолша. Каждая базовая станция имеет свой временной сдвиг при формировании кода и поэтому может быть однозначно определена в сети. Основано это на свойстве псевдослучайных двоичных кодов: значение автокорреляционного момента приближается к нулю для всех временных смещений более одной битовой длины.

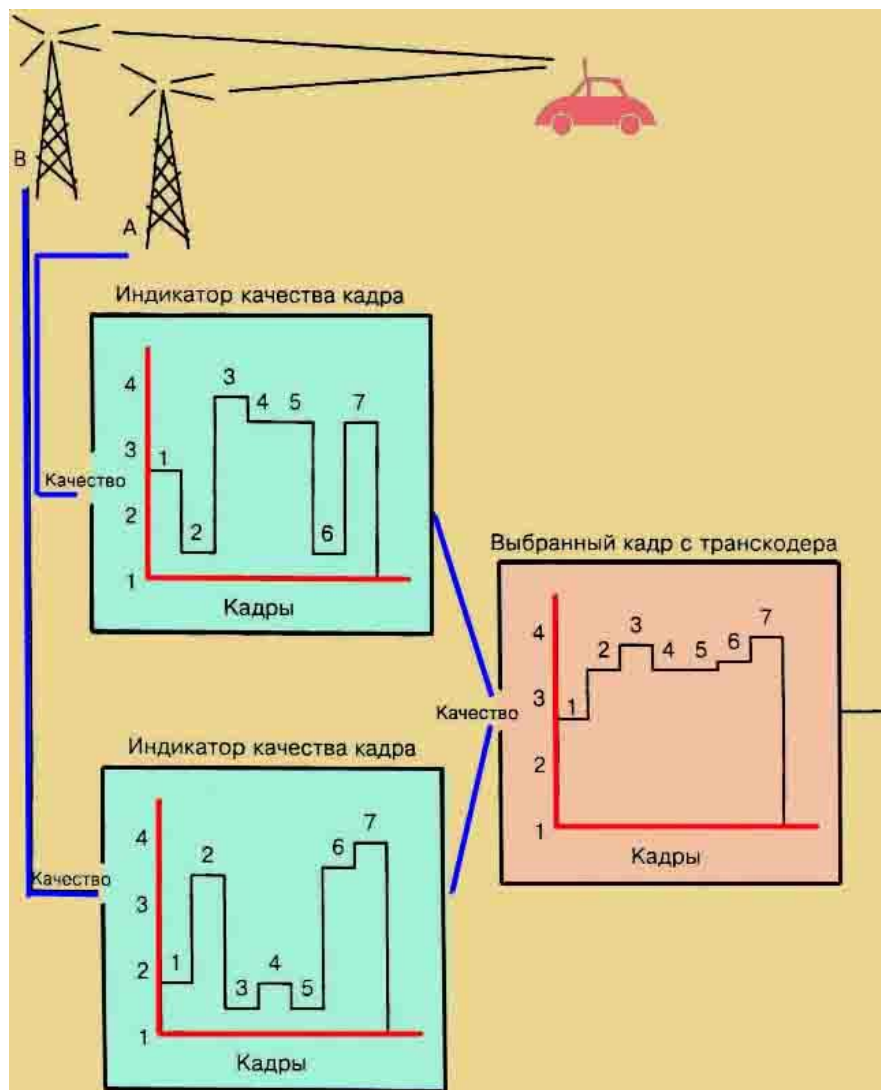
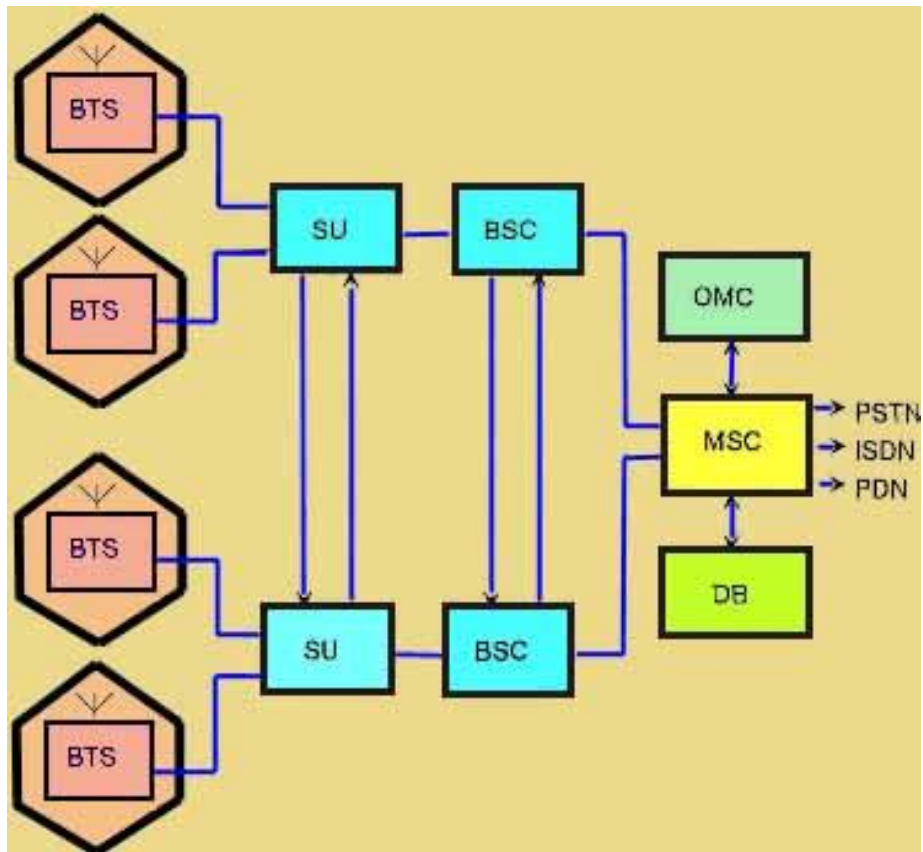


Рис. 4.1



BTS (Base Transceiver Station) - базовая приемопередающая станция
 SU (Selector Unit) - устройство выбора кадра
 DB (Data Base)- база данных об абонентах и оборудовании

Рис. 4.2

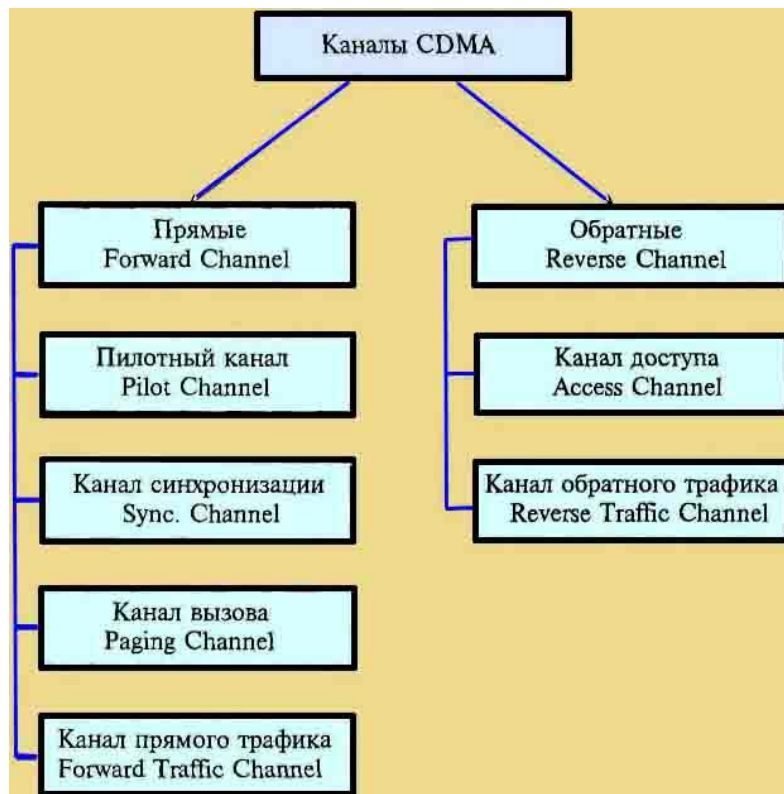


Рис. 4.3

В обратном канале использован другой алгоритм формирования спектра, поскольку сигналы от удалённых терминалов достигают базовой станции по различным путям. Пользовательские данные также сгруппированы во фреймы длительностью 20 мс. Подвижная станция не может использовать преимущества трансляции опорного сигнала. В этом случае необходимо было бы передавать два сигнала, что значительно усложнило бы демодуляцию в приемнике базовой станции. В обратном канале применяется сверточное кодирование со скоростью $1/3$, что повышает скорости передачи данных с базовой 9,6 до 28,8 Кбит/с, и перемежение в пакете длительностью 20 мс. После перемежения выходной поток разбивается на слова по шесть битов в каждом. Шестибитовому слову можно поставить в соответствие один из 64 кодов Уолша. Таким образом, каждый абонентский терминал использует весь их набор. После этой операции скорость потока данных повышается до 307,2 Кбит/с. Далее поток преобразуется с помощью длинного кода, аналогичного используемому базовой станцией. На этом этапе происходит разделение пользователей. Абонентская емкость системы определяется обратным каналом. Для ее увеличения применяется регулирование мощности в обратном канале, методы пространственного разнесения приема на базовой станции и др. Окончательное формирование потоков данных происходит таким же образом, как и в базовой станции, за исключением дополнительного элемента задержки на $1/2$ длительности символа в 0-канале для реализации смещенной QPSK.

После включения MS настраивается на рабочую частоту сети и ищет сигнал базовой станции (в сети используется общий для всех базовых и подвижных станций короткий код). Вероятно, она обнаружит несколько сигналов разных базовых станций, которые можно различить по временному сдвигу в коротком коде. Подвижная станция выбирает сигнал с большим уровнем и, таким образом, получает когерентную опору для осуществления последующей демодуляции сигнала синхронизации. Этому сигналу поставлен в соответствие 32-й код Уолша. В нем передается информация о будущем содержании 42-разрядного регистра сдвига, используемого для формирования длинного кода. Эта информация посылается с опережением относительно информационного канала на 320 мс. Поэтому подвижная станция имеет достаточно времени для декодирования сообщения и загрузки информации в регистр. Таким образом достигается синхронизация с сетевым временем. После этого подвижная станция начинает мониторинг одного из каналов вызова. Если абонент пытается войти в сеть, то его станция будет пытаться осуществить соединение с базовой по одному из каналов доступа. В этом случае для формирования длинного кода используется двоичная маска, параметры которой индивидуальны для каждой базовой станции сети. Если одновременно несколько пользователей пытаются осуществить соединение, то возникает конфликт. Если базовая станция не подтверждает попытку соединения по каналу вызова, то абонентская выжидает произвольное время и делает следующую попытку.

После принятия вызова подвижной станции базовая станция назначает канал для соединения, имеющий соответствующий код Уолша. После этого подвижная станция изменяет параметры двоичной маски в соответствии со своим идентификационным номером и переходит в режим приема и передачи речевой информации.

С учетом вышеизложенного можно сказать, что система CDMA потенциально имеет большую емкость. Кроме того, она позволяет отказаться от частотного планирования сети, хотя при этом предполагает проведение тщательного баланса мощностей излучений станций.

Состав

- Канал доступа - обеспечивает связь подвижной станции с базовой станцией, когда подвижная станция еще не использует канал трафика. Канал доступа используется для установления вызовов и ответов на сообщения, передаваемые по каналу вызова (Paging Channel), команды и запросы на регистрацию в сети. Каналы доступа совмещаются (объединяются) с каналами вызова.

- Канал обратного трафика - обеспечивает передачу речевых сообщений и управляющей информации с подвижной станции на базовую станцию.

На рис. 4.4 показана процедура установления обычного соединения (входящий вызов к подвижной станции).

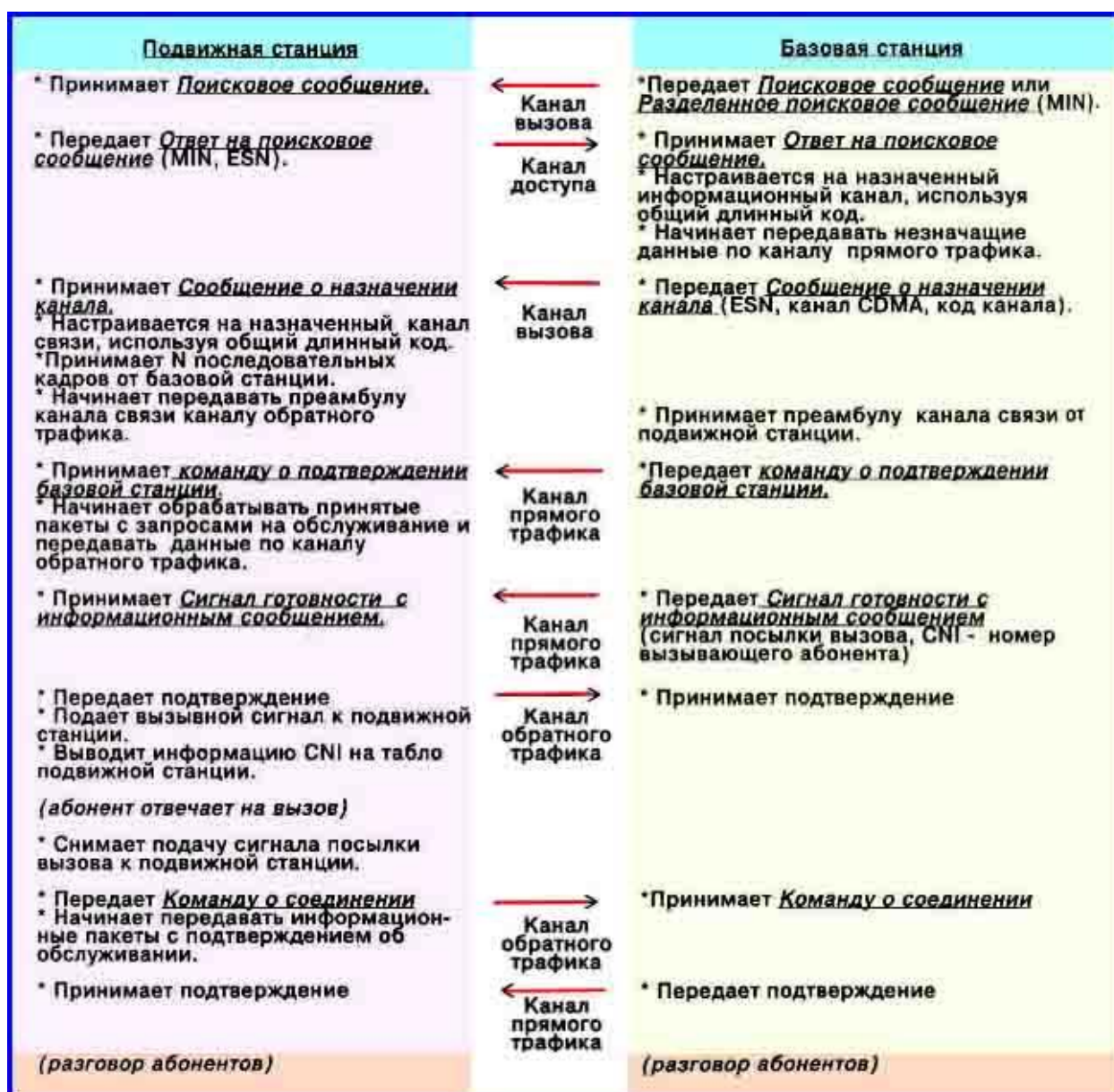


Рис.4.4

На рис.4.5 показана процедура прохождения обычного вызова (исходящий вызов от подвижной станции).

Базовая станция одновременно может передавать 64 канала, из которых 2 канала используются для синхронизации, 7 - для персонального вызова (Paging), остальные 55 - для передачи речевых сообщений (Traffic).



Рис. 4.5

Структура каналов передачи базовой станции показана на рис. 4.6. На рис. 4.7, показана схема формирования сигнала передатчиком базовой станции. Структурная схема приемника подвижной станции показана на рис. 4.8.

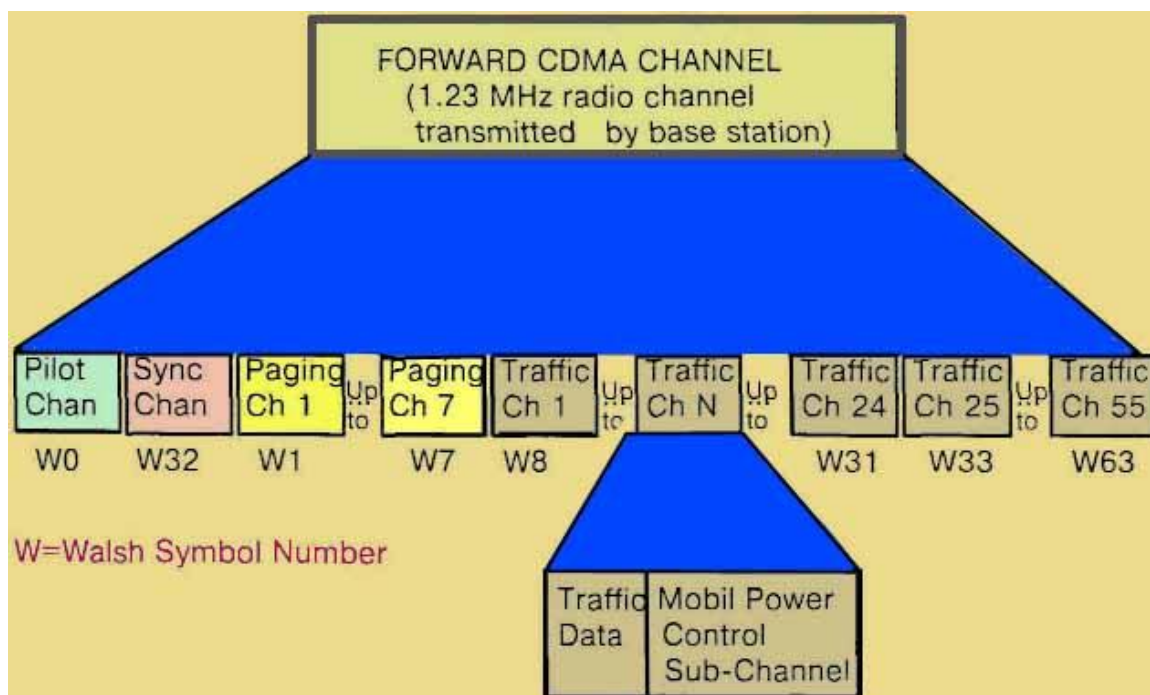
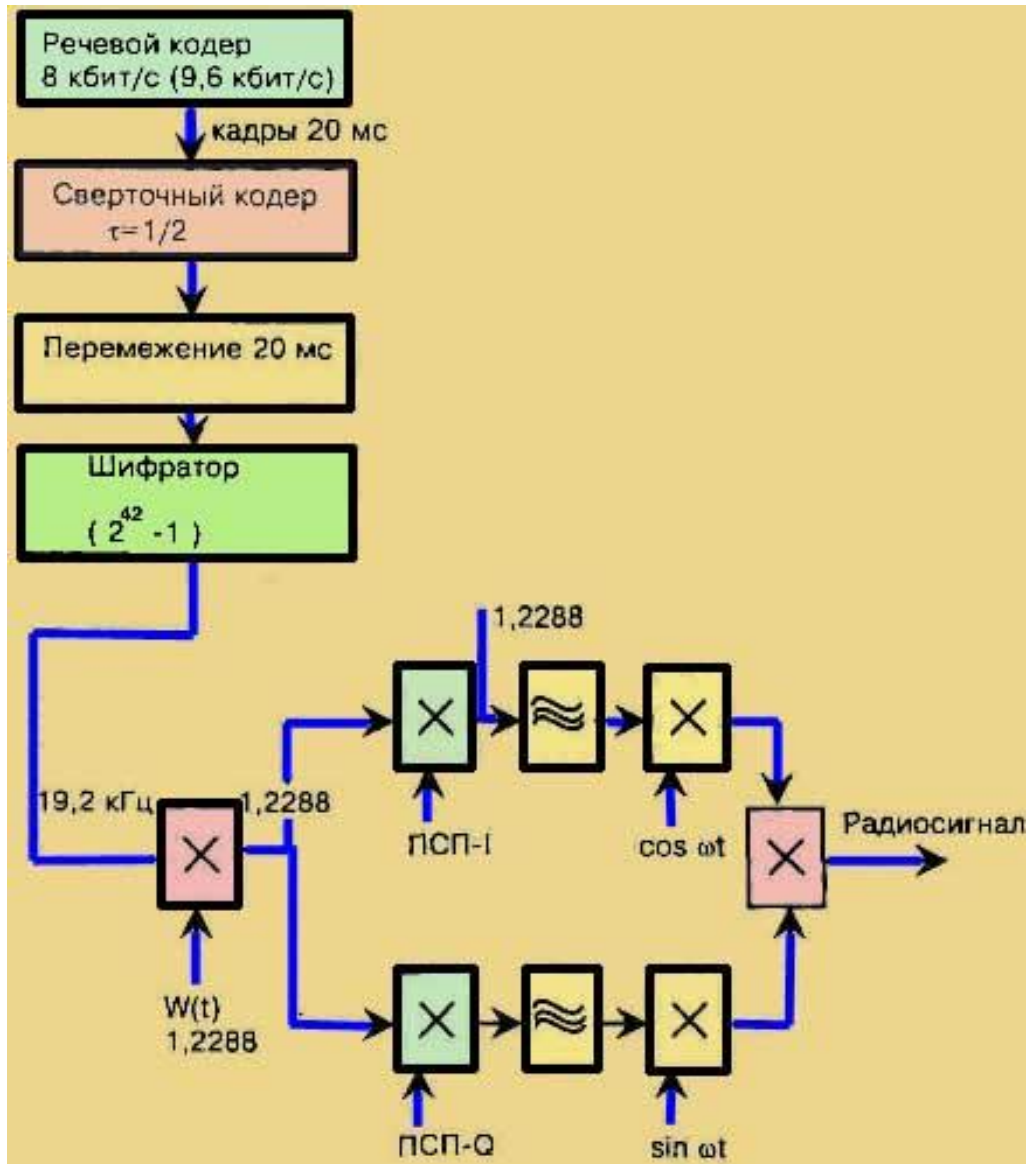


Рис. 4.6

Для передачи всех 64 каналов применяется одна и та же псевдослучайная последовательность. В каждом канале при передаче используется одна из 64 последовательностей Уолша. При изменении знака бита информационного сообщения фаза используемой последовательности Уолша изменяется на 180 градусов. Так как эти последовательности взаимно ортогональны, то взаимные помехи между каналами передачи одной базовой станции отсутствуют. Помехи по каналам передачи базовой станции создают лишь соседние базовые станции, которые работают в той же полосе радиочастот и используют ту же самую ПСП, но с другим циклическим сдвигом.

При передаче каждая подвижная станция использует ПСП с разными циклическими сдвигами, что дает возможность базовой станции при приеме разделить сигналы от подвижных станций. Структура каналов передачи подвижной станции показана на рис. 4.9. Структурная схема формирования сигнала подвижной станцией приведена на рис. 4.10. На рис. 4.11 показана структурная схема приемника базовой станции.



- W(t) - последовательность Уолша (одна из 64).
- ПСП-I/Q - квадратурные компоненты ПСП 215
- T/to= 128

Рис. 4.7

Рассмотренные условия работы системы CDMA IS-95 определяют высокие требования к регулировке уровней мощности сигналов подвижных станций, принимаемых базовой станцией.

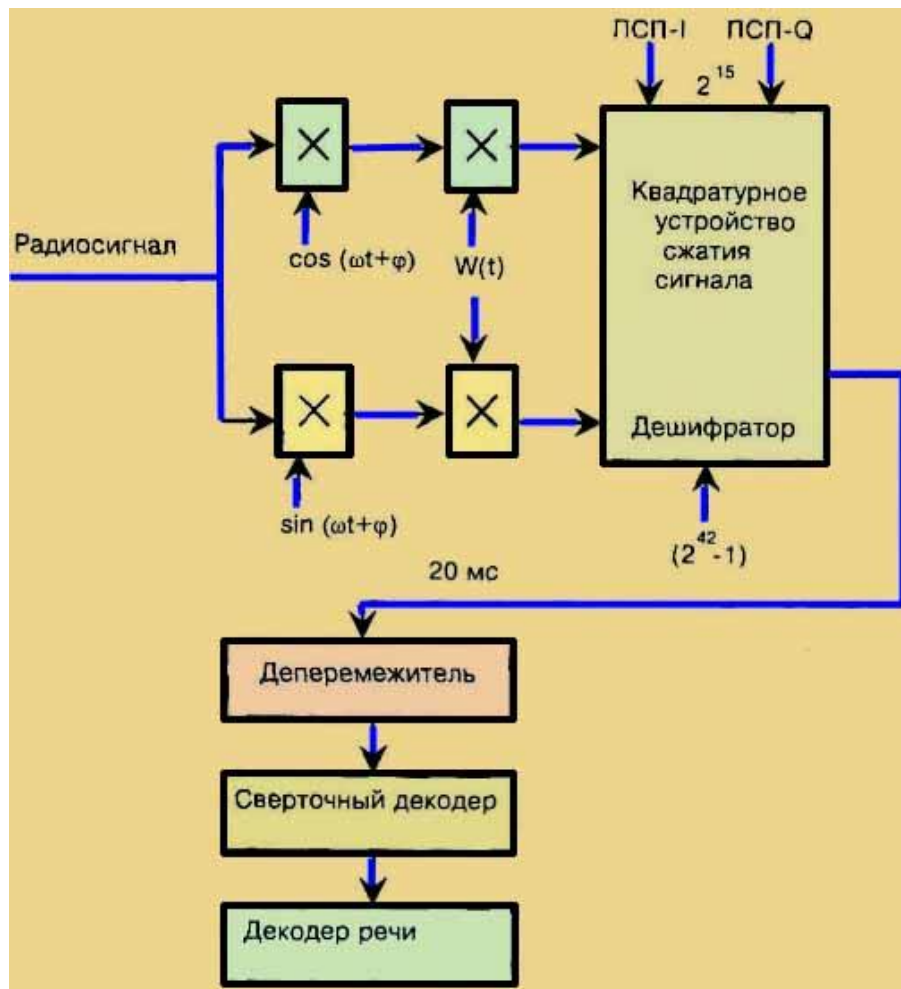


Рис. 4.8

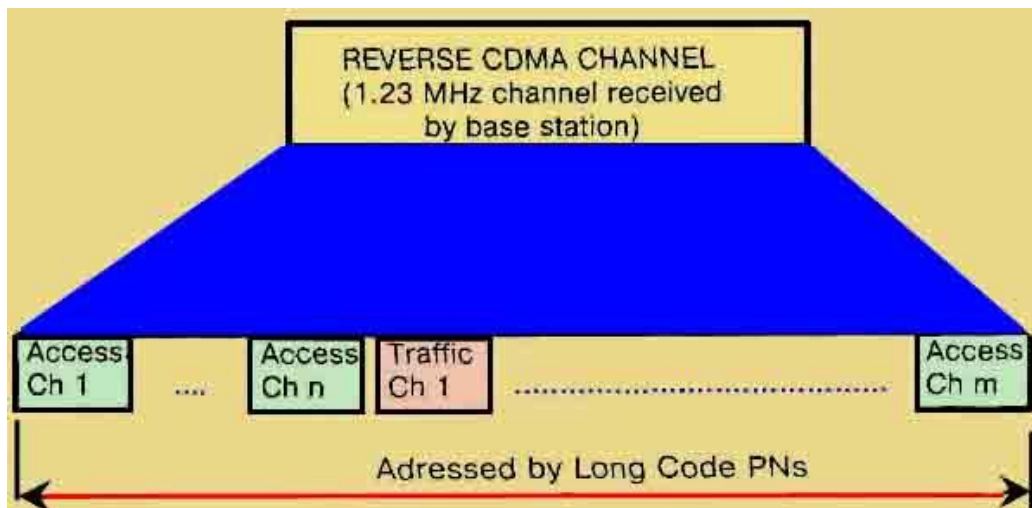
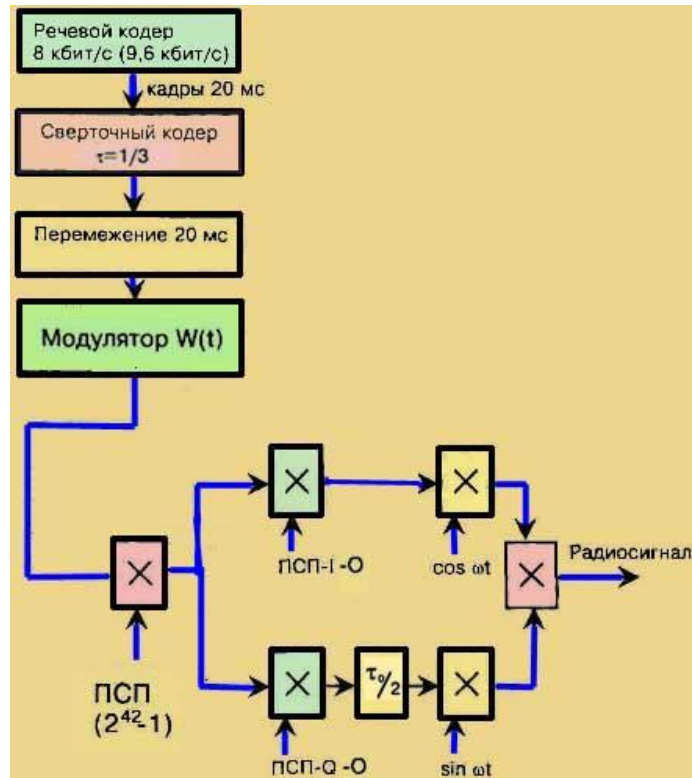


Рис.4.9



- Модулятор $W(t)$ преобразует 6 бит в одну из $2^6 = 64$ последовательностей Уолша
- ПСП-I/Q-O - универсальная последовательность для всех подвижных станций
- $T/t_o = 128$

Рис. 4.10

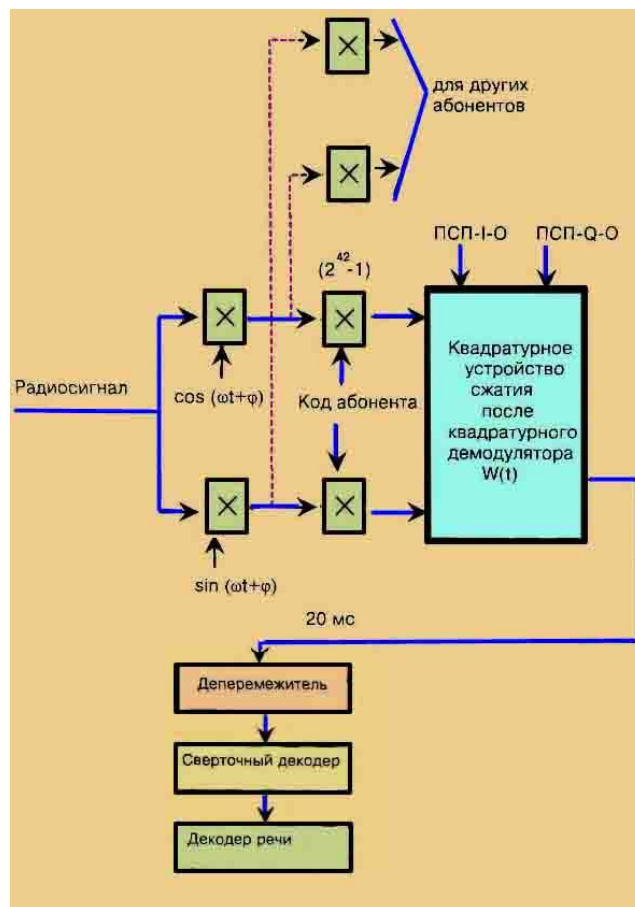


Рис. 4.11

Абонентская емкость ячейки системы CDMA IS-95 оптимизируется использованием сложного алгоритма регулировки, который ограничивает мощность, излучаемую каждым абонентским терминалом, до необходимого уровня для получения приемлемой вероятности ошибки. В системе предусмотрено медленное (статическое) управление мощностью и быстрое. Команды быстрого управления посылаются со скоростью 800 бод и встроены в разговорные фреймы. Без быстрого управления мощностью замирания, связанные с распространением радиоволн в структурах с отражающими объектами (стены домов, металлические конструкции и так далее), привели бы к значительному ухудшению характеристик системы. Медленное управление мощностью обеспечивает эквивалентное выравнивание расстояний от мобильных терминалов до базовой станции.

В системе предусматриваются три механизма регулировки мощности:

- в прямом канале — разомкнутая петля
- в прямом канале — замкнутая петля
- в обратном канале.

Рассмотрим процесс регулирования мощности передающих устройств в обратном канале. Каждая подвижная станция непрерывно передает информацию об уровне ошибок в принимаемом сигнале. На основании этой информации базовая станция распределяет излучаемую мощность меж абонентами таким образом, чтобы в каждом случае обеспечить приемлемое качество речи. Абоненты, на пути к которым радиосигнал испытывает большее затухание, получают возможность излучать сигнал большей мощности. Основная цель регулировки мощности в обратном канале — оптимизация площади соты. Регулирование мощности как в прямом, так и в обратном канале влияет и на срок службы аккумуляторов подвижных станций. Тесты показывают, что средняя излучаемая мощность подвижной станции в сети меньше, чем в системах, использующих другие методы доступа. Это непосредственно связано с такими параметрами радиотелефона, как длительность непрерывного занятия канала и время нахождения в режиме ожидания.

Процесс регулирования мощности в прямом канале происходит несколько иначе. В нем возможны два варианта регулирования: по открытому циклу (разомкнутая петля) и по замкнутому циклу (замкнутая петля).

Рассмотрим открытый цикл регулирования мощности (менее точный). Подвижная станция после включения ищет сигнал базовой станции. После синхронизации подвижной станции по этому сигналу производится замер его мощности и вычисляется мощность передаваемого сигнала, необходимая для обеспечения соединения с базовой станцией. Вычисления основываются на том, что сумма уровней предполагаемой мощности излучаемого сигнала и мощности принятого сигнала должна быть постоянна и равна — 73 дБ. Если уровень принятого сигнала, например, равен —85 дБ, то уровень излученной мощности должен быть равен ± 12 дБ. Этот процесс повторяется каждые 20 мс, но он все же не обеспечивает желаемой точности регулировки мощности, так как прямой и обратный каналы работают в разных частотных диапазонах (разнос частот 45 МГц) и, следовательно, имеют различные уровни затухания при распространении и по-разному подвержены воздействию помех.

Рассмотрим процесс регулирования мощности при замкнутом цикле. Механизм регулирования мощности при этом позволяет точно отрегулировать мощность передаваемого сигнала. Базовая станция постоянно оценивает вероятность ошибки в каждом принимаемом сигнале. Если она превышает программно заданный порог, то

базовая станция дает команду соответствующей подвижной станции увеличить мощность излучения. Регулировка осуществляется с шагом 1 дБ. Этот процесс повторяется каждые 1,25 мс. Цель такого процесса регулирования заключается в том, чтобы каждая подвижная станция излучала сигнал минимальной мощности, которая достаточна для обеспечения приемлемого качества речи. За счет того, что все подвижные станции излучают сигналы необходимой для нормальной работы мощности, и не более; их взаимное влияние минимизируется, и абонентская емкость системы подрастает. Подвижные станции должны обеспечивать регулирование выходной мощности в широком динамическом диапазоне — до 85 дБ. Такие факторы, как число пользователей и расстояние до них от базовой станции влияют на значение максимальной излучаемой мощности. Принимая это во внимание, можно сказать, что требования к линейности передаточной функции усилителя мощности, работающего при изменении уровня входного сигнала и пределах 20 дБ, чрезвычайно высоки. Линейность передаточной функции усилителя — фактор, критичный при обеспечении желаемых характеристик системы. Требуемую линейность обеспечивают сложные и дорогостоящие методы линеаризации (усилители с предварительными искажениями или усилители со связью вперед). Спектр излучаемого CDMA-сигнала, который получается в результате объединения множества кодированных по Уолшу базовых сигналов, близок к спектру шумового сигнала с отношением пикового значения к среднему около 11 дБ. Это означает, что для достижения одинакового качества связи в базовой станции GSM необходим усилитель с выходной мощностью 44 Вт; в стандарте D-AMPS (АДС) это значение снижается до 31 Вт, а в CDMA — до 10 Вт. Поэтому значительный теоретический запас энергопотенциала в радиоканале, который получается за счет использования метода расширения спектра, при сопоставимой практической реализации базового оборудования оказывается значительно меньше. Поэтому системы с кодовым разделением каналов не обеспечивают ожидаемого увеличения площади радиопокрытия базовой станции.

Высокие требования к регулировке уровня мощности подвижной станции можно отнести к недостатку системы Qualcomm. Вторым недостатком CDMA Qualcomm является необходимость использования одинаковых по размерам сот на всей сети, в противном случае возникают взаимные помехи от сигналов подвижных станций, которые находятся в соседних сотах разного размера. В этом случае также возникает проблема "эстафетной передачи".

В системе CDMA IS-95 применяются квадратурная фазовая манипуляция (QPSK) базовой и смещенная QPSK в подвижных станциях. При этом информация извлекается путем анализа изменения фазы сигнала, поэтому фазовая стабильность системы — критичный фактор при обеспечении минимальной вероятности появления ошибки в сообщениях. Применение смещенной QPSK позволяет снизить требования к линейности усилителя мощности подвижной станции, так как амплитуда выходного сигнала при этом виде модуляции изменяется значительно меньше. До того, как интерференционные помехи будут подавлены методами цифровой обработки сигналов, они должны пройти через высокочастотный тракт приемника и не вызвать насыщения малошумящего широкополосного усилителя (МШУ) и смесителя. Это заставляет разработчиков системы искать баланс между динамическими и шумовыми характеристиками приемника.

Передача сообщений в стандарте IS-95 осуществляется кадрами. Используемые принципы приема позволяют анализировать ошибки в каждом информационном кадре. Если количество ошибок превышает допустимый уровень, приводящий к недопустимому ухудшению качества речи, этот кадр стирается (frame erasure).

С частотой ошибок или " частотой стирания битов " однозначно связано отношение энергии информационного символа к спектральной плотности шума E_0/N_0 . На рис. 4.12 приведены зависимости вероятности ошибки в кадре (Prob. Frame Error) от величины отношения E_0/N_0 (белый шум) для прямого и обратного каналов с учетом модуляции, кодирования и перемежения.

При увеличении количества активных абонентов в соте из-за взаимных помех отношение E_0/N_0 снижается, а частота ошибок увеличивается. В этой связи разные фирмы принимают свои допустимые значения частоты ошибок. Например, фирма Motorola считает допустимой для CDMA IS-95 частоту ошибок в 1%, что соответствует с учетом замираний отношению $E_0/N_0 = 7-8$ дБ. При этом пропускная способность систем IS-95 в среднем в 15 раз превышает пропускную способность аналоговых систем AMPS.

Фирма Qualcomm за допустимую величину частоты ошибок принимает значение 3%. Это является одной из причин, по которым Qualcomm заявляет, что емкость CDMA IS-95 в 20 - 30 раз превышает емкость аналоговых AMPS.

Отношение $E_0/N_0 = 7 - 8$ дБ и допустимая частота ошибок в 1% позволяет организовать 60 активных каналов на трехсекторную соту. Зависимость количества активных каналов связи (ТЧН) для обратного канала от величины отношения E_0/N_0 для 3-х секторной соты показана на рис. 4.13.

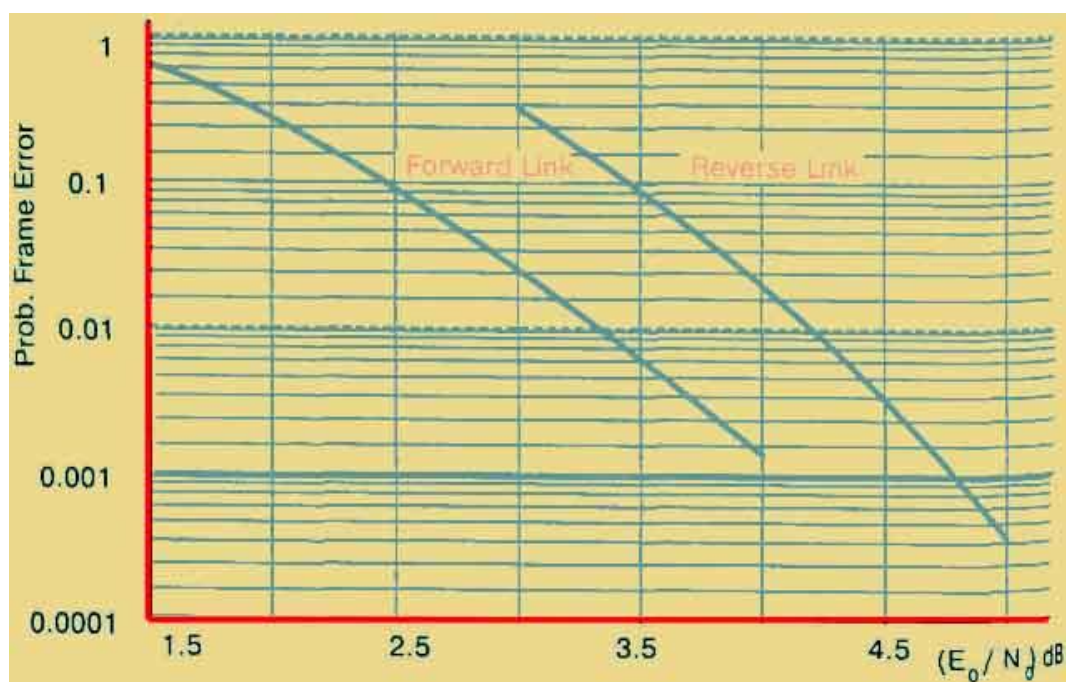


Рис. 4.12

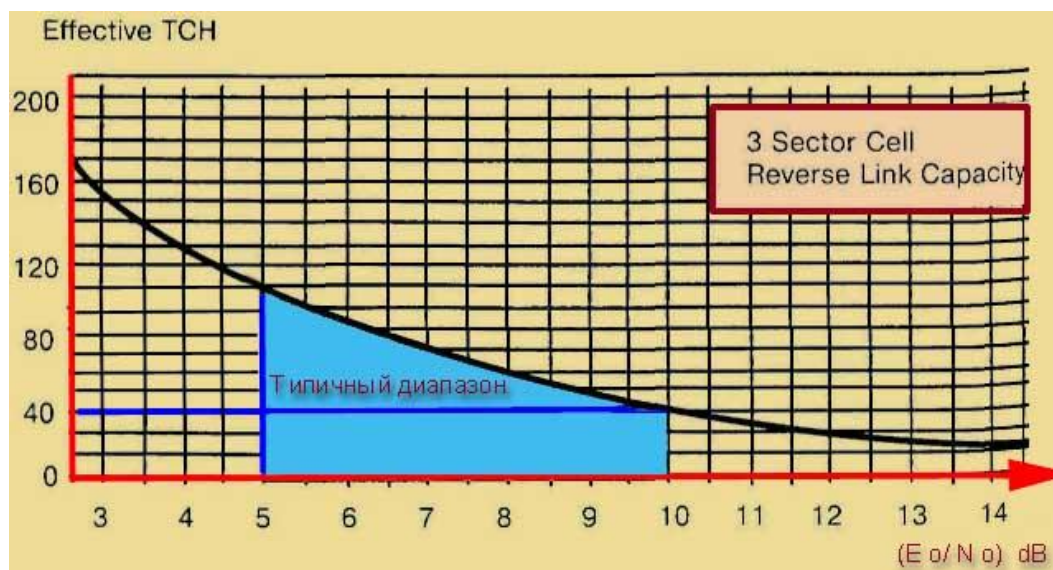


Рис. 4.13

Кодирование речи

Важным моментом для уменьшения взаимной интерференции каналов от различных абонентов является кодирование речи. Кодирование позволяет существенно уменьшить среднюю мощность передатчика. Известно, что человеческая речь — это прерывистый источник сигнала. Из измерений фирмы Bell Laboratories следует, что активность речи составляет 35–40% от общего ресурса времени. Если использовать этот фактор, то можно ещё в два или более раз увеличить ёмкость сети. На практике этот коэффициент активности составляет 50% благодаря тому, что в период молчания подвижные и базовая станции должны поддерживать физический канал связи, и мощность не может быть сведена до нуля. Таким образом, преимущество CDMA IS-95 перед AMPS может достигать 26 раз. В IS-95 используется вокодер с переменной скоростью кодирования на основе алгоритма предикативного линейного предсказания кода QCELP (Code Excited Linear Predictive). Этот алгоритм учитывает особенности человеческой речи. Вокодер перекодирует цифровой поток, имеющий скорость 64 Кбит/с, в поток со скоростью 8 или 13 Кбит/с. В ходе этого преобразования информационный поток делится на кадры, и содержащие паузы интервалы удаляются. Речевой кодек определяет голосовую активность и в паузах (во время молчания) уменьшает скорость в канале до 1200 бод. Возможны также промежуточные значения 2400, 4800. Результирующий поток имеет скорость от 1 до 8 Кбит/с. Вокодер приемной стороны объединяет кадры в единый поток и делает обратное преобразование. Другой важной особенностью вокодера с переменной скоростью кодирования является использование адаптивного порога для определения требуемой скорости кодирования данных. Уровень порога изменяется в соответствии с фоновым шумом. Результатом этого является подавление фона и улучшение качества речи даже в шумной обстановке. Вокодер позволяет подмешивать в речевой канал вторичный трафик, т. е. служебную информацию. Кодирование речи обеспечивает очень высокую степень конфиденциальности. Согласно отзыву гонконгской компании Hutchison Telecom, «подслушивание разговоров практически исключено минимум благодаря технике кодирования речи в CDMA».

Борьба с многолучевостью

В стандарте используется раздельная обработка отраженных сигналов, приходящих с разными задержками, и последующее их весовое сложение, что значительно снижает отрицательное влияние эффекта многолучевости. При раздельной обработке лучей в каждом канале приема на базовой станции используется 4 параллельно и независимо работающих коррелятора, а на подвижной станции - 3 коррелятора. Приемник с несколькими каналами приема и обработки сигнала получил название Rake-приемника. Он имеет 4 канала приема, в трех каналах одновременно обрабатываются три наиболее сильных сигнала (в четвертом канале постоянно осуществляется поиск сигнала с более высоким уровнем). При этом опорный сигнал на разные корреляторы подается с небольшим сдвигом во времени, соизмеримым с разницей по времени при прохождении радиоволн по различным траекториям. Выходные сигналы корреляторов суммируются. Таким образом, если уровень сигнала свёртки от одного из многолучевых сигналов в текущий момент времени оказывается равным нулю (в результате интерференционной картины распределения поля), то свёртка от задержанного сигнала будет отличной от нуля. Таким образом в системе с кодовым разделением каналов реализуется метод временного разнесения приема. Многолучевое распространение радиосигналов, с которым приходится бороться всем стандартам сотовой связи, в данном случае становится помощником. В случае построения фиксированных сетей многолучевые отражения позволяют снизить требования к уровню сигнала, приходящего к абонентской станции.

Организация эстафетной передачи

В случае подвижной связи абонентская станция может одновременно принимать и обрабатывать сигналы нескольких базовых станций. Это позволяет осуществлять мягкую эстафетную передачу абонента между базовыми станциями. Преимущество мягкой передачи заключается в том, что исключается возможность потери связи при движении абонента вдоль границы сот, когда имеет место эффект «пинг-понга». Транскодер, входящий в состав основного оборудования, проводит оценку качества приема сигналов от двух базовых станций последовательно кадр за кадром, как показано на рис .1 . Процесс выбора лучшего кадра приводит к тому, что результирующий сигнал может быть сформирован в процессе непрерывной коммутации и последующего "склеивания" кадров, принимаемых разными базовыми станциями, участвующими в "эстафетной передаче". Мягкое переключение обеспечивает высокое качество приема речевых сообщений и устраняет перерывы в сеансах связи, что имеет место в сотовых сетях связи других стандартов. Недостатком такого процесса управления является одновременное использование двух базовых станций.

Аспекты безопасности в стандарте IS-95

Стандарт IS-95 обеспечивает высокую степень безопасности передаваемых сообщений и данных об абонентах. Прежде всего он имеет более сложный, чем GSM, радиointерфейс, обеспечивающий передачу сообщений кадрами с использованием канального кодирования и перемежения с последующим "расширением" передаваемых сигналов с помощью составных ШПС, сформированных на основе 64 видов последовательностей Уолша и псевдослучайными последовательностями с количеством элементов 215 и 242.

Безопасность связи обеспечивается также применением процедур аутентификации и шифрования сообщений.

Процедура аутентификации в стандарте IS-95 соответствует процедуре аутентификации стандарта D-AMPS (IS-54B).

В подвижной станции хранится один ключ A и один набор общих секретных данных, которые используются при работе как в режиме с частотным разделением каналов, так и в режиме CDMA IS-95. Подвижная станция может передавать "цифровую подпись" для аутентификации, состоящую из 18 бит. Эта информация передается в начале сообщения (в ответе подвижной станции на запрос сети при поиске станции), добавляется к регистрационному сообщению или пакету данных, передаваемых по каналу доступа. Предусматривается возможность обновления общих секретных данных в подвижной станции.

Шифрование сообщений, передаваемых по каналу связи (ТСН), осуществляется также с использованием процедур стандарта IS-54B.

В стандарте IS-95 используется также режим "частный характер связи", обеспечиваемый с помощью секретной маски в виде длинного кода. Этот процесс также аналогичен процессу формирования маски в виде длинного кода, который описан в стандарте IS-54B.

Состав оборудования

Подвижная станция стандарта IS-95

Фирмы Qualcomm и Motorola разработали двухрежимные CDMA IS-95 подвижные станции, которые поддерживают связь с существующими сетями аналоговых стандартов с частотной модуляцией (AMPS и N-AMPS). Это обстоятельство дает значительные преимущества абонентам CDMA IS-95, так как позволяет использовать свой радиотелефон там, где существующие аналоговые сотовые сети обеспечивают радиопокрытие.

Структурная схема подвижной станции для CDMA IS-95 фирмы Qualcomm приведена на рис. 4.14, Основное отличие между абонентскими станциями CDMA IS-95 и существующими станциями аналоговых стандартов заключается в добавлении в состав подвижных станций CDMA IS-95 функций цифровой обработки сигналов, которые реализованы в настоящее время на трех заказных СБИС. Эти три интегральные схемы конструктивно объединяются в одном устройстве.

Базовая станция стандарта IS-95

В системах связи CDMA IS-95 используются соты с круговой диаграммой направленности антенн или секторные соты (обычно 120-градусные).

На рис.15 показана типовая структурная схема базовой станции (BTS) для соты с круговой диаграммой направленности антенны с цифровым оборудованием, в состав которого входят каналные блоки. Каждый каналный блок может быть сконфигурирован как информационный канал или как служебный канал. Для синхронизации работы сети используется приемник GPS (глобальная система местопределения). Сюда входят генератор, формирующий секундные импульсы, и опорный тактовый генератор.

Отсек приемопередатчика преобразует сигналы промежуточной частоты, сформированные в отсеке цифрового блока, в радиочастотный сигнал на несущей частоте и обеспечивает обратное преобразование принимаемого сигнала на промежуточную частоту. В направлении передачи сигнал проходит от приемопередатчика через усилитель мощности и фильтр к передающей антенне. В обратном направлении тракт приема начинается с приемных антенн, фильтра, усилителя с низким коэффициентом шума. Затем в приемопередатчике сигнал преобразуется на промежуточную частоту и поступает в отсек цифрового оборудования. Следует отметить, что передающий и приемные тракты

подключаются непосредственно к своим антеннам, что позволяет исключить дорогостоящие сумматоры мощностей и потери мощности при сложении.

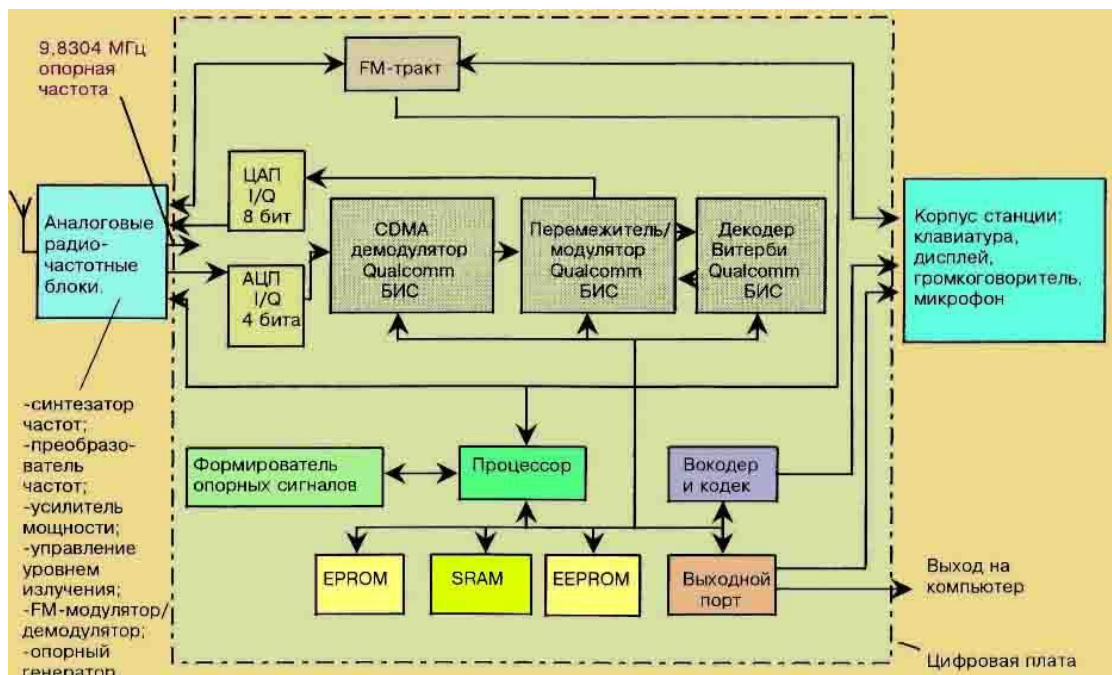


Рис. 4.14

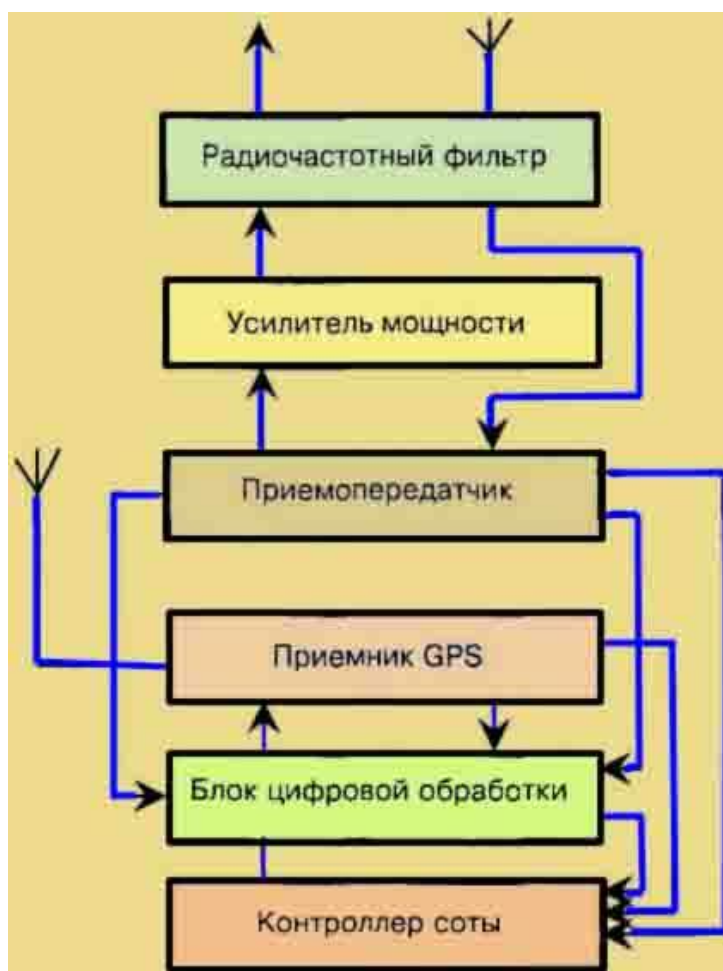


Рис. 4. 15

Управление режимами работы цифрового оборудования и приемопередатчика осуществляется контроллером соты (CC). Контроллер соты обеспечивает требуемые режимы и алгоритмы работы оборудования внутри соты, назначает и конфигурирует ресурсы BTS для обслуживания нагрузки и вызовов, формирует статистическую информацию о работе соты, контролирует распределение сигналов опорных частот. Он также управляет объединением портов канальных блоков для передачи сообщений в цифровую линию к контроллеру сети (BSC) и центру коммутации подвижной связи (MSC).

Рассмотренные принципы построения системы стандарта IS-95, возможность одновременной работы подвижных станций в существующих сетях сотовой связи определяют перспективность развития сетей связи CDMA в регионах, где уже действуют сети связи стандартов AMPS, N-AMPS и D-AMPS. Совместное использование сотовых сетей связи указанных стандартов с частотным и кодовым разделением каналов обеспечит значительное увеличение количества обслуживаемых абонентов, расширит состав услуг и зону покрытия связью. Ниже приведены основные характеристики CDMA IS-95 и их краткое описание, определяющие достоинства и перспективность систем сотовой связи с кодовым разделением каналов.

Характеристики CDMA IS-95 и их описание:

- Высокая пропускная способность. Полевые испытания, проводившиеся в различных условиях, подтвердили, что при высокой нагрузке пропускная

способность систем CDMA в среднем в 15 раз превышает пропускную способность аналоговых систем. Если выражать это в Эрлангах при заданном качестве обслуживания, то преимущества систем CDMA еще более очевидны. При использовании существующих вокодеров, которые работают на половинной скорости передачи, пропускная способность увеличивается еще в 1,7 раза (при том, что для сети CDMA необходимо на 30-40% базовых станций меньше, чем для GSM, и в 2-3 раза меньше, чем для AMPS). Дополнительная секторизация (свыше 3) также увеличивает пропускную способность. Существует возможность выделения требуемой полосы частот по потребности. Кроме того, максимальная дальность связи (в отличии от TDMA-систем) ограничена лишь мощностью и радиовидимостью.

- Высококачественная связь. Вокодер, работающий на переменной скорости передачи, обеспечивает преобразование речевых сигналов в цифровую форму и высококачественное воспроизведение речи. Фоновые сигналы заглушаются даже при большой нагрузке. Система независимо отслеживает поступающие отдельные сигналы при многолучевом распространении, что значительно снижает подверженность замираниям. Это свойство дает дополнительные преимущества CDMA в условиях городов с высотными застройками. Система CDMA обеспечивает меньшую задержку в передаче голосового сообщения, чем другие системы подвижной связи. При использовании CDMA не приходится применять изошренные средства для подавления эхо-сигнала. Метод мягкого хэндовера абонента, применяемый в системах CDMA, обеспечивает почти прозрачную передачу вызовов между сотами. Такой надежный метод передачи практически исключает потерю вызовов и снижает нагрузку на коммутационное оборудование. Кроме того, излучаемая мобильными аппаратами средняя мощность в сотовых системах CDMA составляет менее 10 мВт, что на 1-2 порядка ниже мощности, требуемой в системах с временным разделением каналов TDMA .
- Возможность дальнейшей эволюции системы. В существующей системе предусмотрены поисковые службы и цифровая передача данных. Существующая структура управления обеспечивает протоколы факсимильной связи. Могут быть предусмотрены и более высокие скорости передачи (в настоящее время используется скорость 9,6 кбит/с). Портативные абонентские станции, основанные только на методе CDMA и совместимые с сотовыми системами и УАТС, могут отвечать перспективным требованиям. CDMA предоставляет дополнительный сервис, обеспечивая одновременную передачу голоса и факса по одному каналу. В технологии CDMA реализованы оригинальные алгоритмы упаковки данных для большей скорости их передачи
- Возможность введения новых функций. При желании с одного и того же аппарата можно получить выход к беспроводной УАТС, домашнему беспроводному телефону, общественным беспроводным цифровым телефонным аппаратам, к сети персональной связи и к сотовым сетям. Обеспечиваются интерфейсы с УАТС, сетью ISDN и коммутируемой телефонной сетью общего пользования. Цифровые сигналы управления позволяют организовать целый ряд служб передачи данных, которые можно добавлять по мере того, как компания-оператор будет вводить новые услуги. Вокодер с переменной скоростью передачи и предусмотренная возможность передачи данных позволяют вводить различные уровни обслуживания. Предусмотренные в системе измерения уровня сигнала и его задержки позволяют определять положение подвижной станции.

- Секретность связи. Цифровая форма сигналов, передача в широкой полосе частот, защита информации для каждого адресата - все это обеспечивает значительно более высокую, чем в других системах, секретность связи.
- Простота перехода (и совместимость с аналоговыми системами). CDMA позволяет увеличить ёмкость базовых станций (в 8–10 раз по сравнению с AMPS , в 4–5 раз — по сравнению с GSM) и обеспечивает более высокое качество обслуживания. Пропускная способность и радиопокрытие позволяют вводить CDMA при значительно меньшем числе сот, чем на существующих сетях. Зона радиохвата антенны и секторизация не зависят от соты и не так тесно связаны, как в узкополосных системах. Последующее расширение может быть поэтапным и может быть местным (чтобы быстро обеспечить радиопокрытие в каком-то одном месте) или глобальным. Абонентские станции CDMA рассчитаны на работу в двух режимах, поэтому они могут подключаться либо к каналам CDMA, либо к аналоговым каналам AMPS. Отсутствие частотного планирования благодаря использованию тех же самых частот в смежных секторах каждой соты также облегчает задачу разработки сетей.
- Цена и наличие оборудования. Существующие оценки стоимости системы CDMA в отношении сетевого и абонентского оборудования показывают, что по стоимости эта система эквивалентна существующим аналоговым системам. Более высокая пропускная способность позволяет организовать связь при значительно меньшем числе сот, чем в аналоговых системах и системах с TDMA, что снижает капитальные и эксплуатационные затраты. Проверенная технология заказных интегральных схем позволила свести технологию сложных схем CDMA к очень простым решениям.

Недостатки IS-95 (общие для CDMA-систем)

- Необходимость сложного регулирования уровня мощности;
- Потеря синхронизации "не успевание" на скорости выше 100-120 км/час;
- Сложности реализации эффективного "мягкого хэндовера".
- Некоторая количественная ограниченность ортогональных последовательностей.
- Неопределенность полноправного легального использования в России.

Стандарт радиотелефонной связи DECT

В 1992 году Европейским институтом телекоммуникационных стандартов (ETSI) был официально опубликован новый беспроводной стандарт - DECT (Digital Enhanced Cordless Telecommunications, усовершенствованная цифровая телефония). Спектр рабочих частот нового стандарта расположился в диапазоне 1880-1900 МГц. Успех нового стандарта стал сенсацией в мире связи.

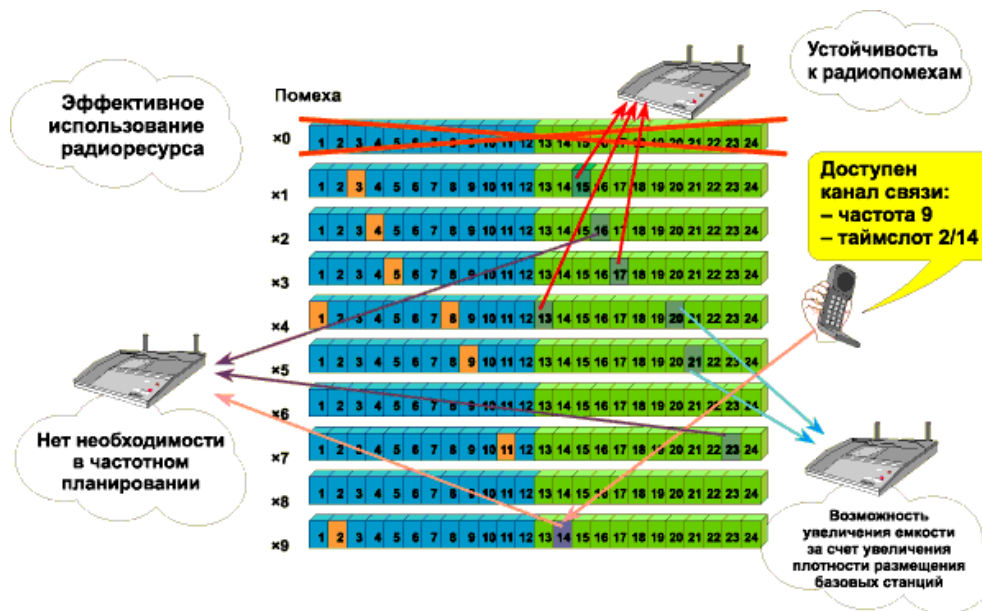


Рис. 4.16

Стандарт DECT описывает технологию радиодоступа для передачи информации исключительно в цифровом виде на расстояния от 5 м до 10 км. Основная характеристика данной технологии - высокая, по сравнению с обычными системами сотовой связи, плотность телефонной емкости в радиосоте малого радиуса. Это полностью цифровой стандарт, поэтому он позволяет предоставлять все услуги цифровой связи, включая широкополосные (ISDN). Область применения DECT - от простого беспроводного телефона до системы, обеспечивающей различные телефонные услуги в рамках городского (или сельского) районного телефонного узла. Говоря конкретнее, Стандарт DECT поддерживает речевую и факсимильную связь, а также передачу данных. Кроме того, он разработан с учетом современных телекоммуникационных тенденций, таких как конвергенция фиксированных и мобильных сетей, интеграция речевой связи и передачи данных, мультимедийные услуги и одновременный сервис от нескольких операторов. Говоря конкретнее, основные сферы применения стандарта DECT - это системы микросотовой связи для бизнеса (беспроводные учрежденческие АТС для средних и крупных организаций, распределенных производств, заводов), устройства абонентского доступа к телекоммуникационной сети общего пользования как альтернатива стандартному проводному подключению (Wireless Local Loop), односотовые радиотелефоны и радио АТС для дома, для малых офисов.

В основе DECT - концепция абсолютной персонализации связи, которая позволяет перейти от старого принципа вторичной сети "телефон каждой семье, квартире, рабочему месту" к принципу "телефон каждому человеку", что должно привести к коренным изменениям первичной сети и, далее, всей инфраструктуры телекоммуникаций. DECT, по сути, завершает развитие систем радиосвязи второго поколения.

На основе его могут быть созданы:

- домашние бесшнуровые многотрубочные системы, которые также подходят для малого офиса
- микросотовые беспроводные корпоративные системы (офисные и учрежденческие АТС с радиодоступом)
- микросотовые системы общего пользования (СТМ)
- системы фиксированного радиодоступа (WLL) и др.

В качестве средства WLL стандарт DECT на сегодня занял почти 50% этого рынка в мире (1-е место), обогнав такие стандарты как CDMA и DAMPS.

Высокая эффективность использования выделенного частотного диапазона достигается за счет отказа от закрепленных частотных каналов. Это становится возможным благодаря процедуре полнодоступного мгновенного динамического выбора свободного канала с оценкой его помехоустойчивости. Такая процедура позволяет устанавливать базовые станции ближе друг к другу без потерь в качестве.

Каналы для передачи речи и данных в DECT-стандарте образуются за счет использования 10 несущих частот по технологии временного разделения с множественным доступом и временного дуплексирования (Multy Carrier/Time-Division Multiple Access/Time-Division Duplexing). Емкость систем DECT (показатель, учитывающий напряженность абонентского трафика, ширину используемого частотного диапазона и площадь покрытия - Эрланг/МГц/кв. км/ выше, чем других цифровых систем мобильной связи и составляет 500 Эрланг/МГц/кв.км /для сравнения: емкость систем стандартов GSM-10, DCS-1800 равна 100 Эрланг/МГц/кв.км). Теоретически одна базовая DECT радиостанция может одновременно предоставлять 120 каналов передачи речи/данных для беспроводных абонентов. Поэтому оборудование DECT подходит для организации мобильной связи там, где на небольшой площади сосредоточено много абонентов. Это важно как для деловых применений, так и для операторов, предоставляющих услуги связи. Подключение абонентов к сетям связи с помощью оборудования DECT (решение вопроса "последней мили") может оказаться экономически эффективнее стандартного кабельного подключения, а в некоторых случаях - единственно возможным. Такие системы быстрее развертываются, проще расширяются, легче в управлении, надежны в эксплуатации.

Абонент подключается с помощью фиксированного устройства доступа (FAU), устанавливаемого, как правило, снаружи жилища или офиса, и выполняющего функции приемопередатчика, являясь устройством, преобразующим DECT-радиосигналы в сигналы обыкновенной аналоговой телефонной линии, что дает возможность пользователю подключить обычное аналоговое оборудование, например телефонные аппараты, факсы и модемы. Оборудование WLL дает полный доступ ко всему сервису телефонной сети.

Системы микросотовой телефонной связи стандарта DECT подключаются к используемой в организации АТС, образуя единую телефонную систему, добавляя к проводным абонентам АТС беспроводных мобильных абонентов. Структура таких систем схожа с обычными, "городскими" системами сотовой связи. Единственное, по сути, отличие - масштабы. Создается своя, микросотовая ведомственная сеть связи, обслуживающая сотрудников. Мобильный абонент получает компактный DECT-радиотелефон. Зона радиообслуживания создается сетью базовых радиостанций, каждая из которых имеет определенную зону действия (микросоту); микросоты, перекрываясь, делают незаметным для мобильного абонента переход из зоны действия одной базовой

радиостанции в другую. Базовые радиостанции подключаются к центральному модулю, который обрабатывает сигналы мобильных абонентов и обеспечивает интерфейс стыковки с АТС (по аналоговым либо цифровым линиям).

Одной из наиболее привлекательных перспектив развития DECT-систем является возможность взаимодействия стандартов DECT и GSM. Оба эти стандарта основаны на цифровой радиопередаче по технологии TDMA. Но между этими стандартами существует и существенная разница в обеспечении мобильности абонента и емкости систем.

Стандарт DECT оптимизирован, прежде всего, для использования при напряженном трафике, характерном для условий, где много абонентов на небольшой площади (заводы, бизнес центры, выставочные центры). Скорость передвижения абонента DECT-систем ограничена пешеходной скоростью человека. Это является существенным требованием к абоненту DECT-систем. Напротив, в стандарте GSM заложены возможность абонента передвигаться на автомобиле или поезде, возможность роуминга в других странах. Но, как уже отмечалось, емкость GSM-стандарта меньше, чем DECT, поэтому невозможно обеспечить напряженный бизнес-трафик без установки дополнительного микросотового GSM-оборудования. Поэтому очень перспективным является совмещение двух стандартов в одном радиотелефоне. Это позволит использовать DECT-стандарт в офисе и GSM вне его.

Корпорация Ericsson, например, выпускает радиотелефоны Freeset, которые способны работать как в DECT, так и в GSM-стандарте. Радиотелефон автоматически переключается в GSM-стандарт, когда абонент покидает зону радиообслуживания системы Freeset. Став, к примеру, абонентом сети мобильной связи, можно использовать такой телефон и как стандартный сотовый аппарат.

DECT-стандарт позволяет организовать передачу данных, что делает возможным построение беспроводных ЛВС на основе оборудования абонентского доступа.

Базовый стандарт DECT CI является описанием технологии доступа, а не подвижной системы связи (как для NMT, TACS, AMPS, GSM/DCS1800), поэтому он содержит полный набор протоколов, обеспечивающих гибкость при соединении с различными сетями. В отличие от описания системы связи описание сети не является частью спецификации DECT. Техническая часть DECT CI - это набор описаний радиоинтерфейсов между стационарным (FP) и подвижными (PP) блоками. Модуль взаимодействия (IWU), оконечное устройство (ES), алгоритмы аутентификации и шифрования не входят в спецификации DECT.

DECT CI можно определить как высокоизбыточный интерфейс с магазином протоколов и сообщений, обеспечивающих согласование сети (локальной или глобальной) с оконечным устройством ES (телефонной трубкой, портом компьютера, выходом факсимильного аппарата). Этот интерфейс должен обеспечивать лишь беспроводность, возможности мобильного и гибкого добавления новых средств и развития приложений (рекомендации ETS 300 175, части 1-8 и ETR 043 "Общие спецификации интерфейса и требований к DECT") - и ничего другого.

Для организации интерфейса передачи данных DECT использует семейство профилей (A/B, C, D, E, F...), которые ориентированы на взаимодействие с локальными сетями, передачу данных мультимедиа и последовательную передачу данных. Профили имеют модульную структуру, тесно взаимосвязаны, обеспечивают аутентификацию и засекречивание. Возможности профилей и услуги передачи данных описаны в документе

ETR 185. DECT обеспечивает высокочастотное уплотнение ($n \cdot 24$ кбит/с), поддерживая скорость передачи данных до 552 кбит/с (69 Кбайт/с). Работа над созданием профилей не завершена, и дальнейшее развитие возможностей DECT будет определяться новыми профилями.

Передача голосового сообщения имеет естественный приоритет (за исключением профиля ISDN-64 и высокоскоростной изохронной службы передачи данных), при этом формирование вызовов осуществляется в промежутках между передачей пакетов, а приоритетность обеспечивается путем обязательного использования процедур приостановки и восстановления передачи.

Для передачи данных предлагается диапазон скоростей 1,2-4,8 кбит/с. При высоком качестве канала (высокая направленность антенн в условиях прямой видимости и почти отсутствующее затухание при передаче) возможно увеличение скорости до 9,6 кбит/с. Такое значение скорости является типичным для всех радиотехнологий, в которых используется передача по модему для кодека со сжатием речи без помехозащиты, - таких как CT2 (бесшнуровой телефон второго поколения, Великобритания), PHS и PACS. Из всех стандартов только DECT предоставляет помехозащищенный (LU7) 64-кбит/с канал для передачи данных по протоколу V.34.

Для ISDN определены два профиля - оконечного устройства системы (ES) и промежуточной системы (IS). Профиль ES обеспечивает услугу ISDN через FP, используя сигнализацию DECT, при этом FP и PP вместе эмулируют терминал ISDN. В профиле также определен характер взаимодействия радиointерфейса протокола DECT с сетевым интерфейсом протокола ISDN. Пользователь получает доступ к услугам через PP, а FP осуществляет взаимодействие с GAP, дополняя его основные функции. Профиль IS обеспечивает беспроводную связь между сетью ISDN и ISDN-терминалами (TE), связанными каналом (2B+D) в точке S в PT. Понятно, что такая схема может потребовать нескольких стандартных несущих DECT с уплотнением. Ведется разработка профиля с каналом (30B+D).

Хотя услуга ISDN требует больших ресурсов системы DECT, за счет возможностей согласования ISDN-телефония обеспечивает ту же эффективность использования спектра, что и обычная телефония. При передаче данных заданного объема достигаются в 6 раз более эффективное использование спектра и меньшая степень загруженности оборудования, чем при передаче через телефонную линию.

В профилях применяется комбинация защищенных и незащищенных каналов. Незащищенным считается дуплексный полнослотовый канал, способный передавать речь со скоростью 32 кбит/с без помехозащиты и BER не хуже 10^{-3} . Защищенным является дуплексный канал с двойным слотом, передающий речь со скоростью 64 кбит/с с помехозащитой (помехозащита по схеме с запросом на повторную передачу и исправлением ошибок), что повышает скорость до 80 кбит/с и увеличивает помехоустойчивость с BER 10^{-3} до BER 10^{-8} .

Что касается эффективности ISDN-RLL, то поскольку осуществляется мгновенное выделение несущей, возможно различное число одновременно используемых В-каналов сети ISDN на радиointерфейсе. Например, СТА с одиночным радиоканалом может обслуживать PABX 20-25 абонентов, тогда как СТА с двумя радиоканалами способен обслуживать 60-70 абонентов (около 0,2 Е трафика на абонента). При использовании секторных направленных антенн, особенно при обеспечении прямой видимости, применение большого числа В-каналов достаточно эффективно.

Набор описаний и процедур магазина интерфейсов стандартизирован ETSI (стандарты профилей DECT). В частности, общий профиль доступа (GAP), профиль взаимодействия DECT/GSM (GIP) и профиль доступа RLL (RAP) включают в себя все требования к изготовителям по совместимости оборудования. Использование профилей может быть обязательным (для базовых профилей) и факультативным (для каждой конфигурации FP и PP - своя номенклатура).

GAP (профиль общего доступа ETS 300 444) является базовым профилем DECT, поддерживающим телефонную связь в полосе 3,1 кГц. Среди требований к профилю - минимальные требования к совместимости, включая управление подвижностью и элементы соблюдения конфиденциальности, а также требования к сети подключения. Этот интерфейс должен быть доступен при запросе от PP и роуминге от FP, к которому PP подключился в процессе роуминга.

Для речепреобразующего устройства принят стандарт кодирования речи ITU-T G.726, обеспечивающий скорость кодирования речи 32 кбит/с по методу Адаптивной ДИКМ.

Администрирование (доступ к различным системам с одного терминала) осуществляется на основе идентификатора права доступа (ARI) в базовом блоке и идентификаторов доступа (PARK) в подвижном блоке. Количество ARI и PARK в блоках определяет конфигурацию системы и возможности ее взаимодействия с другими DECT-системами. Стандарт позволяет организовывать вторичные идентификаторы права доступа (SARI) между выделенными базовыми станциями - с целью их совместного использования, обеспечения общего доступа через частную сеть, предоставления доступа к нескольким провайдерам услуг и др.

Сравнение беспроводных системам связи DECT и IS-95.

Некоторый интерес представляет сравнение DECT и PHS. PHS (переносные системы связи общего пользования) - это японский стандарт, который его разработчики считают аналогом и конкурентом DECT. Основанные на этом стандарте услуги за пределами Японии не оказываются, лишь фирма NEC предлагает общий доступ по RLL с той же дальностью, которую обеспечивает DECT (5 км). С точки зрения анализа рынка представляет интерес тот факт, что PHS (продукты на его основе начали продаваться раньше, чем продукты DECT-технологии) получил широкое признание в Японии, куда было поставлено более 4,2 млн. аппаратов для пешеходного населения в течение чуть более года.

Не вдаваясь в подробности, можно отметить, что PHS (как и все другие разработки подобного рода) имеет существенный недостаток - постоянную привязку несущих частот. Это делает систему в целом менее помехозащищенной, чем при динамическом распределении диапазона, что не компенсируется сокращением времени на установку частоты несущей (поскольку нет необходимости в выборе канала подвижными средствами). Возможности DECT по работе с мультимедийными приложениями не оставляют PHS никаких шансов.

Однако стоит сказать и о недостатках DECT, а также принятых в нем компромиссах. Технология DECT имеет худшие, чем в PHS, показатели допуска на временное рассеяние. Допуск на время рассеяния - важный параметр, который определяет стоимость инфраструктуры в условиях низкой плотности трафика для приложений, используемых вне помещений. Допуск на распространение задержки в DECT (эффективное значение

задержки при высокой плотности базовых станции составляет 200 нс), правда, достаточен для того, чтобы не ограничивать потенциальные технические и экономические возможности в следующих инфраструктурах: больших промышленных зонах (открытые и закрытые помещения), зонах СТМ с 300-400-метровыми интервалами между базовыми станциями, 5-километровых (или более) зонах распространения сигнала от радиорелейных станций, всех зонах с малой напряженностью поля и экстремальным значением времени распространения. Кроме того, задержка может быть компенсирована за счет установки беспроводной ретрансляционной станции WRS.

Сейчас широко рекламируются системы с кодовым разделением каналов (CDMA), особенно системы IS-95, поэтому имеет смысл провести сравнение последней с DECT при использовании в местной сети. (Большинство публикаций по данному вопросу принадлежат сторонникам и разработчикам CDMA, поэтому сведения могут быть не вполне объективными. Вообще говоря, подобные сравнения справедливы только для оценки максимальной емкости соты DECT, окруженной множеством других сот, а в случае одиночной соты неуместны.

Все расчеты проводились путем моделирования, причем одна и та же фирма осуществляла на основе выбранного сценария развертывания моделирование как для DECT, так и для IS-95. Сценарий развертывания CDMA базировался на следующей конфигурации системы: ячейка из трех секторов с семью несущими частотами CDMA в выделенном частотном диапазоне шириной 20 МГц, скорость передачи речи 8 кбит/с. Постаравшись быть как можно более объективными, сделаем осторожные выводы.

При передаче речи емкость зоны CDMA по меньшей мере в 2-3 раза выше емкости системы DECT, однако DECT больше подходит для услуг передачи данных. Надо также отметить, что IS-95 непригодна для ISDN и мультимедийных приложений, что роняет ее престиж как технологии последнего поколения.

Самым важным недостатком IS-95 можно считать то, что два или более операторов не могут совместно использовать спектр в одной географической зоне. Необходимо делить его между операторами, а кроме того, выделять специальные промежуточные полосы защиты. Два оператора CDMA могут совместно использовать тот же спектр в смежных географических областях только за счет уменьшения емкости. Кроме того, при наличии выделенного спектра для WLL IS-95 в том же спектре допустимо присутствие и WLL DECT.

Совместное применение операторами CDMA и DECT одного спектра в соседних географических областях возможно при некотором уменьшении телефонной емкости и координировании размеров зон/сот в пограничных областях. На это затрачиваются меньшие или такие же усилия, как в уже описанной ситуации совместного использования спектра двумя операторами CDMA.

Для речевых услуг использование технологии CDMA оказывается вдвое более рентабельным при очень низкой плотности абонентов. Применение DECT, в свою очередь, в два раза рентабельней для районов со средней и высокой плотностью абонентов. Точка излома рентабельности - 7 абонентов на 1 км².

Сравнение возможных услуг, предоставляемых DECT и IS-95 (на базе CDMA) для сельской WLL с одинаковым частотным ресурсом

Параметр WLL	DECT	IS-95 (CDMA)
Передача речи	85 E (скорость передачи 32 кбит/с)	158-248 E (скорость передачи 13 кбит/с)
Прозрачный модем	До 28,8 кбит/с	-
Канал ИКМ 64 кбит/с	+	-
ISDN	+	-
Пакетная передача данных	До 552 кбит/с	9,6 кбит/с (в перспективе до 14,4 кбит/с)
Радиус зоны охвата	До 5 км	Больше 5 км

5. СТАНДАРТЫ КОДИРОВАНИЯ В ПЕЙДЖИНГОВОЙ СВЯЗИ

Персональный радиовывоз (пейджинг) - услуга электросвязи, обеспечивающая беспроводную одностороннюю передачу информации в пределах обслуживаемой зоны. По назначению системы пейджингового радиовещания (СПРВ) можно разделить на частные (ведомственные) и общего пользования.

Частные СПРВ обеспечивают передачу сообщений в локальных зонах или на ограниченной территории в интересах отдельных групп абонентов. Как правило, передача сообщений в таких системах осуществляется с пультов управления диспетчерами без взаимодействия с телефонной сетью общего пользования (ТФОП).

Под СПРВ общего пользования понимается совокупность технических средств, через которые через ТФОП происходит передача в радиоканале сообщений ограниченного объема. Развитие СПРВ происходит путем внедрения техники автоматического взаимодействия с ТФОП, применения цифровых способов передачи вызовов (адресов) и сообщений в буквенно-цифровом коде, повышения пропускной способности и помехоустойчивости, через миниатюризацию и уменьшение потребления электроэнергии оконечными устройствами.

СПРВ разрабатывались для предоставления услуг в полосах частот 80-931 МГц. Конкретные номиналы частот выделялись на основе национальных условий использования СПРВ, а также в зависимости от вида передаваемых сообщений.

В настоящее время различными фирмами США, Великобритании, Японии и других стран разработаны многочисленные типы национальных и частных СПРВ. Ключевым фактором в развитии СПРВ явилась стандартизация радиоинтерфейса.

Характеристика протоколов пейджинговой связи

Передача адресной информации и сообщений в цифровых системах (в том числе и пейджинговых) осуществляется в определенном формате (протоколе) кодирования. История создания и развития протоколов пейджинговой связи насчитывает более полутора десятков различных форматов связи. Первым протоколом пейджинговой связи является двухтоновый формат, разработанный в 50-х годах фирмой MULTITON и предусматривающий передачу на радиостанцию адреса – двух тоновых посылок различной частоты.

Долгое время после этого разрабатывались и применялись форматы связи, обеспечивающие работу тоновых пейджером. К середине 70-х годов были разработаны и внедрены широко применяемые и сегодня протоколы POCSAG, GOLEY, NEC, предусматривающие модуляцию высокочастотного сигнала двоичным кодом.

Протоколом чемпионом по количеству используемых в мире в последнее десятилетие пейджером, работающих в этом формате, является **POCSAG**. Это действительно универсальный протокол, позволяющий передавать цифровые, буквенно-цифровые и тоновые сообщения на скорости 512, 1200 и 2400 бод, что поддерживает уникальную адресацию по 2 млн. номеров пейджером и обеспечивает ресурс одной частоты СПРВ по количеству обслуживаемых абонентов в пределах 10 – 20 тыс.

Пейджинговый стандарт **GSC** был разработан компанией Motorola в 1983 г. на основе последовательного кода Голя - GSC (Golay Sequential Code). Код GSC может использоваться в сетях персонального радиовывоза для передачи как исключительно сигналов вызова, так и вызова совместно с речевым сообщением в аналоговом или буквенно-цифровом виде. В зависимости от поставленной задачи формируются различные виды пакетов. В передаваемом пакете содержатся избыточные биты (паритетности), что позволяет при приеме осуществлять исправление двух ошибок в кодовом слове. Скорость передачи пакета составляет 600 бит/с.

Стандарт **АРОС**, изобретённый компанией PHILIPS, является почти обычным стандартом POCSAG, в котором предусмотрена замена (при передаче) наиболее распространенных слов и фраз кодовым трёхбайтовым сообщением. Функцию кодировки автоматически выполняет кодировщик сигнала POCSAG (пейджинговый терминал), имеющий соответствующую опцию. При приёме сигнала и его декодировании, пейджер (также имеющий функцию работы с АРОС) заменяет кодовое значение на соответствующее слово (фразу). Такая модернизация стандарта POCSAG,

позволяет сжимать трафик не более чем на 20 – 25 %, что, безусловно, важно и полезно, особенно для случаев дефицита частотных ресурсов.

Однако, опыт компании PHILIPS не получил широкого распространения, возможно, возможно, потому что, во-первых, эту инициативу не поддержали основные производители пейджинговых систем, а во-вторых, появились новые высокоэффективные протоколы пейджинговой связи: **FLEX** (и сопровождающее его семейство **ReFLEX, InFLEXion**), разработанные компанией MOTOROLA, и **ERMES**, разработанный Международным союзом электросвязи. Новые протоколы более сложны и совершенны, обладают в 3 – 8 раз большей абонентской ёмкостью на один частотный канал, эффективны для роуминга и подключения сервисных подсистем, имеют ряд других преимуществ.

Следует упомянуть и о формате **RDS**. В таких системах передача сигналов персонального радиовызова ведётся вещательными радиостанциями за счёт уплотнения существующих радиовещательных каналов (на поднесущей).

Двусторонний пейджинг – вид пейджинговой связи в котором предусмотрена, в дополнение к обычной функции приёма сообщений, посылка (передача) сообщения самим пейджером на специальную сеть приёмных устройств (станций). Сначала такие системы появились в США (где была построена сеть двусторонней пейджинговой связи с использованием протокола ReFLEX), затем в Австралии и в ряде государств ближнего востока (где была реализована технология NEXUS).

Разработка технологии двусторонней пейджинговой связи ReFLEX компанией Motorola велась с начала 90-х годов. Первые опытные сети были не совсем эффективны (наблюдались потери сообщений, была очень высокая стоимость оборудования), однако после усовершенствования протокола, доработки и отладки оборудования сеть двусторонней пейджинговой связи стала работать стабильно и была расширена до национальной.

Технология NEXUS (Израиль) была применена в австралийском Сиднее для построения полностью автоматизированной (работающей без участия операторов пейджинга) сети пейджинговой связи. Существенными достоинствами технологии NEXUS являются, во-первых, простота конструкции сети обратной связи (количество передатчиков и станций приёма практически совпадают) и, во-вторых, направленность технологии на широкое применение в транспорте и промышленности (например, для контроля за движущимися объектами, для сбора телеметрической информации о состоянии объектов).

Таблица 5.1 – Протоколы пейджинговой связи

Наименование протокола	Используемые частоты, МГц	Скорость передачи, бод	Требуемая полоса частотного канала, кГц	Наличие нумерации сообщений	Возможность роуминга
POCSAG	Любые пейджинговые	512, 1200, 2400	25	Есть*	Есть*
RDS	88 – 108, на поднесущей 57 МГц вещательной радиостанции FM диапазона	1200	-	Есть*	Есть*
ERMES	169, 425-169, 800	6250	25	Есть	Есть
FLEX	Любые пейджинговые	1600, 3200, 6400	25	Есть	Есть
ReFLEX 25 - передача на пейджеры - приём с пейджеров	929-931, 940-941 901-902	1600, 3200, 6400	25 или 50	Есть	Есть

ReFLEX 50 - передача на пейджеры - приём с пейджеров	929-931, 940-941 901-902	до 25600	50	Есть	Есть
InFLEXion - передача на пейджеры - приём с пейджеров	929-931, 940-941 901-902	Цифровая компрессия звука	50	Есть	Есть
* Реализуется программным обеспечением пейджинг-центра.					

Далее мы подробно рассмотрим наиболее известные протоколы систем персонального радиовызова POCSAG, FLEX, ERMES и RDS. Все эти протоколы являются аналого-цифровыми (т.е. вся информация в эфире передаётся в виде 0 и 1, представленных с помощью частотной манипуляции).

Протоколы пейджинговой связи

Протокол POCSAG

Одним из самых распространенных на сегодняшний день форматов пейджинговой передачи является протокол POCSAG, разработанный Британским почтовым ведомством. Он предусматривает скорость передачи информации 512, 1200 и 2400 бит/сек. Сообщения передаются в асинхронном режиме: пакет сообщения может стартовать в любой момент времени и длина его не определена. Общая структура сигнала в формате POCSAG приведена на рисунке 5.1:

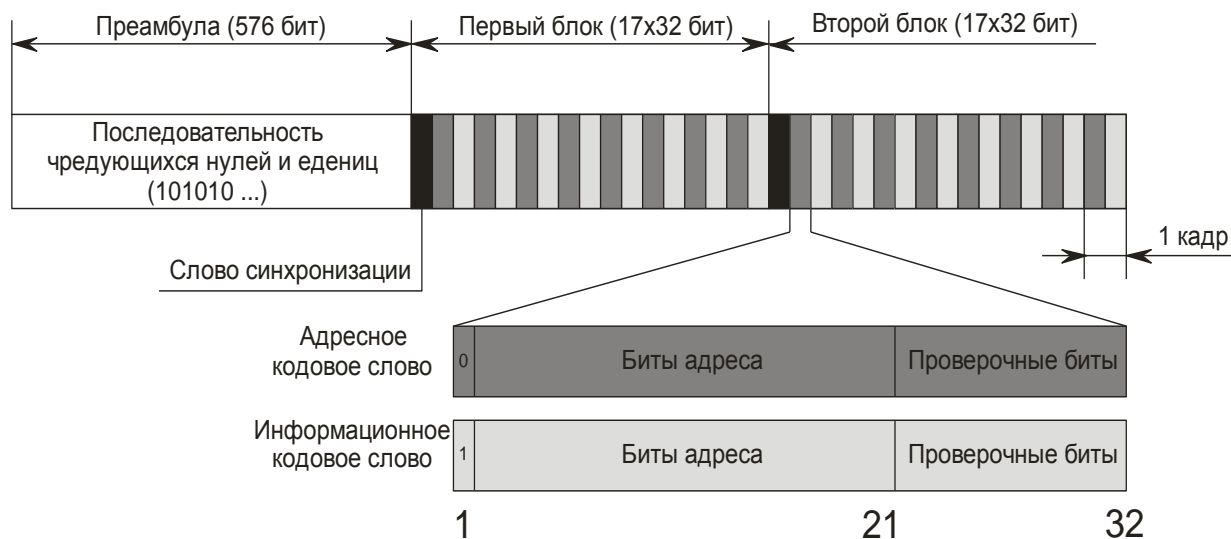


Рис. 5.1. Общая структура сигнала в формате POCSAG.

Сигнал в формате POCSAG начинается с преамбулы, состоящей из 576 бит чередующихся 0 и 1. Преамбула служит для вывода приемного устройства (пейджера) из "спящего" состояния в режим "приема" и его тактовой синхронизации. После преамбулы следует поток блоков, содержащих физические адреса пейджеров и тексты сообщений. Длина кодовой последовательности в формате POCSAG не определена, блоки следуют один за другим каждый со своим кодовым словом синхронизации - для подстройки синхронизации приемников (при передаче длинных сообщений). Каждый блок состоит из 17-ти 32-битных слов. Первое из них является словом синхронизации (фиксированная последовательность 32 бит), далее идет последовательность из восьми двойных слов или кадров (фреймов), нумеруемых с 0-го по 7-й. Каждое 32-разрядное слово содержит 21

информационный бит и 11 избыточных (контрольных) бит, которые служат для определения и корректировки ошибок. Протокол предусматривает коррекцию ошибок по алгоритму Бокгауза-Чоудхурри-Хоквингема, сокращенно БЧХ(32,12), при котором в одном 32-битном кодовом слове корректируется ошибка при приеме одного неверного бита (либо 2, если расстояние между ними не превышает 6 бит), а возникновение от 2 до 5 ошибок детектируется (т.е. это слово исключается и в большинстве моделей текстовых пейджеров эта часть обозначается скобками). В зависимости от функционального назначения блоки делятся на адресные, в которых передается физический адрес пейджера, и информационные, содержащие текст сообщения.

Основное отличие протокола POCSAG от других протоколов пейджинговой передачи заключается в способе приема содержащегося в начале каждого пейджингового сообщения физического адреса пейджера - кэпкода (CapCode), которому оно адресовано. Все возможные 2 млн. физических адресов разбиты на 8 групп, соответствующие 8 кадрам (frames) адресного блока. Адресный блок состоит из адресного кодового слова и предшествующих "пустых" слов (специальные фиксированные 32-битовые последовательности) и формируется следующим образом: физический адрес пейджера делится на 8. Остаток от деления дает номер фрейма в первое слово которого записывается частное от деления. Во все предыдущие фреймы записываются "пустые" слова (специальные фиксированные 32-битовые последовательности), а все оставшиеся до конца адресного блока слова пропускаются, т.е. сразу за адресным словом начинается следующий блок. Фактически остаток от деления является номером интервала времени (кадра frame), в котором данный пейджер будет вести прием и распознавание своего номера. Пейджер принимает только кадры, соответствующие его адресу. Это позволяет в восемь раз увеличить адресную емкость системы и значительно повысить срок службы элементов питания.

Информационный блок служит для передачи цифровой и алфавитно-цифровой информации на пейджер, заданный адресным блоком. Он содержит слово синхронизации, информационные слова, и, если сообщение закончилось, "пустые" слова до конца блока.

В протоколе POCSAG не оговаривается какие физические значения сигнала принимаются за 0, а какие за 1. Поэтому различные пейджеры (или режимы приема пейджера) воспринимают эту кодировку с точностью до наоборот. Отсюда появилось понятие инверсной кодировки POCSAG. Инверсная кодировка POCSAG полностью совпадает с описанной выше, за исключением того, что нулевые биты заменяются единичными, а единичные биты - нулевыми.

Увеличение скорости передачи сообщений ведет к увеличению пропускной способности системы, однако при этом снижается устойчивость к помехам, а главное - снижается чувствительность радиоприема, т.е. фактически - радиус рабочей зоны приема сообщений. Для подавляющего большинства пейджеров чувствительность в зависимости от скорости передачи равна следующим значениям: 512 бит/сек - 5 мкВ/м; 1200 бит/сек - 7 мкВ/м; 2400 бит/сек - 9 мкВ/м.

Протокол FLEX

Протокол пейджинговой связи FLEX разработан фирмой Motorola. Основным достоинством этого протокола является высокая скорость передачи данных - 1600, 3200 и 6400 бит/сек, а, следовательно, высокая пропускная способность. Так, если в стандарте POCSAG ресурс частоты составляет 10-15 тысяч абонентов, то во FLEX-системах ресурс частотного канала лежит в пределах 20-80 тысяч абонентов. В отличие от протокола POCSAG протокол FLEX использует синхронную передачу данных, т.е. синхронизация передатчика и приемника производится по абсолютному значению времени. Структура формата FLEX приведена на рисунке 5.2.

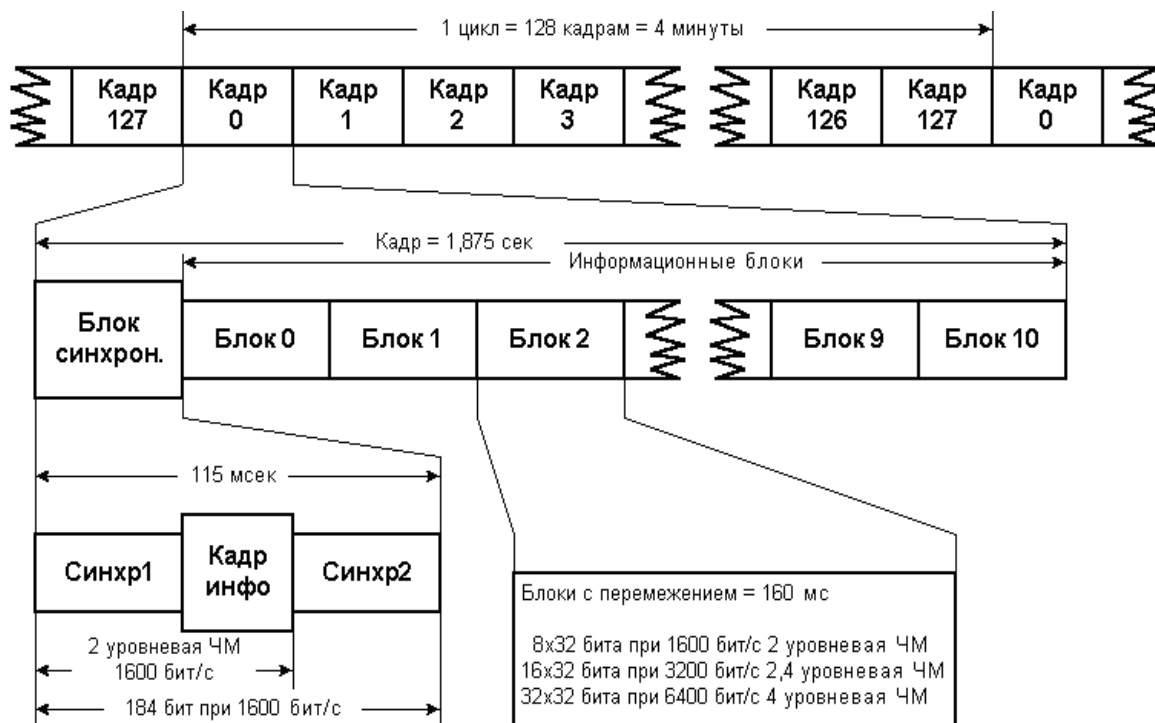


Рис. 5.2. Структура формата FLEX

При скорости 1600 бит/сек используется 2-уровневая частотная модуляция. При скорости 3200 бит/сек может использоваться как 2-уровневая, так и 4-уровневая частотная модуляция. При скорости 6400 бит/сек используется 4-уровневая частотная модуляция. Значения девиации для различных двоичных данных при 2-уровневой и 4-уровневой частотной модуляции приведены на диаграмме рис. 5.3.

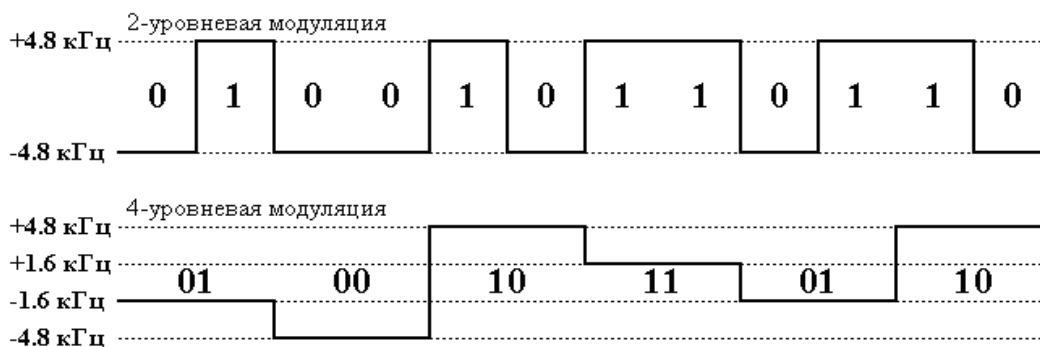


Рис. 5.3. Значения девиации при частотной модуляции

Данные в протоколе FLEX формируются в кадры, которые передаются последовательно со скоростью 32 кадра в минуту (1,875 сек на кадр). Полный цикл протокола FLEX состоит из 128 кадров, которые нумеруются от 0 до 127 и передаются ровно 4 минуты. Каждый час делится на 15 циклов, пронумерованных от 0 до 14.

Так как протокол FLEX является синхронным, для его синхронизации используются сигналы точного времени, передаваемые в начале каждого часа в кадре 0 цикла 0. При передаче этого кадра осуществляется синхронизация приемников.

Каждый кадр протокола FLEX передается 1,875 сек и состоит из блока синхронизации (115 мсек) и 11 информационных блоков (по 160 мсек на блок).

Блок синхронизации обеспечивает синхронизацию кадра и настройку пейджеров (фрагменты "Синхрон. 1" и "Синхрон.2"), а также несет информацию о номере цикла и кадра (фрагмент "Кадр инфо").

Информационные блоки содержат служебную информацию, адресное поле, задающее адреса пейджеров, которым адресованы сообщения, векторное поле, указывающее, где расположены сообщения в поле сообщений и их длину и непосредственно поле сообщений, содержащее сами сообщения.

Последовательность расположения полей в кадре показана на рис. 5.4.

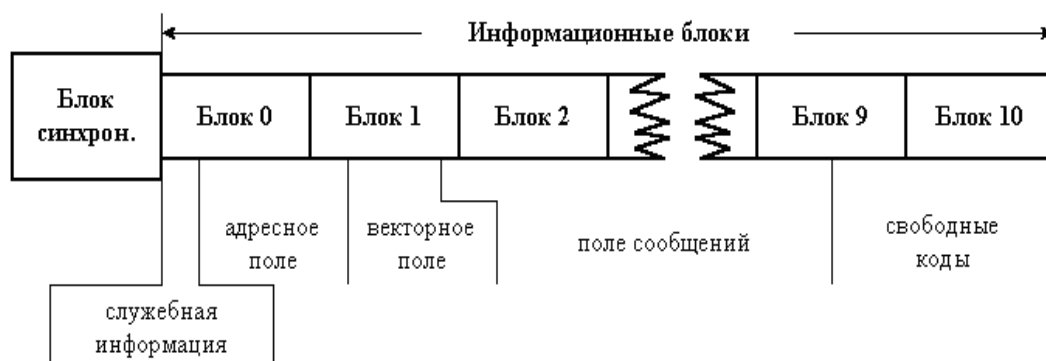


Рис. 5.4. Последовательность расположения полей в кадре

Поля не привязаны к границам блока. Порядок расположения адресов пейджеров в адресном поле должен соответствовать порядку расположения векторов в векторном поле. Адреса пейджеров могут задаваться одним кодовым словом (короткий адрес), поддерживая при этом до 2 миллионов адресов, или двумя кодовыми словами (длинный адрес), поддерживая до 5 миллиардов адресов.

При кодировании информации используется код БЧХ, позволяющий восстанавливать единичные ошибки передачи данных. Кроме того, используемая в протоколе последовательность передачи сформированных бит информации позволяет восстанавливать принятые данные при пропадании сигнала на интервале до 10 мсек.

Каждый пейджер, работающий с протоколом FLEX, может принимать сообщения на любой из допустимых скоростей передачи данных (1600, 3200 или 6400 бит/с). Одним из важных следствий синхронного протокола является то, что сообщения для каждого конкретного пейджера можно помещать в кадр с определенным номером. Это позволяет пейджеру избирательно принимать один или несколько кадров из всего четырехминутного цикла протокола FLEX, в которые помещаются сообщения на его адрес. Если пейджер не обнаруживает своего адреса в своем кадре, он прекращает прием. Такая организация связи позволяет резко повысить срок службы батареек пейджера.

Еще одной важной отличительной особенностью протокола FLEX является возможность работы совместно с другими протоколами связи. Для этого в цикле выделяются определенные кадры для работы по протоколу FLEX, а промежутки между ними отдаются для работы по другим протоколам, например, POCSAG. Это позволяет компании оператору не создавая новой инфраструктуры, постепенно перейти от работы в протоколе POCSAG на работу в протоколе FLEX.

К достоинствам протокола FLEX следует отнести:

- повышенную скорость передачи данных, а, следовательно, повышенную пропускную способность на один частотный канал;
- возможность поддержания большого количества адресов (до 5 миллиардов);
- улучшенные характеристики помехоустойчивости канала передачи;
- обеспечение энерго-экономичного режима работы пейджеров;
- возможность совместной работы с другими протоколами.

Протокол ERMES

Протокол ERMES был разработан как общеевропейский протокол пейджинговой связи. Он включает в себя, кроме собственно протокола передачи данных, ряд организационных положений и технических решений в рамках Меморандума о взаимопонимании, подписанного руководителями администраций 16 стран Европы в январе 1990 г. с целью координации усилий по созданию общеевропейской СПРВ. К достоинствам протокола ERMES следует отнести следующее:

- повышенную скорость передачи данных, а, следовательно, повышенную пропускную способность на один канал;
- обеспечение энерго-экономичного режима работы пейджеров;
- возможность передачи произвольного набора данных объемом до 64 кбит;
- возможность удобной организации роуминга во всех регионах, охваченных сетью ERMES.

Для функционирования СПРВ по протоколу связи ERMES выделяется единый диапазон частот (или его часть) 169,4 - 169,8 МГц, в котором организуются 16 частотных каналов с разносом частот в 25 кГц. Для приема сигнала используются сканирующие по частоте абонентские приемники (пейджеры). Скорость передачи данных составляет 6,25 кбит/сек.

Системы персонального радиовызова на базе протокола ERMES обеспечивают следующие услуги:

- передачу цифровых сообщений длиной до 1600 знаков;
- передачу буквенно-цифровых сообщений длиной до 9000 символов;
- передачу произвольного набора данных объемом до 64 кбит;
- возможность приема вызова и сообщений одним унифицированным приемником (пейджером) во всех странах, входящих в объединенную СПРВ ERMES.

Структура протокола ERMES приведена на рис. 5.5.

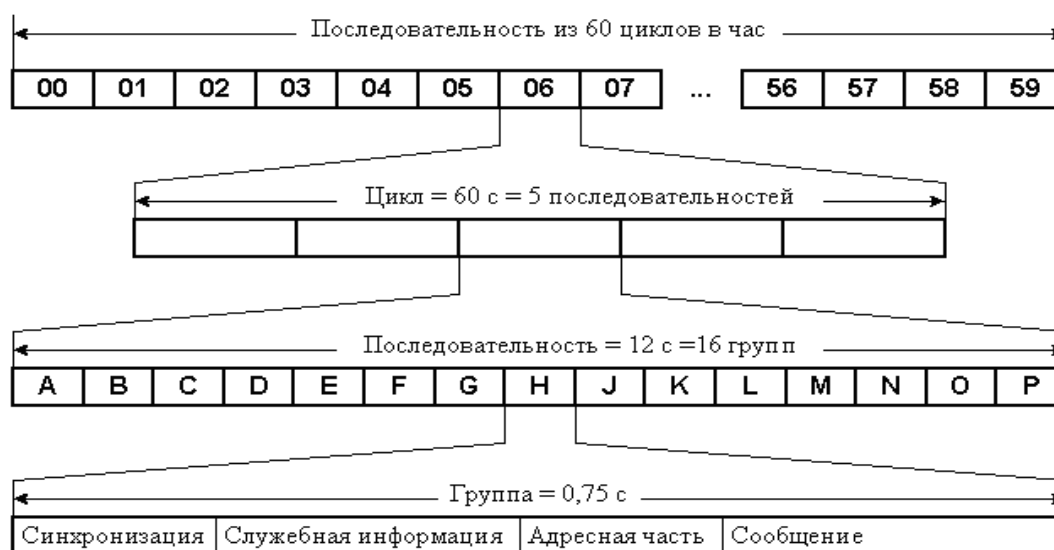


Рис. 5.5. Структура протокола ERMES

Каждый час передается 60 циклов по одной минуте каждый. Каждый минутный цикл содержит 5 последовательностей по 12 сек. Каждая из последовательностей включает в себя 16 типов групп, которые обозначаются буквами латинского алфавита от А до Р. Каждая группа имеет длину 0,75 сек и состоит из четырех блоков: синхронизации; служебной информации; адреса; информационного сообщения.

Порядок расположения групп внутри последовательности для каждого частотного канала свой и устроен так, что позволяет пейджеру в пределах последовательности просмотреть свою группу в режиме сканирования на всех 16 частотах. Порядок расположения групп для каждого частотного

канала показан в табл. 5.1 (выделенные группы показывают порядок сканирования пейджера для группы А).

Протокол ERMES использует помехоустойчивое кодирование передаваемой информации с прямой коррекцией ошибок (FEC), циклический код (30,18), кодовое расстояние Хемминга - 6.

Приемники персонального вызова (пейджеры) в системе ERMES работают следующим образом. Находясь в зоне приема "своей" базовой станции пейджер принимает сообщения на ее частоте. При попадании в другой регион пейджер, не "слыша" сигнал на своей частоте, переходит в режим сканирования по каналам ERMES и, обнаружив сигнал, начинает принимать информацию на частоте базовой станции данного региона.

Таблица 5.1. Порядок расположения групп для каждого региона

Канал	Последовательность = 12 с															Следующая последовательность								
01	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H
02	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G
03	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F
04	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E
05	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D
06	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C
07	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B
08	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A
09	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
10	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
11	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N
12	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L	M
13	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K	L
14	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J	K
15	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I	J
16	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H	I

Протокол RDS

Протокол RDS (Radio Data System) получил путёвку в жизнь в начале 90-х годов в качестве многофункционального формата передачи данных как на адресные, так и на безадресные приёмники. Принцип передачи данных основан на уплотнении сигнала вещательной станции, работающей в FM и УКВ диапазонах. Передача данных происходит путём замешивания в комплексный стереосигнал на поднесущей частоте 57 кГц с девиацией 2 кГц частотно-модулированного сигнала RDS. Спектр суммарного сигнала показан на рисунке 5.6 (где А и В – сигналы левого и правого каналов стереовещания).

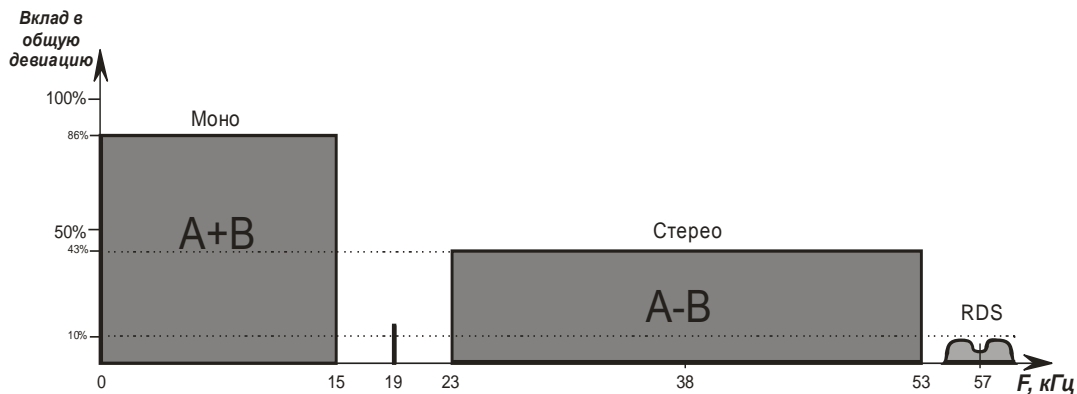


Рис. 5.6. Спектр суммарного сигнала

Помимо пейджинговых сообщений, формат RDS позволяет передавать на радиоприёмники с декодером сигнала RDS различную текстовую информацию в виде неподвижной или бегущей строки – это может быть название принимаемой радиостанции, темп музыки, рекламные тексты. Более того, радиоприёмник, при переезде из одного города или области в другие, может сам настраиваться на требуемую радиостанцию или выбранный тип передачи (классическая музыка, рок, известия и пр.) и, при передаче экстренных сообщений, переключаться из других режимов (проигрывание компакт-дисков и аудиокассет) на приём.

Протокол RDS рассчитан на работу с фиксированной скоростью 1187 бит/с и имеет структуру, показанную на рисунке 5.7.

Самый большой элемент в структуре формата называется «группой» и содержит 104 бита информации. Каждая группа включает в себя 4 блока по 26 битов каждый. Блок состоит из 16-разрядного информационного слова и 10-разрядного контрольного слова. Передача данных полностью синхронна и не имеет разрывов между группами или блоками. Информационное слово служит непосредственно для передачи данных. Контрольное слово – для синхронизации и исправления ошибок.

Информационные слова группы RDS содержат следующую информацию.

Группа начинается с 16-разрядного, так называемого PI-кода (Program Identification), индивидуального для каждой страны, который является признаком RDS передачи, и, соответственно, страны, в которой эта передача ведётся.

Следующие пять бит (начало второго блока) определяют тип передачи данных: радиотекст, передача времени и даты, радиопейджинг и пр.

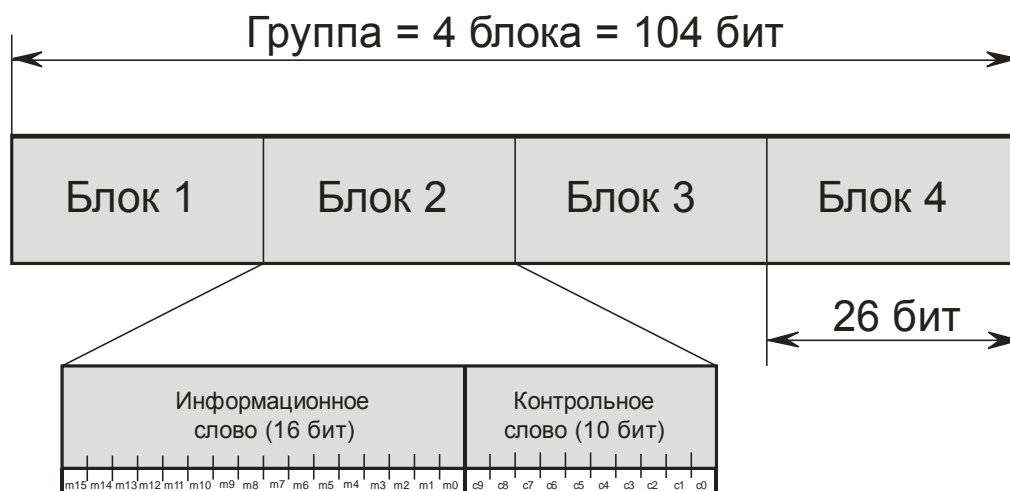


Рис. 5.7. Структура протокола RDS

Один бит (бит TP – Traffic program) управляет переключением радиоприёмника из режима проигрывания аудиокассеты или CD-диска в режим приёма при передаче важных

информационных сообщений. Следующие 5 бит формируют название программы, которое высвечивается на дисплее радиоприёмника при приёме вещательной станции. Это могут быть новости (News), спортивная информация (Sport), типы передаваемой музыки (например, Rock, Jazz, Classic) и т. д.

Далее идёт (последние 5 бит второго информационного слова) 5-ти разрядный адресный код AC (Address Code), который определяет местоположение данных передаваемых сообщений и команд, в том числе и адрес пейджерного приёмника.

При передаче пейджерного сообщения тип передачи данных задаётся как 01110, а адрес пейджера и само сообщение передаются в нескольких последовательных группах и занимают в каждой группе два последних блока. Первоначально следует адрес пейджера, а затем символы самого сообщения.

В организации передачи пейджерного сообщения участвуют и другие RDS группы, предназначенные для передачи времени и даты, а также синхронизации RDS приёмников. Синхронизационная метка передаётся каждую секунду, а время и дата – каждую минуту.

Стандарт RDS рассчитан для одновременной поддержки 4 пейджерных сетей. Поскольку формат RDS «не привязан» к конкретной частоте, а работает в диапазоне частот (FM/УКВ), пейджер для своей настройки производит сканирование всего диапазона. После настройки на одну частоту вещательной станции в течении 1с происходит синхронизация приёмника, в течении 2 с определяется код страны и признак сетей пейджеринга. Если они не соответствуют кодам, хранящимся в памяти пейджера, то он настраивается на волну другой радиостанции. После нахождения своей сети пейджер в течении 15 с переходит в режим экономии батареи. Организация экономии расхода электроэнергии достигается за счёт активизации приёмника в отдельные интервалы времени, определяемые его индивидуальным номером, и аналогична подобной организации в стандарте POCSAG. Спецификация RDS-стандарта – уплотнение сигнала вещательной станции – позволяет операторам связи в большинстве случаев с меньшими капиталовложениями, чем для других систем, развернуть СПРВ. Экономия объясняется отсутствием расходов на частотное присвоение, антенно-фидерное устройство и передатчик, которые являются весьма дорогостоящим оборудованием.

В настоящее время в связи с очень быстрым и успешным развитием сотовой связи, пейджер ушёл из широкого круга потребителей. Хорошо отлаженные помехозащищающие алгоритмы приема информации пейджерной связи нашли своё место в системах автомобильной сигнализации и системах удалённого управления электронными устройствами. Протокол RDS уверенно занял своё место в сетях радиовещания и телевидения.

6. ПЕРСПЕКТИВНЫЕ СПУТНИКОВЫЕ СИСТЕМЫ СВЯЗИ

В настоящее время спутниковая связь составляет относительно небольшой удельный вес в общем объёме телекоммуникационной индустрии, однако темпы развития спутниковой связи стремительно наращиваются в последние годы.

Спутниковая промышленность все активнее вовлекается в процессы консолидации и глобализации. Многочисленные промышленные альянсы, образовавшиеся в последние годы, ярко подтверждают эти тенденции: Hughes участвует в бизнесе PanAmSat, Loral - Orion, Boeing - Elipso, Alcatel - SkyBridge, Motorola, Boeing и Matra Marconi-Teledesic, Lockheed Martin-Comsat. В Европе в настоящее время доминируют два промышленных альянса, определяющую техническую политику европейской спутниковой связи: Alcatel Space (объединение AeroSpaciale и Thomson CSF) и альянс Matra Marconi Space, DASA-Raumfahrt-infrastruktur, Darnier Satellitensysteme и Aienia Spazio.

Как показывают различные маркетинговые прогнозы мировой рынок спутниковой связи в ближайшие 5-10 лет будет развиваться значительными темпами. Производство спутников остается относительно стабильным сегментом общего рынка космической промышленности с мировым годовым оборотом порядка 10 млрд. долл. Наиболее быстро будет развиваться рынок услуг спутниковой связи: от 18 млрд. долл. в 1997 г. к прогнозируемым 150 млрд. долл. в 2007 г. В настоящее время услуги спутниковой связи составляют около 2,7 % (22 млрд. долл.) от общего глобального телекоммуникационного рынка услуг связи (800 млрд. долл.). К 2005г. удельный вес спутниковой связи на глобальном рынке услуг возрос до 5,5% (75 млрд. долл.) от общего оборота телекоммуникационного рынка (1200 млрд. долл.). Значительный прирост объема мирового телекоммуникационного рынка (50% за 5 лет) объясняется прежде всего высокими темпами развития мобильной связи и широкополосных услуг мультимедиа.

Абонентская база к 2005г. может вырасти до 30 млн. пользователей, а к 2010г. - до 50 млн. Однако, уход с этого рынка системы Iridium, а также задержки с вводом в эксплуатацию других глобальных систем могут привести к более осторожным прогнозным оценкам. Существует общее мнение, что только 2-3% общего числа абонентов мобильной связи в ближайшие 10-15 лет выберут для себя персональную спутниковую связь как один из основных видов услуг. Поэтому прогнозное значение 50 млн. абонентов ССС к 2010г. должно учитывать рост общей абонентской базы мобильной связи к этому времени до 1,7-2,5 млрд. человек. В целом эти два прогнозных значения можно характеризовать как достаточно вероятные.

Если принять эту пропорцию (2-3%) абонентов "спутниковой/наземной" мобильной связи, как действующую и для России, то к 2010г. можно прогнозировать число абонентов 250 тыс. (персональная спутниковая связь) и 10 млн. (наземная мобильная связь).

Отметим общую степень условности этих оценок так как они не учитывают темпы развития платёжеспособного спроса и технико-экономические показатели будущих ССС в России, таких как тарифы связи, стоимость терминалов и др.

В 1998г. на геостационарной орбите находилось примерно 215 коммерческих спутников. По данным МСЭ в период до 2006г. планировалось запустить на орбиту свыше 2700 космических аппаратов (КА) общей стоимостью более 24 млрд. долл. в том числе около 1000 КА нового поколения, использующие диапазон Ка 20/30 ГГц. Производство спутников связи возросло после 2005г, а к 2015г. общее число запущенных КА может увеличиться до 10-11 тыс.

Общие инвестиции на мировом рынке спутниковых систем за десятилетие 1997-2006 гг. составило около 600 млрд. долл., в том числе в космическом сегменте и средства выведения на орбиту 60-80 млрд. долл., в наземные сети связи - 120-150 млрд. долл., в оборудование абонентского доступа и предоставления услуг (связи, вещание, доступа к Интернету, мультимедиа) - более 400 млрд. долл. Геостационарные широкополосные

системы (после неудачи Iridium) получили дополнительные импульсы своего развития. В Европе новые проекты на базе геостационарных спутников реализуются по программам Eutelsat, MEDSAT, EuroSkyWay и др. в США Fsrlink, Cyberstar, EchoStar, KaStar. На основе новых геостационарных ССС будут развиваться широкополосные системы мультимедийной связи, корпоративные Интернет сети, высокоскоростные сети. Потребности российского рынка на период до 2005г. составляли около 250 стволов, в том числе 45 стволов только для цифрового вещания. Общий ресурс всех КА, предполагаемых к запуску на отечественных спутниках связи, оценивается на уровне 200-220 стволов.

Глобальные системы спутниковой связи (Iridium, Globalstar и ICO), развёрнутые в 1998-2000 гг., позволяют на большом практическом материале всесторонне оценить технико-экономические параметры современных спутниковых технологий связи. Результаты испытаний первых эксплуатационных этапов, хотя и не всегда положительные, подтверждают важное значение правильного выбора стратегических направлений перехода к новому поколению ССС.

Проекты будущих ССС, которые будут развёрнуты в ближайшие 2-5 лет (Ellipso, Costellation, SkyBridge, Teledesic и др.), определяют новые технические решения по реализации широкополосных и мультимедийных услуг связи.

Проект Teledesic всё ещё остаётся наиболее амбициозным предприятием, в котором в результате недавних финансовых инициатив Крейга Мак Коу произошел важный поворот в сторону комбинированной схемы ICO-Teledesic.

Для широкополосной спутниковой связи планируется осваивать новые частотные полосы в диапазонах Ка и Кв, которые частично используются для фиксированных телефонных сетей на базе широкополосных спутниковых служб.

Технологии малых низколетящих спутников (Little LEO) будут испытываться в глобальной ССС Orbcomm, а также в ряде проектов региональных спутниковых сетей: E-Sat, Final Analysis, LEO One.

Новая технология внеземной связи на базе высокоподнятых платформ HAPS (High Altitude Platforms) набирает в последнее время всё более сильную поддержку у разработчиков и региональных администраций связи.

На состоявшейся в мае - июне 2000г. в Стамбуле Всемирной конференции радиосвязи WRC-2000 впервые были приняты принципиальные решения об использовании платформ HAPS в рамках ИМТ-2000:

- платформы HAPS могут использоваться в качестве базовых станций для наземных компонент ИМТ-2000 в полосах 1885-1980 МГц, 2010 - 2025 МГц и 2110 - 2170 МГц (в Регионах 1 и 3), а также в полосах 1885 - 1980 МГц и 2110 - 2160 МГц (в Регионе 2); использование приложений ИМТ-2000 на основе HAPS, как базовых станций, не должно противодействовать использованию этих полос любой другой станцией, для которой эти полосы были выделены, и в то же время данная радиорегуляция ИТУ не устанавливает никакого приоритета;
- указанные полосы выделены для услуг фиксированной и мобильной связи на совместной первичной основе;
- рекомендации ИТУ-R не касаются вопросов распределения адресов и координации между HAPS и другими. Существуют, в том числе PCS, MMDS и фиксированные службы, работающие в настоящее время в некоторых странах в полосах 188 - 2025 МГц и 2110 - 2200 МГц.

Платформы HAPS определяются новыми рекомендациями ИТУ как "станция, расположенная на объекте на высоте 20-50 км в определенной, фиксированной позиции относительно Земли". Платформы HAPS предназначены для минимальных сетевых инфраструктур. HAPS позволяют организовывать предоставление услуг с большой зоной покрытия и высокой плотностью расположения абонентов. В настоящее время готовится к запуску первая платформа HAPS- проект Skystation, в котором участвуют Alenia Spazio (торговые узлы связи) и Thomson CSF (наземная электроника и терминалы).

Новое поколение ССС будет характеризоваться рядом важных отличительных свойств: применение широкополосных спутниковых технологий связи, обеспечивающих высокоскоростную передачу данных; освоение новых диапазонов радиочастот Ка и Ку для работы широкополосных спутников GEO и LEO; значительное расширение спектра услуг связи для конечных пользователей :мобильная персональная связь, доступ к Интернету, передача видеoinформации, видеоконференцсвязь, мультимедийное широковещание, услуги определения местонахождения и т.п.; внедрение новых бортовых систем связи, спутниковых антенн, оптических систем межспутниковой связи, следящих антенн абонентских станций, портативных мобильных терминалов и т.п.; применение стандартных транспортных протоколов, адаптированных к особенностям физических спутниковых каналов: TCP/IP, ATM и т.д.

Проблемы освоения новых Ку и Ка диапазонов для спутниковой связи имеют сложный технологический характер для всех конфигураций ССС. Пример первой экспериментальной ССС ACTS (США, военные применения), начавшей действовать в 1993 г. в Ка-диапазоне на GEO орбите, показал сложность борьбы с атмосферными эффектами (дождь, влажность, температурные колебания) и необходимость разработки специального компенсационного протокола передачи данных.

Компания Logal планирует уже к 2002 году ввести в эксплуатацию одну из первых коммерческих систем Cyberstar в Ка-диапазоне. ССС Cyberstar разрабатывается как конфигурация 3-х спутниковых GEO (на первом этапе будет использован спутник TBD в Ку-диапазоне). Интересно заметить, что с переходом к высоким частотам (от Ку к Ка-диапазону) планируется повысить производительность передачи данных от 400 кбит/с до 30 Мбит/с, а стоимость мобильных терминалов сохранить при этом на уровне 800-900 долл.

В целом проблемы разработки новых технологий ССС могут формулироваться и решаться только на основе долгосрочных (5-10 лет) целевых научно-технических программ. Примеры таких программ, на период 1999 - 2004 гг. дают программы исследований космоса и новых спутниковых технологий, принятые в рамках Европейского космического агентства (ESA), Программы ESA (ARTES, Galileo и EOEP) и Европейской Комиссии (программы ACTS и IST) дают широкую панораму разработок новых ССС.

Общий бюджет ESA на НИР/ОКР составляет на 1999 - 2000 гг. примерно 360 млн. долл. /год. Проект новой спутниковой навигационной системы Galileo оценён в 3 млрд. евро на период 2000-2008 г.г. Создание ССС нового поколения сегодня невозможно без трех важнейших составляющих: Долгосрочных целевых программ, высокого уровня финансирования на государственном уровне и глубокого международного сотрудничества.

Спутниковые системы на основе технологии VSAT.

Как показывает мировой опыт, наиболее перспективным направлением создания и развития корпоративных сетей является применение спутниковых систем, базирующихся на технологии VSAT (Very Small Aperture Terminal), т.е. малогабаритных спутниковых терминалов и антенн диаметром от 1 до 2,5 м.

В настоящее время терминалы VSAT занимают наиболее объемный сегмент на традиционном рынке терминалов спутниковой связи. Ежегодная прибыль от их продаж составляет сегодня около 250 млн. долл., а объем продаж только приемопередающих станций вскоре достигнет отметки 500 тыс. Вместе с этим происходит быстрое уменьшение стоимости VSAT-оборудования (за прошедшее десятилетие цены упали в 5-10 раз) и снижение тарифов на услуги во VSAT-сетях (современные цифры иногда достигают 3 центов за минуту). А аналитики рынка продолжают утверждать, что такая тенденция сохранится еще в течение 5-10 лет.

Таким образом, дорогостоящие магистральные системы типа «точка-точка», долгое время монополизирующие спутниковые радиоресурсы, сегодня уступили место корпоративным сетям типа «точка-многоточие», состоящим обычно из мощной центральной станции, выполняющей роль концентратора - маршрутизатора, и набора периферийных станций типа VSAT.

Корпоративные VSAT – сети.

Лидером среди мировых поставщиков терминалов VSAT является американская компания Hughes (более половины всех контрактов). Далее следуют компании NEC, AT&T Tridon, GTE Spacenet, Scientific Atlanta. Эти фирмы в настоящее время активно осваивают ведущие рынки развивающихся стран, в том числе и российский.

Таблица 6.1. Основные характеристики VSAT-станций компании Hughes

Тип станции	PES	TES	GES	TRES
Размер антенн, м	1,8; 2,4 (C, Ku) 0,75; 1; 1,2 (Ku)	1,2; 2,4	1,8; 2,4; 3,8 (C) 1,2; 1,8; 2,4 (Ku)	1,8; 2,4; 3,8 (C, Ku)
Скорость передачи, кбит/с	1,2-64 (синхр.) 19,2 (асинхр.)	9,6-32	9,6-8448	32-2048
Мощность передатчика, Вт	0,5; 1; 2 (Ku) 1,0 (C)	0,5; 5 (C) 2 (Ku)	20 Вт (C) и 16 (Ku)	5; 20 (C) 2; 8 (Ku)
Энергопотребление, Вт	Н/д	75 (20 ожидание)	Н/д	2
Размеры, мм	Н/д	380x300x90	439x109x482 190x150x310	330x66x272 (модем)
Масса, кг	Н/д	8,5	10,2 (IDU) 8,2 (ODU)	1,5 (модем) +2,7 (питание)
Рабочая температура блока ODU, оС	От -30 до +55	От -30 до +55	От -40 до +55	От -40 до +55
Примечание. Н/д - нет данных.				

Следует также заметить, что для мирового рынка производителей абонентской аппаратуры VSAT характерна очень жесткая конкурентная борьба, а потому проникновение на него новых производителей крайне затруднено. Наиболее реальный путь для новичков к получению своего "кусочка пирога" - сотрудничество с теми компаниями, которые уже прочно заняли определенную нишу на этом рынке. Вероятно, такой путь будет наименее болезненным и для российских производителей VSAT-станций.

Больше всех других VSAT-терминалов в российских сетях связи распространены станции семейства NEXSTAR корпорации NEC. В состав типовой абонентской станции NEXSTAR входят наружный (ODU) и внутренний (IDU) блоки и двухрефлекторная перенацеливаемая по азимуту и углу места антенна (диаметр зеркала от 1,2 до 3,8 м), разработанная на базе схемы Кассегрейна. Ее важная характеристика - максимальная ветровая нагрузка - 108 км/час.

Оборудование наружного блока состоит из трех компактных влагонепроницаемых блоков: МШУ, преобразователя частоты и усилителя мощности. В условиях низких

температур применяется дополнительный обогреватель, что позволяет эксплуатировать станцию в условиях северных районов страны (при температурах ниже 50С). МШУ обеспечивает коэффициент усиления 72 дБ при шумовой температуре 60 К, а выходная мощность передатчика составляет от 5 до 20 Вт.

Станция может быть сконфигурирована для работы как в режиме с предоставлением каналов по требованию DAMA, так и в режиме с закрепленными каналами PAMA. Требуемый тип соединения устанавливается оператором.

Таблица 6.2. Основные характеристики блока NEXTAR ODU

Передача		Прием	
Входная частота, МГц	180+-20	Входная частота, МГц	3,7-4,2
Выходная частота, ГГц	5,925-6,425	Выходная частота, МГц	1135+-20
Уровень входного сигнала, дБ/мВт	От -5 до 40	Усиление, дБ	72
Выходная мощность, Вт (насыщение)		Разброс усиления, дБ	+12/-8
Пределы регулировки выходной мощности (шаг 0,5 дБ), дБ	14	Шумовая температура, К	60

VSAT-сеть на базе станций NEXTAR обычно состоит из двух взаимно независимых по способу доступа сетей: NEXTAR AA/TDMA и NEXTAR BOD, построенных на разных принципах разделения ресурса спутникового ретранслятора. Такой принцип построения сети нашел отражение и в структуре VSAT-станции. В состав земной станции NEXTAR входят два внутренних блока: BOD IDU и AA/TDMA IDU.

Блок AA/TDMA IDU расположен рядом с оконечной аппаратурой обработки данных DTE (data terminal equipment); он поддерживает протокол X.25 и имеет три синхронных интерфейса RS-232 (скорость 1,2-19,2 кбит/с).

Плата голосового канала (VO CH Card) поддерживает три вида телефонных интерфейсов: 2W FXS, 2W FXO и 4W E&M. Режим двухпроводного интерфейса FXS обеспечивает прямую телефонную или факсимильную связь (скорость от 0,3 до 9,6 кбит/с). Режим FXO обеспечивает эмуляцию связи с местной или учрежденческой АТС, при этом может использоваться как импульсный, так и тоновый набор номера.

Алгоритм кодирования программно загружается из системы управления сетью в каждую плату VO CH. Стандартно поддерживаются два алгоритма кодирования речи - ADPCM, G.721 (со скоростью 32 кбит/с) и LD-CELP, G.728 (16 кбит/с). Передача информации осуществляется со скоростью 64 кбит/с (BPSK) и 128 кбит/с (QPSK).

Плата свободного канала (CL CH Card) имеет один синхронный интерфейс, который может поддерживать скорость передачи данных от 9,6 до 2048 кбит/с. Стандартный синхронный интерфейс соответствует спецификации RS-449/442. Интерфейсы V.35 или G.703 реализуются с помощью соответствующих дополнительных плат.

Оборудование центральной Hub-станции, обычно называемой шлюзом, способно обслужить до 3 тыс. абонентских станций или до 8 тыс. каналов, а информационная нагрузка может достигать 16 тыс. вызовов в час.

Принципы построения центральной ЗС сходны с теми, которые использованы в абонентской станции NEXTAR - она тоже состоит из трех частей: антенн, высокочастотных блоков и сетевого оборудования, включающего модемы, контроллеры и систему управления сетью. На Hub-станции используются антенны большого диаметра (от 4,5 до 11 м) с системой автоматического слежения за спутником. Количество антенн (обычно две-три) зависит от числа одновременно отслеживаемых спутников.

В состав радиочастотной части Hub-станции входят МШУ, преобразователи частоты, усилители мощности. Однако в отличие от абонентских станций все перечисленные компоненты оборудования имеют 100%-ное резервирование по схеме 1+1 для обеспечения высокой надежности. Интерфейс между радиочастотным и сетевым оборудованием обеспечивается по каналу на промежуточной частоте 140 МГц.

Четырехканальный модем представляет собой функционально законченный блок, который кроме канальных плат (VO CH Card или CL CH Card) имеет модем ОКС (общего канала сигнализации) и блок питания. Полностью укомплектованная стойка из шести модемов дает возможность организовать 24 канала.

Система управления сетью, реализованная на базе шлюза, построена как локальная сеть с одним сервером и несколькими рабочими станциями операторов. Первичный DAMA-контроллер (PDC) управляет процессом установления соединений с абонентскими терминалами в режиме реального времени автоматически, без участия оператора. Он же осуществляет сбор биллинговой информации о каждом звонке. Биллинговая информация поступает в подсистему хранения данных BISE (Billing Information Storage Equipment). Конфигурация центральной станции имеет модульную структуру, что позволяет рационально наращивать трафик и расширять ассортимент предоставляемых услуг по мере развития сети.

Система «Ямал»

Известный в нашей стране производитель оборудования космической связи РКК "Энергия" разрабатывает и производит три типа ЗС, различающихся по пропускной способности: центральную ЗС (ЦЗС) для телепортов, узловую ЗС (УЗС) и абонентскую ЗС. В настоящее время они используются в сети "Ямал".

Таблица 6.3. Основные технические характеристики ЗС системы "Ямал"

Параметр	Тип ЗС		
	Центральная	Узловая	Абонентская
Суммарная пропускная способность, кбит	Более 8448	До 4096	До 2048
Рабочий диапазон частот, МГц			
Прием	3620-4200		
Передача	5850-6425		
Диаметр антенны, м	4,5/5,0/6,0	4,5/5,0/6,0	2,5/3,5/4,5
Мощность передатчика, Вт	400/700	125/150	5/10/20/40
Температура шума МШУ, К	35-65		
Вид модуляции	ФМ-2/ФМ-4		
Кодирование	сверточное, R=1/2, 3/4, 7/8		
Потребляемая мощность, кВт	18	6,0	1,5

Земные станции сети "Ямал" обеспечивают передачу информации со скоростью до 2048 Мбит/с (магистральные каналы) и до 192 кбит/с (VSAT-терминалы) и предназначены для организации радиотелефонной связи с различными типами сигнализации, факсимильной связи со скоростью 2,4- 9,6 кбит/с, передачи данных со скоростью не выше 115 кбит/с (синхронные), а также видеоконференцсвязи.

ЗС комплектуются различными типами антенн (в основном антенным постом "Пихта", оснащаемым позиционером "Бусна", в котором используются экстремальные методы наведения, и усилителями мощности фирм MATRA MARCONI, 125 Вт и SKY DATE, 20 Вт). В этих ЗС применяются модемы типа SDM (SDM-100, SDM-600) и мультиплексоры CX-1000.

Модульная структура ЗС "Ямал" обеспечивает замену любого блока и наращивание пропускной способности без изменения конфигурации, что позволяет легко модернизировать ее при моральном устаревании, а также вводить новые функции без всяких дополнительных доработок станции. Такой подход гарантирует также независимость от какого-либо определенного производителя, допуская применение аппаратуры любого типа. Например, в качестве каналообразующего оборудования на первом этапе в составе ЗС использовался модем MD7000, затем SDM-100 и SDM-6000, что позволило без доводки оборудования перейти на новые методы кодирования речи. ЗС сети "Ямал" используют расширенный С-диапазон частот: 5760- 6125 МГц (передача) и 3460-3800 МГц (прием). Серийно выпускаемая приемопередающая аппаратура имеет нижнюю границу диапазонов 5850 и 3650 МГц соответственно. Сегодня многие международные организации (Intelsat, Inmarsat, USAsat, Aziasat) и администрации связи (в Индии, Китае, Сингапуре, Индонезии и других странах) подали заявки в МСЭ на этот расширенный диапазон как на рабочий. Поэтому следует ожидать его активного освоения и разработки соответствующего оборудования, начиная от антенных постов и заканчивая преобразователями частоты.

Следует отметить, что, поскольку С-диапазон космических аппаратов (КА) "Ямал" смещен, а ЗС должны работать и через спутники стандартного С-диапазона, суммарная рабочая полоса частот ЗС "Ямал" составляет более 600 МГц.

Использование уплотнения при поляризации сигнала накладывает на ЗС специфические обязательства. Согласно требованиям ОТГ Минсвязи, коэффициент эллиптичности антенной системы должен быть не менее 0,92, развязка по поляризации - 27,6 дБ. Для удовлетворения этих требований, учитывая, что на КА "Ямал" применяются антенны с коэффициентом эллиптичности 0,82, развязка по поляризации в системе с двумя КА на геостационарной орбите в одной точке стояния составит от 17 до 27,6 дБ.

Ограниченный запас частотного ресурса на российских КА приводит к необходимости работать одновременно через несколько стволов одного и того же ретранслятора. Для этого в ЗС предусматриваются дополнительные тракты приема-передачи, которые выполняют также функции резервирования, предотвращая полный отказ станции. Еще одна особенность ЗС "Ямал" - совмещение нескольких функций в одном аппаратном средстве, что делает ее более универсальной и в конечном счете более рентабельной.

Одна из основных проблем при эксплуатации сетей спутниковой связи в России - необходимость применять системы наведения на VSAT-терминалах, имеющая по крайней мере три источника.

Во-первых, разработанные ранее системы наведения по целеуказаниям (в основном для военного применения) никогда не найдут широкого распространения для ССС коммерческого назначения из-за их большой стоимости и сложности.

Во-вторых, отечественные и западные операторы и производители ЗС при работе в России используют антенные посты нашего производства. К сожалению, такая экономия приводит к дополнительным сложностям, так как наши алгоритмы систем наведения оставляют желать лучшего, не говоря уж о надежности работы, особенно в жестких климатических условиях.

Третий источник - использование спутников-ретрансляторов серий "Горизонт" и "Экспресс". В них не только не предусмотрено излучение специального пилот-сигнала, как во всех зарубежных спутниках связи. При приеме сигнала от этих российских КА на границе зоны обслуживания возникают большие колебания (нестабильность) уровня сигнала. Но эти области нестабильного приема как раз и включают районы Севера, где в основном и используется сеть "Ямал". Поэтому для VSAT-станции "Ямал" разработана специальная система стабилизации на основе отдельного канала/тракта в рамках ЗС, обеспечивающего получение устойчивого сигнала управления для системы наведения.

Специфика условий эксплуатации ЗС "Ямал" (чаще всего в северных и труднодоступных районах), а также назначение системы (для газодобывающей промышленности) определили высокие требования к надежности станций: коэффициент готовности ЗС должен составлять не менее 0,9999. Чтобы обеспечить столь высокую надежность, в ЗС используются схемы как "холодного", так и "горячего" резервирования. Подтвержденная наработка на отказ уже установленных ЗС составляет в настоящее время более 10 000 ч для телепортов и УЗС и более 15 000 ч для VSAT-станций. Ожидаемая наработка на отказ новых, разрабатываемых ЗС будет не менее 50 000 ч.

Станция полностью автоматизирована: контроль и управление, архивирование сведений об отказах, определение неисправностей, переключение режимов работы и т. д. происходят с помощью встроенных микропроцессоров. Разработка новых блоков ведется также с учетом современных требований контроля и управления. В частности, предусматривается шлейфовый контроль по промежуточной частоте и по радиочастоте, а также измерения излучаемой мощности, что позволяет отслеживать параметры не только ЗС, но и спутниковой радиолинии.

ЗС оснащена стандартными интерфейсами и стационарным контроллером, что обеспечивает возможность работы станции как в автономном режиме, так и с помощью дистанционного управления по командам из центра управления связью.

Поскольку большую часть частотного ресурса КА "Ямал" планируется использовать за пределами России, разработка земных станций ССС "Ямал" ведется с учетом требований и отечественных, и международных стандартов.

Мультимедийные терминалы VSAT

Описание VSAT-оборудования было бы неполным без упоминания о мультимедийных терминалах. Из-за отсутствия общепринятого названия для передачи в общем потоке информации от разных видов служб связи или потому, что неопределенное название более всего подходит для данного периода развития телекоммуникаций, сети, предоставляющие разнородные услуги, сегодня называют мультимедиа-сетями. Они обеспечивают своих абонентов целым спектром услуг от простой электронной почты до организации видеоконференций и интерактивного телевидения. Отчасти этот термин указывает на конвергенцию услуг связи и вещания, когда-то очень далеких друг от друга. А по прогнозам аналитиков рынка, слияние связи и вещания неизбежно приведет к созданию широкополосных VSAT-технологий.

Сегодня разработкой мультимедийных терминалов, способных объединить традиционную телефонную связь, низкоскоростную передачу информации, телевидение, радиовещание, IP и DVB-потоки данных, в мире занят не один десяток фирм. Безусловным лидером среди них является американская компания HNS.

С появлением мультимедийных VSAT терминалов возникла и новая аббревиатура MMV (Multimedia VSAT). Терминалы MMV предназначены для высокоскоростной передачи информации, телевизионного и звукового вещания. Их базовой областью применения является доступ в Internet, работа в корпоративных интрасетях, интерактивное дистанционное обучение, а также однонаправленные передачи типа циркулярных широковещательных трансляций, деловое телевидение, широковещательное распространение файлов.

До недавнего времени одним из главных препятствий на пути создания корпоративных мультимедийных сетей являлась низкая пропускная способность спутниковых станций, не позволяющая доставлять удаленным пользователям Web-страницы или организовывать видеопросмотры. Несколько лет назад компанией HNS было предложено решение проблемы в виде малогабаритной VSAT-станции IP-Advantage с антенной диаметром один метр.

На удаленные станции данные передаются через центральную со скоростью до 24 Мбит/с с помощью исходящего канала IP-Advantage. В обратном направлении короткие запросы транспортируются со скоростью в 3 раза выше, чем в ISDN канале - до 200 кбит/с.

В России же об этом типе терминалов знают только понаслышке, хотя на последней выставке Cable & Satellite интерес к еще одной новой разработке Hughes проявили многие операторы.

Мультимедийный терминал DirecWay, разработанный этой компанией в 1999 г., является результатом интеграции хорошо себя зарекомендовавших в реальных условиях эксплуатации изделия PES с оборудованием DirectPC, которое обеспечивает работу широкополосных Internet-приложений.

Спутниковый канал обеспечивает передачу информации от серверов к удаленным терминалам со скоростью 64, 128 или 256 кбит/с, а прием - со скоростью от 550 кбит/с до 24 Мбит/с, при этом скорость на одно TCP-соединение может достигать 2,5 Мбит/с. Терминал DirecWay MMV поддерживает работу всех традиционных IP-приложений. Телевизионное и звуковое вещание принимается как на обычный телевизор, так и на ПК. Терминалы DirecWay MMV будут выпускаться с антеннами диаметром от 0,75 до 2,4 м для диапазонов частот C и Ku.

В России существуют и другие производители VSAT-станций, например ЗАО "Сатис-ТЛ-94". Однако почти для всех для них характерна одна тенденция: при выпуске основных модулей ЗС используются зарубежные комплектующие. Что же касается антенных систем, то эта российская продукция традиционно не уступает зарубежным образцам, а по ряду параметров и превосходит их.

Европейские проекты ACTS

Сегодня много говорится о мультимедиа – одновременной передаче различных видов информации, а также об интерактивных услугах, смысл которых состоит в установлении обратной связи от получателя информации к ее источнику. Тем не менее, пока еще не совсем ясно, как будут эти нововведения применяться в будущем: то ли для покупок по телевизору, то ли для обращения к врачу через компьютер, то ли для различных "виртуальных" развлечений. Вероятнее всего, будут иметь место самые разнообразные применения, поэтому надо стремиться учитывать все возможные направления развития мультимедиа.

Предоставление услуг мультимедиа предполагает наличие оборудования с пропускной способностью на порядок более высокой, чем существует в настоящее время (в частности, видеопрограммы могут занимать память объемом от нескольких гигабайт и выше). Поэтому существующие сети связи не годятся для функционирования интерактивных служб мультимедиа, которые требуют высокоскоростных линий передачи. Локальные (LAN) и территориальные (MAN) вычислительные сети, используемые для передачи пакетов данных, непригодны для трансляции непрерывных сигналов мультимедиа.

Преодолеть эти трудности можно путем сжатия сигналов, позволяющего снизить требуемый объем памяти и пропускную способность каналов.

Развитие мультимедиа будет положительно сказываться на занятости населения, поскольку деятельность, связанная с созданием программного обеспечения и предоставлением услуг, может дать работу многим людям. Предприниматели малого бизнеса смогут предлагать свои услуги с помощью мультимедийных средств. Внедрение мультимедиа поможет решить и другие социальные задачи. Например, если бы часть жителей большого города смогли выполнять свою работу на персональном компьютере (ПК), не выходя из дома, это позволило бы обществу справиться со многими проблемами, в частности, решить транспортную проблему. Тем не менее, пока уровень развития

компьютерной техники и особенно средств связи недостаточен для того, чтобы работать вне офиса.

В последнее время мультимедийное теле- и радиовещание приобретает такой существенный признак, как интерактивность, т.е. возможность пользователя (в частности, телезрителя) влиять на состав и характер транслируемой ему информации. Интерактивность постепенно превращается в повседневную реальность.

Вероятно, именно в этом направлении – интерактивные мультимедиа-услуги – пролегает магистральный путь дальнейшего совершенствования традиционного телевидения и радио, и в ближайшие годы на нем следует ожидать еще более впечатляющих успехов.

Конкретный пример практической реализации принципов мультимедийного телерадиовещания представляют проекты европейской исследовательской программы "Передовые технологии и услуги связи" – ACTS.

Серьезные исследования и эксперименты в области предоставления интерактивных многофункциональных (мультимедиа) услуг ведутся в рамках специальной европейской исследовательской программы "Передовые услуги и технологии связи" (Advanced Communications Technologies & Services – ACTS). Программа ACTS построена на результатах реализации предшествующей программы RACE (Research into Advanced Communications for Europe, 1985-1995), которая была учреждена с целью исследования проблем введения интегральной широкополосной связи (IBC) с учетом развития ISDN и национальных стратегий внедрения широкополосных услуг к 1995 году.

Программа ACTS представляет собой следующий шаг в направлении создания глобального информационного общества. В ней принимают участие основные европейские операторы телекоммуникационных сетей и сетей кабельного телевидения (КТВ), ведущие вещательные компании и крупнейшие производители телекоммуникационного оборудования совместно с европейскими исследовательскими организациями.

Одной из основных научно-технических областей программы ACTS является область – "Интерактивные цифровые мультимедиа-услуги". Основная цель работ в этой области состоит в том, чтобы стимулировать появление европейских интерактивных цифровых мультимедийных услуг связи по крайней мере так же быстро, как в других развитых странах. Широкое внедрение этих услуг предполагается с 2001 года. Среди работ выделены следующие направления:

Интеграция существующих широкополосных услуг, включая эфирное, кабельное и спутниковое ТВ, с коммутируемыми цифровыми услугами сетей общего пользования.

Предоставление технологий для введения новых услуг: от поддержки профессиональной телеработы до развлекательных услуг общего пользования (видеотелефония высокого качества, видеоконференции и т.п.).

Разработка перспективных систем сжатия изображений для эффективного использования ширины полосы передачи, 3D-видеосвязи и телеприсутствия.

Интероперабельность интерактивных мультимедиа-услуг. 1

В вышеназванной области программы ACTS существуют, по крайней мере, три десятка проектов, направленных на исследование, разработку и экспериментальную эксплуатацию сетей с полным набором услуг в целях реализации трансъевропейской широкополосной инфраструктуры связи к концу 2000 года.

Выделим среди них некоторые характерные проекты, относящиеся к исследованиям, разработкам и демонстрациям систем связи с интерактивными мультимедиа-услугами на базе сетей кабельного и сотового телевидения.

Проект AMUSE (Advanced Multimedia Service for Residential Users – Передовые мультимедиа-услуги для пользователей жилого сектора), в котором проводились эксперименты по обеспечению интерактивных мультимедиа-услуг для реальных абонентов жилого сектора, используя АТМ-сеть, продемонстрировал осуществимость и востребованность будущих коммерческих мультимедиа-услуг. Такие услуги "по

требованию", как просмотр новостей, фильмов, музыкальных и спортивных программ, а также "покупка из дома", были продемонстрированы с различными уровнями интерактивности. Обеспечивался высокоскоростной доступ в Интернет. В интерактивном режиме участники экспериментов (150 отдельных пользователей из 6 европейских стран) могли загружать цифровые видео- и аудиоматериалы и неподвижные изображения. Сигналы передавались по существующим сетям КТВ и гибридным радио-волоконно-оптическим сетям через различные виды терминалов от ПК до обычного телевизора с приставкой set-top box в формате MPEG-2. Причем эволюция последних рассматривалась в направлении создания универсальных абонентских устройств-"телепьютеров". Проект CABSINET (Cellular Access to Broadband Services and Interactive Television — Сотовый доступ к широкополосным услугам и интерактивному ТВ) направлен на исследование возможностей предоставления интерактивного широкополосного беспроводного доступа широкому кругу пользователей.

Российское участие в программе ACTS

Одним из основных среди исследовательских проектов в области цифровых интерактивных мультимедиа-услуг является проект "Интегральная широкополосная связь на широкополосных сетях" (Integrated Broadband Communications on Broadcast Networks – IBCoBN). Начатый в 1996 г. проект завершился в декабре 1999 года.

В проекте IBCoBN участвовало 14 полноправных партнеров и 16 субконтракторов, среди которых были исследовательские организации, университеты и кабельные операторы из Бельгии, Великобритании, Германии, Испании, Швеции и других стран ЕС. От России в проекте на правах полноправного партнера участвовало государственное унитарное предприятие НИИ "Рубин" (С.-Петербург), имеющее опыт системного интегратора сетей связи и управления. В НИИ "Рубин" проект вело дочернее предприятие "Рубин – Телекоммуникационные технологии и сети" ("Рубин–ТТС"). Его специалисты занимались исследованием рынка потенциальных пользователей сетей с полным набором услуг, прогнозированием трафика для различных классов пользователей, разработкой профилей архитектур и сценариев спроса и развития сетей КТВ в направлении создания сетей с полным набором услуг, а также проводили эксперименты на стенде и на действующих сетях КТВ.

Цели проекта IBCoBN включали:

1. Внедрение интегральной широкополосной связи в существующие и вновь создаваемые сети КТВ стран-членов ЕС.
2. Выявление потребностей всех типов квартирных пользователей (в том числе пожилых и нетрудоспособных людей), а также предприятий малого и среднего бизнеса в услугах широкополосной связи.
3. Создание общих спецификаций, охватывающих комплекс оборудования для реализации интегральных сетей на базе сетей КТВ, и рекомендаций для разработки соответствующих общеевропейских стандартов и протоколов для таких сетей.
4. Определение спецификаций для создания архитектуры сети с полным набором услуг и сценариев преобразования как существующих, так и строящихся сетей КТВ в интегральные широкополосные сети связи.
5. Проведение экспериментов по внедрению интегральной широкополосной связи в действующих сетях КТВ стран-участниц проекта.
6. Исследование потребностей сектора кабельного ТВ на долгосрочный период в рамках Европейской кабельной лаборатории, участники которой могли бы в кооперации определить стратегические направления развития локальных и

региональных интерактивных широкополосных кабельных сетей и координировать свои действия по их созданию.

Развитие спутниковой связи в программе ИМТ-2000

Одним из наиболее грандиозных проектов конца XX века является программа ИМТ-2000. В ее основе лежит идея создания нового семейства систем подвижной связи третьего поколения (3G), охватывающего технологии беспроводного доступа, наземной сотовой и спутниковой связи. В настоящее время в Международном союзе электросвязи (МСЭ) завершается процесс стандартизации новых технологий, участие в которой принимали многие региональные и национальные организации Европы, Северной Америки и Азиатско-Тихоокеанского региона.

После ряда безуспешных попыток выработать и согласовать единые требования к системам 3-го поколения (см. «Сети», 2000, № 1, с. 39) МСЭ решил подойти к этой проблеме с других позиций. Суть новой концепции состоит в сохранении идеи глобального роуминга, но лишь в качестве идеологической основы для объединения существующих аналоговых и цифровых сетей с системами, базирующимися на новом семействе стандартов 3-го поколения, которое получило обозначение IFS (ИМТ-2000 Family of Systems). Приняв как данность не один, а семейство стандартов и отказавшись тем самым от принципа глобального международного стандарта, МСЭ активизировал свои усилия на их гармонизации.

Концепция систем 3-го поколения нацелена на создание условий для предоставления услуг мультимедиа, включая высокоскоростную передачу информации, видео и речи, факсимильных сообщений и данных любому абоненту с помощью мобильного терминала, имеющего единый номер. Стоимость услуги должна быть минимальна при приемлемом качестве и уровне безопасности. Главная цель разработки систем 3-го поколения — удовлетворение потребности массового рынка в персональной связи, и ее достижение будет зависеть как от тарифов для сетей общего пользования, так и от стоимости абонентского терминала.

Программа ИМТ-2000 базируется на ряде признаков, определяющих принципы построения систем 3-го поколения и их архитектуру. Уже на первом этапе развертывания они должны обеспечивать определенные значения скорости передачи для различных степеней мобильности абонента (т. е. разных скоростей его движения) в зависимости от величины зоны покрытия:

- до 2,048 Мбит/с при низкой мобильности (скорость менее 3 км/ч) и локальной зоне покрытия;
- до 144 кбит/с при высокой мобильности (до 120 км/ч) и широкой зоне покрытия;
- до 64 (144) кбит/с при глобальном покрытии (спутниковая связь).

Таблица 6.4. Услуги систем 3-го поколения

Вид услуги	Скорость передачи, кбит/с	Средняя длительность сообщения, с	Режим работы	Услуги
Голосовая связь	4—32	60	Коммутация каналов	Речь, голосовая почта
Низкоскоростной обмен данными	9,6—14,4	30	Коммутация пакетов	SMS, определение местоположения
Передача	к До 64	156	Коммутация	Услуги сетей ISDN

коммутируемым данным (ISDN)			каналов	
Интерактивный обмен мультимедиа-данными	128—384	144	Коммутация каналов	Видеотелефонная связь, передача изображений и больших объемов информации
Асимметричная передача мультимедиа-данных	384—2048	14—53	Коммутация пакетов	Работа с сетями Internet и интрасетями

Что же касается набора услуг, то он фактически приближается к предоставляемому в сетях фиксированной связи. Это и высокоскоростной доступ в Internet, и мультимедиа (табл. 6.4). Очевидно, что достижение таких высоких скоростей при ограниченном частотном ресурсе и работе в каналах с замираниями потребует разработки принципиально новых подходов к построению радиоинтерфейса.

Архитектура систем будущего включает два основных элемента: сетевую инфраструктуру (Access Network) и магистральные базовые сети (Core Network). Такая структура обеспечивает возможность наращивания инфраструктуры путем последовательной модификации ее составных элементов, но чтобы гарантировать работу сетей в долгосрочной перспективе, необходимо помнить об абонентской части архитектуры — терминалах, которые за счет изменяемой конфигурации должны удовлетворять требованиям многих стандартов.

В рамках концепции ИМТ-2000 допустимы две стратегии перехода к 3G-системам: постепенное (эволюционное) и «одномоментное» (революционное). Рассмотрим те преимущества и недостатки, которые таит каждая из них (табл. 6.5).

Таблица 6.5. Две стратегии внедрения услуг 3-го поколения мобильной связи

Определяющий фактор	Эволюционный подход	Революционный подход
Метод использования частотного ресурса	Работа в старых диапазонах	Освоение новых диапазонов
Принцип предоставления услуг	Постепенно расширяемый ассортимент услуг	Новые услуги с начала развертывания
Пропускная способность	Постепенно наращиваемая	Изначально высокая
Стратегия создания сетевой инфраструктуры	Медленный и постепенный переход от 2G к 3G по мере появления спроса на услуги	Создание опытных районов («островков») с полным набором услуг
Технологический уровень	Новые технологии в отдельных элементах	Все технологии — новейшие
Архитектура сети	Максимальное использование существующей инфраструктуры	Новая
Коммерческий риск	Низкий	Высокий
Состав операторов	В основном те же, что и в 2G	Операторы, купившие лицензии на услуги 3G
Глобальный роуминг	С ограничениями	Без ограничений
Капитальные затраты	Незначительные	Значительные

Революция предполагает внедрение всех новейших технологий и новых интерфейсов, однако предусматривает полную замену существующего оборудования и ПО, что сопряжено с большими капитальными затратами и определенным коммерческим риском. Для отработки данной стратегии в разных районах мира уже создаются экспериментальные сети.

Один из важнейших признаков, принципиально разделяющих два подхода, — способ освоения частотного ресурса. При революционном сценарии требуется новый частотный ресурс. Япония и Европа намерены пойти по этому пути и выделить для систем 3-го поколения «индивидуальные» полосы радиочастот (подробнее см. «Сети», 2000, № 1, с. 34). Подход в США абсолютно иной — там спектр, выделенный для IMT-2000, уже занят службой PCS и 3G-системы будут работать в старых полосах частот вместе с существующими сетями стандартов TDMA/AMPS.

Эволюционное внедрение требует меньших капитальных затрат и предполагает плавную замену оборудования в зависимости от спроса на конкретные виды услуг. Такой подход позволяет максимально использовать существующую инфраструктуру сети связи, внедряя новые сетевые элементы в процессе последовательной модернизации.

Приверженцы двух наиболее массовых технологий 2-го поколения — TDMA/AMPS и GSM — стали сторонниками эволюционного пути развития. Сегодня эти системы имеют ограниченные возможности по наращиванию пропускной способности и видам услуг в рамках выделенного частотного диапазона. Рост их емкости без дополнительного расширения радиочастотного спектра возможен лишь за счет перехода на полускоростные каналы (GSM), введения многосекторных антенн или использования спектрально-эффективных методов модуляции (8PSK и др.).

В борьбе за лидерство при принятии мировых стандартов 3-го поколения образовались два лагеря, оформившиеся в виде двух партнерских объединений: 3GPP и 3GPP2.

В первое объединение — 3GPP — входят ETSI (Европа), ARIB (Япония), Комитет T1 (США), а также три региональных органа стандартизации от Азиатско-Тихоокеанского региона — CWTS (Китай), TTA (Корея) и TTC (Япония). Важно отметить, что совместные позиции ETSI и ARIB должны упрочиться с внедрением экспериментальных сетей на базе WCDMA, активно разрабатываемых с участием компаний DoCoMo, Ericsson и Nokia.

Основной вклад партнерства 3GPP в программу IMT-2000 — гармонизация пяти проектов: UTRA FDD (ETSI), WCDMA (ARIB), WCDMA NA (T1P1, США), WIMS (TR-46.1, США) и CDMA II (TTA). Его участники намерены предложить два варианта радиointерфейса. Первый — 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.

Другой тип радиointерфейса — IMT-TC (IMT-2000 Time-Code), представленный этим объединением 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.

С технической точки зрения основное отличие вариантов IMT-DS и IMT-TC от ранее поступивших в МСЭ предложений — в базовой чиповой скорости. В этих проектах она изменена с 4,096 Мчип/с на 3,84 Мчип/с (табл. 6.6).

Таблица 6.6. Характеристики радиointерфейсов для IMT-2000

Показатель	Технология				
	IMT-DS	IMT-MC	IMT-TC	IMT-SC	IMT-FT
Авторы технических спецификаций	3GPP, ARIB, ETSI	3GPP2, TTA TR-45.3	3GPP, ETSI,	3GPP2, UWCC, CWTS	ETSI TTA TR-45.3
Базовая технология	WCDMA, UTRA FDD	cdma2000	UTRA TDD TD-SCDMA	UWC-136	DECT EP
Метод доступа	DS-CDMA	MC-CDMA	TDMA/CDMA	TDMA	MC-TDMA
Дуплексный разнос	FDD	FDD	TDD	FDD	FDD/TDD
Чиповая скорость, Мчип/с	3,84	3,6884	3,84 (UTRA) 1,28 (SCDMA)	Н/д	Н/д
Скорость передачи, кбит/с	Н/д	Н/д	Н/д	384; 2048	1152; 2304; 3456
Вид модуляции	QPSK/BPSK HPSK*	QPSK/BPSK	QPSK/BPSK HPSK*	BOQAM QOQAM	GFSK; p/2- DPSK p/4- DQPSK p/8- D8PSK
Длина кадра, мс	10	5 и 20	10	4,6	10

Примечание. Н/д — нет данных. * HPSK (Hybrid Phase-Shift Keying) — гибридная фазовая манипуляция (известная также как OCQPSK).

Аббревиатура IMT-FT (IMT-2000 Frequency Time) присвоена проекту DECT EP, который поступил от ETSI. Новый стандарт на микросотовую систему DECT предполагает применение комбинированного частотно-временного дуплексного разнеса 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.

Во второе партнерское объединение — 3GPP2 — входят Ассоциация промышленности связи TTA (представленная подкомитетами TTA TR-45.3 и TTA TR-45.3) и ряд азиатских региональных организаций: ARIB, CWTS, TTA и TTC. Члены 3GPP2 являются сторонниками эволюционного развития двух технологий сотовой связи 2-го поколения TDMA (IS-136) и cdmaOne (IS-95), которые в настоящее время широко распространены в США.

Предложения от этого партнерства представлены двумя вариантами радиointерфейсов, получившими обозначение IMT-MC (IMT-2000 Multi Carrier) и IMT-SC (IMT-2000 Single Carrier), см. табл.6.6. Первый из них — IMT-MC — 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 разнесом, предполагается работа в непарных полосах частот. Радиointерфейс IMT-SC базируется на спецификациях проекта стандарта UWC-136; в нем определено поэтапное расширение возможностей существующей системы TDMA при условии работы системы в парных полосах частот.

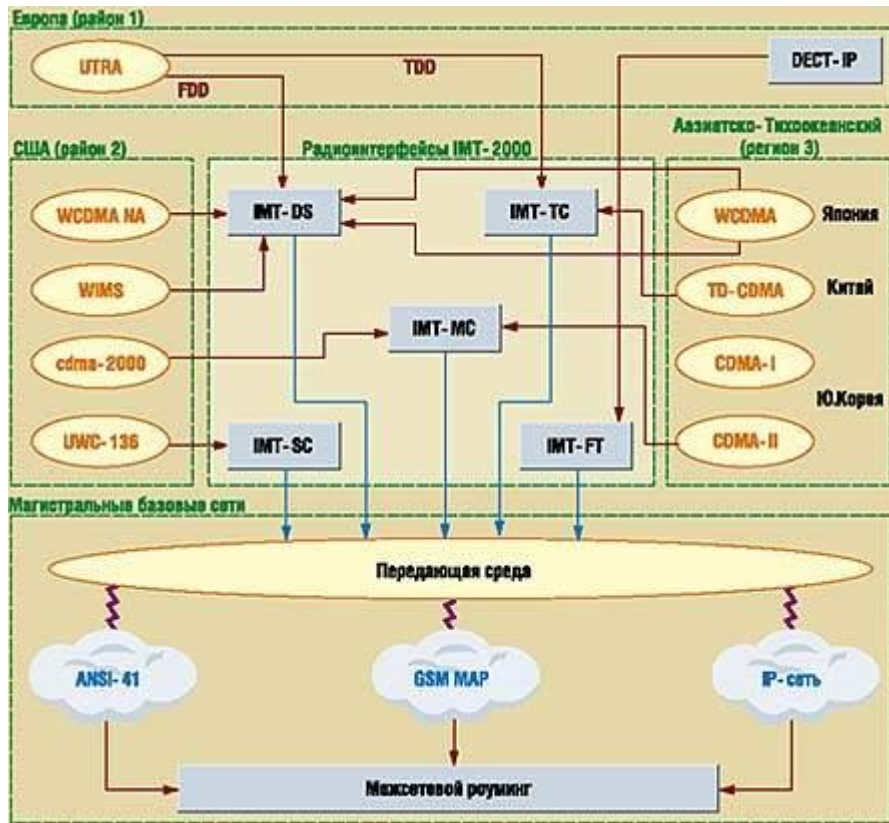


Рис. 6.1. Структура радиointерфейсов для IMT-2000.

Согласно концепции IMT-2000, система нового поколения подразделяется на две составные части: сети радиодоступа и магистральную базовую сеть. Подходы к их проектированию принципиально различны.

Эффективность сетей радиодоступа в значительной степени зависит от новизны технологий, которые в них используются. Смена поколений, как правило, означает и смену идеологии построения этих сетей. Магистральные сети более «инерционны». В них инвестированы значительные средства, которые операторы желают сохранить при переходе к 3-му поколению. Кроме того, существующие базовые сети не являются сдерживающим фактором для внедрения современных 3G-услуг. Поэтому их инфраструктура будет развиваться эволюционным путем, опираясь на существующие сети GSM, TDMA (IS-136), IP, IN и ISDN, что подтверждают и исследования, проведенные в рамках IMT-2000.

Сегодня в качестве магистральных предполагается использовать сеть, базирующуюся на IP-технологии, а также усовершенствованные опорные сети GSM MAP и ANSI-41, которые развернуты для наиболее развитых стандартов мобильной связи 2-го поколения — европейского GSM и североамериканских TDMA (IS-136) и CDMA (IS-95). Взаимодействие между тремя магистральными сетями — GSM MAP, ANSI-41 и базовой IP-сетью — будет осуществляться через межсетевой интерфейс NNI (Network-to-Network Interface).

Стандартный модуль идентификации пользователя UIM (User Identity Module) обеспечит глобальный роуминг независимо от метода радиодоступа или типа транспортной сети в том или ином географическом регионе.

В настоящее время важнее всего дать возможность всем операторам действующих сетей использовать существующую инфраструктуру при реализации набора новых услуг IMT-2000. В связи с этим МСЭ считает необходимым начать разработки единого протокола NNI, обеспечивающего глобальный роуминг в рамках 3G-систем.

Транспортная сеть должна обеспечить межсетевое взаимодействие и «прозрачность» доступа к услугам независимо от местонахождения абонентов. Чтобы реализовать это требование на практике, предусматривается создание специального конвертора, или шлюза, IWG (Interworking Gateway), который и будет поддерживать глобальный роуминг при любом протоколе радиодоступа.

Многофункциональная космическая телекоммуникационная система «Ростелсат».

Разработку многофункциональной космической телекоммуникационной платформы осуществляет АО "Ростелсат". По грандиозности своих масштабов предлагаемая система превосходит большинство из известных зарубежных проектов систем. Орбитальную группировку планируется создать из двух взаимоувязанных комплексов:

низкоорбитального сегмента, состоящего из 91 КА на 7 круговых приполярных орбитах высотой 700 км и наклоном 82° (подсистема "Ростелсат - Н");

среднеорбитальной группировки, в состав которой входят 24 КА на 4 круговых приполярных орбитах высотой 10355 км и наклоном 73° (подсистема "Ростелсат - В");

Низкоорбитальная подсистема "Ростелсат-Н" будет включать в свой состав три базовые сети:

- сеть подвижных абонентских станций, работающих в S-диапазоне частот (2,1/1,9 и 2,6 ГГц) и обеспечивающих связь между подвижными объектами с максимальной скоростью до 19,2 кбит/с (между возимыми) и 64 кбит/с (между носимыми);
- сеть стационарных абонентских станций, работающих в Ku диапазоне (11/13 ГГц) со скоростью от 64 кбит/с до 2048 кбит/с;
- сеть мониторинговых станций, работающих в диапазоне 11 ГГц и предназначенных для сбора информации со скоростью до 32 Мбит/с (дистанционное зондирование Земли с получением и обработкой информации практически в реальном масштабе времени).

На первом этапе создания системы орбитальная группировка "Ростелсат - Н" будет состоять из 70 КА, расположенных в 7 орбитальных плоскостях высотой 700 км и наклоном 82° (по 10 КА в каждой плоскости). На втором этапе орбитальная группировка будет доведена до 91 КА путем размещения в указанных орбитальных плоскостях дополнительно по 3 КА.

Зона обслуживания каждого КА представляет собой пятно на поверхности Земли диаметром 3500 км. Зоны радиовидимости всех КА покрывают Землю и обеспечивают видимость КА в зоне обслуживания под углом места не менее 10°.

В состав подсистемы "Ростелсат - В" будут входить:

- сети абонентских терминалов, обеспечивающих речевой обмен и передачу данных в S-диапазоне со скоростью от 1,2 до 64 кбит/с при связи с подвижными объектами;
- сети стационарных абонентских терминалов с любым набором стандартных скоростей до 2048 кбит/с, включая мультимедийные услуги;
- сеть цифрового телевидения со скоростью до 8 Мбит/с.

Космический сегмент подсистемы "Ростелсат-В" содержит в своем составе орбитальную группировку из 24 средневысотных КА (высота орбита 10360 км, наклонение 82,5°), располагаемых в четырех орбитальных плоскостях. В каждой плоскости расположено по 6 КА. Зона обслуживания отдельного КА имеет диаметр 7000 км и разбита на 625 сот протяженностью 160...200 км (для диапазона 20/30 ГГц) и 19 сот размером 1250 км (для диапазона 7/8 ГГц).

Зона обслуживания всех КА непрерывно покрывает всю поверхность Земли и обеспечивает видимость КА в зоне обслуживания под углом места 40° и выше.

На борту КА предполагается установить 91-лучевую антенну для связи с подвижными объектами и 19-лучевую - для связи со стационарными станциями и фидерными линиями. Суммарная пропускная способность в пересчете на один КА составит около 7000 каналов. В 1995-1996 гг. многие российские предприятия, специализирующиеся в области ракетно-космической и связной техники, столкнулись с резким сокращением государственных заказов. На основании имеющихся у них технологических и конструктивных заделов был предложен ряд проектов создания низкоорбитальных систем спутниковой связи, такие как "Гонец", "Сигнал", "Курьер", "Эликон-Стир", "СПС-Спутник" и др. Однако отсутствие устойчивого финансирования не позволило пока довести большинство из них до стадии практической реализации.

Успешная реализация российских проектов низкоорбитальных и среднеорбитальных систем спутниковой связи в сильной степени зависят от общего экономического состояния страны, от возможности привлечения необходимых инвестиций.

Спутниковая система связи Inmarsat

Созданная в 1979 году с целью удовлетворения потребностей в спутниковой связи на морских судах и безопасности мореплавания, Инмарсат в настоящее время управляет глобальной спутниковой группировкой, которая используется независимыми сервис-провайдерами для предоставления услуг голосовой, факсимильной телексной и мультимедийной связи для пользователей, находящихся в движении и в районах с отсутствием традиционных видов связи. Продолжая развивать и совершенствовать связь на море, Инмарсат расширил сферу своего влияния на наземный, автомобильный и авиационный рынки. Таким образом, на сегодня пользователями системы являются тысячи абонентов, которые живут или работают в удаленных районах, где отсутствует наземная связь, или путешествуют по всему миру. Пользователями системы являются журналисты и телеоператоры, спасательные организации и министерства по чрезвычайным ситуациям, транспортные компании, перевозящие грузы, авиалинии, авиапассажиры и органы управления воздушным движением, работники государственных учреждений, подразделения гражданской обороны, а также главы государств.

Зона покрытия

Спутники системы Инмарсат покрывают около 98% земной поверхности. Гарантированная связь обеспечивается в среднем от 75° ю. ш. до 75° с. ш.

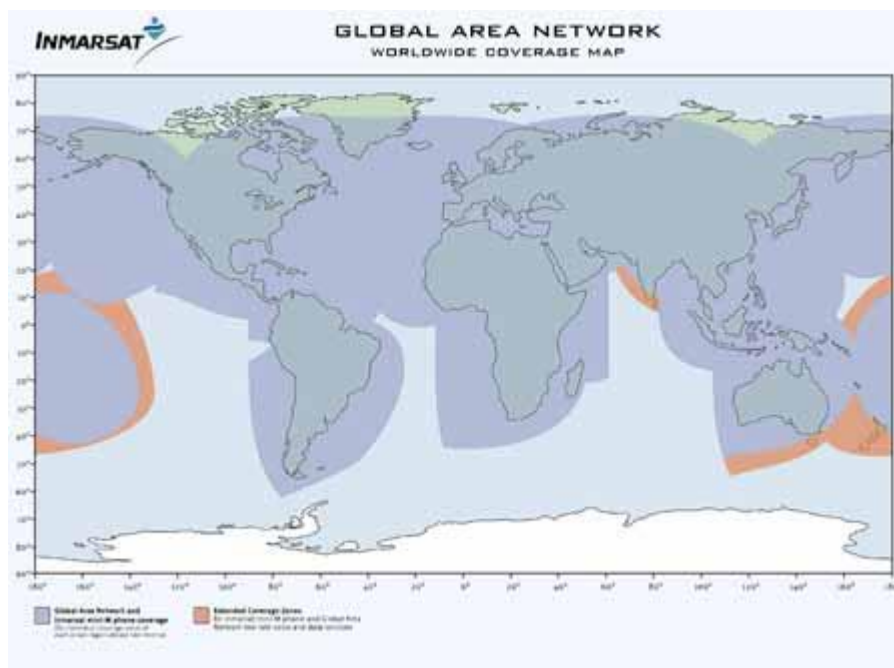


Рис. 6.2. – Зона покрытия спутников системы.

Состав, виды услуг и особенности построения

В состав системы Inmarsat входят:

- космический сегмент, состоящий из рабочих и запасных геостационарных КА с ретрансляторами и командно-измерительного комплекса (наземных станций слежения и др.);
- наземный сегмент, включающий в себя береговые земные станции (БЗС), координирующие сетевые станции (КСС), и эксплуатационный контрольный центр (ЭКЦ);
- парк земных станций и терминалов: мобильные (морские суда, самолеты), носимые и стационарные; терминалы предназначены как для коллективного, так и индивидуального пользования.

Работа системы Inmarsat осуществляется в диапазонах частот, выделенных на первичной основе для подвижной спутниковой службы. Для связи с подвижными абонентами используется L-диапазон частот: 1626,5-1660,5 МГц (линия "Земля - спутник") и 1525,0-1559,0 МГц (линия "спутник - Земля"). Работа фидерных линий осуществляется в С-диапазоне: 6425-6450 МГц (линия "Земля - спутник") и 3600-3623 (3600-3630) МГц (линия "спутник - Земля").

Контроль за работой системы осуществляет эксплуатационный контрольный центр, который обеспечивает прием и обработку информации о состоянии работоспособности всех элементов системы, контролирует характеристики космического сегмента, реализует планы ввода в эксплуатацию новых технических средств.

Береговые земные станции служат промежуточными звеньями между спутниками системы Inmarsat и береговыми абонентами, с которыми они могут соединяться по международным и национальным телефонным и телеграфным сетям. Связь объектов в системе Inmarsat осуществляется только через БЗС. Все береговые станции системы Inmarsat обеспечивают для судов, терпящих бедствие, возможность быстрого соединения по телефонному или телексному каналу со службами, участвующими в поисково-спасательных работах.

В каждой подспутниковой зоне Inmarsat работают несколько стандартных БЗС, одна из которых выполняет функции координирующей сетевой станции. КСС следит за работой спутниковой сети в данном регионе, распределяет пропускную способность

ретранслятора между береговыми станциями. В функции КСС входит передача сообщений абонентам сети на основной (1537,750 МГц) или резервной (1538,475 МГц) вызывных частотах, а также ретрансляция других категорий специальных сообщений.

На первых этапах создания системы Inmarsat связь организовывалась через арендуемые у других организаций спутники Marisat, Marecs и Intelsat-5MSC. В настоящее время орбитальная группировка системы Inmarsat состоит из 6 КА Inmarsat (4 КА типа Inmarsat-2 и 2 КА типа Inmarsat-3) и 7 КА старого поколения (типа Marisat и Intelsat-5MCS)

Подспутниковая зона орбитальной группировки системы Inmarsat охватывает 4 океанических региона: Атлантический восточный (АОР-В), Атлантический западный АОР-З, Индийский (ИОР) и Тихоокеанский (ТОР). Над каждым из океанических регионов находятся по одному действующему и по два запасных спутника, что обеспечивает покрытие практически всей поверхности земного шара, за исключением приполярных районов.

Береговые земные станции

В системе Inmarsat функционируют 40 береговых станций, расположенных в различных странах мира, в том числе на территории СНГ (Одесса и Находка). Эти станции обслуживают абонентов в Атлантическом, Индийском и Тихоокеанском регионах. Береговые станции находятся во владении тех стран, на чьей территории они размещены. Их эксплуатация осуществляется уполномоченными на это организациями национальных администраций.

Алгоритмы работы БЗС и их основные тактико-технические параметры должны находиться в строгом соответствии с требованиями организации Inmarsat. Каждая БЗС имеет закрепленную за ней несущую, которая уплотняется 22 телеграфными каналами. Телефонные каналы не закреплены за конкретными станциями, а находятся в «общем пользовании». Береговые станции имеют выход в национальные и международные сети телефонной и телексной связи.

Работа абонента, имеющего аппаратуру определенного стандарта, через береговую станцию может осуществляться только в том случае, если БЗС имеет соответствующее оборудование. В частности, все БЗС оснащены оборудованием, поддерживающим связь со станциями стандарта Inmarsat-A. Что же касается высокоскоростного режима передачи данных, то он осуществляется только через некоторые из них. Аналогичная ситуация и с оснащением БЗС оборудованием других стандартов. Например, протоколы стандарта Inmarsat-C поддерживают около 20 БЗС, причем на территории РФ таких станций нет. Услуги стандартов Inmarsat-M и Inmarsat-B предлагаются еще меньшим числом БЗС, в основном вновь созданными береговыми станциями.

На береговых станциях используются параболические антенны, диаметром 12–15 м. Стоимость береговой станции в зависимости от комплектации составляет 1,0–2,5 млн долл.

Парк абонентских станций

В системе Inmarsat подвижные объекты оснащаются разными типами оконечного абонентского оборудования, которое должно удовлетворять специфическим требованиям отдельных категорий пользователей, известным как «стандарты». Наиболее широкое распространение получили следующие виды стандартов:

Стандарт Inmarsat-A. Станции этого стандарта предназначены для работы в сетях телефонной, факсимильной, телексной и телеграфной связи. Они оснащены параболической антенной диаметром 0,8–1,2 м. Связь устанавливается после набора номера в автоматическом режиме.

К настоящему времени выпущена 71 модель станций, разработка новых станций этого

стандарта прекращена.

Стандарт Inmarsat-B. Цифровая ЗС, предлагающая расширение функциональных услуг Стандарта А с одновременным снижением их стоимости. Передача речи и данных осуществляется со скоростью 24 кбит/с. Размеры антенны те же, что и для станций Стандарта А. В коммерческую эксплуатацию эта подсистема введена в 1994 г. Планировалось, что постепенно станции Стандарта В заменят парк Стандарта А. Модели наземных ЗС могут быть размещены в 1–2 чемоданах или установлены непосредственно на транспортных средствах.

Стандарт Inmarsat-C. Малогабаритная станция персональной связи с ненаправленной или слабонаправленной антенной, обеспечивающая передачу информации в пакетном режиме. Обмен данными, в том числе короткими сообщениями, осуществляется со скоростью 600 бит/с. В настоящее время ни в РФ, ни в странах СНГ серийное производство станций Стандарта С не освоено.

Стандарт Inmarsat-M. Малогабаритная станция спутниковой связи, обеспечивающая радиотелефонную и факсимильную связь, передачу данных. Передача информации осуществляется со скоростью 8 кбит/с (данные). Используется антенна диаметром 40–50 см.

Стандарт Inmarsat-Mini-M. Малогабаритная станция, предназначенная для радиотелефонной и пейджинговой связи.

В системе Inmarsat используются несколько типов самолетных станций, предназначенных для обеспечения следующих видов услуг:

- Inmarsat-Aero-H – 6-канальная, работающая в режимах: радиотелефонная связь, факс, телекс; высокоскоростная передача данных – для обслуживания экипажей воздушных судов и пассажиров на международных авиалиниях;

- Inmarsat-Aero-I – 4-канальная, работающая в режимах: радиотелефонная связь, факс, телекс; высокоскоростная передача данных – для обслуживания экипажей воздушных судов и пассажиров на международных авиалиниях;

- Inmarsat-Aero-L – одноканальная, режим низкоскоростной передачи данных для обеспечения безопасности полетов воздушных судов;

- Inmarsat-Aero-C – одноканальная, режим низкоскоростной передачи данных, удовлетворяющая требованиям Стандарта Inmarsat-C.

Таблица 6.7. – Основные характеристики стандартов.

Стандарт	А	В	С	М	Mini-M
Год начала эксплуатации	1976	1992	1991	1993	1997
Скорость передачи, кбит/с	до 64	24 (речь) до 64 (данные)	0,6	до 8	4,8 (речь) 2,4 (данные)
Модуляция	ЧМ	QPSK	BPSK	QPSK	BPSK, OQPSK
СЛ, дБ/К	-4	-4	-23	-12...-10	н/д
ЭИИМ, дБВТ	36	33	14±2	27	11-17
Полоса, кГц	50	20	5	10	10
Стоимость терминала, долл.	25000	25000	5000	15000-25000	4000

Стоимость долл./мин	услуг,	8-12	5,5	1 долл. за 1 Кбит	5,5	3
------------------------	--------	------	-----	----------------------	-----	---

Спутники Инмарсат

В системе Инмарсат используются геостационарные спутники, которые "неподвижно висят" над заданными точками над экватором Земли. На каждом спутнике имеются, по крайней мере, два ретранслятора, один из которых ретранслирует сообщения в направлении от Земных станций к терминалам, а второй - в обратном направлении.

Спутники системы Инмарсат располагаются на геостационарной орбите на высоте 22 223 мили (35 786 км).

Четыре спутника Инмарсат-2 были произведены международным консорциумом, возглавляемым подразделением The Space&Communications компании "British Aerospace" (в настоящий момент входит в состав англо-французской компании "Matra Marconi Space"). Подрядчиками выступили "Hughes Aircraft" (США), "Fokker" (Нидерланды), "Matra" (Франция), "MBV" (Германия), "NEC" (Япония), и "Spar" (Канада). Центры управления спутниковой группировкой сооружались при непосредственном участии компаний: "CLTC" (Китай), "CNES" (Франция), "SED" (Канада), "Telespazio" (Италия), и "Intelsat". Инмарсат-2 - это спутники со стабилизацией в трех плоскостях, на основе платформы "Eurostar", разработанные компаниями "British Aerospace" и "Matra Espace" (обе в настоящее время входят в группу "Matra Marconi Space").

Спутники рассчитаны на 10-летний срок эксплуатации. Предпусковой вес составил 1300 кг, орбитальный вес - 800 кг при 1200 Вт излучаемой мощности. Телекоммуникационное оборудование включает 2 транспондера, обеспечивающих работу на передачу (с С- на L-диапазон) и на прием (с L- на С-диапазон) при работе с наземным оборудованием на частотах 6,4/1,5 и 1,6/3,6 ГГц. Эффективная изотропная излучаемая мощность (ЭИИМ) L-диапазона составляет 39 ДБВт. Каждый спутник обеспечивает покрытие приблизительно 1/3 части Земли. В зависимости от нагрузки, полоса частот и ЭИИМ перераспределяется между судовыми, авиационными и наземными пользователями.

Сами спутники изготовлены американской компанией "Lockheed Martin Astro Space", системы обеспечения и управления разработаны на основе платформы "Series 4000" компании "Astro Space Series". Английское подразделение "Matra Marconi Space" подготовило телекоммуникационную часть, включающую антенны, повторители и другое коммуникационное оборудование. Все оборудование связи функционирует в С- и L-диапазонах. Антенны и электронное оборудование каждого спутника настроено на оптимальное покрытие определенной части Земли ("footprint"). Несомненное преимущество спутников Инмарсат-3 заключается в способности концентрировать мощность в определенной зоне. Каждый спутник имеет до 7 зональных лучей и один глобальный. Количество задействованных лучей напрямую зависит от интенсивности использования связи. Помимо вышеперечисленного спутники способны использовать часть L-диапазона несоприкасающихся лучей, удваивая, таким образом, пропускную способность спутника. Предстартовый вес каждого спутника составил 2066 кг. ЭИИМ каждого спутника составляет 48 ДБВт, где ЭИИМ (эффективная изотропная излучаемая мощность) означает, какую энергию может сконцентрировать спутник в обслуживаемой области.

3 спутника Инмарсат-4 были запущены в 2004 году и разрабатывались компанией "Astrium" (предыдущее название - Matra Marconi Space). Мощность новых спутников в 100 раз выше, чем у предыдущих, что позволяет передавать данные со скоростью до 432 Кбит/с. Усовершенствованная технология позволяет снизить тарифы до 75% от

существующих в стандарте Инмарсат-M4. Новая услуга называется В-GAN - Broadband Global Area Network (широкополосная глобальная сеть).

Inmarsat ВGAN.

Появление на рынке связи новой услуги Inmarsat ВGAN (Broadband Global Area Network — глобальная широкополосная сеть) позволяет говорить о настоящем прорыве в этой области. Мы уже привыкли к услугам широкополосной связи в густонаселенных районах с развитыми каналами связи. С появлением Inmarsat ВGAN Вы можете воспользоваться ей в любой, даже самой отдаленной точке мира.

Итак, Inmarsat ВGAN – это новая спутниковая мобильная услуга, совмещающая высокоскоростную передачу данных и высококачественную телефонию, реализованная через выведенные на орбиту в 2005 году спутники Inmarsat-4 (I-4).



Рис.6.3. Структурная схема сети Inmarsat ВGAN

Первый из спутников I-4 (F-1) запущен 11 марта 2005 года. Услуги сети ВGAN в настоящее время доступны на территории Европы, Африки, на Ближнем Востоке и Азии. После выведения на орбиту второго спутника (F-2) 8 ноября 2005 года в зону покрытия войдет также и Америка (в середине 2006 года).

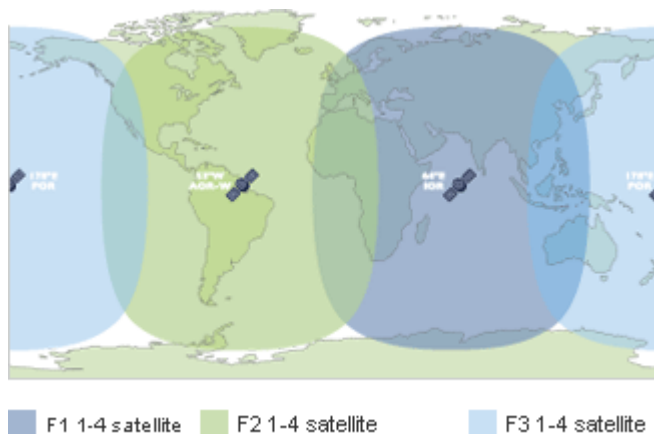


Рис. 6.4. Зона покрытия спутников сети Inmarsat ВGAN.

Наземным сегментом в цепи передачи данных сети Inmarsat BGAN, посредством которого любой пользователь может подключиться к высокоскоростным спутниковым каналам, являются легкие переносные спутниковые терминалы. Это недорогие, надежные, компактные, простые в эксплуатации устройства весом чуть более 1 кг позволяют организовать «мобильный офис» в любой, даже самой удаленной точке мира, где нет ни телефонных сетей общего пользования, ни сотовой связи, тем самым расширяя понятие «границ компании» до глобальных масштабов.

Абонентский терминал **EXPLORER™ 500** позволяет говорить по телефону через спутник, обеспечивает высокоскоростной доступ в Интернет и поддерживает все виды связи (факс, e-mail, видеоконференция). Терминал имеет интерфейсы LAN, RJ11, Bluetooth, USB. Возможна одновременная работа нескольких пользователей по разным интерфейсам.

Настройка на спутник проста и осуществляется по встроенным компасу и индикатору сигнала и не требует специального оборудования.



Рис.6.5. Абонентский терминал EXPLORER™ 500.

Скорость вниз - до 460 КБит/с, вверх - до 128 КБит/с.
Питание: переменный ток 220В, постоянный ток 12В (автомобиль), встроенный аккумулятор (до 1,5 часа в режиме передачи 144 КБит или до 36 час в ждущем режиме).
Габариты: 217x217x52 мм, масса: около 1,5 кг.

Inmarsat FLEET

Принципиально новый, революционный стандарт INMARSAT, обеспечивающий постоянный диалоговый режим доступа в Интернет, благодаря протоколу пакетной передачи данных (MPDS), при использовании которого пользователь оплачивает только объем принятых и переданных данных, а не время занятия канала. Обеспечивает экономичную, круглосуточную, оперативную связь для любого судна фактически в любой точке мирового океана и делает возможным организацию современного мобильного офиса в море.

Морские системы связи Inmarsat Fleet от KVN включают в себя более десятка видов, но в российских условиях реально использовать системы Fleet 77 и Fleet 55:

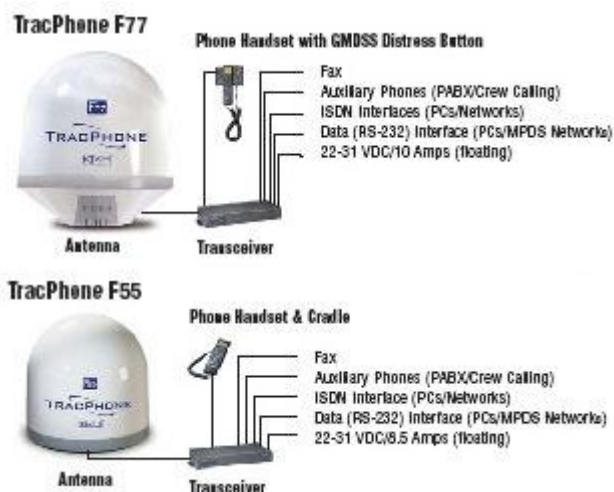


Рис.6.6. Системы Fleet 77 и Fleet 55.

Обе системы предназначены для предоставления пользователям быстрых интернет/интранет соединений, видеоконференций, глобального голосового/факсового сервиса.

Inmarsat Fleet системы позволяют пользователям работу по протоколам ISDN (Integrated Services Digital Network) и MPDS (Mobile Packet Data Service). ISDN протокол с поминутной тарификацией рассчитан на качественную голосовую и факсовую связь, видеоконференции, передачу больших файлов. MPDS протокол с помегабайтной тарификацией предназначен для состояния "всегда online" - время нахождения в сети не учитывается.

Инмарсат Fleet полностью совместим с корабельными системами связи и может выступать (при подключении к IP-роутеру) в качестве хаба для всего корабельного комплекса связного оборудования.

Характеристики системы:

- Масса антенны с обтекателем: 26 кг (F77), 18 кг (F55)
- Масса приемопередатчика: 2,6 кг
- Масса телефонной трубки/рычага: 0,25 кг/ 0,15 кг
- Голосовая связь: 4.8 Kbps AMBE, 64 Kbps трансляция
- Европейский ISDN интерфейс: Шина ISDN NT1 S/T, ITU-T I.430, совместимый с ISO 8877 разъем RJ 45
- Интерфейс USB
- Интерфейс данных: Серийный EIA совместимый стандартный RS-232E, встроенный Hayes совместимый модем, до 115 Kbps, разъем DB-9 female
- Интерфейс факса: 2-проводной 600 Ом CCITT rec. G.473, T.30 Группы III факс, разъем модулятора RJ-11, совместимый с факсом Группы 4 (используя канал ISDN)
- Скорость загрузки данных (протоколы ISDN и MPDS): 64 Кбит/с, с использованием фирменного программного обеспечения Velocity™ Acceleration software от KVH - до 320 Кбит/с
- Питание: 21 – 34 В пост. тока (15 А макс.)
Потребляемая мощность: 200 Вт (макс.)
- Размеры приемопередатчика: 5,5 x 37,7 x 16,4 см
- Размеры телефонной трубки/крэдла: 20 x 5 x 3 см/ 16 x 6,1 x 2,7 см
- Скорость асинхр. данных: Европа ISDN 64 Kbps и США ISDN 56 Kbps

- Телефонный интерфейс: 2-проводной 600 Ом ССИТТ rec. G.473, стандартные DTMF телефоны, разъём модулятора RJ-11.



Рис.6.7. Пример использования систем.

Inmarsat R-BGAN

Система Inmarsat R-BGAN - региональная система широкополосной пакетной высокоскоростной передачи данных (Regional Broadband Global Area Network). Новая система R-BGAN обеспечивает:

- возможность доступа в сети передачи данных из удаленных районов, где отсутствуют обычные средства связи;
- скорость передачи данных в спутниковом канале до 144 Кбит/сек.;
- конфиденциальность сеансов связи;
- доступ в сети Интернет и Интранет к серверам HTTP/FTP;
- передачу/прием электронной почты;
- передачу/прием голосовых сообщений с использованием IP – протокола;
- передачу/прием цифровых видео изображений;
- передачу/прием цифровых видео потоков в режиме реального времени;
- передачу/прием факсимильных сообщений с использованием IP – протокола;
- организацию видеоконференций с использованием IP – протокола;
- использование стандартных SIM-карт GPRS для организации связи.

Система R-BGAN состоит из двух компонентов: космического сегмента и наземной сотовой сети общей радиослужбы с коммутацией пакетов (GPRS). Удачное сочетание этих двух компонентов дает возможность абоненту наиболее оптимально и с минимальными затратами использовать возможности системы R-BGAN.

Для организации сеанса связи в системе R-BGAN абонент, имеющий свой персональный компьютер должен приобрести:

- необходимую регистрацию и SIM – карту;
- спутниковый модем;
- необходимое программное обеспечение для загрузки в свой компьютер.

Спутниковый модем представляет собой портативный терминал спутниковой связи, разработанный компанией Hughes Network Systems и подключаемый к компьютеру посредством одного из интерфейсов:

- последовательный универсальный порт – USB;
- радиолиния связи по технологии Bluetooth;
- Ethernet.

Другие интерфейсы также можно реализовать в зависимости от типа изделия. Для абонента работа со спутниковым модемом аналогична работе с ISDN – модемом наземных сетей передачи данных.



Рис.6.8. Терминал Inmarsat R-BGAN.

Модемы R-BGAN - первая стадия разработки системы спутниковой связи Инмарсат нового поколения. До июля 2005 года связь осуществлялась через арендованные на спутнике Thuraya ретрансляторы. Затем после запуска и ввода в эксплуатацию спутника Инмарсат I-4F1 связь была переведена на него. Это позволило расширить зону охвата системы R-BGAN и улучшить качество связи. С вводом в эксплуатацию спутника Инмарсат I-4F2 связь через R-BGAN стала доступна также в Северной и Южной Америках.

В настоящее время модемы R-BGAN работают в рамках Глобальной Широкополосной Сети Инмарсат (BGAN).

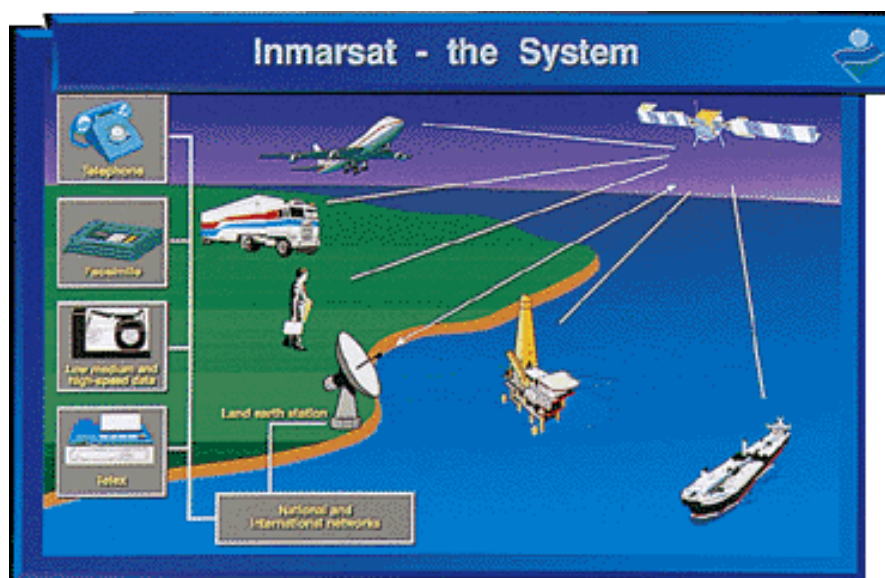


Рис. 6.9. Структура системы.

Зона покрытия

Как показано на карте (рис.6.10), сеть R-BGAN охватывает Европу, Россию (западные регионы, Дальний восток, юг России), страны СНГ, Ближний Восток, Северную, Центральную и Западную Африку, Индию.

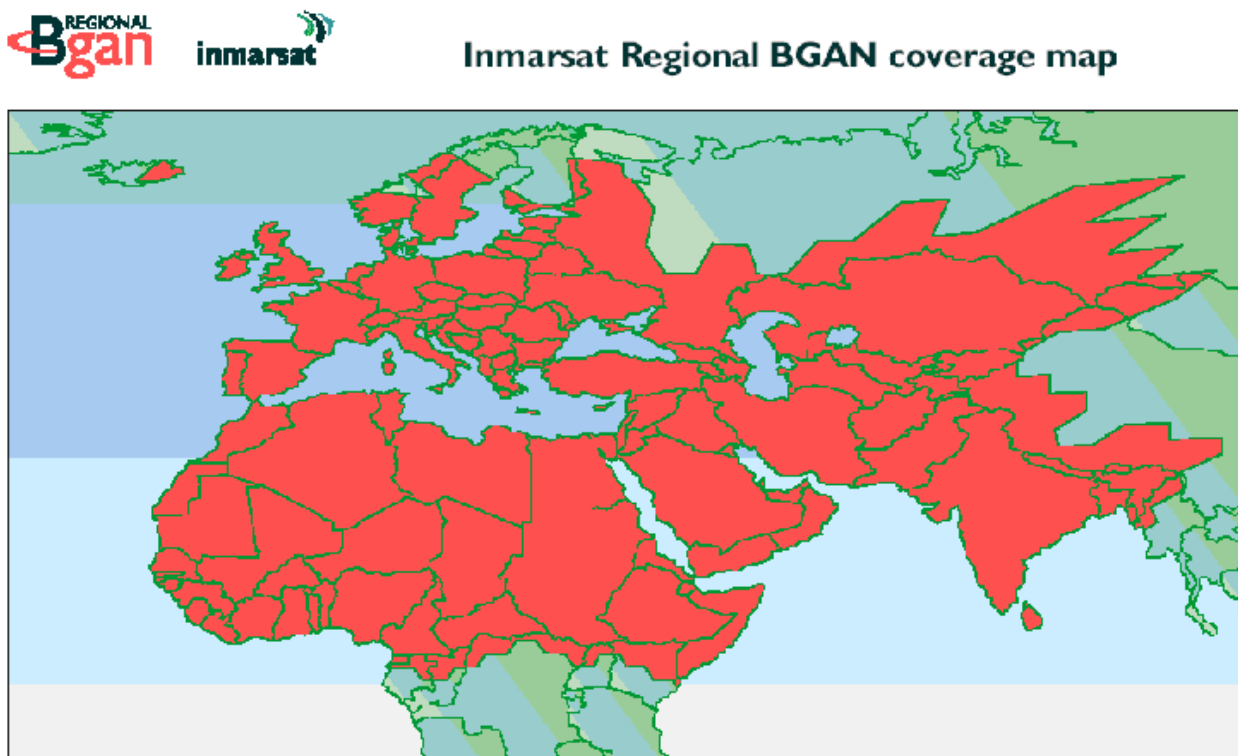


Рис.6.10. Зона покрытия системы Inmarsat R-BGAN.

Российский рынок спутниковой связи в своих основных структурных характеристиках повторяет этапы развития мирового рынка. В настоящее время в России уже сформировались три крупных сегмента этого рынка. Первый и самый молодой сегмент этого рынка связан с развитием таких сетей персональной спутниковой связи, как Iridium, Inmarsat, Globalstar, а в перспективе ICO, Ellipso и Thuraya. Терминалы персональной связи существенно отличаются от VSAT-станций. Они более компактны, универсальны, сопрягаются с сетями сотовой связи, а самое главное, работают при движении абонента. Вместе с тем персональная связь пока не способна обеспечить тот же комплекс и качество услуг, которые предоставляют VSAT-станции, да и тарифы в сетях персональной связи существенно выше.

Второй, достаточно крупный сегмент связан с развитием корпоративных сетей, базирующихся на технологии VSAT, т.е. на использовании малогабаритных спутниковых терминалов с антеннами диаметром от 1,8 до 2,5 м. На сегодняшний день в мире насчитывается около 300 тыс. станций VSAT. В России количество установленных VSAT-станций составляет не менее 3,2 % от общего числа этих земных станций в мире (около 10 тыс. станций). Однако все аналитики считают, что данный рынок далек от насыщения даже в развитых странах. Поэтому прогнозируется продолжение в 2000 г. роста объемов производства VSAT-терминалов: по некоторым данным, их общее число превысит 500 тыс., а в России может увеличиться до 20 тыс. станций.

Третий сегмент охватывает системы непосредственного телевизионного вещания, работающие главным образом в Ku-диапазоне частот (14/11 ГГц), что позволяет использовать на приеме малые земные станции, стоимость которых не превышает 500

долл. Этот вид спутникового вещания ориентируется в первую очередь на массовые услуги высокоскоростного доступа к Интернету, системы домашнего и офисного приёма ТВ-программ, а также на сельское население и малые города со слабо развитой кабельной инфраструктурой. В ближайшие годы по оценкам ФЦ "Телеком", наибольший доход на российском рынке ССС (до 60-70% от общего) ожидается именно в этом сегменте.

На каждом из этих трёх сегментов в последние годы достигнуты крупные практические результаты. Анализ опыта разработки и применения ССС на данных рыночных сегментах имеет важное значение при определении перспективных направлений развития спутниковой связи.

СПУТНИКОВЫЕ СИСТЕМЫ ПЕРСОНАЛЬНОЙ РАДИОСВЯЗИ

До настоящего времени развитие спутниковых систем было связано главным образом с организацией магистральных линий связи для удаленных регионов со слабой инфраструктурой телекоммуникаций или между континентами. В последнее десятилетие распространение получили малоапертурные наземные станции типа VSAT, обеспечившие возможность организации межрегиональных и корпоративных спутниковых телекоммуникаций с голосовой связью и цифровой передачей данных "из конца в конец" при достаточно низкой стоимости.

В течение этого же десятилетия наземные коммуникационные сети обогатились новыми технологиями и средствами, которые на рубеже столетий позволили реализовать на основе волоконно-оптических линий связи кольцо глобальной системы высокоскоростных коммуникаций, охватившее наиболее развитые страны на всех континентах. Распространению глобальных телекоммуникаций способствует подъем в технологиях магистральных систем коммутации (от ISDN к SDH) и широкополосных радиоретрансляционных и волоконно-оптических линий связи, а также внедрение дешевых беспроводных систем подвижной связи и средств передачи данных. Однако эта "супермагистраль" не может решить все проблемы. Поэтому активно развиваются и другие технологии, в том числе и средства беспроводных коммуникаций - как наземных, так и спутниковых.

Повсеместная компьютеризация общества, внедрение международной сети Интернет с доступом к информационным ресурсам Web-систем, появление мультимедийных средств, - все это предъявило новые требования к телекоммуникационным системам и общественным услугам, касающиеся доступности, реактивности, скорости передачи информации и полосы пропускания линий связи. Удовлетворение общественных потребностей в свою очередь вызвало бурный рост промышленности при тиражировании известных технологий и средств телекоммуникации, устройств удаленного доступа и подвижной связи, а, следовательно, и значительное снижение их стоимости.

Сегодня крупные рынки общественных услуг представляют собой действенный стимул для развития новых средств и систем телекоммуникации и сетевых технологий. Так, бурный рост Интернета послужил ускорению развития универсальных средств и систем подвижных телекоммуникаций, в частности, универсальных подвижных телекоммуникационных систем (UMTS), в которых на основе использования имеющихся в настоящее время технологий решаются проблемы повышения эффективности коммуникаций при снижении стоимости оборудования и обслуживания.

Новые тенденции в распространении информационных технологий вызывают необходимость получения телекоммуникационных услуг в любом месте, где может оказаться человек. Эти потребности все более расширяются: от обычного телефона и средств подвижной голосовой связи - к получению доступа к информационным ресурсам с помощью компьютера. Более того, появляется необходимость не только передавать графические данные и диаграммы, но и получать видовые, картографические и

"движущиеся" изображения, организуя интерактивную видеоконференцсвязь. Существует также класс приложений, требующих удаленного участия в прикладных процессах контроля, наблюдения, позиционирования и управления в реальном времени, взаимодействия с движущимися объектами и системами. Происходит переход к более сложным приложениям и системам, причем с явным перевесом в сторону использования быстрых и глобальных телекоммуникаций.

Система персональной спутниковой радиосвязи ICO

Система ICO состоит из космического сегмента и специализированной наземной сети. Космический сегмент ICO включает 10 операционных спутников и два резервных, действующих на средней околоземной орбите (МEO) с удалением на 10355 км. Каждый спутник покрывает около 30 процентов поверхности Земли. Орбитальная группировка разрабатывалась со значительным перекрытием поверхностных зон, гарантируя, что в любое время как минимум два спутника окажутся в виду пользователя и наземной станции.

Спутники свяжутся с наземными пользователями через сеть ICONET, которая будет состоять из 12 земных станций или спутниковых узлов доступа (SAN), размещенных по всей поверхности земного шара и связанных с наземными магистральными сетями. Спутниковые узлы доступа SAN будут включать три элемента: антенны со связанным оборудованием для взаимосвязи со спутниками ICO; коммутаторы и маршрутизаторы для управления трафиком внутри ICONET и других территориальных сетей, в частности, общедоступных коммутируемых телефонных сетей; и, наконец, базы данных, чтобы поддерживать управление движением спутников.

Каждый спутниковый узел доступа SAN будет содержать базу данных, чтобы поддерживать терминалы пользователей, приписанных к этому узлу. Через фидерный канал антенны будет поддерживаться связь между спутниками и узлами доступа SAN. В любое время каждый спутник будет находиться в прямом контакте с двумя или четырьмя узлами SAN.

Связь между пользователями и спутниками будет устанавливаться через сервисные антенны спутников. Использование множества сервисных лучей связи на каждом спутнике, а также использование каждой частоты множеством потребителей позволит увеличить эффективность распределения спектра.

Спутники функционируют в S-диапазоне и C-диапазоне и используют бортовую цифровую обработку и схему множественного доступа с разделением времени (TDMA), чтобы одновременно обработать до 4500 обращений на спутник по телефону. Согласно требованиям спектра, каналы системных служб ICO работают в полосе 2 ГГц (связь между спутниковым и карманным или пользовательским терминалом). Определено, что системы подвижных спутниковых служб могут использовать частоты 1.98-2.01 ГГц для каналов "вверх" и 2.17-2.20 ГГц для каналов "вниз". ICO выбрал диапазоны 5 ГГц и 7 ГГц для операционной фидерной связи (соединения между спутниками и наземными шлюзовыми станциями, SAN). ICO использует фидерную связь в полосе 5.15-5.25 ГГц ("Земля - Космос") и в полосе 6.97-7.075 ГГц ("Космос - Земля").

Разрозненность стандартов и недоступность некоторых географических областей стимулирует развитие оборудования для спутниковых телефонов. ICO не предполагает, что спутниковое обслуживание карманных телефонов будет когда-либо предоставляться по ценам, конкурирующим с подобными и хорошо разработанными наземными системами. Но спутниковый телефон становится идеальным дополнением для обслуживания в тех областях, где местные наземные системы не обеспечивают необходимых потребностей пользователей в обслуживании, или там где просто нет никаких служб связи.

Ожидается, что службы ICO будут востребованы пользователями международных и национальных сотовых систем связи, которые передвигаются вне областей покрытия

этих систем. Это прежде всего представители бизнеса, промышленности и правительственных организаций, транспортной отрасли, аэронавигационного и морского секторов, а также резиденты сельских и удаленных областей, испытывающие нехватку адекватной локальной инфраструктуры передачи данных.

Система персональной спутниковой радиосвязи SKYBRIDGE

В спутниковые проекты AlcatelSpace активно включается использование ATM. AlcatelSpace объявила, что создаваемая компанией объединенная система Alcatel Alsthom и SkyBridge зарегистрирована в FCC для начала проектирования и ввода в эксплуатацию как глобальная сеть со службой фиксированной спутниковой связи на не геостационарных спутниках для обеспечения передачи данных, голоса и видео с широкополосными услугами. Предложенная система будет иметь группировку из 64 спутников на орбите с высотой 1457 км.

Для этого Alcatel Alsthom и LoralSpace&Communications сформировали стратегическое партнерство для совместной разработки, развертывания и эксплуатации высокоскоростной глобальной спутниковой сети для мультимедиа, которая предоставит широкополосные услуги различным категориям пользователей. Соглашение включает перекрестные капиталовложения в низкоорбитальные спутники проекта SkyBridge Alcatel's и в проект пяти геостационарных спутников CyberStar компании Loral.

Услуги через геостационарные спутники предоставляются на рынке с 1999 года, а группировки LEO-спутников должны появиться в 2001 году. Геостационарные системы хорошо подходят для поставки радиопередач и разнообразных асимметричных услуг. Низкоорбитальные системы, благодаря малому времени задержки распространения сигнала, наиболее эффективны для поставки высокоинтерактивных услуг. LEO-система обеспечивает глобальное покрытие, тогда как геостационарные системы могут быть нацелены на региональные рынки.

Благодаря глобальной возможности покрытия, SkyBridge позволит сервисным поставщикам предложить подписчикам непрерывные интерактивные широкополосные услуги, независимо от их расположения или характера их локальной инфраструктуры связи. Каждый спутник освещает область в радиусе 3000 км, при максимум 45 "пятнах" земной поверхности: каждое такое "пятно" соответствует области покрытия одного шлюза с радиусом действия 350 км.

Космическая система Loral предлагает спутниковую систему, называемую CyberStar, которая состоит из трех GEO-спутников. Loral использует для сервисных операций "вверх" спектр полосы в диапазонах 28.35-28.6 и 29.5-30.0 ГГц, и полосы для сервисных операций "вниз" в диапазонах 18.95-19.2 и 19.7-20.2 ГГц. Loral запрашивает полномочия для межспутниковых связей, используя полосу в диапазоне 60 ГГц. Каждый спутник в системе CyberStar имеет бортовую обработку и возможности переключения для поддержки максимальной гибкости связи. Антенны каждого спутника обеспечивают покрытие регионов 27 лучами. Для протоколов "вверх" Loral использует FDM/TDM, для протоколов "вниз" - TDM. Сеть CyberStar ориентирована на обеспечение услуг типа видеотелефона и видеоконференцсвязи, быстродействующих сетей передачи данных и службы "полосы по требованию".

Шлюзы состоят из подсистемы маршрутизации и ATM-коммутаторов с обеспечением интерфейсов к арендованным каналам и локальным станциям, к наземным IP-сетям типа Интернет, к узкополосным и широкополосным магистральным сетям. Средства управления шлюзами и трафиком SkyBridge соответствуют областям покрытия.

В системе SkyBridge используются скоростные средства коммуникаций, соответствующие существующим наземным широкополосным сетям. Малое время распространения сигналов в низкоорбитальной системе (около 20 миллисекунд) облегчает адаптацию существующих приложений или протоколов. Связь между конечными пользователями и системой асимметрична. Скорость передачи данных к пользователю

составляет до 60 Мбит/с, на возвратном канале от пользователя - до 2 Мбит/с. Асимметричность каналов оптимизирована для Интернет-коммуникаций, которые характеризуются произвольными пакетами асимметричной передачи данных.

Система SkyBridge будет использовать спектр частоты в полосе Ku-диапазона при полной защите существующих "геостационарных" и земных пользователей с повторным использованием частот.

SkyBridge поставит различные интерактивные широкополосные услуги для бизнеса и других потребителей, в том числе быстродействующий доступ к Интернету и интерактивным службам, доступ к корпоративным сетям для телекоммуникаций и удаленной работы, соединение с локальными и территориальными вычислительными сетями, услуги телеобразования, телеобучения и телемедицины, развлечения и культурные услуги типа "видео по требованию". Кроме того, будут предоставляться услуги по запросу: расширенные и узкополосные услуги для речевой связи и передачи данных, для видеоконференцсвязи.

Система персональной спутниковой радиосвязи TELEDESIC

Спутниковая система Teledesic предложена к реализации г-ном Крейгом Маккау, председателем компании McCaw Cellular, и Биллом Гейтсом, президентом компании Microsoft. Партнером глобального проекта Teledesic и генеральным подрядчиком в разработке широкополосного "Небесного Интернета" ("Internet-in-the-Sky") стал Boeing. Boeing должен разработать и начать запуски спутников Teledesic-сети.

Спутниковая система Teledesic должна состоять из 288 низкоорбитальных спутников, с разделением на 12 орбитальных плоскостей по 24 спутника. Спутники Teledesic будут запущены на орбиту с высотой до 1400 км. Проектируемая группировка Teledesic должна поддерживать сетевые требования к качеству, пропускной способности и целостности. В соответствии со всемирным распределением частот для фиксированной спутниковой службы, которая может предоставить существенную полосу пропускания для обеспечения высокого качества в быстродействующих беспроводных каналах и удовлетворения требований, - это полоса Ka-диапазона. Низкая высота орбиты используется для обеспечения малой задержки "из конца в конец" и надежности коммуникационных каналов с использованием небольших антенн и терминалов малой мощности. Комбинация низкой высоты спутника с высокой плотностью узконаправленных лучей, покрывающих "пятнами" небольшие территории, и большое количество спутников обеспечат глобальное покрытие.

Использование совокупности нескольких сотен низкоорбитальных спутников Teledesic должно создать доступную во всем мире сеть, подобную оптоволоконным каналам, для предоставления услуг передачи данных, доступа к широкополосной сети Интернет, видеоконференцсвязи, высококачественного голоса и т.д. Teledesic предложит "полосу по требованию", позволяющую пользователям корректировать полосу пропускания канала для соответствующего согласования по объемам передачи и приложениям.

Сеть Teledesic предложит большую емкость и услуги "полосы по требованию" через стандартные и подвижные терминалы пользователя. Ширина полосы канала будет назначаться динамически и несимметрично, со скоростью для каналов "вверх" от 16 Кбит/с до 2 Мбит/с, и на канале "вниз" - до 28 Мбит/с.

Teledesic также будет обеспечивать, хотя и с меньшим числом, каналы с высоким трафиком (от 155 Мбит/с до 1.2 Гбит/с) для соединений со шлюзом или для Giga-терминалов и пользователей со специальными потребностями.

В сети Teledesic будет использоваться технология быстрой пакетной коммутации, основанной на технологии асинхронного режима передачи АТМ. Вся связь будет тождественно обрабатываться внутри сети как потоки коротких пакетов фиксированной длины, которые могут нести в кодированной цифровой форме голос или данные.

Преобразование формата пакета происходит в терминалах. Технология быстрой пакетной коммутации идеально подходит для динамического характера низкоорбитальных систем. Каждый спутник в группировке - узел быстрой пакетной коммутации, который может поддерживать межспутниковые коммуникации со смежными спутниками.

В сети используется комбинация методов множественного (коллективного) доступа с гарантированной эффективностью использования спектра. Все коммуникации будут происходить между спутником и терминалами в течение назначенного слота времени (TDMA). На канале "вверх" внутри каждого слота времени терминалы используют множественный доступ с разделением частоты (FDMA), а на канале "вниз" - множественный доступ с асинхронным разделением времени (ATDMA).

Teledesic будет функционировать в Ka-полосе: для сервисных связей - сегменты полосы 28.6-29.1 ГГц (вверх) и 18.8-19.3 ГГц (вниз); для Giga-каналов шлюзовых станций и терминалов - сегменты полосы 27.6-28.4 ГГц (вверх) и 17.8-18.6 ГГц (вниз). Каждый спутник Teledesic также использует межспутниковые каналы связи с восемью другими спутниками и с подобными и смежными системами. Для межспутниковых коммуникаций (ISL) используются полосы: 59.5-60.5 ГГц и 62.5-63.5 ГГц. Начало эксплуатации Teledesic планируется на 2002 год.

Мобильная спутниковая связь Иридиум.

Концепцию системы Iridium предложили инженеры компании Motorola - Рэй Леопольд, Кен Петерсон и Бэри Бертайгер. Они предвидели успех группировки из низкоорбитальных спутников. Исследования и разработки начались в 1987 году. Начав оказание услуг с 1-го ноября 1998, компания Iridium LLC (основанная в 1991 и инвестировавшая в проект около 7 миллиардов долларов) объявила 17 марта 2000 года о прекращении обслуживания абонентов. Однако 22 ноября 2000 года вновь образованная компания Iridium Satellite LLC, подписав контракт на обслуживание с Министерством Обороны США, приступила к переводу активов и передаче управления группировкой компании Boeing. С 12 декабря 2000 года обслуживание абонентов Пентагона и Правительства США возобновлено. Коммерческая эксплуатация системы возобновилась 28 марта 2001 года.

Система Иридиум нашла поддержку инвесторов в лице 19-ти стратегических партнеров со всего мира, включая: группу компаний "AIG", корпорацию "Iridium Africa", корпорацию "Iridium SudAmerica", корпорацию "Iridium Middle East", ГКНПЦ им. Хруничева, корпорацию "Lockheed Martin", "Iridium Canada, Inc.", "Iridium China (Hong Kong) Ltd.", "Iridium India Telecom Limited", "Iridium Italia S.p.A.", компанию "Raytheon", "SK Telecom", холдинг "South Pacific Iridium", "Sprint Iridium, Inc.", "Thai Satellite Telecommunications Co., Ltd.", "Motorola, Inc.", "Nippon Iridium (Bermuda) Limited", "Vebacom Holdings, Inc.", "Pacific Asia Communications Ltd."

Система Iridium - это беспроводная телефонная сеть мобильной персональной связи, работающая на низкоорбитальных спутниках и разработанная для предоставления набора стандартных телефонных услуг - голосовая связь, передача факсимильных сообщений и компьютерных данных. Она сделала революционный переворот в области связи для профессионалов бизнеса, путешественников, жителей, проживающих в районах с неразвитой или отсутствующей связью, служб спасения, а также других лиц, которым необходима многофункциональная и удобная спутниковая связь в виде спутникового телефона-трубки с единым глобальным номером. В отличие от наземных сетей связи, спутниковая система отслеживает местоположение телефона, обеспечивая, таким образом, прохождение сигнала до абонента вне зависимости от его местонахождения. Иными словами, вы можете позвонить абоненту системы Iridium, не зная, где именно он находится. Телефоны Iridium обеспечивают высококачественное соединение для голосовой связи и предполагают интерфейсное соединение с ноутбуками, "палмтопами",

электронными органайзерами и другим телекоммуникационным оборудованием. Относительно короткое расстояние до спутника уменьшило задержку сигнала и улучшило качество разговора.



Рис. 6.11. Система Iridium.

Космический сегмент Иридиум состоит из 66-ти низкоорбитальных и 6 запасных спутников, расположенных в 6-ти орбитальных плоскостях с углом наклона 86,4 градуса. В сети реализован уникальный механизм межспутниковых связей, который используется для передачи сигнала с одного спутника на другой без необходимости ретрансляции этого сигнала на Землю. Межспутниковые связи Иридиум теоретически позволяют этой сети функционировать при наличии всего лишь одной станции сопряжения, на которую будут поступать все абонентские звонки. Каждый спутник покрывает зону шириной в 4000 км. В связи с высокой скоростью пролета спутников (приблизительно 1 оборот вокруг Земли в час), сигнал абонента Iridium передается от спутника к спутнику, не вызывая прерывания. Наземные станции сопряжения связаны одновременно как минимум с двумя спутниками из группировки.

Общие характеристики:

- Вес спутника - 700 кг (1500 фунтов).
- Зональные лучи - 48 на каждом спутнике.
- Мощность канала - 16 ДБ (средняя).
- Срок службы - 5-8 лет.

Используемые частоты:

- телефон Iridium - спутник 1616-1626,5 МГц
- спутник - телефон Iridium 1616-1626,5 МГц
- спутник - спутник 23,18-23,38 ГГц
- спутник - наземная станция сопряжения 19,4-19,6 ГГц
- наземная станция сопряжения - спутник 29,1-29,3 ГГц



Рис. 6.12. Спутник Iridium.

Все спутники были запущены ракетами "Delta II" компании Boeing (5 спутников Iridium на запуск), "Протон" ГКНПЦ им. Хруничева (семь спутников Iridium за запуск) и "Лонг Марк 2с" компании China Great Wall (два спутника Iridium за запуск).

Технические данные о космическом сегменте Иридиум:

- количество спутников на орбите: 66 основных и 6 резервных
- количество орбитальных плоскостей: 6 (11 спутников в каждой плоскости)
- высота орбиты: 780 км
- наклонение орбитальной плоскости: 86,4 град.
- период обращения спутника: 100 мин. 28 сек.
- масса спутника: 689 кг.
- количество лучей, формируемых одним спутником: 48
- диаметр луча: около 50 км
- срок службы спутника: 7-9 лет

Запуск спутников Иридиум осуществлялся ракетносителями Delta II, Long March 2С и Протон.

Наземный сегмент Иридиум представлен сетевой координирующей станцией и станциями сопряжения. Координирующая станция управляет всей сетью Иридиум и осуществляет ее непрерывный мониторинг. Станции сопряжения служат шлюзами между спутниковым сегментом и наземными телефонными сетями и сетями передачи данных. Через станции сопряжения проходят все звонки со спутниковых телефонов Иридиум на наземные сети общего пользования. Помимо этого, на станции сопряжения присутствует и поддерживается база данных абонентов Иридиум, на этой же станции формируется биллинговая информация для выставления счетов абонентам за услуги спутниковой связи. В качестве абонентского коммутатора на станциях сопряжения системы Иридиум используется Siemens GSM-D900.

Частоты, используемые для связи в сети Иридиум:

- спутник Иридиум - спутниковый телефон или спутниковый пейджер: 1616 - 1626,5 МГц
- межспутниковые связи: 23,18 - 23,38 ГГц
- наземная станция - спутники Иридиум: 29,1 - 29,3 ГГц
- спутники Иридиум - наземная станция: 19,4 - 19,6 ГГц

Пользовательский сегмент Иридиум - это спутниковые телефоны и спутниковые пейджеры, посредством которых абонент получает доступ в сеть Иридиум и пользуется ее услугами. Спутниковые телефоны Иридиум внешне выглядят как "трубки" и работают в двух режимах - спутниковом и сотовом GSM. Спутниковые пейджеры способны принимать сообщения, находясь в любой точке планеты.

Таблица 6.8. Плюсы и минусы системы Iridium

Система спутниковой связи Иридиум

- + Надежная и проверенная временем (существует уже более 25 лет, является официальной системой обеспечения безопасности мореплавания)
- + Работает на всей территории земного шара, за исключением полярных областей
- + Достаточно конфиденциальна
- + Простая в использовании, есть подробные инструкции на русском языке
- + Входящие звонки бесплатно, исходящие - \$2.80 независимо от положения телефона и вызываемого абонента
- + Есть онлайн-биллинговая система, позволяющая из любой точки планеты посмотреть через Интернет состояние своего счета, подробную статистику телефонных звонков, распечатать ее
- + Большое количество дополнительных аксессуаров, включая автомобильные комплекты, факсы и другое
- Относительно высокая стоимость телефонов (от \$3000)
- Относительно высокая стоимость исходящих звонков (\$2.80)
- Относительно большие размеры и вес терминалов (52 x 270 X 200 мм, 2.2 кг и 57 x 260 X 260 мм, 1.4 кг)
- Необходимость получения разрешения на использование телефона на территории каждой конкретной страны (компания ТЕССКОМ продает телефоны с разрешением на использование на территории России, получение же разрешения на использование телефона на территории других стран может занять некоторое время из-за необходимости оформления большого количества документов, уплаты пошлин и т.д.)

Система персональной спутниковой радиосвязи GLOBALSTAR

Целевая задача разработки проекта Globalstar была определена в начале 90-х годов компаниями Loral Space & Communications (Нью-Йорк) и Qualcomm Inc. (Сан-Диего, шт. Калифорния). Разработку проекта осуществляет компания Globalstar, Сан-Хосе, шт. Калифорния. Для работ по проекту Globalstar действует международный консорциум, взаимодействующий с операторами более чем в 100 странах.

Стратегическими инвесторами и партнерами Globalstar являются более 12 компаний, в том числе Alcatel Espace (Франция), Finmecanica (Италия), DASA (Deutsche Aerospace AG/Daimler-Benz AG, Германия).

Идеология построения системы Globalstar состоит в использовании методов сотовой связи при выносе в космическое пространство ретрансляторов базовых станций. При разработке этой системы в основном использовался опыт создания сотовых систем связи с кодовым разделением каналов (CDMA) фирмы Qualcomm.

Принцип организации связи в системе "Глобалстар" заключается в работе абонентов системы через ИСЗ, которые посредством фидерных радиолиний соединены с наземными станциями сопряжения осуществляющими все соединения абонентов. Организация магистральных каналов связи между станциями сопряжения осуществляется наземными каналами связи. В состав системы также входят центр управления наземной сетью и центр управления и контроля орбитальной группировки. Предполагаемое распределение наземных станций сопряжения показано на рис.6.14.

Определение координат абонентов производится на базовой станции. В том случае, когда 2 ИСЗ пространственно доступны для абонента и станции сопряжения может использоваться метод определения основанный на измерении разности времен прихода сигналов абонента на станцию сопряжения. Если абоненту виден только один ИСЗ то

станция сопряжения может определять его координаты запросным методом, при котором измеряется и накапливается информация о дальности от абонента до КА.

В дополнение к перечисленным методам определения координат отрабатывается и готовится к внедрению методика точного измерения с использованием станций дифференциальных поправок

В диапазоне широт $27^{\circ} \div 51^{\circ}$ где достигается гарантированное двукратное покрытие возможно определение координат наземных подвижных абонентов в режиме реального времени по двум ИСЗ.

Максимум наблюдаемости созвездий ИСЗ высокой кратности достигается на широте 35° . Таким образом, потенциально наиболее благоприятные места для функционирования системы находятся в широтном поясе, находящемся на территории США, Китая, стран Азии и Африки. Именно в этих областях наиболее благоприятные условия для формирования динамических планов управления связью для БС. Для России можно оптимальными для работы системы будут области южнее 51° .

Учитывая особенности организации связи в системе “Глобалстар” можно говорить о том, что каждая станция сопряжения будет контролировать абонентов вокруг нее находящихся хотя и на значительной, но вполне определенной территории. Так на Рис показаны зоны, контролируемые станциями в г. Павлово-Посаде, г. Новосибирске, г. Хабаровске. Черным цветом выделена область, в которой с вероятностью 100% гарантируется одновременная радиовидимость ИСЗ “Глобалстар” под углом места не менее 10° абонентами и станцией сопряжения. Зеленым цветом показаны области пересечения зон контролируемых этими СС. Для станции сопряжения расположенной в г. Павлово-Посаде показаны зоны по нескольким уровням вероятности реализации 90%, 50%, 0.5%. Зоны на Рис вычислены без учета действующих на СС алгоритмов отбора рабочих ИСЗ, которые сопровождаются этими СС и которые участвуют в организации связи. Реальные зоны будут иметь несколько меньший размер. Так как зоны обслуживания простираются далеко за пределы России, возникающие коллизии с абонентами СС других стран решаются алгоритмом организации связи и управления, действующим с использованием измеряемых СС координат абонентов.

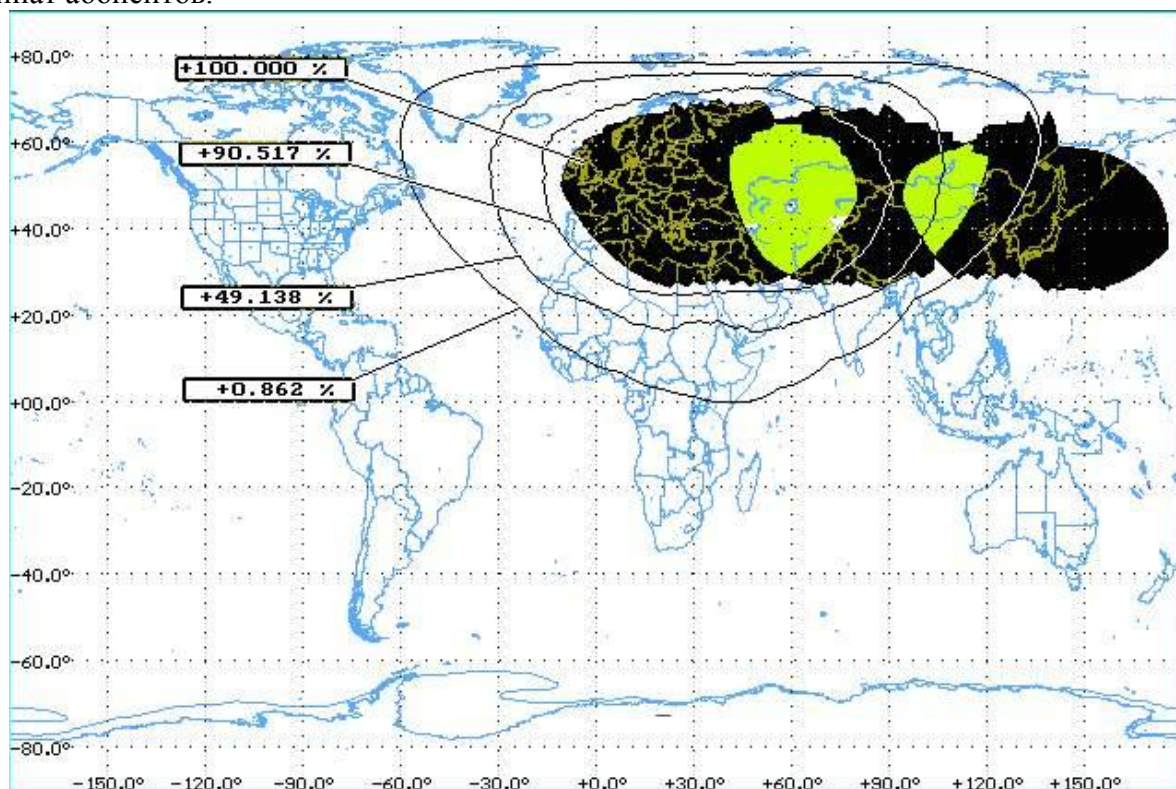


Рис. 6.13. Зоны, контролируемые станциями в г. Павлово-Посаде, г. Новосибирске, г. Хабаровске.

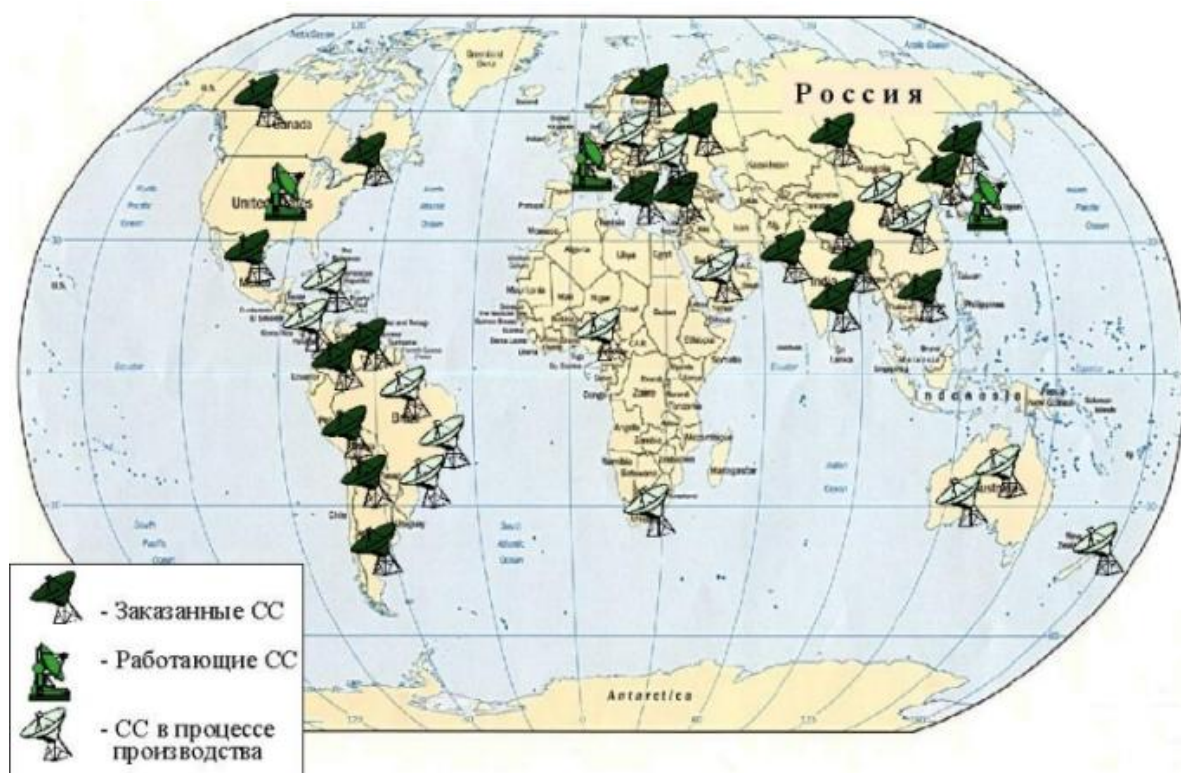


Рис. 6.14. Размещение базовых станций “Глобалстар” по поверхности Земли

ИСЗ “Глобалстар” не осуществляют обработку сигналов на борту. Они функционируют в диапазоне абонентских радиолиний 1610-1626,5 МГц на линии Земля - ИСЗ и 2483,5-2500 МГц на линии ИСЗ-Земля. В диапазоне фидерных радиолиний используются частоты 5091-5250 МГц на линии Земля – ИСЗ и 6875-7055 МГц на линии ИСЗ-Земля. Общий вид ИСЗ “Глобалстар” показан на Рис. Масса космического аппарата 450 КГ. Спутники выполнены, как гравитационно нейтральные объекты, стабилизация которых осуществляется исполнительными органами использующими данные о геомагнитном поле.



Рис. 6.15. Спутник Глобалстар.

Система Globalstar предназначена для передачи речи и данных, организации пейджинговой связи, определения местонахождения подвижных объектов, передачи коротких сообщений и экстренных вызовов.

Система Globalstar предоставляет абонентам следующие виды услуг:

- речевая связь. Продолжительность переговоров - 3 минуты (без прерывания связи) - будет обеспечиваться с вероятностью 99%. Время установления связи равно времени установления связи между абонентами наземной сотовой связи и не превышает 2 секунд;

- передача данных. Скорость передачи - от 2,4 до 9,6 кбит/с с возможностью агрегирования каналов. Вероятность ошибки в канале передачи данных - не более 10⁻⁶. Предусматривается предоставление пользователям дополнительных услуг, таких как телефакс, передача факсимильных сообщений;

- определение местоположения. Производится с точностью, которая зависит от нескольких факторов: количества одновременно "видимых" КА, точности определения координат КА, взаимного расположения пользователя, КА и станции сопряжения (СС), стабильности абонентского эталона частоты.

Система спутниковой связи Globalstar структурно разделена на три основных сегмента - космический, наземный и пользовательский.

Космический сегмент

Орбитальная группировка системы Globalstar состоит из 48 основных и 8 резервных КА. Спутники расположены в 8 орбитальных плоскостях по 6 КА в каждой. КА выводятся на круговые орбиты высотой 1414 км с наклоном к экватору 52°. Период обращения на этих орбитах равен 114 минутам. Фазовый сдвиг между КА в соседних орбитальных плоскостях составляет 7,5°. Такая структура космического сегмента обеспечивает одновременное наблюдение на средних широтах – основном регионе обслуживания – не менее 2 КА. По этому показателю система Globalstar существенно отличается от конкурирующей системы Iridium, где структура космического сегмента основана на односпутниковом покрытии территории.

Наземный сегмент управления

В состав наземной сети управления Globalstar входят две основные подсистемы – центр управления наземной сетью GOCC (Ground Operations Control Center) и центр управления контроля орбитальной группировкой SOCC (Satellite Operations Control Center). Обе подсистемы связаны между собой с помощью сети Globalstar Data Network, к которой подключены наземные станции сопряжения. Центр управления и контроля орбитальной группировки SOCC совместно с командно-телеметрическими станциями (TT&C station) производит контроль орбит, обработку телеметрической информации и формирование команд. Кроме того, SOCC отслеживает текущее состояние КА и информирует центр управления сетью о доступных КА, их ресурсах и эфемеридах.

В задачи центра управления сетью GOCC входит планирование трафика, выделение и закрепление сетевых ресурсов, слежение за функционированием системы. Центр SOCC не имеет собственного радиотехнического оборудования. По наземной линии связи он постоянно подключен к одной из СС. Эта станция сопряжения, в отличие от остальных, должна быть доукомплектована аппаратурой для приема телеметрии с борта КА и передачи команд управления. Центр управления SOCC размещен в Сан-Хосе, шт. Калифорния, резервный центр управления связью – в Эльдorado (шт. Калифорния).

Космический аппарат

Спутники в системе Globalstar выполнены без обработки информации (bent-pipe) и межспутниковых линий связи. Бортовой комплекс L/S диапазона содержит приемные и передающие активные фазированные антенные решетки (АФАР). Всего формируется 16

лучей. Усиление и форма лучей подобраны так, чтобы у поверхности Земли формировалась многосотовая зона покрытия. Коэффициент усиления в периферийных лучах выше, чем в первом, что необходимо для создания равномерной плотности потока мощности. Общая пропускная способность ретранслятора на один КА – 2400 эквивалентных телефонных каналов.

Масса каждого КА – 450 кг, максимальная мощность солнечных батарей – 1100 Вт. Планируемый срок активного существования – 7,5 лет. На спутниках устанавливается трехосная система стабилизации. Точность удержания аппарата на орбитальной позиции составляет не хуже $\pm 1^\circ$ вдоль орбиты и $\pm 1^\circ$ в сторону от орбиты. Основные компании-операторы, обеспечивающие запуск КА Globalstar на этапах формирования орбитальной группировки и последующей замены КА в ходе эксплуатации системы: Boeing (США), НПО «Южное» (Украина), Starsem (Франция).

Станции сопряжения и абонентские терминалы

Станции сопряжения

Станции сопряжения в системе Globalstar играют важную роль. Через них осуществляются все соединения с абонентами. Для глобального покрытия основных регионов земной поверхности с учетом национальных границ и минимизации наземных сетей в России. Такая технология позволит обеспечить большую надежность связи, чем при использовании для маршрутизации межспутниковых каналов связи. Региональный принцип построения системы привлекает администрации разных стран, позволяя им сделать Globalstar частью своей национальной сети. Учитывая, что основную часть трафика в каждом регионе обычно составляют местные вызовы (более 80%), это позволит местным телекоммуникационным компаниям получать доход от эксплуатации системы.

Станция сопряжения предназначена для решения следующих задач: организация информационного обмена в обслуживаемом регионе; распределение сетевых ресурсов; подключение абонентов Globalstar к сетям общего пользования. Все вызовы (местные и международные) обрабатываются и коммутируются в СС, причем время установления соединения не будет превышать 5 секунд, а максимальная задержка сигнала – 150 мс. В состав СС входят 4 идентичных приемопередающих комплекта, оснащенных следящими параболическими антеннами, подсистемы формирования и обработки ШПС-сигналов, интерфейсного оборудования и автоматизированных рабочих мест операторов, позволяющих производить учет графика и вычисление местоположения абонента по навигационным данным.

Абонентские терминалы

В системе Globalstar выпускаются три основных типа терминалов – портативные, мобильные и стационарные.

Стационарные терминалы предназначены для работы только в системе Globalstar. Портативные и мобильные могут функционировать в сотовой сети одного из стандартов GSM, CDMA, AMPS. Мощность мобильного АТ не превышает 2 Вт, портативного – 0,6 Вт.

Компании Qualcomm, Telit, Ericsson выпускают портативные и мобильные терминалы трех типов – трехрежимные (Globalstar/AMPS/ CDMA), двухрежимные (Globalstar/ GSM) и однорежимные (Globalstar).

В состав терминалов входит устройство автоматической регулировки мощности передатчика, которое позволяет снизить мощность передатчика до 2 мВт. Регулировка уровня мощности осуществляется автономно в каждом CDMA-канале. Команда на

изменение значения мощности передается со станции сопряжения. Аппаратура СС измеряет уровень принимаемого сигнала от каждого терминала индивидуально, сравнивает его с пороговым и передает команду абоненту на увеличение или уменьшение мощности. Эта процедура позволяет выровнять сигналы на входе ретранслятора, снизить уровень взаимных помех и максимизировать пропускную способность.

Пропускная способность

Пропускная способность КА, определяемая как максимальное число эквивалентных каналов по 2,4 кбит/с, в зоне, создаваемой 16-лучевой антенной, по оценке разработчиков системы Globalstar составляет 2400 каналов. Реальная пропускная способность будет ниже, вследствие работы на более высокой скорости (4,8 кбит/с), а также возможности использования одного канала в смежном КА при ведении связи с одним наземным абонентом.

Стоимость услуг и сроки развертывания

На территории России уже построены 3 станции сопряжения (в Москве, Новосибирске Хабаровске), которые обеспечивают охват 98% территории России с гарантированным качеством услуг южнее 70° с.ш. Все станции российского сегмента объединены в единую наземную сеть, связанную с центром управления Globalstar. Национальным оператором в России является ЗАО «ГлобалТел», которое основано ОАО «Ростелеком» и компанией Globalstar. Коммерческая деятельность на территории РФ по предоставлению услуг связи населению началась в конце 2000 г., планируемый рынок Globalstar России – 7,5% мирового.

Общая стоимость проекта Globalstar составляет около 2,6 млрд. долл., хотя реально эта сумма выше, так как в нее не включены затраты на строительство 150–210 станций сопряжения. Предполагаемые эксплуатационные расходы в год достигнут 227 млн. долл.

Ориентировочная стоимость основных элементов системы Globalstar: КА – 14 млн. долл., станция сопряжения – 6,5 млн. долл., радиотелефонный терминал – 700–1000 долл., стационарный терминал – не более 2,5 тыс. долл.

В среднем тариф за телефонный разговор составит 1 долл. в минуту.

Таблица 6.9. Плюсы и минусы системы Глобалстар

Система спутниковой связи Глобалстар

- + Очень портативные и легкие телефоны, размером и весом немного больше сотового телефона
- + Простая в использовании, есть подробные инструкции на русском языке
- + Автоматическое переключение между спутниковой и сотовой связью (если телефон определил, что он находится в зоне покрытия оператора сотовой связи, с которым у Глобалстар есть договор, телефон автоматически переключается на сотовую связь, а в ее отсутствие - использует спутниковый канал)
- + Относительно невысокая стоимость телефонов (от \$699)
- + Относительно недорогой трафик (от \$1.39 при использовании спутникового канала, еще дешевле - при переключении на сотовый канал)
- + Большое количество дополнительных аксессуаров, включая автомобильные комплекты, факсы и т.д.
- Дополнительное разрешение на использование не требуется (однако перед ввозом такого телефона в каждую конкретную страну желательно ознакомиться с ее законодательством - в некоторых странах использование телефонов запрещено или ограничено)

7. БЕСПРОВОДНЫЕ ЛОКАЛЬНЫЕ СЕТИ НА ОСНОВЕ СТАНДАРТОВ IEEE 802.11

Беспроводные локальные компьютерные сети, или сети Wi-Fi, или иначе сети стандарта IEEE 802.11 приобретают всё большую популярность и сегодня можно с уверенностью сказать: «Технология Wi-Fi меняет мир». Эти изменения касаются того, как мы работаем, играем и взаимодействуем друг с другом.

В течение нескольких лет беспроводные сети проходили процесс стандартизации, цена становилась доступнее, улучшалась технология производства аппаратуры.

Сегодня БС позволяют предоставить подключение пользователей там, где затруднено кабельное подключение или необходима полная мобильность. При этом беспроводные сети без проблем взаимодействуют с проводными сетями.

А если учитывать, что потребность в беспроводном доступе к локальным сетям, к сети Интернет растёт по мере увеличения числа мобильных устройств, таких как ноутбуки и карманные компьютеры, то можно сказать что мы наблюдаем настоящий взрыв технологий беспроводных локальных сетей.

Область применения беспроводных локальных сетей безгранична, они применяются везде, где существует сложность прокладки кабеля и требуется мобильность пользователей. Это малый офис и большое предприятие, выставки презентации и конференции, гостиницы и аэропорты, больницы, складские и торговые организации и многое другое.

Беспроводная локальная сеть зачастую является единственным экономически оправданным решением - когда кабельная система отсутствует или низкого качества, что наблюдается в нашей стране.

Стандарт IEEE 802.11, разработка которого была завершена в 1997г., является базовым стандартом и определяет протоколы, необходимы для организации беспроводных локальных сетей (WLAN). Основные из них – протокол управления доступом к среде MAC (Medium Access Control – нижний подуровень канального уровня) и протокол РНУ передачи сигналов в физической среде. В качестве последней допускается использование радиоволн и инфракрасного излучения.



Рис. 7.1. Уровни модели ISO/OSI и их соответствие стандарту 802.11

Стандарт IEEE 802.11 играет для радиосетей такую же интегрирующую роль, как стандарт IEEE 802.3 для сетей Ethernet и IEEE 802.5 для Token Ring.

Стандартом IEEE 802.11 определен единственный подуровень MAC, взаимодействующий с тремя типами протоколов физического уровня, соответствующих различным технологиям передачи сигналов - по радиоканалам в диапазоне 2,4 ГГц с широкополосной модуляцией с прямым расширением спектра (DSSS) и перескоком частоты (FHSS), а также с помощью инфракрасного излучения. Спецификациями стандарта предусмотрены два значения скорости передачи данных - 1 и 2 Мбит/с.

По сравнению с проводными ЛС Ethernet возможности подуровня MAC расширены за счет включения в него ряда функций, обычно выполняемых протоколами более высокого уровня, в частности, процедур фрагментации и ретрансляции пакетов. Это вызвано стремлением повысить эффективную пропускную способность системы благодаря снижению накладных расходов на повторную передачу пакетов.

В качестве основного метода доступа к среде стандартом IEEE 802.11 определен механизм CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance - множественный доступ с обнаружением несущей и предотвращением коллизий).

На сегодняшний день существует множество модификаций стандарта IEEE 802.11, рассмотрим наиболее популярные из них.

Стандарт IEEE 802.11a

Является наиболее "широкополосным" из семейства стандартов IEEE 802.11, предусматривая скорость передачи данных до 54 Мбит/с (редакцией стандарта, утвержденной в 1999 г., определены три обязательных скорости - 6, 12 и 24 Мбит/с и пять необязательных - 9, 18, 36, 48 и 54 Мбит/с).

В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями IEEE 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM). Наиболее существенное различие между этим методом и радиотехнологиями DSSS и FHSS заключается в том, что OFDM предполагает параллельную передачу полезного сигнала одновременно по нескольким частотам диапазона, в то время как технологии расширения спектра передают сигналы последовательно. В результате повышается пропускная способность канала и качество сигнала.

К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а так же меньший радиус действия (оборудование для 2,4 ГГц может работать на расстоянии до 300м, а для 5ГГц - около 100м).

Стандарт IEEE 802.11b

Благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных ЛС Ethernet, а также ориентации на "освоенный" диапазон 2,4 ГГц, этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

В окончательной редакции стандарт IEEE 802.11b, известный также как Wi-Fi (wireless fidelity), был принят в 1999г. В качестве базовой радиотехнологии в нем используется метод DSSS с 8-разрядными последовательностями Уолша.

Поскольку оборудование, работающее на максимальной скорости 11 Мбит/с имеет меньший радиус действия, чем на более низких скоростях, то стандартом 802.11b предусмотрено автоматическое понижение скорости при ухудшении качества сигнала.

Как и в случае базового стандарта IEEE 802.11, четкие механизмы роуминга спецификациями IEEE 802.11b не определены.

Стандарт IEEE 802.11g

Данную модификацию стандарта можно считать панацеей от всех бед, т.к. здесь сочетаются скорость IEEE 802.11a (54 Мбит/с) и совместимость с сетями IEEE 802.11b. Конечно же, максимальная скорость в 54 Мбит/с достигается только при работе с подобными устройствами. Если же беспроводная сеть является смешанной, то есть в ней присутствуют и устройства совместимых стандартов (IEEE 802.11b или IEEE 802.11b+), то максимальная скорость обмена данными будет ограничена пиковой скоростью обмена старых устройств.

Скоростные свойства стандартов

Подавляющее число беспроводных локальных сетей (Wireless Local Area Network, WLAN) работает сегодня в полосе частот 2,4 ГГц в соответствии со стандартом передачи данных IEEE 802.11b. Стандарт IEEE 802.11b представляет собой первое расширение стандарта IEEE 802.11 с повышенной скоростью передачи данных см. Таблицу 7.1. Для него новым видом модуляции стала дополняющая манипуляция кодом (Code Complementary Keying, CCK).

Таблица 7.1. Скорость передачи данных в стандарте IEEE 802.11b

Стандарт передачи	Скорость передачи данных	Вид модуляции
IEEE 802.11	1 Мбит/с	DBPSK
IEEE 802.11	2 Мбит/с	DQPSK
IEEE 802.11b	5,5 Мбит/с	ССК
IEEE 802.11b	11 Мбит/с	ССК

Повышением скорости передачи данных в полосе частот 2,4 ГГц (по программе «Дальнейшее повышение скорости передачи в диапазоне 2,4 ГГц») занималась рабочая группа IEEE 802.11g. Ее целью являлось внедрение новых видов модуляции, например ортогонального частотного мультиплексирования (Orthogonal Frequency Division Multiplexing, OFDM), и тем самым повышение скорости передачи в полосе частот 2,4 ГГц, максимальное значение которой на данный момент составляет 54 Мбит/с.

Проект стандарта в качестве обязательных методов модуляции определяет ССК и OFDM. Таким образом, это расширение остается обратно совместимым с существующими приложениями стандарта IEEE 802.11b. Дополнительно, как опциональные методы передачи данных, были введены кодировка с двоичной сверткой пакетов (Packet Binary Convolution Coding, PBCC) и ССК-OFDM (см. Таблицу 7.2).

Таблица 7.2. Скорость передачи данных в стандарте IEEE 802.11g

Стандарт передачи	Скорость передачи данных	Вид модуляции
IEEE 802.11g (обязательный)	5,5/11 Мбит/с	ССК
IEEE 802.11g (обязательный)	до 54 Мбит/с	OFDM
IEEE 802.11g (опциональный)	до 33 Мбит/с	PBCC
IEEE 802.11g (опциональный)	до 54 Мбит/с	ССК-OFDM

Радиус действия в полосе 2,4 ГГц

Практическим правилом передачи данных в беспроводных локальных сетях является обратно пропорциональная зависимость между скоростью передачи данных и радиусом действия: чем больше скорость, тем меньше радиус. С точки зрения техники передачи это объясняется тем, что при повышении скорости передачи чувствительность радиоприёма снижается соответствующим образом. В Таблице 7.3 приведена чувствительность приемников наиболее распространенных систем IEEE 802.11b.

Таблица 7.3. Чувствительность приемника распространенных систем стандарта IEEE 802.11b при различных скоростях передачи данных

Скорость передачи данных	Чувствительность приемника
11 Мбит/с	-82 дБм
5,5 Мбит/с	-87 дБм
2 Мбит/с	-91 дБм
1 Мбит/с	-94 дБм

На каком расстоянии может находиться мобильный абонент при такой чувствительности, определено в Таблице 7.4.

Таблица 7.4. Средний радиус действия стандартных точек доступа IEEE 802.11b

Среда	Радиус действия
Открытая местность, зона прямой видимости	около 300 м
Открытая местность с препятствиями	до 100 м
Большой офис	до 40 м
Жилой дом	до 20 м

Указанные радиусы действия представляют собой средние значения для стандартных точек доступа IEEE 802.11b. В зависимости от местных условий (много бетона или толстые стены) действительные значения радиуса действия могут оказаться существенно меньше.

Таблица 7.5. Чувствительность приемника радиокарты IEEE 802.11g при различных скоростях передачи данных.

Скорость передачи данных	Чувствительность приемника
54 Мбит/с	-73 дБм
48 Мбит/с	-76 дБм
36 Мбит/с	-77 дБм
24 Мбит/с	-78 дБм
18 Мбит/с	-80 дБм
12 Мбит/с	-82 дБм
9 Мбит/с	-85 дБм
6 Мбит/с	-86 дБм

В Таблице 7.5 представлены данные о чувствительности приемников радиокарт стандарта IEEE 802.11g при различных скоростях передачи данных. В случае стандартов IEEE 802.11b и IEEE 802.11g при сравнимых скоростях передачи данных в 11 и 12 Мбит/с соответственно чувствительность приемников равна 82 дБм (децибел милливатт). Более высокая скорость передачи в стандарте IEEE 802.11g приводит к заметному сокращению чувствительности приемника, а вместе с ней и ожидаемого радиуса действия.



Рис. 7.2. Радиус действия в частотном диапазоне 2,4 ГГц (802.11g) при модуляции OFDM: скорость передачи данных 54 Мбит/с достигается лишь на расстоянии до 14 м

На Рисунке 7.2 такой переход представлен схематически. Скорость передачи в 54 Мбит/с достигается в открытой офисной среде лишь на расстоянии до 14 м. При наличии какого-либо препятствия (к примеру, перегородки), которое должно быть преодолено, скорость снижается. Чувствительность при 11 Мбит/с (в случае модуляции ССК/802.11b) и чувствительность при 12 Мбит/с (в случае модуляции OFDM/802.11g), как правило, совпадают, поэтому такая скорость передачи может поддерживаться на расстоянии до 40 м от точки доступа.

Архитектура беспроводных сетей

IEEE 802.11 определяет два типа оборудования – клиент, который обычно представляет собой компьютер, укомплектованный беспроводной сетевой интерфейсной картой (Network Interface Card, NIC), и точку доступа (Access point, AP), которая выполняет роль моста между беспроводной и проводной сетями. Точка доступа обычно содержит в себе приёмопередатчик, интерфейс проводной сети (IEEE 802.3), а также программное обеспечение, занимающееся обработкой данных. В качестве беспроводной станции может выступать ISA, PCI или PC Card сетевая карта в стандарте 802.11, либо встроенные решения, например, телефонная гарнитура IEEE 802.11.

Стандарт IEEE 802.11 определяет два режима работы сети – режим "Ad-hoc" (или каждый с каждым) и *клиент/сервер* (или режим инфраструктуры – infrastructure mode). В режиме клиент/сервер (рис. 7.3.) беспроводная сеть состоит из как минимум одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных оконечных станций. Такая конфигурация носит название базового набора служб (Basic Service Set, BSS). Два или более BSS, образующих единую подсеть, формируют расширенный набор служб (Extended Service Set, ESS). Так как большинству беспроводных станций требуется получать доступ к файловым серверам, принтерам, Интернет, доступным в проводной локальной сети, они будут работать в режиме клиент/сервер.

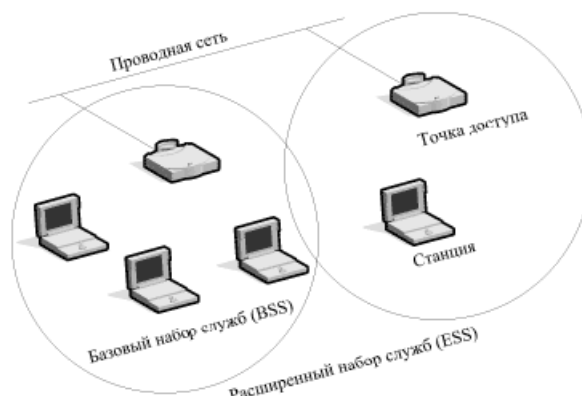


Рис. 7.3 Архитектура сети "клиент/сервер"

Режим "Ad-hoc" (также называемый точка-точка, или независимый базовый набор служб, IBSS) – это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования специальной точки доступа (рис. 7.4). Такой режим полезен в том случае, если инфраструктура беспроводной сети не сформирована (например, отель, выставочный зал, аэропорт), либо по каким-то причинам не может быть сформирована.



Рис. 7.4 Архитектура сети "Ad-hoc"

Базовые механизмы защиты данных в беспроводных сетях. Технология DSSS и FHSS.

Технология DSSS (расширение спектра радиосигнала по принципу прямой последовательности) использует шумоподобный сигнал (ШПС) для передачи данных в радиоэфире на частотах в диапазоне 2400 - 2485 МГц.

DSSS технология была разработана ранее для применения в военных радиосистемах с высокой помехозащищенностью и с низкой вероятностью радиоперехвата.

Пропускная способность современных DSSS систем стандарта IEEE 802.11b - 11 Мбит/сек.

DSSS системы имеют ширину излучения 22 МГц и используют последовательности длиной 11бит, что позволяет создавать 11 кратную избыточность сигнала, а, следовательно, повысить в 11 раз помехоустойчивость системы.

DSSS системы могут работать при слабом сигнале, обеспечивая передачу данных на большие расстояния.

На данный момент на рынке также представлена еще одна технология стандарта IEEE 802.11 - FHSS (Frequency-Hopping Spread-Spectrum - расширение спектра радиосигнала путем скачкообразной перестройки частоты).

При методе **DSSS** каждый информационный символ представляется 11-разрядным кодом Баркера вида 11100010010. Коды Баркера обладают наилучшими среди известных псевдослучайных последовательностей свойствами шумоподобности, что и обусловило их применение в аппаратуре беспроводных сетей. Для передачи единичного и нулевого сим-

волов сообщения используются прямая и инверсная последовательности соответственно. Для модуляции несущего колебания в этом случае используются уже не исходные символы сообщения, а прямые или инверсные последовательности Баркера, так, как показано на рис. 7.4:

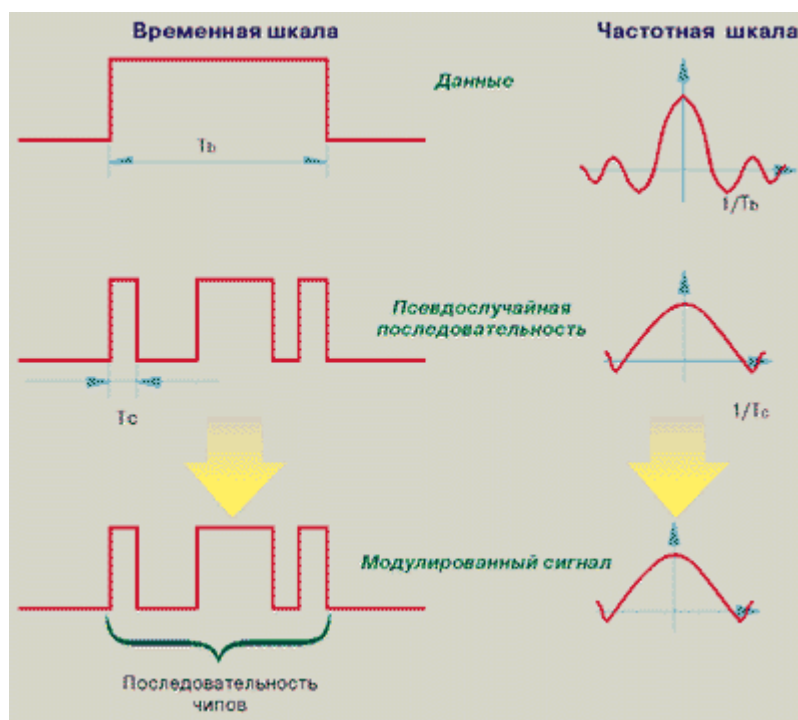


Рис. 7.4. Формирование широкополосного сигнала по методу DSSS

Спектр мощности сигнала с **DSSS** показан на рис. 7.5. Там же, для сравнения, показан спектр мощности сигнала, используемого при традиционных технологиях передачи. Из рисунка видно, что при переходе к **DSSS** происходит "размазывание" мощности сигнала в полосе частот, в 11 раз превышающей полосу исходного узкополосного сигнала. Здесь следует упомянуть о довольно часто встречающемся в литературе тезисе о том, что при переходе к технологии **DSSS** возможна работа на пониженных мощностях передатчика. Это верно только в том смысле, что снижается спектральная плотность мощности излучаемого сигнала при неизменной излучаемой передатчиком мощности.

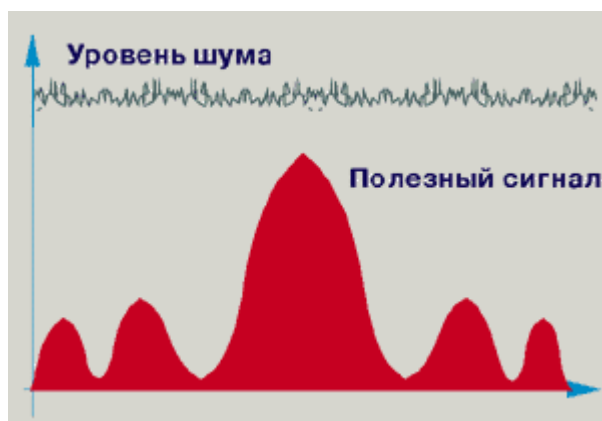


Рис. 7.5. Соотношение уровня шума и полезного сигнала при модуляции по методу DSSS.

Для лучшего понимания спектральных соотношений рассмотрим конкретный пример, характерный для аппаратуры фирмы Aironet. Передача ведется со скоростью 2

Мбит/с, что при использовании узкополосной технологии требует полосы частот 4 МГц. При переходе к технологии DSSS полоса частот расширяется в 11 раз и становится равной 44 МГц. В то же время, в документации на аппаратуру указано значение полосы частот, необходимой для передачи, равное 22 МГц. Это кажущееся несоответствие легко понять, если внимательно посмотреть на спектр сигнала с DSSS, показанный на рис. 4.2. По 25% полосы частот слева и справа заняты маломощными спектральными составляющими, которые обрезаются в передатчике, в результате ширина спектра передаваемого сигнала уменьшается вдвое и становится равной 22 МГц. Отсечение этих спектральных составляющих приводит к незначительному искажению формы передаваемого сигнала, практически не влияющему на качество передачи.

В приемнике полученный сигнал умножается на код Баркера, в результате он становится узкополосным, поэтому его фильтруют в узкой полосе частот, равной удвоенной скорости передачи. Любая помеха, попадающая в полосу исходного широкополосного сигнала, после умножения на код Баркера, наоборот, становится широкополосной, поэтому в узкую информационную полосу попадает лишь часть помехи, примерно в 11 раз меньшая по мощности помехи, действующей на входе приемника. В результате демодуляции полученного узкополосного сигнала, выполняемой с помощью обычного демодулятора, выделяется передаваемое сообщение. Главной проблемой, возникающей при решении этой задачи, является обеспечение синхронизации приемника по передаваемому сигналу. На уровне физического канала необходимо обеспечить синхронизацию по фазе несущего колебания, тактовой частоте кода Баркера и тактовой частоте сообщения. Для решения этой задачи передатчик не реже, чем один раз за 100 мс передает специальный синхросигнал. При плохом качестве канала частота передачи синхросигнала может быть увеличена изменением соответствующего пункта в меню настройки аппаратуры.

Применение технологии DSSS позволяет также эффективно бороться с интерференционной помехой, возникающей в результате отражения сигнала от стен и местных предметов, что особенно актуально для закрытых помещений.

При методе FHSS передача ведется обычными методами, как в традиционных узкополосных системах, но несущая частота сигнала периодически изменяется, что позволяет легко исправить ошибочно принятые на пораженной помехами частоте блоки, путем их повторной передачи на другой частотной позиции. Порядок следования частот должен быть одинаковым на передающей и приемной стороне или у всех устройств сети при сетевом варианте использования. Это достигается одинаковой настройкой аппаратуры и передачей специальных синхросигналов, определяющих моменты начала очередного цикла смены частот.

Стандартом IEEE 802.11 предусмотрено использование 79 частотных позиций при времени передачи на каждой в течение 20 мс. Порядок смены частотных позиций определяется псевдослучайным кодом, что обеспечивает определенную конфиденциальность передачи.

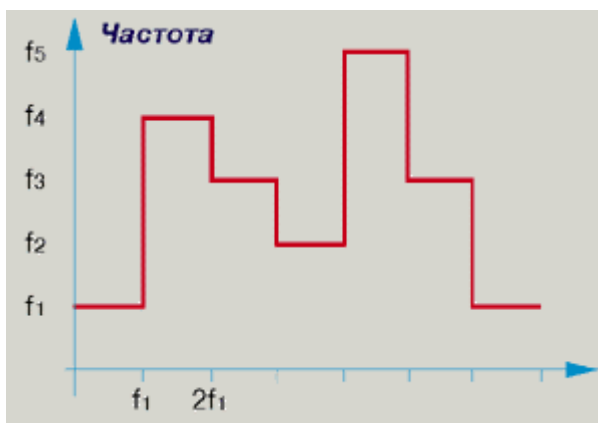


Рис. 7.6. Частотные скачки при формировании сигнала по методу FHSS

Для примера на рис. 7.6 представлена частотно - временная матрица сигнала FHSS, состоящая из 7 частотных позиций. После использования всех частот начинается их повторное использование в уникальном, установленном для данной пары передатчик - приемник или сети, порядке.

Следует оговориться, что защита информации, обеспечиваемая методами FHSS и DSSS не надежная, и представляет собой лишь дополнительная функцию, основное же предназначение методов расширения спектра это обеспечение надежности связи в условиях многолучевости.

Таблица 7.6. Сравнение технологии DSSS и FHSS

Параметр	DSSS	FHSS
Диапазон рабочих частот	2400-2485 МГц	2400-2485 МГц
Ширина полосы излучения	22 МГц	1 МГц
Коэффициент избыточности сигнала (коэффициент надежности)	11	1
Чувствительность к узкополосным помехам	низкая	высокая
Чувствительность к широкополосным помехам	высокая	высокая
Максимальная скорость передачи данных	11 Мбит/сек	3 Мбит/сек
Зависимость количества ошибок от расстояния	средняя	высокая

- с использованием технологии DSSS в диапазоне 2,4 ГГц могут одновременно работать (без перекрытия) три станции. С использованием технологии FHSS число таких станций равно 26 – число возможных последовательностей в одном сете (больше невозможно по требованию 6 МГц);

- дальность приема/передачи с использованием DSSS больше чем при FHSS, за счет более широкого спектра несущей;

- когда уровень шума превышает некоторый определенный уровень, DSSS станции перестают работать вообще, в то время как FHSS станции имеют проблемы только на отдельных частотных скачках, что легко разрешается и в этом смысле последние считаются более помехозащищенными;

- DSSS станции передают сигнал непрерывно, для FHSS станций существуют служебные интервалы времени (синхронизации частот). Поэтому первые имеют более высокую производительность на той же битовой скорости или, что то же самое могут реализовывать более высокие битовые скорости;

- DSSS станции значительно более чувствительны к задержкам и искажениям сигнала, возникающих при эффекте отражения, так как используют более короткие импульсы.

Таким образом FHSS-технология в диапазоне 2,4 ГГц должна преимущественно применяться внутри зданий или на частной территории при отсутствии помех радиоприемникам, включая широкополосные, находящимся вне этих зданий и территорий. Для наружного применения в локальных сетях, размещаемых в помещениях, где велика опасность интерференционных помех наиболее приспособлена DSSS-технология в диапазоне 2,4 ГГц.

Фильтрации MAC адресов

Аутентификация с использованием MAC-адресов не специфицирована стандартом IEEE 802.11, однако обеспечивается многими производителями. В ходе аутентификации с использованием MAC-адресов проверяется соответствие MAC-адреса клиента локально сконфигурированному списку адресов или списку, хранящемуся на внешнем аутентификационном сервере (рис. 7.7).

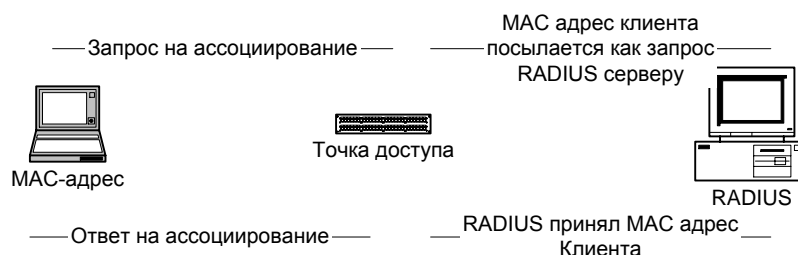


Рис. 7.7. Аутентификация с использованием MAC-адреса

Аутентификация с использованием MAC адресов усиливает действия открытой аутентификации и аутентификации с использованием совместного ключа, тем самым потенциально снижая вероятность того, что неавторизованные устройства получают доступ к сети.

Необходимо отметить, что MAC-адреса пересылаются с помощью незашифрованных фреймов стандарта IEEE 802.11, поэтому беспроводные LAN довольно уязвимы для атак, в ходе которых злоумышленник проходит аутентификацию путем имитации законного MAC-адреса. Имитация MAC-адреса возможна для сетевых карт, позволяющих заменять универсально-назначаемый адрес UAA локально-назначаемым адресом. В Windows это делается очень легко, а в UNIX это возможно осуществить через корневую команду оболочки. Если нападающий удостоверился и связался с беспроводной сетью, то затем он сканирует порты и пытается узнать списки пользователей и пароли, пытается "подражать" клиентам.

Использование механизмов защиты, встроенных в точки доступа

Помимо поддержки собственно стандартов безопасности, поставщики беспроводных устройств наделяют свои разработки множеством других функций защиты, включая средства контроля за доступом, формирования VPN, обнаружения и блокирования действий хакеров.

Из этого перечня в протестированных продуктах чаще всего встречается функция контроля за доступом на MAC-уровне. Ее реализовали 3Com, Actiontec, Airespace, Aruba, Buffalo, Cisco, HP, Netgear, Proxim, SMC и Trapeze. Для использования данной функции вам придется выяснить Ethernet-адреса всех беспроводных адаптеров, подключающихся к сети. Эта процедура может показаться утомительной, но позволит защититься от непрофессиональных злоумышленников.

Средства контроля за доступом по MAC-адресам бывают двух типов. Точка доступа для домашней беспроводной сети требует постоянного хранения на ней статического перечня MAC-адресов. Этот метод оказался столь популярным, что производители точек доступа и беспроводных коммутаторов стали применять его в более сложных сетевых конфигурациях: несколько точек доступа могут обращаться к списку статических MAC-адресов, хранящемуся на сервере RADIUS, с целью определить, какому оборудованию разрешено подключение к сети.

Второй тип систем контроля за доступом представляет собой брандмауэр, интегрированный с точкой доступа. В одних продуктах, например в точке доступа WL-450 компании 3Com, реализована простейшая фильтрация пакетов, в основном для защиты WLAN от сетевого «мусора», вроде широковещательного трафика IPX-маршрутизации. Другие изделия поддерживают набор более изощренных фильтров. Скажем, коммутатор Airespace 4000 и точки доступа производства Buffalo, Cisco, HP и Proxim позволяют расширить сферу контроля за доступом вплоть до уровня IP. А компания Aruba встроила в свой беспроводной коммутатор Aruba 800 полнофункциональный брандмауэр.

Средства контроля за доступом фирмы Tpareze работают с пользователями, прошедшими полную процедуру аутентификации. В большинстве продуктов списки доступа определяются для той WLAN, в которой производилась регистрация. В результате все пользователи, работающие в данной локальной сети, получают один и тот же список. Инженеры компании Tpareze решили «привязать» список допустимых IP-адресов к пользователям, прошедшим аутентификацию. Вследствие этого список доступа каждого потребителя определяется исходя из его регистрационной информации. Похожую схему опционально предлагает и Airespace. Использование для целей аутентификации сервера RADIUS позволяет также присвоить имя списку контроля за доступом, который относится к конкретному пользователю.

Тем, кто сделал ставку на протокол IPSec, пригодятся серверы VPN-туннелей, встроенные в беспроводные коммутаторы производства Aruba и Airespace. Конечно, вам не придется самостоятельно формировать туннели для соединения с точкой доступа или беспроводным коммутатором — упомянутые компании сумели автоматизировать эту процедуру. Вы можете также поместить рядом с WLAN отдельное VPN-устройство, правда, рискуя лишиться части преимуществ, которые сулит интегрированный сервер VPN-туннелей. Речь идет о строгой привязке беспроводного клиента к туннелю IPSec или об упрощении топологии сети, в которой имеется несколько мест выхода из WLAN в кабельную инфраструктуру.

Протокол безопасности WEP

В 1997 г., когда базовый стандарт IEEE 802.11 ратифицировали, в IEEE был одобрен механизм Wired Equivalent Privacy (WEP), который использует шифрование в качестве средства обеспечения безопасности в беспроводных сетях. WEP работает на втором уровне модели OSI и применяет для шифрования 40-битный ключ, что явно недостаточно. Еще в октябре 2000 г. был опубликован документ IEEE 802.11-00/362 под названием "Unsafe at any key size; An analysis of the WEP encapsulation", созданный Джесси Уолкером (Jesse R. Walker), где описываются проблемы алгоритма WEP и атаки, которые могут быть организованы с использованием его уязвимостей. Данная проблема получила развитие в двух работах, опубликованных с интервалом в месяц: "Intercepting Mobile Communications: The Insecurity of 802.11" от сотрудников университета Беркли, представленной на 7-й ежегодной конференции по мобильной вычислительной технике и сетям в июле 2001 г., и "Weaknesses in the Key Scheduling Algorithm of RC4" (совместно подготовлена специалистами Cisco Systems и факультета вычислительной техники израильского института Weizmann), вышедшей в свет в августе 2001 г. В этом же году появилась и первая утилита, разработанная Адамом Стаблфилдом (Adam Stubblefield), в которой на практике были реализованы теоретические выкладки вышеприведенных авторов и которая взламывала WEP-шифр в течение нескольких часов. На сегодняшний день существуют утилиты, позволяющие взломать WEP за 5-30 с.

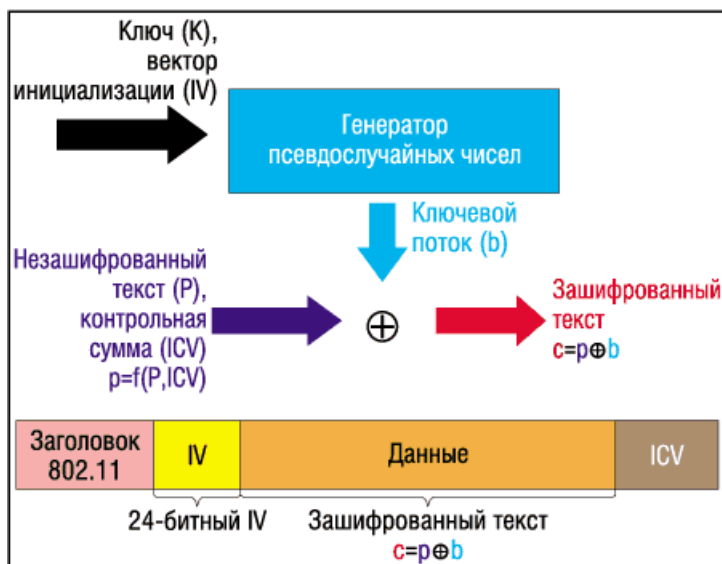


Рис. 7.8. Схема работы шифрования по протоколу WEP

Проблемы алгоритма WEP носят комплексный характер и кроются в целой серии слабых мест: механизме обмена ключами (а точнее, практически полном его отсутствии); малых разрядностях ключа и вектора инициализации (Initialization Vector - IV); механизме проверки целостности передаваемых данных; способе аутентификации и алгоритме шифрования RC4.

Процесс шифрования WEP выполняется в два этапа. Вначале подсчитывается контрольная сумма (Integrity Checksum Value - ICV) с применением алгоритма Cyclic Redundancy Check (CRC-32), добавляемая в конец незашифрованного сообщения и служащая для проверки его целостности принимаемой стороной. На втором этапе осуществляется непосредственно шифрование. Ключ для WEP-шифрования - общий секретный ключ, который должны знать устройства на обеих сторонах беспроводного канала передачи данных. Этот секретный 40-битный ключ вместе со случайным 24-битным IV является входной последовательностью для генератора псевдослучайных чисел, базирующегося на шифре Вернама для генерации строки случайных символов, называемой ключевым потоком (key stream). Данная операция выполняется с целью избежания методов взлома, основанных на статистических свойствах открытого текста.

IV используется, чтобы обеспечить для каждого сообщения свой уникальный ключевой поток. Зашифрованное сообщение (рис. 7.8) образуется в результате выполнения операции XOR над незашифрованным сообщением с ICV и ключевым потоком. Чтобы получатель мог прочитать его, в передаваемый пакет в открытом виде добавляется IV. Когда информация принимается на другой стороне, производится обратный процесс.

Значение **b** получатель вычисляет, применив код Вернама к входной последовательности, состоящей из ключа **K** (который он знает заранее) и IV, пришедшего этим же сообщением в открытом виде. Для каждого очередного пакета процесс повторяется с новым выбранным значением IV. К числу известных свойств алгоритма RC4 относится то, что при использовании одного и того же значения ключа и вектора инициализации мы всегда будем получать одинаковое значение **b**, следовательно, применение операции XOR к двум текстам, зашифрованным RC4 с помощью того же значения **b**, представляет собой не что иное, как операцию XOR к двум начальным текстам.

Таким образом, мы можем получить незашифрованный текст, являющийся результатом операции XOR между двумя другими оригинальными текстами. Процедура их извлечения не составляет большого труда. Наличие оригинального текста и IV позволяет

вычислить ключ, что в дальнейшем даст возможность читать все сообщения данной беспроводной сети.

После несложного анализа можно легко рассчитать, когда повторится **b**. Так как ключ **K** постоянный, а количество вариантов IV составляет $2^{24}=16\ 777\ 216$, то при достаточной загрузке точки доступа, среднем размере пакета в беспроводной сети, равном 1500 байт (12 000 бит), и средней скорости передачи данных, например 5 Mbps (при максимальной 11 Mbps), мы получим, что точкой доступа будет передаваться 416 сообщений в секунду, или же 1 497 600 сообщений в час, т. е. повторение произойдет через 11 ч 12 мин ($2^{24}/1\ 497\ 600=11,2$ ч). Данная проблема носит название "коллизия векторов". Существует большое количество способов, позволяющих ускорить этот процесс. Кроме того, могут применяться атаки "с известным простым текстом", когда одному из пользователей сети посылается сообщение с заранее известным содержанием и прослушивается зашифрованный трафик. В этом случае, имея три составляющие из четырех (незашифрованный текст, вектор инициализации и зашифрованный текст), можно вычислить ключ. В упоминавшейся выше работе "Intercepting Mobile Communications: The Insecurity of 802.11" было описано множество типов атак, включая довольно сложные, использующие манипуляции с сообщениями и их подмену, основанные на ненадежном методе проверки целостности сообщений (CRC-32) и аутентификации клиентов. С ICV, используемым в WEP-алгоритме, дела обстоят аналогично. Значение CRC-32 подсчитывается на основе поля данных сообщения. Это хороший метод для определения ошибок, возникающих при передаче информации, но он не обеспечивает целостность данных, т. е. не гарантирует, что они не были подменены в процессе передачи. Контрольная сумма CRC-32 имеет линейное свойство: $CRC(A \text{ XOR } B)=CRC(A)\text{XOR } CRC(B)$, предоставляющее нарушителю возможность легко модифицировать зашифрованный пакет без знания WEP-ключа и пересчитать для него новое значение ICV. Появившаяся в 2001 г. спецификация WEP2, которая увеличила длину ключа до 104 бит, не решила проблемы, так как длина вектора инициализации и способ проверки целостности данных остались прежними. Большинство типов атак реализовывались так же просто, как и раньше.

Защита беспроводных сетей на сетевом уровне.

Использование IPSec для защиты трафика беспроводных клиентов

Протокол IPSec применяется для усиления криптографической защиты информации в протоколе L2TP (L2TP with IPsec). Этот протокол был разработан для создания средств обеспечения защищенной передачи пакетов протокола IPv6. Основная задача IPSec - обмен сеансными ключами, используемыми для шифрования данных, и их администрирование. В протоколе применяется схема обмена ключами IKE (Internet Key Exchange), которая в настоящее время утверждается в качестве стандарта IETF. Схема IKE представляет собой два похожих модуля: IKE aggressive mode - для быстрого распределения ключей и IKE X.509 certificates - для использования сертификатов публичных ключей. Протокол IPSec выделяет два заголовка в IP-пакете, которые используются системами аутентификации и шифрования данных: AH (Authentication Header - заголовок аутентификации) и ESP (Encapsulating Security Payload - заголовок протокола безопасного закрытия содержания).

Спецификация IPSec предусматривает применение AH и ESP к IP-пакету двумя способами. В стандартном режиме передачи данных аутентификации и шифрованию подвергается только заголовок IP-пакета. В режиме туннелирования аутентификация и шифрование распространяются на весь пакет. При выборе режима нужно определить, какой фактор более важен: скорость доставки данных или безопасность информации. Существует три модификации протокола IPSec:

IPsec gateway - для связи между различными сетями;

IPsec client for Windows - для связи с клиентской Windows-машиной;

IPsec client for Macintosh - для связи с клиентской Macintosh-машиной.

Применение технологии VPN для защиты беспроводных сетей

Технология VPN позволяет задействовать Internet для частной связи безо всякого риска. Вместо того чтобы устанавливать связь напрямую через Internet, клиент VPN формирует защищенное соединение с узлом VPN. Он шифрует пакеты данных, а затем пересылает их по каналам Internet на узел VPN, где пакеты расшифровываются. Взломщик, перехвативший зашифрованные пакеты в Internet, сможет извлечь из них полезную информацию, только расшифровав их. Подобная задача рядовому хакеру не по силам.

Для защиты беспроводной локальной сети можно воспользоваться технологией VPN, встроенной в Windows 2000. Организация VPN производится так:

- Установите беспроводную сеть в соответствии с инструкциями изготовителя;
- На каждой клиентской машине Windows 2000 Professional, подключаемой к беспроводной локальной сети, нужно щелкнуть на кнопке Start, а затем выбрать пункты Settings, Network and Dial-up Connections. Щелкнув правой кнопкой мыши на значке беспроводного адаптера, следует выбрать пункт Properties, а затем убрать флажки Client for Microsoft Networks и File and Printer Sharing for Microsoft Networks. Необходимо убедиться, что по-прежнему выбран протокол Internet (TCP/IP);
- На машине Windows 2000 Server нужно выбрать из меню Start пункты Settings, Network and Dial-up Connections и Make New Connection, чтобы запустить мастер Network Connection Wizard. Нажав Next, следует установить флажок Accept incoming connections. На следующем экране необходимо убедиться, что флажок All connection devices не установлен. Затем на странице Incoming Virtual Private Connection (входное соединение VPN) нужно щелкнуть сначала на кнопке Allow Virtual Private Connection, а затем на Next. Теперь требуется выбрать пользователей, которым будет разрешен доступ к виртуальному соединению (нельзя разрешать доступ пользователю Guest). Затем следует убедиться, что выбраны все сетевые компоненты. На последней странице, где приведено имя полученного соединения, следует нажать Finish.
- На каждом клиенте нужно выбрать Start, Settings, Network and Dial-up Connections и Make New Connection, чтобы запустить мастер Network Connection Wizard. Щелкнув на кнопке Next, следует выбрать пункт Connect to a private network through the Internet. На следующем экране необходимо ввести имя или IP-адрес сервера DNS, а затем щелкнуть Next. Можно создать соединения для всех пользователей или только для тех, кто зарегистрирован. В завершение можно изменить имя соединения и щелкнуть на кнопке Finish.
- На клиентском компьютере появляется окно Connect Virtual Private Connection. Чтобы завершить организацию соединения, пользователь должен ввести свое имя и пароль. После этого между клиентом и сервером устанавливается связь, подобная прямому соединению между машинами в локальной сети.

В результате данной процедуры просмотр документов, как и работа с общими файлами и принтерами, происходит через VPN. Взломщик, находящийся вне здания и располагающийся беспроводной платой, может обнаружить сеть, но не в состоянии прочитать данные, хранящиеся на машинах. Конечно, взломщик может догадаться о существовании VPN и попытаться получить доступ к ней. Но для этого необходимо отгадать имя пользователя и пароль. Очевидно, что, организовав VPN, нельзя разрешать гостевой доступ и назначать пустой пароль. Кроме того, если, как это часто бывает, в Windows 2000 заданы слишком очевидные пароли для учетной записи Administrator, настало время изменить их.

Стандарты WPA (Wi-Fi Protected Access) и IEEE 802.11i

Ещё в мае 2001 г. группа IEEE Task Group I (TGi) начала работу над новым проектом IEEE 802.11i (MAC Enhancements for Enhanced Security), призванным обеспечить достаточную безопасность в беспроводных сетях. В ноябре 2003 г. состоялось последнее заседание группы, на котором была одобрена 7-я версия предварительного стандарта.

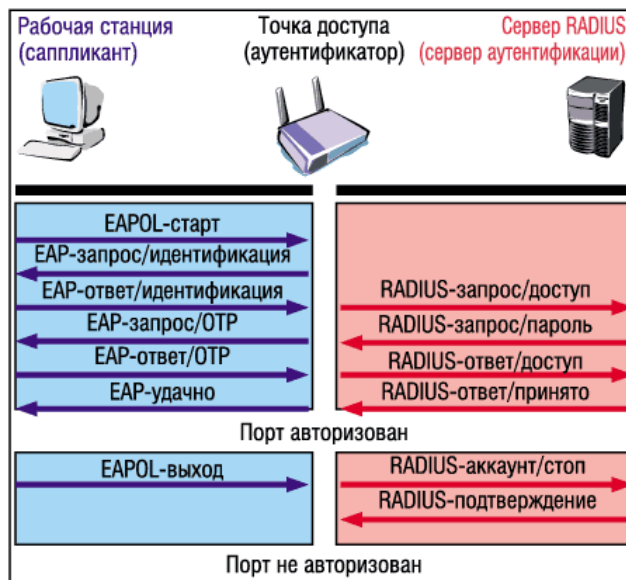


Рис. 7.9. Схема аутентификации пользователя в соответствии со стандартом 802.1x.

Основные производители Wi-Fi-оборудования в лице организации WECA (Wireless Ethernet Compatibility Alliance), иначе именуемой Wi-Fi Alliance, устав ждать ратификацию стандарта IEEE 802.11i, совместно с IEEE в ноябре 2002 г. анонсировали спецификацию Wi-Fi Protected Access (WPA). WPA базируется на компонентах ожидаемого стандарта IEEE 802.11i, которые к настоящему времени уже стабильны и не подвергаются переработке, а также могут быть развернуты в существующих сетях IEEE 802.11 без внесения аппаратных изменений в устройства. В WPA включены следующие компоненты IEEE 802.11i: протоколы IEEE 802.1x и TKIP (Temporal Key Integrity Protocol).

Протокол IEEE 802.1x

Протокол IEEE 802.1x, являющийся стандартом с августа 2001 г., обеспечивает контроль доступа на уровне портов. Основная его идея заключается в том, что разблокирование сетевого порта и обеспечение доступа клиента к сети происходит только после успешной аутентификации, которая выполняется на втором уровне модели OSI. 802.1x может использоваться совместно с протоколами более высоких уровней для генерации и управления ключами шифрования.

Протокол аутентификации EAP

IEEE 802.1x использует протокол EAP (Extensible Authentication Protocol), изначально разрабатывавшийся для работы поверх PPP (Point-to-Point Protocol) для передачи сообщений между тремя участниками аутентификации в ЛВС-окружении. Этот вид инкапсуляции известен как EAP over LANs, или EAPOL. EAP нельзя назвать методом аутентификации. Он определяет основную протокольную структуру для выбора специфического метода аутентификации. При использовании EAP аутентификатору не требуется "по-

нимать" детали различных методов аутентификации. В данном случае он выступает только как промежуточное звено, которое переупаковывает EAP-пакеты при их следовании между саппликантом (supplicant - объект на конце сегмента "точка-точка", которому необходима аутентификация: это может быть клиентское ПО на компьютере, PDA или другом беспроводном устройстве) и сервером аутентификации. Такая технология предоставляет разработчикам возможность выбора между разными видами аутентификации, что является несомненным преимуществом.

Протоколом EAP на сегодняшний день предусмотрено уже более десяти различных методов аутентификации, но следует отметить следующие два метода, EAP-TTLS и EAP-PEAP. В отличие от остальных эти два метода перед непосредственной аутентификацией пользователя сначала образуют TLS-туннель между клиентом и сервером аутентификации. А уже внутри этого туннеля осуществляется сама аутентификация, с использованием как стандартного EAP (MD5, TLS), так и старых не-EAP методов (PAP, CHAP, MS-CHAP, MS-CHAP v.2), последние работают только с EAP-TTLS (PEAP используется только совместно с EAP методами). Предварительное туннелирование повышает безопасность аутентификации, защищая от атак типа «man-in-middle», «session hijacking» или атаки по словарю.

Протокол TKIP, метод Michael и технология WPA

Temporal Key Integrity Protocol (TKIP) – второй протокол, предусмотренный спецификацией WPA. TKIP предназначен для решения основных проблем WEP в области шифрования данных. Для совместимости с существующим аппаратным обеспечением TKIP использует тот же алгоритм шифрования, что и WEP – RC4. TKIP подразумевает несколько способов повышения защищённости беспроводных сетей: динамические ключи, изменённый метод генерации ключей, более надёжный механизм проверки целостности сообщений, увеличенный по длине вектор инициализации, нумерация пакетов.

В отличие от WEP, где для контроля целостности передаваемых данных использовалась CRC-32, TKIP применяет так называемый Message Integrity Code (MIC), обеспечивающий криптографическую контрольную сумму от нескольких полей (адрес источника, адрес назначения и поля данных). Так как классические MIC – алгоритмы (например, HMAC-MD5 или HMAC-SHA1) для существующего беспроводного оборудования являлись очень «тяжёлыми» и требовали больших вычислительных затрат, то специально для использования в беспроводных сетях Нильсом Фергюсоном (Niels Ferguson) был разработан алгоритм Michael. Для шифрования он применяет 64-битный ключ и выполняет действия над 32-битными блоками данных. MIC включается в зашифрованную часть фрейма между полем данных и полем ICV.

Для обеспечения целостности данных в протоколе TKIP, помимо механизма MIC, предусмотрена ещё одна функция, отсутствовавшая в WEP, - нумерация пакетов. В качестве номера используется IV, который теперь называется TKIP Sequence Counter (TSC) и имеет длину 48 бит, в отличие от 24 бит в WEP. Увеличение длины IV до 48 бит позволяет избежать коллизии векторов и гарантирует, что они не повторятся на протяжении более тысячи лет.

Основным и самым важным отличием TKIP от WEP является механизм управления ключами, позволяющий периодически изменять ключи и производить обмен ими между всеми участниками сетевого взаимодействия: саппликантом, аутентификатором и сервером аутентификации. В процессе работы и аутентификации на разных этапах взаимодействия и для различных целей генерируются специализированные ключи.

В стандартах With IEEE 802.11 и WEP за целостность данных отвечает 32-разрядное значение проверки целостности (ICV), которое прилагается к трафику IEEE 802.11 и шифруется с помощью WEP. Несмотря на то, что значение проверки целостности

шифруется, криптографический анализ позволяет таким образом изменить данные и значение ICV, что принимающая сторона этого не заметит.

В WPA метод, называемый Michael, определяет новый алгоритм, который рассчитывает 8-разрядный код целостности сообщения (MIC) с помощью средств, имеющихся у устройств беспроводного доступа. Значения MIC располагаются в кадре IEEE 802.11 между фрагментом данных и 4-разрядным ключом ICV. Значение MIC шифруется наряду с данными и значением ICV.

Кроме того, метод Michael позволяет защитить от повторов. Для этого в IEEE 802.11 используется счётчик кадров.

Стандарт IEEE 802.11i

Стандарт IEEE 802.11i, иначе называемый WPA2, предусматривает новые, более надёжные механизмы обеспечения целостности и конфиденциальности данных:

- протокол CCMP (Counter-Mode-CBC-MAC Protocol), основанный на режиме Counter Cipher-Block Chaining Mode (CCM) алгоритма шифрования Advanced Encryption Standard (AES). CCM объединяет два механизма: Counter (CTR) для обеспечения конфиденциальности и Cipher Block Chaining Message Authentication Code (CBC-MAC) для аутентификации;
- протокол WRAP (Wireless Robust Authentication Protocol), основанный на режиме Offset Codebook (OCB) алгоритма шифрования AES;
- протокол TKIP для обеспечения обратной совместимости с ранее выпускавшимся оборудованием;
- взаимная аутентификация и доставка ключей на основе протоколов IEEE 802.1x/EAP;
- безопасный Independent Basic Service Set (IBSS) для повышения безопасности в сетях Ad-Нос.

Использование механизмов шифрования и аутентификации, определённых в стандарте IEEE 802.11i, потребует от устройств более высокой вычислительной мощности и применения специализированных микросхем, которые будут решать возлагаемые на них задачи. Поэтому, скорее всего, после ратификации стандарта появятся принципиально новые устройства.

В таблице 7.7 приведён краткий сравнительный анализ стандартов.

Таблица 7.7. Сравнение стандартов

Стандарт	Средства обеспечения безопасности	Достоинства	Недостатки
WEP	Шифрование RC4, статические ключи, аутентификация IEEE 802.1x по желанию пользователя	Лучше хоть какая-то безопасность, чем никакой; поддержка WEP в большинстве устройств IEEE 802.11	Слишком много брешей для использования в корпоративной среде; для защиты беспроводных ЛВС зачастую приходится применять дополнительные средства наподобие виртуальных частных сетей
WPA	TKIP, динамические ключи, Michael, обязательная аутентификация IEEE 802.1x (EAP и RADIUS либо предус-	Обратная совместимость с WEP, возможность интеграции в существующие беспроводные сети путём про-	Временное решение проблемы на переходный период до утверждения более надёжного стандарта IEEE 802.11i

	тановленный общий ключ)	стого обновления микропрограмм	
IEEE 802.11i	Шифрование AES, CCMP, WRAP, управление ключами IEEE 802.11i, аутентификация IEEE 802.1x	Более стойкое, чем в WEP, шифрование, надёжная схема управления ключами	Необходимость нового оборудования и наборов микросхем; несовместимость с нынешним оборудованием Wi-Fi

Угрозы для беспроводных сетей

Не смотря на все рассмотренные методы и способы защиты существует множество угроз для БСПД, что определяется самой средой передачи информации. Рассмотрим известные виды угроз:

Прослушивание (Sniffing или war driving)

Сбор информации об атакуемом объекте — это необходимый этап при подготовке атаки. К сожалению администраторов и владельцев беспроводной сети, пассивное прослушивание и анализ передаваемой информации может предоставить сторонним наблюдателям достаточно данных для успешного проникновения в сеть. И предусмотренные разработчиками методы защиты не смогут этому помешать.

Для сбора информации достаточно войти в зону покрытия сети, и, воспользовавшись рабочей станцией с беспроводным сетевым интерфейсом, подключить программный анализатор сетевого трафика (например, Kismet или Ethereal). Если WEP-кодирование не включено (обычная заводская настройка оборудования), наблюдатель видит в открытом виде все данные, передаваемые в сети. Если WEP-кодирование все-таки включено, то, следует заметить, кодируются только данные, передаваемые в сетевом пакете, а заголовок пакета передается в открытом виде. Из анализа заголовка можно извлечь информацию об идентификаторе сети, аппаратных адресах узлов доступа и клиентов сети, а также значение вектора инициализации, используемое получателем для дешифровки полученных данных.

Подделка аппаратного адреса (MAC spoofing)

Использование механизма идентификации клиентов по аппаратным адресам сетевых интерфейсов для доступа к сетевым ресурсам — не самая лучшая идея. Перехватив и проанализировав сетевой трафик, можно за короткое время получить список аппаратных адресов всех активных клиентов. Задача же изменения аппаратного адреса своего сетевого интерфейса давно решена. Под «линуксоподобными» операционными системами достаточно воспользоваться стандартной сетевой утилитой ifconfig, а для Windows-систем надо трудиться несколько больше, переставляя драйвер сетевого интерфейса или устанавливая дополнительную утилиту.

Взлом криптозащиты

Данный вид угроз обусловлен не надёжностью используемых протоколов шифрования.

Посредник (Man-In-The-Middle)

Данный вид атаки использует функцию роуминга клиентов в беспроводных сетях. Злоумышленник на своей рабочей станции имитирует узел доступа с более мощным сигналом, чем реальный узел доступа. Клиент беспроводной сети автоматически переключается на новый узел доступа, передавая на него весь свой трафик. В свою очередь, злоумышленник передает этот трафик реальному узлу доступа под видом клиентской рабочей станции. Таким образом, система злоумышленника включается в обмен данными между клиентом и узлом доступа как посредник, что и дало название данному виду атаки — Man-In-The-Middle (пер. с англ. — посредник). Эта атака опасна тем, что позволяет взламывать защищенные соединения (VPN), устанавливаемые по беспроводной сети, вызывая

принудительную реавторизацию VPN-клиента. В результате злоумышленник получает авторизационные данные скомпрометированного им клиента.

Отказ в обслуживании

Сама среда передачи данных предоставляет возможность силовой атаки на беспроводные сети. Цель подобного нападения — снижение производительности сети или ухудшение качества сетевого обслуживания вплоть до полного паралича сети. Атаки подобного вида называются DoS (Denial of Service) или DDoS (Distributed DoS). В процессе нападения злоумышленник передает трафик, объем которого превышает возможности пропускной способности сетевого оборудования. Или сетевые пакеты со специально нарушенной внутренней структурой. Или имитируя команды узла доступа, вызывает отключение клиентов и т.д. и т.п. Злоумышленник может избирательно атаковать как отдельную рабочую станцию или точку доступа, так и всех клиентов сети. DoS-атака может быть и преднамеренной. Например, вызванная включением радиопередающего оборудования, работающего на той же частоте, что и беспроводная сеть.

Сетевой взлом клиентов беспроводной сети

Существует опасность сетевого взлома через программное обеспечение.

8. ПЕРСОНАЛЬНЫЕ СЕТИ РАДИОДОСТУПА. СТАНДАРТЫ IEEE 802.15, Bluetooth

Семейство стандартов IEEE 802.15 предназначено для организации беспроводных персональных сетей (Wireless Personal Area Networks, WPANs) отличительной чертой которых является небольшой радиус действия сетевых устройств. Все они описывают два нижних уровня протоколов модели взаимодействия открытых систем (OSI): физический (PHY) и уровень доступа к среде передачи (MAC). Место этих стандартов в семействе IEEE 802 для беспроводных сетей иллюстрируется на рисунке 8.1.

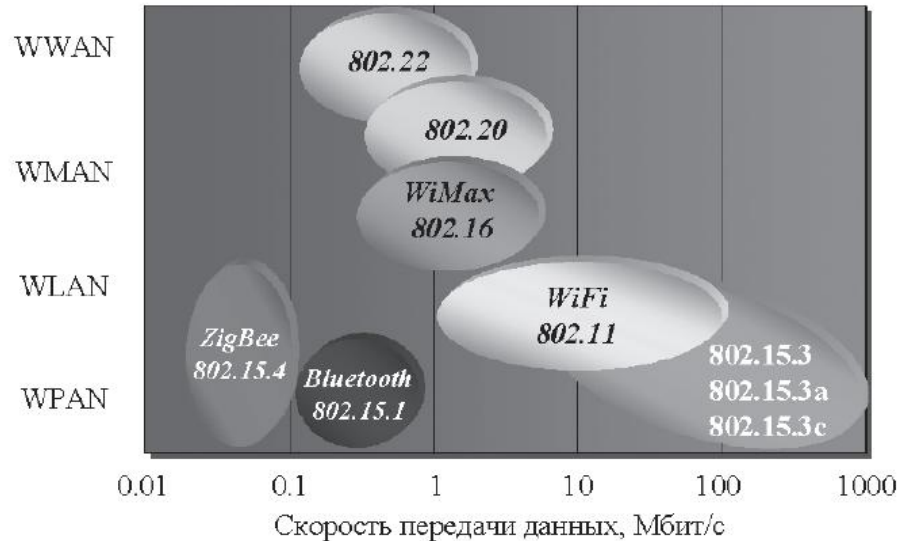


Рис. 8.1. Семейство стандартов IEEE 802 для построения беспроводных сетей

Стандарт IEEE 802.15.1 (Bluetooth) ориентирован на поддержку высокоскоростных мультимедийных приложений. Следствием является и относительно высокая стоимость сетевых устройств. Стандарт IEEE 802.15.3 ориентирован на ещё большую скорость передачи мультимедийных данных в WPAN, а стандарты IEEE 802.15.3a – на значительно большую скорость передачи данных за счёт использования сверхширокополосных сигналов (Ultra Wide Band, UWB). Разрабатываемый стандарт IEEE 802.15.3c является альтернативой стандарту IEEE 802.15.3a на физическом уровне. Эти стандарты, по сути, призваны воплотить в жизнь беспроводной прототип компьютерной технологии USB. Форум по продвижению стандарта IEEE 802.15.3a имеет название Wireless USB.

Стандарт IEEE 802.15.4 утверждён в 2003 году и ориентирован на организацию WPAN с небольшими скоростями передачи данных (Low Rate WPANs, LR_WPANs) при радиусе действия сетевых устройств от 10 до 75 м. Скорость передачи данных ограничена величиной 250 кбит/с. Низкая скорость передачи данных, однако, при прочих равных условиях требует и низкого энергопотребления сетевых устройств. Это, в свою очередь, позволяет упростить создание таких устройств, работающих с автономным энергопитанием. Поэтому стандарт имеет вполне конкретную рыночную нишу и ориентирован на разработку дешёвых сетевых беспроводных устройств, при необходимости работающих от автономного питания. Помимо низкой скорости передачи данных используются и относительно короткие пакеты данных (до 104 байт). Передача коротких пакетов является отличительной чертой систем управления, мониторинга и сбора данных от сенсоров (датчиков).

Bluetooth

Еще недавно проблем с выбором средства соединения различных устройств друг с другом или с компьютером практически не возникало. Кабель (коаксиальный, витая медная пара, многожильный шлейф) представлялся самым оптимальным и практически единственным решением. Однако появившиеся лэптопы и ноутбуки, сотовые телефоны и персональные цифровые помощники, CD- и MP3-плееры и масса иных мобильных устройств, часто подсоединяемых как друг к другу, так и к стационарным компьютерам, создали проблему. Кабель стал неудобен – подключаться надо часто, размеры самого кабеля с разъемами едва ли не больше собственно подключаемого устройства и т.д. На этом фоне резко возросла актуальность беспроводных локальных технологий, обеспечивающих столь же простое подключение устройства, сколь просто происходит обращение к диску собственного персонального компьютера. При этом пользователи не привязаны к какому-либо месту.

Bluetooth. Это короткое слово в последнее время всё чаще и чаще мелькает в новостях. Все уже слышали, что это технология беспроводных сетей. Однако подобные технологии существовали и раньше, но ни одна из них не имела и не имеет такой мощной и всесторонней поддержки, и ни про одну из них столько не говорилось. Что же такого особенного в Bluetooth?

Само слово Bluetooth можно перевести как "голубой зуб", или "голубая челюсть", что, конечно же, никоим образом не описывает ни сути технологии, ни чего-либо ещё. В далеком 908 году у ютландского короля Горма Старого и его супруги Тиры родился сын – Харальд. Ему была уготована великая судьба. Харальд I Блаатанд (в поздней транскрипции – Bluetooth, Синезубый - прозвище свое он получил из-за потемневшего переднего зуба (есть, правда, и другие версии)), сумев подчинить своей воле разрозненных викингов, объединил Данию с Южной Норвегией и Южной Швецией, создав единое Датское Королевство. Он же способствовал распространению в Скандинавии христианства, что бесспорно послужило единению культур.

Прошло почти 11 веков. В феврале 1998 года компании Ericsson, IBM, Intel, Toshiba и Nokia решили объединить свои усилия для создания технологии беспроводного соединения мобильных устройств, организовав специальную группу SIG (Special Interest Group). И прозвище короля Харальда I – Bluetooth – вновь стало символом объединения. Видимо, свою роль сыграло и то, что основы технологии были еще в 1994 году проработаны шведской компанией Ericsson. Логотип Bluetooth составляют руны, обозначающие инициалы короля.

Изначально группа была открыта для сотрудничества, и сейчас в Bluetooth SIG Promoters, которая занимается разработкой стандарта, входят 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, и Toshiba. В настоящее время действует версия 1.0 в спецификации, выпущенная 1 декабря 1999 года. В момент выпуска спецификации было объявлено, что она не является финальной, и финальная спецификация должна выйти ещё через три года. А эти три года должны уйти на "обкатку в боевых условиях". Кроме вышперечисленных компаний, в группу Bluetooth может абсолютно бесплатно войти любая компания, которая планирует производить или разрабатывать устройства и ПО на основе спецификаций Bluetooth. В настоящее в эту группу уже вошли около 2500 компаний самых различных направлений, так что перспективы у Bluetooth действительно неплохие.

Спецификация Bluetooth описывает пакетный способ передачи информации с временным мультиплексированием. Радиообмен происходит в полосе частот 2400–2483,5 МГц ISM-диапазона. В радиотракте применен метод расширения спектра посредством частотных скачков и двухуровневая частотная модуляция с фильтром Гаусса (binary Gaussian Frequency Shift Keying).

Метод частотных скачков подразумевает, что вся отведенная для передачи полоса частот подразделяется на определенное количество подканалов шириной 1 МГц каждый. Канал представляет собой псевдослучайную последовательность скачков по 79 или 23 ра-

диочастотным подканалам (табл. 8.1). Каждый канал делится на временные сегменты продолжительностью 625 мкс, причем каждому сегменту соответствует определенный подканал. Передатчик в каждый момент времени использует только один подканал. Эти скачки происходят синхронно в передатчике и приемнике в заранее зафиксированной псевдослучайной последовательности. За секунду может происходить до 1600 частотных скачков. Такой метод обеспечивает конфиденциальность и некоторую помехозащищенность передачи. Помехозащищенность обеспечивается тем, что если на каком-либо подканале передаваемый пакет не смог быть принят, то приемник сообщает об этом и передача пакета повторяется на одном из следующих подканалов, уже на другой частоте.

Таблица 8.1. Разделение полосы частот на подканалы в стандарте Bluetooth

Страна	Частота, МГц	Диапазон, МГц	Число каналов
Европа* и США	2400 – 2483,5	$f = 2402 + k$	$k=0-78$
Япония	2471 – 2497	$f = 2473 + k$	$k=0-22$
Испания	2445 – 2475	$f = 2449 + k$	$k=0-22$
Франция	2446,5 – 2483,5	$f = 2454 + k$	$k=0-22$

Примечание: *Кроме Испании и Франции

Протокол Bluetooth поддерживает как соединения типа точка-точка, так и точка-многоточка. Два или более использующих один и тот же канал устройства образуют пикосеть (piconet). Одно из устройств работает как основное (master), а остальные – как подчиненные (slaves). В одной пикосети может быть до семи активных подчиненных устройств, при этом остальные подчиненные устройства находятся в состоянии "парковки", оставаясь синхронизированными с основным устройством. Взаимодействующие пикосети образуют "распределенную сеть" (scatternet).

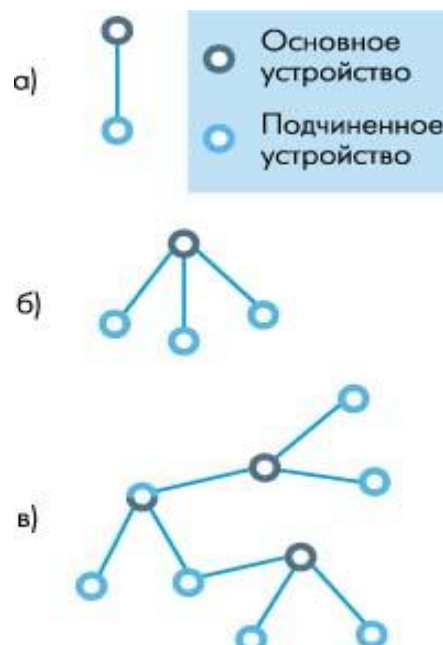


Рис. 8.2. Пикосеть с одним подчиненным устройством (а), несколькими (б) и распределенная сеть (в)

В каждой пикосети действует только одно основное устройство, однако подчиненные устройства могут входить в различные пикосети. Кроме того, основное устройство одной пикосети может являться подчиненным в другой (рис. 8.2).

Таким образом, в scatternet могут объединяться столько Bluetooth устройств, сколько необходимо, логические связи могут образовываться так, как это требуется, и могут изменяться как угодно, в случае необходимости. Единственное условие, различные piconet входящие в один scatternet должны иметь разные каналы связи, то есть работать на различных частотах и иметь различные hopping channel. Hopping - это регулярная смена частот, определяемая параметрами hopping sequence. Всего спецификация предусматривает 10 вариантов hopping sequence, 5 с циклом в 79 смен и 5 с циклом в 23 смены. С любым hopping sequence частоты сменяются 1600 hops/sec. Используется hopping для того, что бы бороться с затуханием радиосигнала и интерференцией. В одной же пикосети все устройства синхронизированы по времени и частотам. Последовательность скачков является уникальной для каждой пикосети и определяется адресом ее основного устройства. Длина цикла псевдослучайной последовательности – 227 элементов.

Как уже говорилось, автоматическая установка соединения между Bluetooth устройствами, находящимися в пределах досягаемости является одной из важнейших особенностей Bluetooth, поэтому первое, с чего начинается работа Bluetooth устройства в незнакомом окружении - это device discovery, или, по-русски, поиск других Bluetooth устройств. Для этого посылается запрос, и ответ на него зависит не только от наличия в радиусе связи активных Bluetooth устройств, но и от режима в котором находятся эти устройства. На этом этапе возможно три основных режима.

Discoverable mode. Находящиеся в этом режиме устройства всегда отвечают на все полученные ими запросы.

Limited discoverable mode. В этом режиме находятся устройства, которые могут отвечать на запросы только ограниченное время, или должны отвечать только при соблюдении определённых условий.

Non-discoverable mode. Находящиеся в этом режиме устройства, как видно из названия режима, не отвечают на новые запросы.

Но это ещё не всё. Даже если удастся обнаружить устройство, оно может быть в connectable mode или в non-connectable mode. В non-connectable mode устройство не позволяет настроить некоторые важные параметры соединения, и, таким образом, оно хоть и может быть обнаружено, обмениваться данными с ним не удастся. Если устройство находится в connectable mode, то на этом этапе Bluetooth устройства договариваются между собой об используемом диапазоне частот, размере страниц, количестве и порядке hop'ов, и других физических параметрах соединения.

Если процесс обнаружения устройств прошёл нормально, то новое Bluetooth устройство получает набор адресов доступных Bluetooth устройств, и за этим следует device name discovery, когда новое устройство выясняет имена всех доступных Bluetooth устройств из списка. Каждое Bluetooth устройство должно иметь свой глобально уникальный адрес (вроде как MAC-адреса у сетевых плат), но на уровне пользователя обычно используется не этот адрес, а имя устройства, которое может быть любым, и ему не обязательно быть глобально уникальным. Имя Bluetooth устройства может быть длиной до 248 байт, и использовать кодовую страницу в соответствии с Unicode UTF-8 (при использовании UCS-2, имя может быть укорочено до 82 символов). Спецификация предусматривает, что Bluetooth устройства не обязаны принимать больше первых 40 символов имени другого Bluetooth устройства. Если же Bluetooth устройство обладает экраном ограниченного размера, и ограниченной вычислительной мощностью, то количество символов, которое оно примет может быть уменьшено до 20.

Ещё одной из важнейших особенностей Bluetooth является автоматическое подключение Bluetooth устройств к службам, предоставляемым другими Bluetooth устройствами. Поэтому, после того как имеется список имён и адресов, выполняется service discovery,

поиск доступных услуг, предоставляемых доступными устройствами. Получение или предоставление каких либо услуг - это то, ради чего всё собственно и затевалось, поэтому для поиска возможных услуг используется специальный протокол, называемый, как несложно догадаться, Service Discovery Protocol (SDP), более подробно он будет описан ниже.

В стандарте Bluetooth предусмотрена дуплексная передача на основе разделения времени (time division duplexing). Основное устройство передает пакеты в нечетные временные сегменты, а подчиненное устройство – в четные (рис.8.3). Пакеты в зависимости от длины могут занимать до пяти временных сегментов. При этом частота канала не меняется до окончания передачи пакета (рис. 8.4).

Протокол Bluetooth может поддерживать асинхронный канал данных, до трех синхронных (с постоянной скоростью) голосовых каналов или канал с одновременной асинхронной передачей данных и синхронной передачей голоса. Скорость каждого голосового канала – 64 Кбит/с в каждом направлении, асинхронного в асимметричном режиме – до 723,2 Кбит/с в прямом и 57,6 кбит/с в обратном направлениях или до 433,9 Кбит/с в каждом направлении в симметричном режиме.

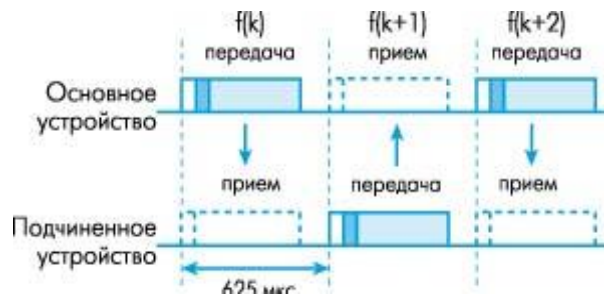


Рис. 8.3. Временные диаграммы работы канала

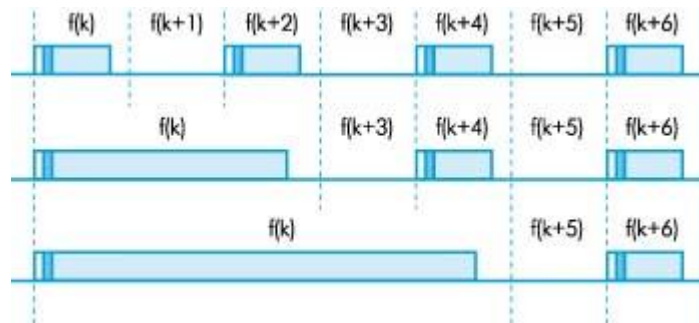


Рис. 8.4. Передача пакетов различной длины

Синхронное соединение (SCO) возможно только в режиме точка-точка. Такой вид связи применяется для передачи информации, чувствительной к задержкам – например, голоса. Основное устройство поддерживает до трех синхронных соединений, вспомогательное – до трех синхронных соединений с одним основным устройством или до двух – с разными основными устройствами. При синхронном соединении основное устройство резервирует временные сегменты, следующие через так называемые SCO-интервалы. Даже если пакет принят с ошибкой, повторно при синхронном соединении он не передается.

При асинхронной связи (ACL) используются временные сегменты, не зарезервированные для синхронного соединения. Асинхронное соединение возможно между основным и всеми активными подчиненными устройствами в пикосети. Основное и подчиненное устройства могут поддерживать только одно асинхронное соединение. Поскольку в пикосети может быть несколько подчиненных устройств, конкретное подчиненное устройство отправляет пакет основному, только если в предыдущем временном интервале на

его адрес пришел пакет от основного устройства. Если в адресном поле ACL-пакета адрес не указан, пакет считается “широковещательным” – его могут читать все устройства. Асинхронное соединение позволяет повторно передавать пакеты, принятые с ошибками.

72 бита	54 бита	0—2745 бит
Код доступа	Заголовок	Передаваемая информация

Рис. 8.5. Структура пакета

Стандартный пакет Bluetooth содержит код доступа длиной 72 бита, 54-битный заголовок и информационное поле длиной не более 2745 бит (рис. 8.5). Однако пакеты могут быть различных типов. Так, пакет может состоять только из кода доступа (в этом случае его длина равна 68 битам) или кода доступа и заголовка.

4 бита	64 бита	4 бита
Преамбула	Слово синхронизации	Трейлер

Рис. 8.6. Структура кода доступа

Код доступа идентифицирует пакеты, принадлежащие одной пикосети, а также используется для синхронизации и процедуры запросов. Он включает преамбулу (5 бита), слово синхронизации (64 бита) и трейлер – 4 бита контрольной суммы (рис. 8.6).

3 бита	4 бита	1 бит	1 бит	1 бит	1 бит
AM_ADDR	TYPE	FLOW	ARQN	SEQN	HEC

Рис.8.7. Структура заголовка

Заголовок содержит информацию для управления связью и состоит из шести полей (рис. 8.7):

AM_ADDR – 3-битный адрес активного элемента (active member address);

TYPE – 4-битный код типа данных;

FLOW – 1 бит управления потоком данных, показывающий готовность устройства к приему;

ARQN – 1 бит подтверждения правильного приема;

SEQN – 1 бит, служащий для определения последовательности пакетов;

HEC – 8-битная контрольная сумма.

Информационное поле, в зависимости от типа пакетов, может содержать либо поля голоса, либо поля данных, либо оба типа полей одновременно.

Безопасность

Естественно, Bluetooth не могла обойтись без такой важной вещи, как технология защиты передаваемых данных, встроенной в сам протокол. В зависимости от выполняемых задач, предусмотрено три режима защиты в которых может находиться устройство.

Security mode 1 (non secure), устройство не может самостоятельно инициировать защитные процедуры.

Security mode 2 (service level enforced security), устройство не инициирует защитные процедуры пока не установлено и не настроено соединение. После того как соединение установлено, процедуры защиты обязательны, и определяются типом и требованиями используемых служб.

Security mode 3 (link level enforced security), защитные процедуры инициируются в процессе установления и настройки соединения. Если удалённое устройство не может пройти требований защиты, то соединение не устанавливается.

Естественно, что Security mode 3 и 2 могут использоваться вместе, то есть сначала устанавливается защищённое соединение, а потом оно ещё защищается в соответствии с требованиями и возможностями конкретной службы.

Основой системы безопасности Bluetooth, используемой в Security mode 3, является понятие сеансового ключа, или Bond. Сеансовый ключ генерируется в процессе соединения двух устройств, и используется для идентификации и шифрования передаваемых данных. Для генерации ключа могут использоваться самые различные составляющие, от заранее известных обоим устройствам значений, до физических адресов устройств. Комбинируя защиту на уровне соединения с защитой на уровне приложений (где может использоваться абсолютно любая из существующих на сегодня систем защиты данных) можно создавать достаточно надёжно защищённые соединения. Но всё равно, очевидной слабостью Bluetooth соединений с точки зрения построения защищённых соединений остаётся возможность перехвата трафика, причём для этого даже не придётся использовать какое-либо специфическое оборудование. Впрочем, эта проблема не нова, и в настоящее время часто приходится использовать открытые сети, вроде Интернет, где возможен перехват трафика, для передачи закрытых данных.

Протоколы и службы

При работе устройств Bluetooth используются специфические протоколы для Bluetooth и общие, используемые в различных телекоммуникационных системах. Все они образуют стек протоколов.

Таблица 8.2. Протокольный стек Bluetooth

Протокольный стек Bluetooth может быть разделен на 4 слоя	
Протокольный слой	Протоколы в стеке
Корневые протоколы "Синего Зуба" (Core protocol)	Baseland, LMP, L2CAP, SDP
Протокол замены кабеля	RFCOMM
Протокол управления телефонией	TCS binary, AT-команды
Воспринятые протоколы (Adopted protocol)	PPP, UDP/TCP/IP, OBEX, WAP, vCARD, vCAL, IrMC, WAE

Примером вертикального списка протоколов может служить список vCard/vCal > OBEX > RFCOMM > L2CAD > Baseband, который используется в протокольных задачах обмена информацией о деловых карточках. Этот протокольный стек содержит соглашение

о внутреннем представлении объектов (vCard) и протокола передачи через эфир (остальная часть стека).

Различные приложения могут использовать различные протокольные стеки. Тем не менее, каждый из этих стеков использует передачу данных (data link) и физический слой, общий для Bluetooth. Смысл каждого из протоколов, специфических для Bluetooth, может быть объяснен отдельно. Все они были разработаны группой специальных интересов Bluetooth SIG. Протоколы RFCOMM и бинарный протокол управления телефонией TCS BIN также были разработаны этой группой, но они основаны, соответственно, на стандарте ETSI TS 07.10 и на рекомендации Q.931 Международного союза электросвязи.

Помимо этих протокольных слоев спецификация Bluetooth определяет также интерфейс контроллера головной машины (HCI — Host Controller Interface), который дает командный интерфейс к контроллеру базовой полосы (baseband controller), диспетчеру соединений (link manager), и доступ к аппаратным регистрам статуса и управления.

Три слоя — слой замены кабеля, слой контроля телефонии и слой воспринятых протоколов (adapted protocol layer) — совместно определяют совокупность протоколов, ориентированных на приложения, которые позволяют прикладным задачам исполняться над корневыми протоколами Bluetooth.

Спецификация Bluetooth является открытой и дополнительные протоколы (например, HTTP, FTP и т.д.) могут быть подключены поверх специфических транспортных протоколов Bluetooth или поверх протоколов, ориентированных на приложения.

Корневые протоколы Bluetooth требуются для большинства приборов, тогда как остальные протоколы используются только там, где они нужны.

Базовая полоса

Базовая полоса и уровень управления подключениями Link Control Layer обеспечивают физическую радиочастотную связь между устройствами Bluetooth, образующими пикосеть. Поскольку радиочастотная система Bluetooth является системой прыгающей частоты распределенного спектра, внутри которой пакеты передаются в определенные временные интервалы на определенных частотах, этот уровень использует процедуры опроса и пейджинга для синхронизации (согласования) прыгающей частоты передачи и таймеров различных приборов Bluetooth.

Этот уровень предоставляет два различных способа физического подключения с соответствующими пакетами базовой полосы — синхронным, (SCO) и асинхронным (ACL).

Протоколы могут передаваться в режиме мультиплексирования по одному и тому же радио-звену (RF link). ACL-пакеты используются только для передачи данных, тогда как SCO-пакет может содержать только аудиоинформацию, или же представлять собой смесь аудио и данных. Для каждого типа данных, включая сообщения об управлении подключениями и контроле, выделяются специальные каналы.

Модель работы с аудио в Bluetooth сравнительно проста и два устройства Bluetooth могут посылать аудио-данные друг другу и получать их, просто открыв аудио-звено (audio link).

Протокол диспетчера подключений

Протокол диспетчера подключений (LMP — Link Manager Protocol) ответственен за установление подключений между устройствами Bluetooth. Сюда же относятся вопросы безопасности, такие как аутентификация и шифрования, связанные генерированием ключей шифрования и подключения, а также с обменом ключами и их проверкой. LMP имеет более высокий приоритет чем остальные протоколы (например, L2CAP), поэтому если канал занят чем-либо другим, то при необходимости передать LMP сообщение он немедленно освобождается.

Кроме того, менеджер подключений контролирует режимы питания и исполнительные циклы приборов Bluetooth, а также состояние подключения того или иного прибора к пикосети.

Протокол управления логическим подключением и адаптацией

Протокол управления логическим подключением и адаптацией (L2CAP — Logical Link Control and Adaptation Protocol) адаптирует протоколы верхнего уровня над базовой полосой.

Logical Link Control and Adaptation Layer Protocol aka L2CAP, является базовым протоколом передачи данных для Bluetooth. Baseband protocol позволяет устанавливать синхронные (Synchronous Connection-Oriented, aka SCO) и асинхронные (Asynchronous Connection-Less, aka ACL) соединения. L2CAP работает только с асинхронными соединениями. Многие протоколы и службы более высокого уровня используют L2CAP как транспортный протокол. В полном соответствии с идеологией Bluetooth L2CAP является простым протоколом, который предъявляет минимум требований к вычислительным мощностям и размеру оперативной памяти устройств, которые его используют. Основные особенности, заложенные в L2CAP таковы:

Protocol Multiplexing. L2CAP является транспортом для многих протоколов и служб, поэтому он обеспечивает возможность разобраться, к какому протоколу или службе относится переданный пакет, что обеспечивает доставку пакета именно тому, кто его ждёт.

Segmentation and Reassembly. Максимальной длиной пакета для L2CAP является 64 килобайта, для baseband protocol это число ещё меньше, всего 341 байт. Однако, иногда требуется передача больших пакетов, поэтому L2CAP обеспечивает разбивку большого пакета на несколько более мелких, и последующую сборку первоначального пакета.

Quality of Service. Благодаря L2CAP Bluetooth устройства могут отслеживать свободные ресурсы соединения и не позволять, чтобы ширина канала или временные задержки для отслеживаемой службы опускались ниже критических значений.

Groups. L2CAP поддерживает адресацию не одному клиенту, а сразу целой группе.

Протокол обнаружения услуг

Одним из важнейших протоколов Bluetooth, который использует L2CAP в качестве транспортного протокола, является Service Discovery Protocol (SDP)

Сейчас никто не сможет представить все возможные способы использования Bluetooth устройств, поэтому при разработке этого протокола пытались учесть как можно больше ситуаций, которые могут возникнуть. Сейчас действует версия 1.0 этого протокола, и основные особенности, которыми он располагает, в настоящее время таковы:

- SDP должен позволять поиск служб по специальным атрибутам этих служб. Например, если имеется несколько принтеров, доступных через Bluetooth, то клиент должен иметь возможность найти именно тот принтер, который ему нужен.
- SDP должен позволять клиенту искать службы по классу. Если немного переделать предыдущий пример, то если клиенту понадобится принтер, то должна быть возможность найти именно устройство печати, не зная про него ничего другого.
- SDP должен позволять просматривать службы без необходимости знать специфические характеристики этих служб. Например, если устройство предоставляющее какую-либо услугу может управляться только специальным программным обеспечением по какому-либо очень редкому или закрытому протоколу, то для SPD это не будет проблемой, всё равно можно будет получить информацию о доступности и названии службы.
- SDP должен предоставлять возможности для обнаружения новых служб, которые появились за время работы.

- SDP должен предоставлять возможность узнавать, когда служба становится недоступной из-за того, что клиент вышел за пределы связи, или по какой-либо другой причине.
- SDP позволяет службам, классам служб и атрибутам служб быть однозначно идентифицированными.
- SDP должен позволять одному устройству находить любую службу на любом другом устройстве без обращения к третьему устройству.
- SDP должен подходить для использования устройствами с ограниченной функциональностью.
- SDP должен позволять увеличивать количество доступной информации о службе. Это означает, что если служба требует подробного и объёмного описания своих возможностей, параметров, ограничений и т. п., то вся эта информация не будет вываливаться на всех, кто просто спросит о доступности службы, а будет предоставлена только тем, кто более пристально заинтересуется именно этой службой.
- SDP должен поддерживать использование промежуточных кэширующих агентов для ускорения или повышения эффективности процесса поиска новых служб. Этот пункт не противоречит пункту 7, потому что использование третьего устройства возможно, но не обязательно.
- SDP должен быть полностью независим от протоколов более высокого уровня, используемых Bluetooth соединением.
- SDP должен работать когда в качестве его транспортного протокола используется L2CAP.
- SDP должен позволять находить и использовать службы которые обеспечивают доступ к другим протоколам обнаружения служб. Это позволяет расширять возможности системы, и использовать службы и устройства которые не имеют Bluetooth интерфейса.
- SDP должен поддерживать создание и определение новых служб без необходимости централизованно регистрироваться.

Кроме этого, есть ряд вещей, которые пока что не входят SDP, но очень возможно, что в следующих редакциях спецификации многие из них станут обязательными:

- SDP 1.0 не предоставляет механизма доступа к службам, только информацию о службах.
- SDP 1.0 не предоставляет возможности оценивать службы. То есть, с его помощью нельзя автоматически выбрать наиболее подходящую службу, если доступно сразу несколько служб, предоставляющих похожий сервис.
- SDP 1.0 не позволяет договариваться о параметрах службы.
- SDP 1.0 не позволяет узнать о загруженности службы, или устройства предоставляющего службу.
- SDP 1.0 не даёт возможности клиенту управлять службой.
- SDP 1.0 не позволяет уведомлять о том, что служба или информация о службе становится недоступной.
- SDP 1.0 не позволяет уведомлять о том, что атрибуты службы изменились.
- В настоящее время спецификация не описывает интерфейс, через который программы должны обращаться к SDP.
- SDP 1.0 в настоящее время не обладает развитым механизмом управления списком служб
- SDP 1.0 не позволяет накапливать и регистрировать службы.

Используя протокол Service Discovery Protocol, можно запросить информацию о самом приборе, о его услугах и о характеристиках этих услуг, а после этого может быть установлено соединение между двумя или несколькими приборами Bluetooth.

Протокол, заменяющий кабель

Ещё одним из протоколов, которые используют L2CAP в качестве транспортного является, как видно из приведённой выше схемы, RFCOMM. Этот протокол эмулирует соединение PPP (point-to-point) по серийному порту (RS-232 или EIA/TIA-232-E, более известным как COM-порты). Он обеспечивает также транспортировку при выполнении услуг верхнего уровня, которые используют последовательную линию как транспортный механизм. Через него работает такие службы как, например, LAN Access. Эта служба может работать как эмуляция Direct cable Connection, когда надо обеспечить связь между всего двумя PC, так и использоваться для полноценного входа в уже существующую локальную сеть. Во втором случае используется устройство под названием LAN Access point, через которое компьютер с Bluetooth оказывается подключен к LAN так, как он мог бы подключиться через dial-up соединение.

Контроль телефонии

Двоичный протокол управления телефонией (TCS Binary или TCS BIN) — протокол, ориентированный на биты. Он определяет контроль сигнализации вызова для установления речевого вызова или вызова данных между устройствами Bluetooth. Вдобавок он определяет процедуры управления мобильностью при манипулировании с группами TCS-приборов Bluetooth.

Управление телефонией — команды AT

Группа специальных интересов Bluetooth SIG определила набор AT-команд, с помощью которых можно управлять мобильным телефоном или модемом в режиме моделей мультииспользования.

Команды, используемые при FAX-услугах, специфицируются реализацией. Это могут быть FAX-услуги класса 1.0 и класса 2.0.

Voice или Bluetooth audio

Voice или Bluetooth audio одна из служб Bluetooth которая использует синхронное соединение. Как уже говорилось, одновременно может передаваться до 3 аудиоканалов. Характеристики звуковых потоков могут различаться, и во многом определяются используемым приложением. Максимально звуковой поток может передаваться с точностью в 16 бит при sampling rate 48 кГц. К сожалению, характеристики Bluetooth не позволяют передавать видеоинформацию с нормальным качеством.

Обычно для передачи аудиоинформации используется специальный протокол, который работает непосредственно с baseband protocol, но для этого с успехом может применяться и L2CAP. L2CAP предоставляет меньше возможностей для передачи аудио информации, чем Bluetooth voice, но этот метод незаменим, когда необходимо, к примеру, обмениваться аудиоинформацией между Bluetooth и не Bluetooth сетями. Кроме этого, данный метод хорош, когда требуется дополнительная защита данных. Bluetooth может обеспечить ещё более надёжную защиту, при большем удобстве и меньшей стоимости.

Протокол точка-точка

В технологии Bluetooth протокол PPP (point-to point protocol) должен работать «поверх» RFCOMM. Соединения PPP служат средством, позволяющим перемещать IP-пакеты с уровня PPP на уровень локальных сетей.

Протокол TCP/UDP/IP

В настоящее время семейство протоколов TCP/IP используется наиболее широко во всем мире. Стеки TCP/IP установлены на самых разных устройствах. Внедрение этих стандартов в приборы Bluetooth позволяет осуществлять связь с любым другим устройством, подключенным к Internet. Такой прибор Bluetooth, будь то сотовый головной ком-

плект «наушники - микрофон» или точка доступа к данным, используется затем как «мостик» к Internet.

TCP/IP/PPP используется во всех сценариях спецификации Bluetooth 1.0 как мостик к Internet, а также как транспортный механизм для протокола WAP.

Протокол OBEX

Протокол IrOBEX (Infrared Object Exchange Protocol) или, короче, OBEX, является сеансовым протоколом, разработанным ассоциацией IrDA для простого, поэтапного обмена объектами. OBEX, обеспечивающий функциональность, сходную с HTTP, использует модель клиента-сервера не зависит ни от транспортного механизма, ни от транспортного API-интерфейса. Наряду с самим протоколом — «грамматикой» для OBEX-переговоров между приборами — OBEX дает также модель для представления объектов и операций. Вдобавок OBEX определяет оглавление папок, которое используется для просмотра содержимого папок, находящихся на удаленных устройствах.

На первом этапе протокол RFCOMM используется как единственный транспортный слой для OBEX; более поздние реализации скорее всего будут поддерживать в качестве транспорта также и TCP/IP.

Формат содержимого

Форматы vCard (обмен электронными деловыми карточками) и vCalendar (обмен электронными календарными данными) являются открытыми спецификациями, которые были разработаны консорциумом Versit и контролируются сегодня консорциумом Internet Mail. Сами по себе vCard и vCalendar не определяют никакого транспортного механизма. Они определяют только форматы данных, которые должны транспортироваться.

Два других формата содержимого, которые передаются протоколом OBEX, — это форматы vMessage («сообщение») и vNote («заметка»). Они также являются открытыми стандартами и используются для обмена сообщениями и замечаниями. Они определены в спецификации Инфракрасных мобильных коммуникаций (IrMC — Infrared Mobile Communications). Там же определен формат журнальных файлов, который необходим для синхронизации данных между отдельными приборами.

Протокол беспроводных приложений

Протокол беспроводных приложений (WAP — Wireless Application Protocol), разработанный Форумом WAP, должен работать в самых разнообразных беспроводных сетях.

Цель состоит в том, чтобы распространить содержимое сети Internet и ее телефонные услуги на цифровые сотовые телефоны и на другие беспроводные терминалы

Идея, стоящая за разработкой WAP, — повторно использовать приложения верхнего уровня, разработанные для среды WAE (WAP Application Environment).

К таким приложениям относятся браузеры WML и WTA, способные взаимодействовать с приложениями на ПК. Построение шлюзов для приложений, обеспечивающих связь между WAP-серверами и приложениями на ПК позволяет реализовать различные виды «скрытой» функциональности, такие как дистанционное управление, передача данных с ПК на телефонную гарнитуру и т.д.

Модели использования

Использование «Синего Зуба» облегчается разработкой моделей использования. Каждая модель использования сопровождается ее «профилем». Профиль определяет протоколы и их специальные свойства (feature), поддерживающие данную модель использования.

Группа специального интереса Bluetooth SIG определила значительный набор моделей использования совместно с их профилями.

Кроме того, имеются четыре профиля «общего назначения», которые широко используются в более специальных профилях.

К ним относятся:

- GAP — типовой профиль доступа;
- SPP — профиль последовательного порта;
- SDAP — профиль обнаружения прикладных услуг;
- GOEP — профиль общего назначения для обмена объектами.

Завершение протокольной архитектуры Bluetooth

Протоколы Bluetooth предназначены для быстрой разработки прикладных задач, использующих эту технологию. Нижние уровни протокольного стека Bluetooth спроектированы так, чтобы обеспечить гибкую основу для дальнейшей разработки протоколов. Другие протоколы, такие как RFCOMM, полученные адаптацией существующих протоколов, которые лишь слегка модифицируются для этих целей. Протоколы верхнего уровня используются без модификации. Благодаря такому подходу существующие прикладные задачи могут использоваться для работы с технологией Bluetooth, а интероперабельность достигается с минимальными усилиями.

Спецификация

Спецификация Bluetooth состоит из двух частей: Core («сердцевина») и Profiles («профили»). Им посвящены соответственно первый и второй тома спецификации. Их объем, округленно, — 1100 и 450 страниц. Кроме того, имеется еще несколько материалов, посвященных идеологии отдельных вопросов: в том числе — бумаги по протокольной архитектуре «Синего Зуба» и по его архитектуре безопасности.

Часть Core состоит из пяти частей:

- часть A: радио спецификация;
- часть B: спецификация основной полосы;
- часть C: протокол Link Manager;
- часть D: спецификация протокола Logical Link Control and Adaptation;
- часть E: протокол обнаружения услуг Service Discovery Protocol.

Кроме того, имеются три части добавлений, маркируемых как части: F:1, F:2, F:3, F:4; H:1, H:2, H:3, H:4; I:1, I:2, I:3, а также девять приложений: Appendix: I — IX. Дадим выборочно более подробные характеристики этих добавлений и приложений.

Часть F:1 — RFCOMM со стандартом TS 07.10.

RFCOMM — простой транспортный протокол, обеспечивающий эмуляцию последовательных портов над протоколом L2 CAP (Logical Link Control and Adaptation Protocol). RFCOMM основан на стандарте TS 07.10; протокол поддерживает только некоторые подмножества TS 07.10.

Часть F:2 — Интероперабельность IrDA.

Ассоциация инфракрасной передачи данных IrDA (Infrared Data Association) в апреле 1999 года выпустила спецификацию протокола IrOBEX (IrDA Object Exchange Protocol — протокол обмена объектами IrDA).

Цель документа F:2 состоит в том, чтобы сделать возможной разработку приложений, которые будут функционировать как в коротковолновом диапазоне (short-range RF), так и в инфракрасной среде (IR media). Каждая из этих двух сред имеет свои преимущества и недостатки.

Вместо того чтобы фрагментировать область приложений, F:2 определяет «пересечение», в котором могут сходиться приложения Bluetooth и IrDA. Этим пересечением и является IrOBEX.

IrOBEX — сеансовый протокол. Этот протокол используется теперь и технологией Bluetooth, позволяя приложениям использовать либо радио-технологию самого Bluetooth, либо инфракрасную технологию IrDA. Однако хотя и IrDA, и Bluetooth рассчитаны на

беспроводную связь, они имеют фундаментальные различия, относящиеся к протоколам нижнего уровня. Поэтому F:2 определяет, каким образом IrOBEX (коротко, OBEX) отображается на RFCOMM и TCP/IP. Первоначально этот протокол был разработан для обмена объектами инфракрасной связи и был помещен внутри иерархии протоколов IrDA. Однако он может появляться над другими транспортными слоями, в данном случае — над RFCOMM и TCP/IP.

Спецификация протокола IrOBEX, выпущенная ассоциацией IrDA, дает модель представления объектов и сеансового протокола, которая структурирует диалог между двумя приборами. Протокол IrOBEX следует диалоговой парадигме «запрос-ответ» (request-response) модели клиент-сервер. Bluetooth определяет IrOBEX только в режиме, ориентированном на установление соединений (connection oriented), хотя IrDA определила его и в режиме без установления соединений (connectionless). Причина в том, что IrOBEX отображается на протоколы архитектуры Bluetooth, ориентированные на установление соединений.

Часть F:3 — Спецификация протокола Telephone Control Protocol Specification.

Часть F:4 — Требование интероперабельности системы Bluetooth как носителя WAP.

Часть H:1 — Функциональная спецификация интерфейса с контроллером головной машины.

Часть H:2 — Транспортный слой HCI USB.

Этот документ рассматривает требования со стороны интерфейса универсальной последовательной шины USB к аппаратуре Bluetooth.

Часть H:3 — Транспортный слой HCI RS232.

Часть H:4 — Транспортный слой HCI UART.

Документы I:1, I:2, I:3 относятся к вопросам тестирования.

Часть I:1 — Тестовый режим Bluetooth. Конфигурация состоит из тестируемого прибора (DUT — Device Under Test) и тестера.

Тестер и тестируемый прибор образуют пикосеть, в которой тестер играет роль ведущего устройства, а тестируемый прибор — ведомого. Тестер имеет полный контроль над всей процедурой тестирования. Контроль осуществляется через эфирный интерфейс с помощью команд протокола LMP. Аппаратные интерфейсы с тестируемым устройством могут существовать, но они не являются объектом стандартизации.

Тестовый режим является специальным состоянием модели Bluetooth.

Когда тестируемый прибор выходит из тестового режима, он входит в состояние ожидания. После отключения питания прибор должен войти в состояние ожидания. Активация прибора может выполняться локально (через аппаратный или локальный интерфейс) или через эфирный интерфейс.

В документе приводится описание тестовых команд и сценариев.

Часть I:2 — Требование совместимости со спецификацией Bluetooth.

Документ I:2 регламентирует организационные и правовые вопросы функционирования движения Bluetooth. В нем различаются две категории участников движения Bluetooth. Они подписывают соответствующие соглашения (соглашение промодуля и соглашение восприемника) и получают те или иные лицензии.

Документ специфицирует требования, которым должно удовлетворять изделие, чтобы быть «совместимым со спецификацией». Кроме того, он дает описание Программы квалификации Bluetooth. Требования, выдвигаемые отдельными правительствами, в документ не входят.

В документе используется специальный глоссарий из 16 терминов, относящихся к совместимости, в том числе спецификация протокола, спецификация профиля, процесс квалификации Bluetooth (рис. 8).

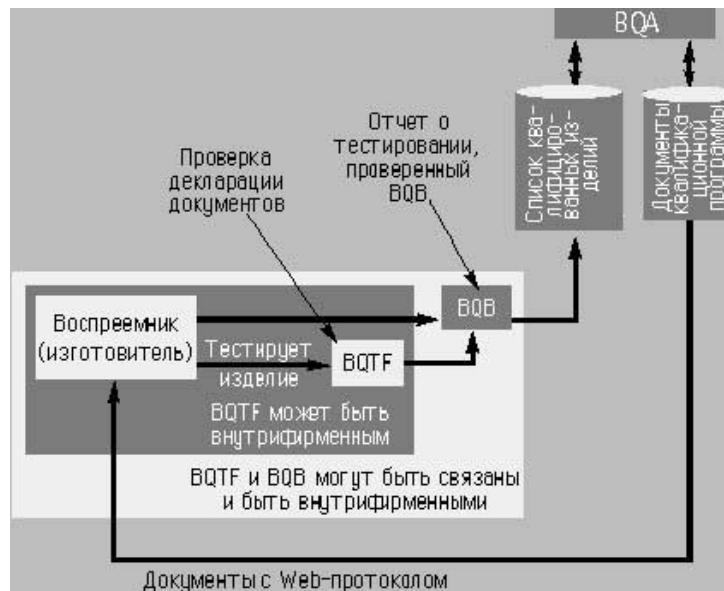


Рис. 8.8. Схема квалификационного процесса Bluetooth

BQTF — установка тестирования квалификации Bluetooth Qualification Tooth Facility; BQA — администратор квалификации Bluetooth Qualification Administrator; BQB — квалификатор Bluetooth Qualification Bod.

Резюме процесса квалификации

Организация - восприемник передает изделие, подлежащее квалификации Bluetooth, на тестовую установку BQTF. Изготовитель должен укомплектовать изделие временными интерфейсами и функциональными устройствами, обеспечивающими саму возможность тестирования. BQTF не обязана обеспечивать «вторичные системы», такие как локальные сети, телефонные сети общего доступа или сети GSM.

Должна быть предоставлена необходимая документация, а именно описание изделия, руководство пользователя и декларация совместимости (Implementation Conformance Statement). Установка BQTF проверяет каждую заявленную в декларации возможность «в соответствии с текущей спецификацией соответствующего теста и политикой, проводимой бюро BQRV. Результаты тестирования и документация по изделию посылаются уполномоченному лицу BQB с заявкой на включение изделия в список «Квалифицированных изделий Bluetooth».

Уполномоченное лицо BQB выпускает Записку о квалифицированном изделии и с разрешения заявителя помещает изделие в базу данных Квалифицированных изделий, в которой с ним может ознакомиться любая другая организация.

Установка BQTF может быть «тестовой палатой» третьей фирмы, или же внутрифирменным подразделением заявителя. Уполномоченное лицо BQB также может быть внешним или внутренним. Как «установка», так и «лицо» должны быть авторизованы бюро BQRD.

Услуги BQTF и BQB не являются бесплатными; заявитель возмещает им расходы и оплачивает все их услуги. Подписание соглашений с BQTF, BQB и, возможно, с BQA о неразглашении информации об изделии, входит в компетенцию заявителя. Бюро BQRD выставляет также счет за каждое квалифицированное изделие. Первоначально устанавливается плата в размере 3 тыс. долл., в дальнейшем она будет раз в год пересматриваться в соответствии с фактическими затратами.

Часть I:3 — Интерфейс управления тестированием.

Настали времена, когда каждый стремится спроектировать собственную расширяющую плату. На материнских платах и на расширяющих платах размещаются «заказные» микросхемы все более богатой функциональности.

Девять приложений, которыми заканчивается первый том спецификаций, таковы.

Приложение I — История версий.

Приложение II — Разработчики.

Приложение III — Сокращения.

Приложение IV — Образцы данных.

Приложение V — Аудио Bluetooth.

Приложение VI — Таймеры Bluetooth.

Приложение VII — Опциональная схема пейджинга.

Приложение VIII — Присвоение номера.

Приложение IX — Последовательности сообщений.

Второй том состоит из 13 профилей:

часть K:1 — Профиль общего доступа;

часть K:2 — Профиль приложения обнаружения услуг;

часть K:3 — Профиль беспроводной телефонии;

часть K:4 — Профиль Interscom;

часть K:5 — Профиль последовательного порта;

часть K:6 — Профиль головного комплекта;

часть K:7 — Профиль коммутируемого выхода на сеть;

часть K:8 — Профиль факса;

часть K:9 — Профиль доступа к локальной сети;

часть K:10 — Профиль общего обмена объектами;

часть K:11 — Профиль помещения объекта в стек;

часть K:12 — Профиль передачи файлов;

часть K:13 — Профиль синхронизации.

Второй том заканчивается тремя приложениями и указателем.

Спецификация Bluetooth сопровождается дополнительными документами технической политики: «Архитектура протокола Bluetooth», «Архитектура системы безопасности Bluetooth», «Архитектура слоя обнаружения услуг Bluetooth».

Часть А спецификации посвящена характеристикам трансивера, работающего на частоте 2,4 ГГц в режиме прыгающих частот. Полоса 2400-2483,5 МГц характеризуется как промышленно-научно-медицинская. В спецификации указываются особые требования отдельных регионов (Испания, Франция, Япония). Какие-либо упоминания о России отсутствуют.

Значительный интерес представляет крупная часть В. Здесь дается определение Bluetooth как радио-звена (radio-link) ближнего действия, предназначенного для замены кабелей, подключающих портативные и фиксированные электрические приборы. Bluetooth действует в нелицензируемой ISM полосе на частоте 2,4 ГГц. Для борьбы с интерференцией и федингом применяется прыгающая частота трансивера. Для полной дуплексной передачи используется схема TDD (Time Division Duplex — «дуплекс с временным разделением»).

В системах Bluetooth определяются пять типов логических каналов: канал управления соединением LC (Link Control); канал передачи информации между диспетчерами связи ведущего и ведомых услуг LM (Link Manager); асинхронный и изохронный каналы пользовательских данных UA/UI; канал синхронных данных пользователя US, реализуемый на связи SCO.

Элементная база Bluetooth

Одно из необходимых условий успеха такой технологии, как Bluetooth – недорогая программно-аппаратная реализация. Это тем более важно, что для многих устройств беспроводное соединение – это фактически дополнительная, хотя и важная функция. И стоимость она должна соответствовать. Однако в случае успеха объем потенциального рынка весьма соблазнителен. И ведущие мировые производители интегральных компонентов не замедлили сделать ставки. Причем столь резко, что выявить лидера крайне затруднительно, поскольку о своем первенстве заявляют многие.



Рис. 8.9. Структура устройства Bluetooth

Столь быстрому старту немало способствовала простота структуры устройств Bluetooth (рис. 8.9). В их состав входят радиомодуль-трансивер, контроллер связи (он же baseband - процессор) и управляющее связью устройство, собственно реализующее протоколы Bluetooth верхних уровней, а также интерфейс с терминальным устройством. Причем если трансивер и контроллер связи (в первых чипсетах для Bluetooth) – это специализированные микросхемы (интегральные или гибридные), то устройство управления связью реализуют на стандартных микроконтроллерах, сигнальных процессорах либо его функции поддерживают центральные процессоры мощных терминальных устройств (например, ноутбуков). Кроме того, в устройствах Bluetooth применяют ИС, используемые в других приложениях, поскольку 2-МГц диапазон освоен достаточно хорошо, а заложенные в Bluetooth технические решения сами по себе особой новизны не содержат. В самом деле, схема модуляции – широко распространенная, технология расширения спектра методом частотных скачков хорошо отработана, мощность мала

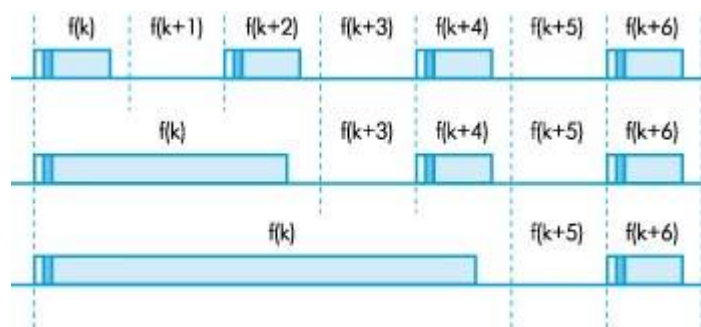


Рис. 8.10. Структурная схема Bluetooth-контроллера PCD 87550

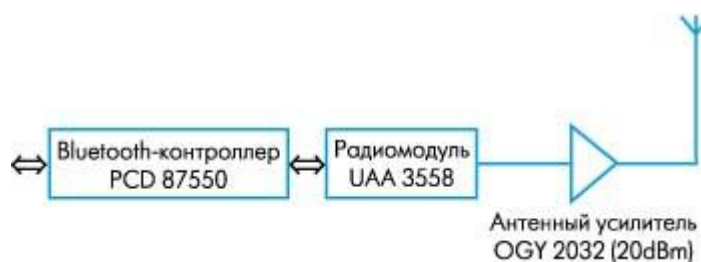


Рис. 8.11. Структура устройства Bluetooth с PCD 87550

Поэтому неудивительно, что первые чипсеты для Bluetooth включали ИС, хорошо знакомые по другим приложениям. Так, одной из первых свое решение для Bluetooth представила фирма Philips Semiconductors, предложив комплект ИС, включающий четыре микросхемы – синтезатор UMA1022, усилитель мощности SA2410, схему модуляции SA639 и трансивер SA2420. Две из них – UMA1022 и SA639 – используются в DECT-устройствах, да и остальные достаточно универсальны. Однако вскоре Philips предложила специализированный чипсет, поддерживающий спецификацию Bluetooth 1.0. Он включает однокристалльный трансивер UAA3558, основанный на оригинальной технологии “низкой промежуточной частоты” (изначально создавался для DECT!), и baseband-процессор серии VWS2600x. Процессор VWS26002 может работать и с трансивером компании Ericsson PBA 313, он содержит ядро 32-разрядного RISC-микроконтроллера ARM7 TDMI (компании ARM), кодек голоса, поддерживает интерфейсы UART, USB, PCM и I2C. Изготавливается процессор по 0,25-мкм КМОП-технологии, поэтому характеризуется малой потребляемой мощностью и низким напряжением: 1,8–2,5 В для цифрового ядра и 2,5–3,3 В для портов ввода/вывода. Вскоре должен стать доступным и перспективный baseband-процессор компании Philips – PCD 87550 (рис. 8.10). При этом структура Bluetooth-адаптера упрощается еще больше (рис. 8.11). А в недалеком будущем Philips намерена выпустить однокристалльную схему, интегрирующую трансивер, схему сопряжения с аналоговой частью и baseband-процессор.

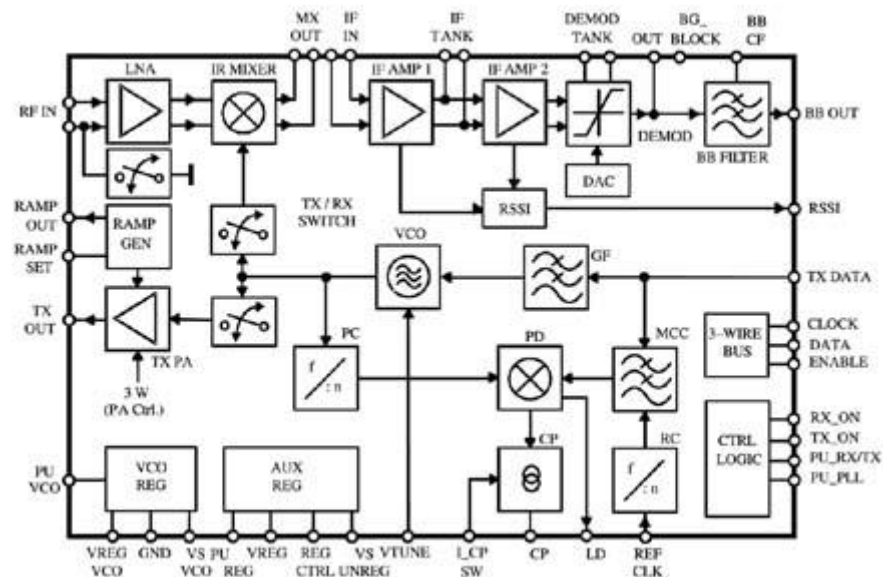


Рис. 8.12. Структура трансивера T2901

Список основных сокращений: DAC Digital to Analog Converter GND Ground (signal/system) LNA Low Noise Amplifier MCC Master Control Console PU Physical Unit (SNA) RAMP Remote Access Maintenance Protocol VCO Voltage Controlled Oscillator

Вообще следует отметить, что ядро ARM TDMI применяется в baseband-процессорах многих фирм. Так, оно интегрировано в Bluetooth baseband-процессор фирмы Ericsson. На основе этого ядра построен и однокристалльный контроллер Bluetooth компании Atmel AT76C551. Его структура во многом аналогична приведенной на рис. 10. Atmel предлагает чипсет, включающий данный контроллер и однокристалльный трансивер T2901 компании Temic Semiconductors (которая теперь вошла в состав Atmel). Структура T2901 представлена на рис. 8.12. Трансивер T2901 обеспечивает радиус действия до 10 м. Если его надо увеличить до 100 м, Atmel предлагает SiGe ИС T7024 (также бывшей Temic Semiconductors), включающей малошумящий предусилитель и 23-dBm усилитель мощности (рис. 8.13).

В отличие от упомянутых выше монолитных ИС, трансивер компании Ericsson PVA31301, хотя и основан на специализированной БиКМОП ИС, но является гибридным модулем, собранным на многослойной керамической подложке (шесть слоев металлизации). В 100-Вт исполнении размеры модуля—10,2x16x1,6 мм.

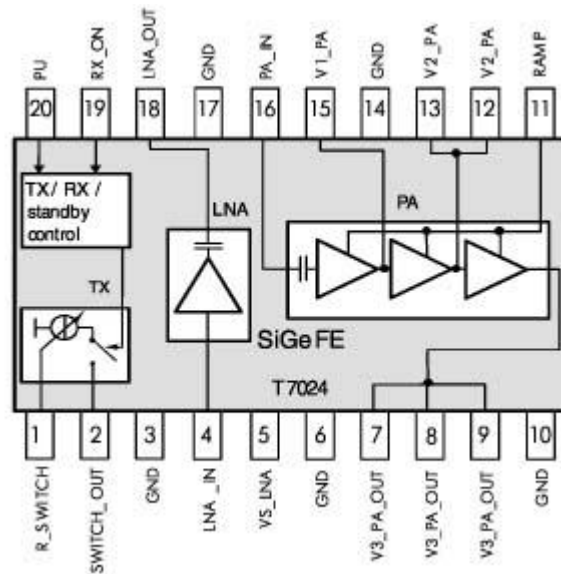


Рис. 8.13. Структура ИС T7024

Список основных сокращений:

GND Ground (signal/system)

LNA Low Noise Amplifier

RAMP Remote Access Maintenance Protocol

Компания Lucent Technologies также производит чипсет для Bluetooth, содержащий однокристалльный передатчик W7020 с низкой потребляемой мощностью (напряжение питания – до 2,7 В), и baseband-контроллер W7400. Свой комплект ИС Odissey выпустила и фирма Silicon Wave. В него входят ИС радиомодема SiW1501 и контроллер связи SiW1601.

Не осталась в стороне и National Semiconductor. Ее чипсет состоит из трансивера со встроенным ФАПЧ LMX3162 и контроллера связи LMX5001. Как и в случае чипсета Odissey, при реализации Bluetooth-устройств на базе этого комплекта схем необходим процессор, выполняющий функции управления связи. Им может быть центральный процессор компьютера или, например, сигнальный процессор ADSP-218x (Analog Devices) с соответствующим программным обеспечением.

Кроме комплектов микросхем, ряд фирм, среди которых Philips и Ericsson, производят конструктивно законченные Bluetooth-модули.

Техническое решение проблемы беспроводной вычислительной сети отработано достаточно давно – стандарт IEEE 802.11, радио-Ethernet, предоставляет широкие возможности для построения профессиональных сетей со скоростью обмена до 11 Мбит/с в нелицензируемом в ряде стран диапазоне ISM (900, 2400 и 5800 МГц). Он же определяет соединения в ИК-диапазоне (до 16 Мбит/с). Основной недостаток IEEE 802.11-относительно высокая сложность и стоимость оборудования. Однако на базе данной спецификации были разработаны беспроводные технологии Bluetooth и HomeRF (SWAP) – более простые и дешевые решения для потребительского рынка.

Таблица 8.3. Сравнительные характеристики технологий Bluetooth и HomeRF

	HomeRF	Bluetooth
Вид модуляции	Шумоподобный сигнал, метод частотных скачков	Шумоподобный сигнал, метод частотных скачков
Число скачков в секунду	50	1600
Мощность передатчика, мВт	100	100
Скорость обмена данными, Мбит/с	1 или 2	1
Способ модуляции	Двух- или четырехуровневая ЧМ	Двухуровневая ЧМ
Количество устройств в сети	До 127	Не ограничено
Защита информации	Blowfish data security	40- и 64-битное шифрование
Радиус действия, м	50	10–100

Спецификация Shared Wireless Access Protocol (SWAP), основной конкурент технологии Bluetooth, предложена группой HomeRF, в которую входят такие гиганты, как Compaq, Ericsson, Hewlett-Packard, Intel и Microsoft. Сравнительные характеристики Bluetooth и HomeRF представлены в табл. 3. Технически это очень близкие системы, что неудивительно, поскольку у них общий “прародитель” – IEEE 802.11. Однако если предлагаемая группой HomeRF локальная сеть – фактически беспроводной аналог домашней сети HomePNA, где все устройства взаимодействуют через компьютер (компьютеры), то идеология Bluetooth иная – это универсальный радиointерфейс, связывающий самые разные устройства друг с другом и не требующий дорогой аппаратной поддержки.

Давайте теперь сравним Bluetooth со своим прародителем - IEEE 802.11. Основные различия между ними можно свести к следующему:

Таблица 8.4. Основные различия технологий Bluetooth и IEEE 802.11

	IEEE 802.11	Bluetooth
1. Назначение	Беспроводные домашние/офисные сети	Замена кабельных соединений для компактных коммуникационных средств
2. Рабочая частота	2.4 ГГц	2.4 ГГц
3. Максимальная скорость передачи данных	11 Мбит/сек (IEEE 802.11b), 2 Мбит/сек (IEEE 802.11)	721 Кбит/сек
4. Дальность действия	100 м	10 м или 100 м
5. Максимальное количество узлов	128 устройств на сеть	8 устройств на одну пикосеть, макс. 10 пикосетей, т.е. до 71 устройства на один scatternet
6. Голосовые каналы	Нет (опционально)	3 канала
7. Доступность	Сейчас	Сейчас
8. Цена	\$100-\$400 за узел	Около \$5 за узел

Как легко заметить, интерфейс Bluetooth намного лучше приспособлен для использования в тех беспроводных устройствах связи, где требуется достаточно низкая цена, нет необходимости в высоких скоростях и желательно низкое энергопотребление. Однако, как уже отмечалось, возможно создание комбинированных сетей, тем более что IEEE 802.11 работает совершенно по другому принципу кодирования передаваемых данных, следовательно, находясь на одной и той же рабочей частоте, оба стандарта будут слышать друг

друга физически, но чужие сигналы будут расценены каждым из них как посторонний шум.

Существует и еще одна технология - IrDA (Infrared Data Association). Она обеспечивает беспроводное соединение между двумя устройствами, такими как мобильные телефоны, КПК и ПК. Однако большое число модификаций, сделанных различными компаниями, несовместимы между собой. Преимущества IrDA — скорость передачи данных (4 Мбит/с) — выше, чем у Bluetooth, устройства на ее основе стоят меньше. Серьезные недостатки — малая дальность передачи данных (1 м), а также то, что порты устройств должны находиться в зоне прямой видимости друг друга.

Таким образом мы приходим к тому, что, при преодолении определенных технических трудностей, различные стандарты беспроводной связи вместо конкуренции взаимодополняют друг друга.

Bluetooth относится к тем технологиям, которые при грамотном использовании могут, в самом деле, перевернуть весь человеческий быт. Уже сейчас на выставках демонстрируются принтеры с Bluetooth, которые не надо подключать к компьютеру, достаточно просто внести его в комнату, включить в розетку, и можно начинать печатать. То же самое верно и в обратном порядке, достаточно просто войти в комнату с ноутбуком, оснащённым Bluetooth в руках, и сразу же можно пользоваться принтером, войти в локальную сеть для обмена файлами и документами, воспользоваться Интернет соединением. RJ-45 розетки для ноутбуков, которые можно встретить в некоторых самолётах и особо продвинутых аэропортах скоро должны отойти в прошлое.

Системы hands free с использованием Bluetooth становятся настолько просты в использовании, насколько это только возможно. Достаточно что бы мобильный телефон с Bluetooth интерфейсом просто находился где-нибудь внутри автомобиля, а его подключение к hands free системе произойдёт автоматически.

Стандартизация, используемая в Bluetooth, позволит делать беспроводные мыши, клавиатуры, джойстики, которые будут подходить к любому PC, и, чтобы начать работу с любимым устройством, достаточно будет просто подойти к компьютеру. Благодаря той же стандартизации, можно рассчитывать на то, что через несколько лет мы избавимся от той кучи дистанционных пультов на диване, отдельного для телевизора, отдельного для видеомэгафона, отдельного для музыкально центра, отдельного для DVD проигрывателя, отдельного для кондиционера и так далее, а будем управлять всей техникой в квартире с мобильного телефона. Но и это ещё не предел.

Интеграция Bluetooth с Интернетом может стать качественно новым этапом в развитии всемирной сетевой инфраструктуры.

В последнее время много говорится о концепции "цифрового дома". Некоторые, хорошо известные и весьма серьёзные корпорации буквально помешались на этом. Технология Bluetooth может поднять эту идею на новую высоту. Представьте себе, у вас имеется брелок (браслет, кольцо, да что угодно), с Bluetooth устройством, способным принимать ваш голос и передавать его на центральный компьютер в доме. Мощный сервер идентифицирует голос, распознает звуковую команду, и по тому же Bluetooth даст команду любой периферии, раскиданной по дому. Таким образом, голосовые команды можно будет давать всему что угодно в доме, телевизорам, лампочкам, шторам, кондиционерам, микроволновым печкам... И при этом не будет никакой необходимости, что бы вся эта периферия обладала достаточной вычислительной мощностью для распознавания голоса, достаточно чтобы подобной мощностью обладал любимый компьютер, стоящий в доме. Более того, командовать своим домом можно будет и через мобильный телефон, практически с любой точки земного шара.

Но есть и свои недостатки у этого объединения. Это же если сейчас пойманный троян грозит только парой потерянных файлов, то в "цифровом доме" возможны гораздо более "интересные" эффекты. Конечно, прямо сейчас можно придумать с десяток мер, кото-

рые сильно затрудняют жизнь взломщикам, но противодействие брони и снаряда продолжается, и конца этому процессу не будет никогда. Но как, всё-таки, удобно всё может быть, если не принимать во внимание "мелкие технические неполадки".

Всё это в перспективе. А сегодня Bluetooth устройства можно встретить в основном только на выставках, или же в продаже, но по ценам, которые никак не могут способствовать их широкому распространению. Кроме этого, большинство демонстрируемых сегодня Bluetooth устройств не могут похвастаться достаточной универсальностью, то есть они далеко не всегда могут просто обнаружить друг друга, не говоря уже про то, чтобы воспользоваться предоставляемыми услугами, если заранее не предусмотрено, что конкретно ЭТА железка должна работать с конкретно этой. На торгово-промышленной выставке CeBIT, прошедшей в начале года, инициатива представить участникам технологию Bluetooth потерпела полную неудачу, поскольку разнообразные устройства создали столько помех, что наладить связь оказалось невозможно. Но ведь это только начало, и как сама технология, так и программное обеспечение будут продолжать совершенствоваться, и когда-нибудь, может быть даже совсем скоро то, что сегодня кажется дикой фантастикой, станет реальностью.

Стандарт IEEE 802.15.4

Сегодня на рынке есть всё необходимое для быстрого распространения сенсорных радиосетей: сенсоры со встроенным цифровым интерфейсом, дешёвые сетевые устройства со встроенными функциями маршрутизации и несколько технологий создания сетей. Сетевые устройства (трансиверы) созданы в соответствии со стандартом IEEE 802.15.4 – 2003. Стандарт ориентирован на поддержку сетевых устройств с автономным питанием, хотя на его основе могут создаваться и низкоскоростные сети со стационарным питанием, но практически с произвольной сетевой топологией.

В 2005 году на основе стандарта альянсом компаний ZigBee утверждена сетевая технология с одноимённым названием, представляющая набор сетевых протоколов для автоматического создания сенсорных сетей, сетей мониторинга и контроля промышленной и медицинской аппаратурой, управления освещением, бытовой аппаратурой и, наконец, воплощения в жизнь концепции «Умный дом». Приведём в оригинале одно из изречений значимости ситуации: «Just as the personal computer was a symbol of the '80s, and the symbol of the '90s is the World Wide Web, the next nonlinear shift, is going to base the advent of cheap sensors» (Paul Saffo, Institute for the Future).

Физический уровень

Для построения персональной сети (Personal Area Network, PAN) выделено три диапазона частот: 2,4 ГГц, 868 и 915 МГц. Для нелицензируемого диапазона 2,4 ГГц выделено 16 частотных каналов, отстоящих друг от друга на 5 МГц. В диапазонах 868 и 915 МГц выделено 1 и 10 частотных каналов соответственно. В диапазоне 915 МГц шаг между частотными каналами составляет 2 МГц. В Европе диапазон 915 МГц является лицензируемым.

Все сетевые устройства в PAN работают в одном частотном канале. В результате в диапазоне 2,4 ГГц возможно развертывание в одном месте 16 различных PAN, не создающих друг другу электромагнитных помех.

В диапазоне 2,4 МГц скорость передачи данных сетевым устройством составляет 250 кбит/с. Используется квадратурная офсетная фазовая модуляция (Offset Quadrature Phase Shift Keying, O_QPSK).

В диапазоне 868 и 915 МГц скорость передачи данных сетевым устройством равна 20 и 40 кбит/с соответственно. Используется относительная двоичная фазовая модуляция (Binary Phase Keying, BPSK).

Для повышения помехоустойчивости приёма по отношению к сосредоточенным помехам используется сигнал с расширенным спектром, состоящий из 32 фазоманипулированных элементов (чипов). Спектр сигнала формируется в соответствии с требованиями на электромагнитную совместимость других беспроводных устройств, работающих в этом же диапазоне. Эти требования регламентируются стандартом IEEE 802.15.2.

Типы физических устройств и их функции в сети

PAN строится с использованием двух типов физических устройств: полнофункционального устройства (Full Function Device, FFD) и устройства с ограниченным набором функций (Reduced Function Device, RFD). Одно FFD может осуществлять связь как с несколькими FFD, так и несколькими RFD. RFD не может осуществлять связь с другим RFD.

Разделение устройств на два типа оправдано различной стоимостью этих устройств, поскольку возможность связи с несколькими устройствами требует от них больших вычислительных ресурсов и большего объема памяти. К примеру, FFD может перед пересылкой данных соседнему устройству использовать оценку качества канала связи (Link Quality Indication, LQI) до этого устройства. Индикатор качества имеет 8 градаций. Использование этой функции позволяет на основе FFD реализовать интеллектуальные устройства для выбора маршрута передачи данных по сети, если в сферу его радиодоступа попадают несколько сетевых устройств. Если попадает лишь одно устройство или же ему достаточно «слышать» лишь одного соседа в сети, то и нет смысла наделять его интеллектом.

Полнофункциональное сетевое устройство может быть настроено для работы в трёх режимах: координатор PAN, координатор и простое устройство.

Функцией координатора PAN (PAN Coordinator) обладает одно FFD в PAN. Это устройство инициирует процесс самоорганизации сети, под которым понимается способность сетевых узлов обнаруживать новые сетевые узлы и включать их в существующую сетевую структуру без вмешательства человека (Self_organizing). В функцию координатора PAN входит сканирование частотных каналов для нахождения свободного канала и создания сети. Найдя свободный канал, координатор PAN формирует 16_разрядный адрес PAN (PAN identifier), который можно интерпретировать как корень дерева адресного пространства сети. После этого координатор PAN может начать «зазывать» в сеть периодически передаваемыми сигналами маяков (Beacons) новые сетевые устройства, которые могут сканировать эфир с целью обнаружения этих сигналов и дальнейшего присоединения к существующей PAN. Для этого служит функция обнаружения сигнала (Energy Detection, ED). В адресном пространстве PAN два типа устройств отличаются специальным битом в поле MAC адреса, значение которого указывает тип устройства (FFD или RFD). PAN может включать 264 сетевых устройств.

Для присоединения к сети удалённых от координатора PAN новых сетевых устройств могут использоваться уже присоединённые к сети FFD в режиме координатора. В этом режиме они, как и изначально координатор PAN, «зазывают» маяками в сеть новые сетевые устройства. В результате формируется кластер из сетевых устройств, которые «слышат» своего координатора. Тем не менее, вся информация о кластере доступна координатору PAN. Подобным образом могут формироваться мультикластеры из сетевых устройств.

При передаче данных между сетевыми устройствами функция координатора сводится к излучению кадров синхронизации доступа к радиоканалу. Эти кадры передаются между сигналами маяков, поэтому временные интервалы между этими сигналами называются кадрами маяков (Beacon Frame). Передача данных по сети, однако, может быть организована и без синхронизации доступа.

При передаче пакета данных (Data Frame) по сети сетевое устройство преобразует его в кадр данных, включающий адрес назначения, преамбулу для синхронизации, 2 про-

верочных байта циклического кода (CRC) для обнаружения ошибок и т.п. Максимальный размер кадра составляет 127 байт. Кадр данных может быть зашифрован 128 - битным ключом в соответствии со стандартом AES (Advanced Encryption Standard).

Базовые топологии сетей

Функциональные возможности физических устройств позволяют строить сети с двумя базовыми топологиями: Star (звезда) и Peer-to-Peer (равный - равному) (рис.8.2).

В центре «звезды» – координатор PAN. Все устройства PAN «слышат» лишь координатора PAN и поэтому могут обращаться друг другу только через него.

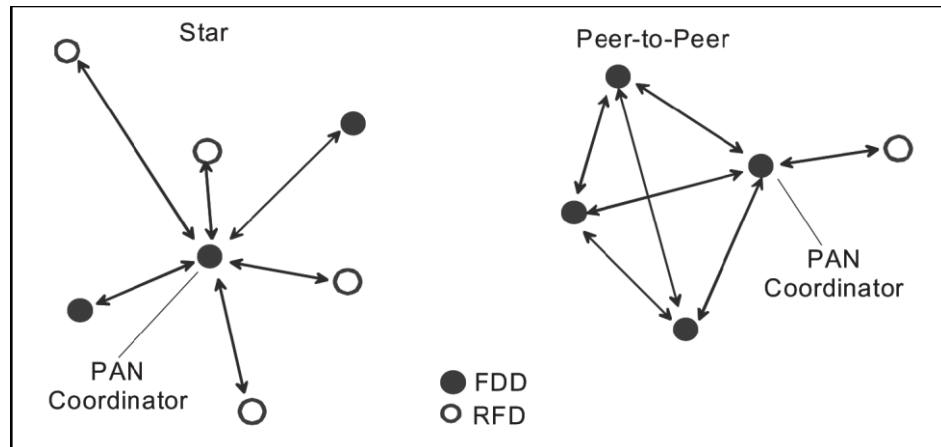


Рис. 8.17. Базовые топологии сетей стандарта IEEE 802.15.4.

Примером сети с топологией «звезда» может служить сеть управления домашней автоматикой и бытовой аппаратурой. Простейшая сетевая топология «точка - точка» является частным случаем топологии «звезда» при взаимодействии двух устройств и, значит, должна содержать координатор PAN. В несколько иной терминологии это означает, что одно из двух устройств должно быть ведущим (master), другое – ведомым (slave). Взаимодействие этих устройств состоится лишь при выполнении двух условий. Во-первых, у ведущего устройства должен быть адрес PAN. Во-вторых, адрес ведомого устройства (к примеру, инфракрасного сенсора телевизора) «прописан» в памяти у ведущего устройства (пульта управления). «Прописка», то есть присоединение устройства к PAN, может выполняться автоматически. Для этого координатор PAN использует сигналы маяков, которые распознаёт любое сетевое устройство. Распознав эти сигналы, оно посылает запрос на присоединение в сеть. В ответ получает сетевой адрес.

В топологии Peer-to-Peer у каждого сетевого устройства есть несколько соседей. Каждого из них оно "слышит" и может с "поговорить с соседом на равных". Поэтому группа соседей может образовать ячейку (Mesh), в которой все могут "поговорить" друг с другом. Такая ячейка и приведена на рис.1. Если, кроме того, устройства постоянно не «спят» и «слушают» своих соседей и не экономят энергопотребление, то сеть из нескольких ячеек может обладать свойством самовосстановления (Self-healing) – способностью выявлять и исправлять неисправности в работе сетевых узлов и связей между узлами без вмешательства человека. Эта способность может быть основана на проверке качества линий связи между FFD благодаря постоянному прослушиванию эфира и наличию функции LQI. В такой сети доставка данных может никак не координироваться из центра, а осуществляться по принципу "взаимовыручки" соседей. Сеть, построенная на базе топологии Peer-to-Peer с децентрализованной доставкой данных, называют сетью Mesh. Роль координатора PAN сводится лишь к функции первого сетевого устройства, являющегося носителем адреса PAN. Для передачи данных по сети координатор PAN не требуется. Конкретные методы реализации подобных сетей стандартом 802.15.4 не рассматриваются и являются предметом сетевых технологий, к примеру, ZigBee.

Возможность самоорганизации и самовосстановления сети на базе топологии Peer-to-Peer позволяет спонтанно и оперативно создавать сети. Примером может служить сеть, узлы которой представляют FFD с сенсором. Большое число таких узлов, разбросанных по некоторой территории, автоматически формирует сеть. Подключив к одному из FFD центр сбора информации, формируется сенсорная радиосеть сбора информации. Если, однако, все сетевые узлы сети (или их большинство) имеют автономное питание, существует проблема ограниченного времени функционирования такой сети (см. раздел «Сети без синхронизации доступа»). Уменьшается оно и с увеличением территории охвата сетью. Тем не менее, существует большое число областей человеческой деятельности, в которых оперативность и отсутствие затрат на координирование является главным критерием. Спонтанно создаваемые сети именуется латинским термином Ad-Hoc, что означает «по случаю». Отличительной чертой таких сетей является ограниченная возможность в расширении во времени и в пространстве.

Алгоритмы доступа к радиоканалу

Базовым алгоритмом доступа к радиоканалу является алгоритм доступа на конкурентной основе с обнаружением несущей частоты и предотвращением коллизий (Carrier Sense Multiple Access / Collision Avoidance, CSMA/CA).

В отличие от стандарта 802.11 в алгоритме CSMA /CA отсутствует механизм предварительного запроса канала доступа, при котором сетевое устройство - отправитель перед отправкой информационного кадра сначала делает запрос устройству - получателю на разрешение передачи. Этот механизм в стандарте 802.11 реализуется с использованием двух кадров: кадра готовности отослать RTS (Ready To Send) и кадра готовности принять и CTS (Clear To Send).

Алгоритм CSMA /CA используется как в сетях без синхронизации, так и в сетях с синхронизацией доступа. В полностью асинхронных сетях использование этого алгоритма в сочетании со «спячкой» сетевых устройств мало эффективно. Наличие синхронизации доступа позволяет экономно расходовать энергопотребление сетевых устройств. Кроме того, в сетях с синхронизацией доступа возможно использование сочетания CSMA/CA с доступом на неконкурентной основе. Эта возможность обеспечивается выделением гарантированного временного слота (Guaranteed Time Slot, GTS) устройству по предварительному от него запросу.

Сети без синхронизации доступа

Рассмотрим использование алгоритма CSMA/CA в сетях без синхронизации доступа к радиоканалу. В таких сетях передача данных производится при отсутствии сигналов маяков, и по этой причине они названы сетями без маяков (Not Beacon - enabled PAN).

Пусть сетевому устройству в случайный момент требуется передать кадр данных. Тогда попытка передачи данных начинается с «прослушивания» эфира.

Если принимается решение о наличии свободного канала (несущая не обнаружена), то через интервал времени, равный некоторому случайному числу из заданного интервала времени T_1 , устройство передаёт кадр данных. Начало времени передачи и выбирается случайным для предотвращения коллизии с кадром данных от другого устройства.

Если было принято решение о том, что канал занят (несущая обнаружена), попытка передачи возобновляется через интервал времени, равный некоторому случайному числу из заданного интервала времени T_2 .

Приём кадра данных может подтверждаться кадром - квитанцией (Acknowledgement Frame). Приём считается правильным в случае отсутствия ошибок в кадре данных. Эта проверка производится кодом CRC. Если кадр - квитанция получена с ошибками, попытка передачи кадра данных производится повторно.

Возможен, однако, и режим доступа без кадра - квитанции. Это позволяет снизить энергопотребление, связанное как с передачей этого сигнала, так и с его приёмом. Этот режим доступа называют неполным алгоритмом CSMA/CA.

Отметим, что использование алгоритма CSMA /CA крайне неэффективно в случае передачи данных «просыпающимися» в случайные моменты времени передатчиками, адресованные в основном «спящим» приёмникам. Для сетей с топологией «звезда» это означает, что координатор PAN должен постоянно «слушать» эфир. Для сетей с топологией Peer-to-Peer все сетевые устройства должны постоянно слушать эфир. Иначе говоря, полностью асинхронный и ничем не координированный режим как доступа, так и спячки, несовместим с алгоритмом CSMA/CA.

Сети с синхронизацией доступа

Доступ к радиоканалу в сетях производится под командованием координатора, который периодически излучает сигналы маяков. Такие сети в стандарте названы сетями с маяками (Beacon - enabled PAN).

В таких сетях доступ к радиоканалу и расписание «сна» сетевых устройств «привязаны» к сигналам маяков от координатора. На рис.18 приведена временная диаграмма возможного алгоритма предоставления доступа. Временной интервал между двумя сигналами маяков (Beacon Interval, BI) от координатора разбит на две части: активную и неактивную (Inactive). Во время неактивной части координатор и все остальные устройства могут «спать». Во время активной части координатор разрешает доступ проснувшимся сетевым устройствам. Активная часть (Active) носит название суперкадра (Superframe). Длительность суперкадра (Superframe Duration, SD) разделена на два интервала. Во время первого интервала (Contention Access Period, CAP) предоставляется доступ на конкурентной основе в соответствии с алгоритмом CSMA/CA. Во время второго интервала (Contention Free Period, CFP) предоставляется доступ с разведением во времени. При этом устройство получает доступ во время закреплённого за ним временного слота (Guaranteed Time Slot, GTS). На рис.18 изображены два таких интервала для разных устройств. Выделение устройству слота предоставляется координатором после предварительного запроса от устройства MAC командой, который делается во время интервала CAP.

Использование алгоритма CSMA /CA при наличии синхронизации имеет особенности, связанные с привязкой случайных параметров алгоритма к временным интервалам (слотам) CAP. Если в на текущем слоте CAP принимается решение о наличии свободного канала (несущая не обнаружена), то кадр данных передаётся в слоте, отстоящим от текущего по номеру на некоторое случайное целое число $C1$. Если было принято решение о том, что канал занят (несущая обнаружена), попытка передачи возобновляется на слоте, отстоящим по номеру от текущего на некоторое случайное целое число $C2$. По этой причине алгоритм носит название слотового CSMA /CA (slotted CSMA/CA) в противоположность рассмотренному выше не слотовому алгоритму (unslotted CSMA/CA) в асинхронной сети.

Параметры синхронного доступа можно выбирать достаточно гибко в зависимости от требований на энергопотребление координатора, сетевых устройств, времени доставки информационных пакетов и достоверности доставки.

Период BI следования сигналов маяков может быть выбран в интервале от 5 мс до 252 с.

Он рассчитывается по формуле $BI = B_{min} * 2^{B0}$,

где B_{min} – минимальный период, $B0$ – число в интервале от 0 до 14. Выбор разумного значения BI позволяет экономить энергопотребление координатору.

Длительность суперкадра SI можно выбирать достаточно произвольно вплоть до величины BI. Очевидно, что с ростом SI растёт и достоверность доставки данных при использовании алгоритма CSMA/CA и заданном времени доставки. Платой за эту возможность является рост энергопотребления сетевых устройств.

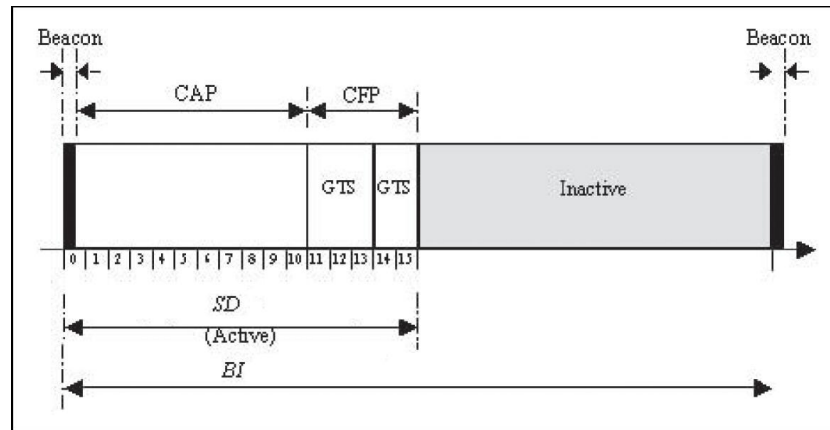


Рис. 8.18. Временная диаграмма при синхронном доступе.

Длительность суперкадра можно перераспределять между CAP и CFP. Для этого суперкадр поделен на 16 тактовых интервалов (рис.8.18). Для CFP может быть отведено до 7 последних интервалов. Возможность перераспределения длительности между CAP и CFP удобна для построения сетей, в которых устройства могут передавать несколько типов сообщений. Для примера, в охранных системах к таким сообщениям относятся сигналы мониторинга от охраняемых объектов, сообщения о постановке на охрану, сообщения о взятии на охрану и, наконец, сигналы тревоги. Для подобных систем можно выбрать параметры рассмотренного алгоритма доступа в зависимости от числа объектов в сети и требований к вероятностям доставки информационных пакетов.

Наконец, длительность слота GTS может состоять из нескольких тактовых интервалов. При отсутствии необходимости у устройства в GTS оно сообщает об этом координатору и он увеличивает CAP, предоставляя больший временный интервал доступа на конкурентной основе с использованием алгоритма CSMA/CA. Эту операцию можно интерпретировать как дефрагментацию суперкадра. Для примера, на рис.8.19 приведена дефрагментация при удалении интервала GTS2 из CFP.

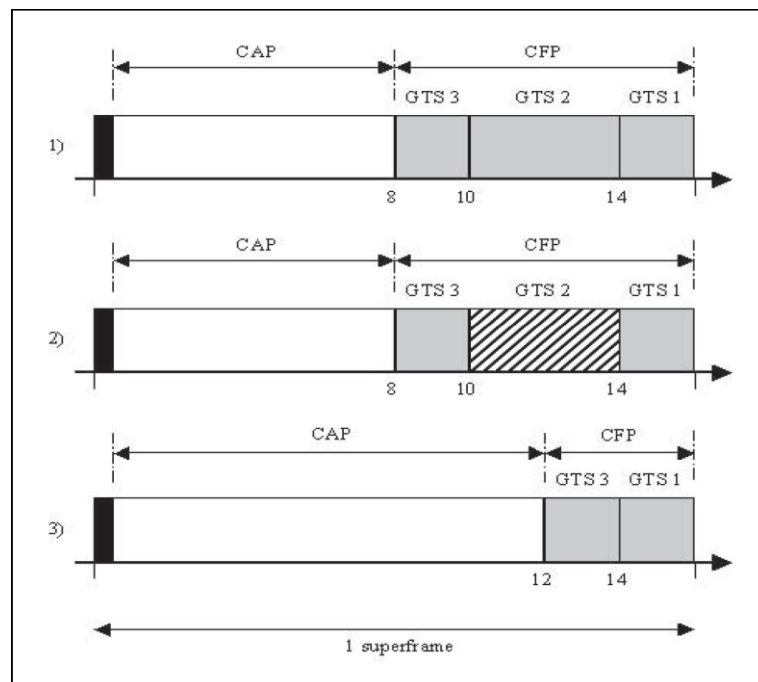


Рис. 8.19. Дефрагментация суперкадра при синхронном доступе.

Итак, стандарт IEEE 802.15.4 является весьма гибким в выборе параметров и позволяет создавать сети, ориентированные как на низкое автономное питание сетевых узлов, так и спонтанно образуемую топологию.

Трансиверы

На рынке трансиверов стандарта IEEE 802.15.4 лидирующие позиции занимают тандем компаний Chipcon и Ember и компания Freescale – отделение компании Motorola по разработке полупроводниковых приборов.

Результатом объединения компаний ChipCon и Ember явилось одно техническое решение трансивера 2420. Микросхемы имеют аббревиатуры CC или EM в зависимости от завода изготовителя. Трансивер позволяет использовать контроллер вместе с программным обеспечением стека протоколов ZigBee.

В конце 2005 года компания Chipcon объявила о выпуске двух изделий CC2430 и CC2431 – однокристальных систем (System-on-Chip, SoC) 802.15.4/ZigBee, не требующих контроллера. В систему CC2431 дополнительно встроена радиометка (Radio Frequency Identification, RFID) – миниатюрный приёмо-передатчик с антенной. Компания Ember также объявила о выпуске SoC EM250.

Компания Freescale выпускает трансивер MC13193, позволяющий использовать программное обеспечение стека протоколов ZigBee. Трансиверы MC13191/2 предполагает разработку сетевого уровня разработчиком сети.

9. СТАНДАРТЫ ГОРОДСКИХ СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА IEEE 802.16 (WiMAX)

Любому пользователю компьютера в идеале хочется мгновенно перекачивать из Интернета на свой ПК все, что заблагорассудится. Телефонный модем позволяет делать это со скоростью около 10 Кб/с, выделенная линия – в несколько сотен Кб/с и только широкополосный доступ позволяет приблизиться к вожделенным Мб/с, которые дают надеяться на просмотр кинофильмов и прочих мультимедийных удовольствий.

Широкополосным доступом в Интернет можно пользоваться уже несколько лет, но он пока недоступен большинству пользователей. На конец 2002 года во всем мире (по данным InStat/MDR) есть около 46 млн. пользователей, больше всего их в США, но и здесь - лишь 17% домов имеют такую возможность. Что же мешает активному распространению широкополосного доступа? Проблема в том, что способы доведения такого доступа до пользователей - DSL или кабельное соединение - имеют ограниченные возможности, поскольку не всегда у пользователей есть кабельное или DSL-оборудование, а кроме того, эти услуги недешевы. Чаще всего они доступны лишь в центрах крупных городов. Корпорация Intel активно работает над новой беспроводной технологией, которая может стать реальной заменой DSL и кабелю и решить проблему «последней мили» в больших городах.

Стандарт беспроводной связи IEEE 802.16 изначально был задуман для организации работы беспроводных сетей на больших городских территориях, он еще называется IEEE WirelessMAN (Metropolitan area network - сеть для городских регионов). Именно этот беспроводной широкополосный доступ и может стать столь необходимым средством “последней мили” в крупных городах.

Широкополосный беспроводной доступ лишен недостатков, присущих DSL и кабельным соединениям. Его проще разворачивать, увеличивать площадь покрытия, он более гибок. Сети IEEE 802.16 очень похожи на традиционные сети мобильной связи: здесь тоже есть базовые станции, которые действуют в радиусе нескольких километров (до 50 км), при этом их не обязательно устанавливать на вышках - для них вполне подходят крыши домов, водонапорные башни или элеваторы. Оборудование пользователя аналогично обычному набору для спутникового телевидения, с его помощью будет осуществляться соединение с базовой станцией.

Стандарт IEEE 802.16 предоставляет бизнесу и домашним пользователям новый и, что очень важно, быстрый способ получить широкополосный доступ к информации. Кроме всех прочих преимуществ, связь через IEEE 802.16 может реализоваться и через совместимое оборудование, например, через точки доступа IEEE 802.11.

История стандарта IEEE 802.16 ведется с 2001 года, когда, собственно, и была начата активная работа по созданию нового беспроводного стандарта широкополосной связи. В декабре 2001 года была принята первая версия стандарта IEEE 802.16-2001, который изначально предусматривал рабочую полосу частоты 10-66 ГГц.

Данный стандарт описывал организацию широкополосной беспроводной связи с топологией «точка-многоточие» и был ориентирован на создание стационарных беспроводных сетей масштаба мегаполиса (Metropolitan Area Network, MAN). Именно поэтому данный стандарт получил также название WirelessMAN. На физическом уровне стандарт IEEE 802.16-2001 предполагал использование всего одной несущей частоты (Single-Carrier, SC), вследствие чего в название протокола добавили буквы SC, то есть WirelessMAN-SC.

Организация связи в частотном диапазоне 10 - 66 ГГц возможна только в зоне прямой видимости между передатчиком и приемником сигнала из-за быстрого затухания коротких длин волн. Это было одной из особенностей протокола WirelessMAN-SC. Однако частотный диапазон с такими характеристиками (то есть с требованием прямой видимости приемника и передатчика и невозможностью работы на отражениях) позволял избежать

одной из главных проблем радиосвязи — многолучевого распространения сигнала. Ширина каналов связи, которые могут быть применены в этом частотном диапазоне, является достаточно большой (типичное значение — 25 или 28 МГц), что позволяет достигать высокой (порядка 120 Мбит/с) скорости передачи данных.

Необходимость построения беспроводной сети только в зоне прямой видимости привела к тому, что устройства стандарта IEEE 802.16 так и не получили широкого распространения. Поэтому несколько позднее, в январе 2003 года, было принято расширение стандарта IEEE 802.16, получившее наименование IEEE 802.16a-2003. Оно предусматривало использование частотного диапазона от 2 до 11 ГГц. Этот стандарт также был ориентирован на создание стационарных беспроводных сетей масштаба мегаполиса. Предполагалось, что данный стандарт станет альтернативой традиционным решениям широкополосного доступа для последней мили — кабельным модемам, xDSL и каналам T1/E1. Кроме того, сети стандарта IEEE 802.16a планировалось применять в качестве дополнительной технологии для подсоединения точек доступа стандарта IEEE 802.11b/g/a к Интернету.

Основным отличием стандарта IEEE 802.16a от базового стандарта 802.16 было использование другого частотного диапазона, который не требует прямой видимости между приемником и передатчиком. Зона покрытия таких беспроводных сетей значительно шире, чем сетей стандарта IEEE 802.16. Опуская пока детали протокола IEEE 802.16a, отметим лишь, что использование частотного диапазона 2-11 ГГц потребовало и существенного пересмотра техники кодирования и модуляции сигнала на физическом уровне.

Логическим продолжением стандарта IEEE 802.16a стал стандарт IEEE 802.16d, который предусматривал возможность реализации фиксированного доступа внутри помещений.

Окончательно стандарт IEEE 802.16d был принят в июле 2004 года и получил название IEEE 802.16-2004, после чего необходимость рассмотрения отдельных стандартов, то есть IEEE 802.16d и IEEE 802.16a, отпала, поскольку окончательная версия стандарта вобрала в себя и стандарт IEEE 802.16d, и IEEE 802.16a.

В настоящее время на стадии разработки находится стандарт IEEE 802.16e, который рассматривает вопросы роуминга между сетями различных беспроводных стандартов, чтобы пользователь без ущерба для сеанса связи мог переходить из беспроводных сетей стандарта IEEE 802.11 в сети IEEE 802.16 и обратно.

Решение вопросов роуминга представляется весьма важным для дальнейшего продвижения беспроводных технологий. Сегодня пользователи сетей стандарта IEEE 802.11 могут пользоваться услугами беспроводного доступа, только находясь на территории хот-спота, или зоны доступа. Покидая такую зону, они теряют возможность соединения. С помощью технологии IEEE 802.16e пользователи получают возможность оптимального соединения: посредством IEEE 802.11 — находясь в пределах соответствующего хот-спота, посредством IEEE 802.16 — находясь в зоне действия городской сети WMAN.

Если протокол IEEE 802.16 — это протокол операторского класса, то протокол IEEE 802.16e ориентирован на конечных пользователей, причем мобильных, и в этом смысле он представляет собой альтернативу стандартам IEEE 802.11a/b/g. По мнению экспертов Intel, в недалеком будущем пользователь, имея ноутбук или КПК со встроенными возможностями стандарта IEEE 802.16e, сможет постоянно оставаться на связи в любой точке города. Мало того, принятие IEEE 802.16 в качестве общеевропейского стандарта позволит активным путешественникам пользоваться роумингом по всей Европе.

История показывает, что одобрение стандарта компетентными организациями не всегда приводит к принятию технологии целевым рынком. Для этого необходимо, чтобы продукты были сертифицированы на их соответствие стандарту, а затем протестированы на взаимодействие. Последнее означает, что конечный пользователь может купить устройство с необходимыми ему характеристиками у того производителя, который ему нра-

вится, и быть уверенным, что оно совместимо с другими сертифицированными продуктами. IEEE подобной деятельностью не занимается, предоставляя ее индустрии. В случае семейства стандартов IEEE 802.11 такую роль играет Wi-Fi Alliance. Для группы стандартов IEEE 802.16 подобную роль играет Worldwide Interoperability for Microwave Access Forum, сокращенно WiMAX Forum — некоммерческая организация, образованная по инициативе корпорации Intel с участием ведущих производителей телекоммуникационного оборудования (Airspan Networks, Alvarion Ltd, Aperto Networks, Fujitsu Microelectronics America, Intel, OFDM Forum, Proxim Corporation, Wi-LAN, Inc. и др.).

Целью организации WiMAX является содействие разработке беспроводного оборудования для доступа к широкополосным сетям, скорейшее развертывание сетей во всем мире, сертификация оборудования IEEE 802.16, а также подготовка спецификаций, призванных обеспечить совместимость оборудования разных производителей. По данным аналитиков, члены WiMAX представляют собой более 75% рынка производителей оборудования широкополосного беспроводного доступа. Поэтому часто по аналогии с тем, как WLAN IEEE 802.11 называют Wi-Fi, для сетей WMAN IEEE 802.16 используют название WiMAX. Рассмотрим несколько подробнее особенности этой технологии.

Структура сетей WiMAX.

Стандарт покрывает диапазон частот от 2 до 11 ГГц. Стабильность частоты должна лежать в пределах $\pm 10^{-6}$. Базовая станция (**BS**), следующая стандарту IEEE 802.16, размещается в здании или на вышке и осуществляет связь со станциями клиентов (**SS** - Subscriber Station) по схеме точка-мультиточка (**PMP**). Возможен сеточный режим связи (**Mesh** - сетка связей точка-точка - **PTP**), когда любые клиенты (**SS**) могут осуществлять связь между собой непосредственно, а антенные системы, как правило, являются всенаправленными. Базовая станция предоставляет соединение с основной сетью и радиоканалы к другим станциям. Диапазон рабочих расстояний может достигать 30 миль (в случае прямой видимости) при типовом радиусе сети 4-6 миль (для режима Mesh при высоте размещения антенны **BS** - 50м), где пропускная способность может быть гарантированной. Предусмотрен также режим мультиточка-мультиточка (**MP- MP**), который имеет ту же функциональность, что и **PMP**. Клиентская станция (**SS**) может быть радио терминалом или повторителем (более типично) для организации локального трафика. Трафик может проходить через несколько повторителей, прежде чем достигнет клиента. Антенны в этом случае являются направленными с возможностью дистанционной настройки. Терминальная станция клиента (**SS**) обычно имеет остронаправленную антенну. По этой причине положение антенны должно быть жестко фиксировано и устойчиво к ветру и другим потенциальным источникам вибрации. Широкополосные системы доступа к радиосети помимо **BS** и **SS** содержат клиентское терминальное оборудование (**TE**), оборудование основной сети, межузловые каналы и повторители (**RS**). Повторители используются часто тогда, когда между конечными точками канала нет прямой видимости. Повторитель передает сигнал от **BS** к одной или нескольким **SS**. В системах **MP-MP** большинство станций являются повторителями. **PTP**-соединения (точка-точка) между базовыми станциями могут поддерживать обмен согласно стандартам от **DS-3** до **OC-3**.

Канал связи предполагает наличие двух практически независимых направлений обмена: отправитель-получатель (**uplink** - восходящий канал) и получатель-отправитель (**downlink** - нисходящий канал; по аналогии со спутниковыми каналами). Эти два субканала используют разные неперекрывающиеся частотные диапазоны. Данный стандарт относится к уровню L2, хотя его взаимосвязь с физическим уровнем (**PHY**) достаточно тесная.

При формировании радиосетей определенную проблему составляет интерференция сигналов смежных каналов и наложении перекрестных наводок с тепловыми шумами. Для таких каналов отношение **I/N** (отношение сигнала интерференции к тепловому шуму) ле-

жит в диапазоне $-6 \div -10$ дБ. Следует, разумеется, учитывать, что уровень интерференционного сигнала варьируется в очень широких пределах.

Радиоволны в диапазоне 10 - 66 ГГц распространяются прямолинейно и подвержены поглощению при наличии дождя или сильного снега. Любые строения или объекты ландшафта препятствуют их распространению, даже если перекрывают видимость между передающей и принимающей антеннами частично. Рекомендуются вертикальная или горизонтальная ориентации поляризации. Предельное расстояние связи (R_H) для высоты положения антенн H_1 и H_2 , сопряженное с кривизной земной поверхности, определяется формулой $R_H = 4.12(\sqrt{H_1} + \sqrt{H_2})$, где R_H измеряется в км, а H_1 и H_2 в метрах.

Для успешной работы канала нужно обеспечить достаточно большое отношение уровней несущей и интерференционного сигнала (C/I). На практике приходится учитывать отношение $C/(I+N)$, где N - уровень теплового шума, а также уровень шумов приемника (~ 6 дБ). Тепловой шум приемника может иметь уровень -138 дБВт/МГц. Уровень интерференционного сигнала может быть примерно тем же. Эти факторы определяют выбор типа антенны, мощность передатчика и предельную длину канала. Чрезмерное увеличение мощности передатчика (с целью улучшения отношения сигнал-шум) не желательно, так как это приводит к возрастанию уровня интерференционного сигнала.

Типовыми рекомендуемыми значениями для BS являются:

Мощность передатчика	+	24 дБм
Коэффициент усиления антенны SS	+	34 dBi
Коэффициент усиления антенны BS	+	19 dBi
Полоса несущей	2	8 МГц

Для SS рекомендуется верхнее значение спектральной плотности $< +30$ дБВт/МГц, аналогичные требования справедливы и для повторителей (RS).

Будем считать, что типовое значение шума приемника равно 6 дБ, тогда спектральная мощность теплового шума приемника вычисляется по формуле:

$$N_o = 10\log(kT_o) + N_F$$

$$N_o = -144 + 6 = -138 \text{ дБВт/МГц, где}$$

N_o - спектральная мощность теплового шума приемника (дБВт/МГц)

kT_o - закон равномерного распределения (-144 дБВт/МГц)

N_F - значение шума приемника (6дБ).

Спектральная плотность потока (**psfd**) в апертуре антенны вычисляется как:

$$psfd = \frac{P_r}{A_e} = \frac{P_r}{\lambda^2 \frac{G}{4\pi}} = P_r - 10\log(\lambda^2) - G + 10\log(4\pi)$$

где

P_r = уровень мощности помех усилителя (-144 дБВт/МГц)

A_e = эффективная апертура антенны

λ = длина волны

G = коэффициент усиления антенны

Если рабочая частота равна 28 ГГц ($\lambda = 0,011$ м), а значение усиления антенны равно 20 дБ, тогда приемлемый уровень помех определяется как:

$$P_{\text{stdBS}} = -144 - 10\log(0.011^2) - 20 + 10 \text{Log}(4p) = -114 \text{ (дБВт/м}^2\text{)МГц.}$$

Заметим, что в данном анализе рассматривалась только базовая станция (составляющая SS не учитывалась). Это в первую очередь связано с тем, что BS обычно размещаются на высоких зданиях и имеют всенаправленные антенны, что увеличивает вероятность обеспечения прямой видимости. С другой стороны SS чаще размещаются на небольших высотах, что уменьшает вероятность гарантированной прямой видимости.

Стандартный полнодуплексный канал базовой станции может иметь пропускную способность 75 Мбит/с. Такой канал обеспечивает до 60 соединений T1 и сотни связей с домами, использующими DSL-подключения (при полосе 20 МГц). В последнем случае предоставляется качество обслуживания (QoS) на уровне “наилучшего возможного”. При этом предоставляется минимальные задержки, что важно при передаче голоса (например, в режиме VoIP). Схема взаимодействия радиосетей в случае использования стандарта IEEE 802.16 показана на рис. 9.1.

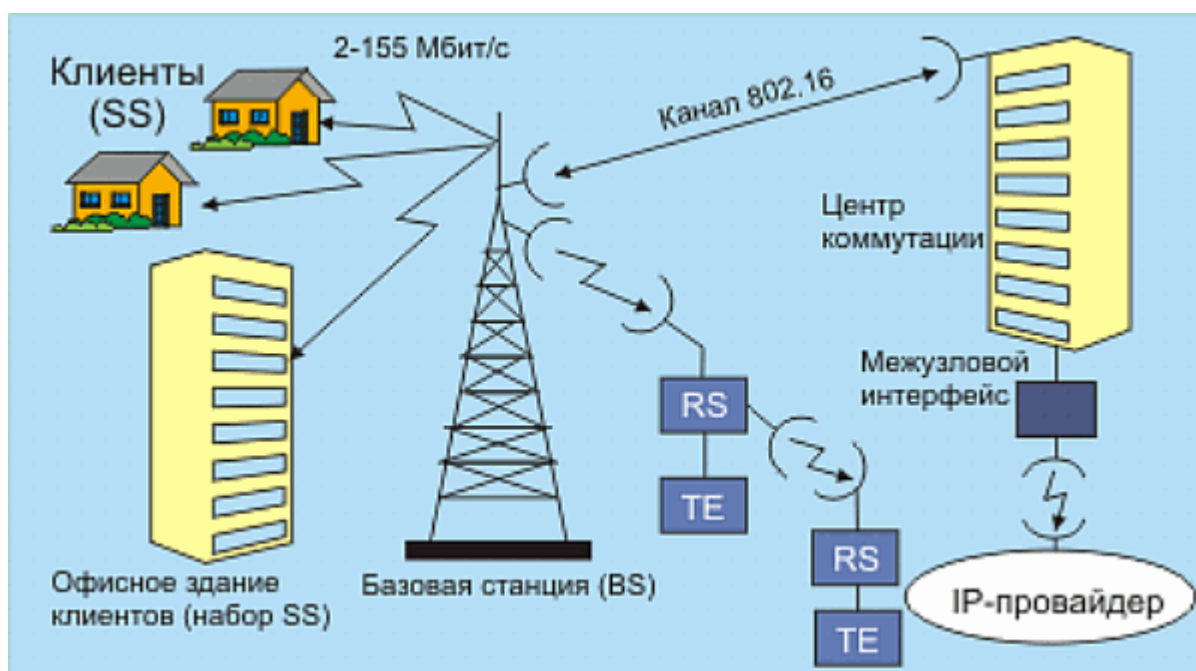


Рис. 9.1. Схема взаимодействия радиосетей стандарта 802.16.

Стандарт IEEE 802.16

Стандарт IEEE 802.16 регламентирует работу на физическом и канальном уровнях и содержит ряд формальных разделов и описание основных протоколов для систем фиксированного беспроводного доступа.

Подуровень конвергенции (Convergence Sublayer - CS) расположен над MAC уровнем и предназначен для организации взаимодействия между более высокими уровнями сети и MAC уровнем. В стандарте определены два типа уровня конвергенции: ATM и пакетный. Первый обеспечивает взаимодействие MAC уровня IEEE 802.16 и ATM протокола, второй – взаимодействие с пакетными протоколами.

MAC уровень - сервисы между MAC уровнем и подуровнем CS, формат фрейма MAC (MAC Protocol Data Units - PDU), сервисы и механизмы поллинга, обеспечивающие поддержку качества обслуживания - QoS:

- Unsolicited Grant Service (UGS), предназначен для поддержки потоков реального времени, генерирующих пакеты данных фиксированного размера, таких, как передача потоков E1 и голоса поверх IP без подавления пауз.
- Real-Time Polling Service (rtPS), предназначен для поддержки потоков реального времени, формирующих пакеты данных переменной длины, таких, как MPEG видео.
- Non-Real-Time Polling Service (nrtPS) предназначен для поддержки потоков, требующих пакетов переменной длины, таких, как широкополосная FTP.
- Best Effort (BE) service предназначен для эффективного обслуживания трафика best effort.

На MAC уровне предусмотрена поддержка дуплекса, синхронизации, разрешение коллизий, возможных на этапе установления системы или на интервалах запроса на передачу. На этом уровне также обеспечивается измерение дальности до абонентских станций, необходимое для корректной работы протокола, обновление описания канала и разделение абонентского оборудования на абонентские группы.

Весь поток данных в сетях IEEE 802.16 – это поток пакетов. На основном подуровне MAC формируются пакеты данных (MAC PDU – MAC Protocol Data Unit, блоки данных MAC-уровня), которые затем передаются на физический уровень, инкапсулируются в физические пакеты и транслируются через канал связи. Пакет MAC PDU (далее – PDU) включает заголовок и поле данных (его может и не быть), за которым может следовать контрольная сумма CRC. Заголовок PDU занимает 6 байт и может быть двух типов – общий и заголовок запроса полосы пропускания. Общий заголовок используется в пакетах, у которых присутствует поле данных. В этом заголовке указывается идентификатор соединения (CID), тип и контрольная сумма заголовка, а также приводится информация о наличии в поле данных подзаголовков и сообщений ARQ.

Заголовок запроса полосы (также 6 байт) применяется, когда АС просит у БС выделить или увеличить ей полосу пропускания в нисходящем канале. При этом в заголовке указывается CID и размер требуемой полосы (в байтах, без учета заголовков физических пакетов). Поля данных после заголовков запроса полосы нет.

Поле данных может содержать: подзаголовки MAC, управляющие сообщения и собственно данные приложений верхних уровней, преобразованные на CS-подуровне. MAC-подзаголовки могут быть пяти типов – упаковки, фрагментации, управления предоставлением канала, а также подзаголовки Mesh-сети и подзаголовков канала быстрой обратной связи (Fast Feedback).

Управляющие сообщения – это основной механизм управления системой IEEE 802.16. Всего зарезервировано 256 типов управляющих сообщений, из них используются 48. Формат управляющих сообщений прост – поле типа сообщения (1 байт) и поле данных (параметров) произвольной длины.

Описание профилей пакетов, управление доступом, механизмы криптозащиты, динамическое изменение работы системы и т.д. (т.е. все функции управления, предоставления доступа, запроса и подтверждения) реализуются через управляющие сообщения.

Доступ к каналу предоставляется исключительно базовой станцией по предварительному запросу. Начальная инициализация АС и запрос канала происходят на основе механизма конкурентного доступа в специально отведенных для этого временных интервалах. БС назначает АС время и длительность доступа к каналам в зависимости от типов данных и приоритетов. Канальный ресурс конкретной АС может изменяться посредством опроса (поллинга) со стороны БС (т.е. БС предоставляет АС окно для запроса ресурсов) или специальных управляющих сообщений со стороны АС при очередной передаче данных.

Уровень безопасности - алгоритмы шифрования на участке между базовой и абонентскими станциями. Уровень безопасности включает два положения:

- Протокол инкапсуляции для шифрования пакетов, включающий несколько вариантов пар шифрование-аутентификация и правила их применения к пакетам MAC уровня.
- Протокол управления ключами шифрования РКМ (Privacy Key Management), обеспечивающий распределение ключей от базовой станции абонентам.

Физический уровень - методы организации дуплекса, способы адаптации, методы множественного доступа и модуляции.

Рассмотрим более подробно физический уровень.

Физический уровень

Как уже отмечалось, одной из особенностей стандарта IEEE 802.16a/d является возможность работы в условиях не прямой видимости. Это достигается за счет использования технологии ортогонального частотного разделения каналов с мультиплексированием (Orthogonal Frequency Division Multiplexing, OFDM), которая позволяет эффективно бороться с таким негативным явлением, как многолучевая интерференция сигналов. Эффект многолучевой интерференции сигналов заключается в том, что в результате многократных отражений сигнала от естественных преград один и тот же сигнал может попадать в приемник различными путями. Но подобные пути распространения имеют и разные длины, а потому для различных путей распространения ослабление сигнала будет неодинаковым. Следовательно, в точке приема результирующий сигнал представляет собой суперпозицию (интерференцию) многих сигналов, имеющих различные амплитуды и смещенных относительно друг друга по времени, что эквивалентно сложению сигналов с разными фазами.

Следствием многолучевой интерференции является искажение принимаемого сигнала. Многолучевая интерференция присуща любому типу сигналов, но особенно негативно она сказывается на широкополосных сигналах. Дело в том, что при использовании широкополосного сигнала в результате интерференции определенные частоты складываются синфазно, что приводит к увеличению сигнала, а некоторые, наоборот, противофазно, вызывая ослабление сигнала на данной частоте.

Говоря о многолучевой интерференции, возникающей при передаче сигналов, различают два крайних случая. В первом из них максимальная задержка между различными сигналами не превышает времени длительности одного символа и интерференция возникает в пределах одного передаваемого символа. Во втором случае максимальная задержка между различными сигналами больше длительности одного символа, а в результате интерференции складываются сигналы, представляющие разные символы, и возникает так называемая межсимвольная интерференция (Inter Symbol Interference, ISI).

Наиболее отрицательно на искажение сигнала влияет межсимвольная интерференция. Поскольку символ — это дискретное состояние сигнала, характеризующееся значениями частоты несущей, амплитуды и фазы, то для различных символов меняются амплитуда и фаза сигнала, а значит, восстановить исходный сигнал крайне сложно.

Чтобы избежать, а точнее, частично компенсировать эффект многолучевого распространения, используются частотные эквалайзеры, однако по мере роста скорости передачи данных либо вследствие увеличения символьной скорости, либо из-за усложнения схемы кодирования эффективность использования эквалайзеров падает.

В результате при более высоких скоростях передачи применяется метод кодирования данных, который состоит в том, что поток передаваемых данных распределяется по множеству частотных подканалов и передача ведется параллельно на всех этих подканалах. При этом высокая скорость передачи достигается именно за счет одновременной передачи данных по всем каналам, а скорость передачи в отдельном подканале вполне может быть невысокой.

Поскольку в каждом из частотных подканалов скорость передачи данных можно сделать не слишком высокой, это создает предпосылки для эффективного подавления межсимвольной интерференции.

При частотном разделении каналов необходимо, чтобы ширина отдельного канала была, с одной стороны, достаточно узкой для минимизации искажения сигнала в пределах отдельного канала, а с другой — достаточно широкой для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно как можно более плотно расположить частотные подканалы, но при этом избежать межканальной интерференции, чтобы обеспечить полную независимость каналов друг от друга. Частотные каналы, удовлетворяющие перечисленным требованиям, называются ортогональными. Несущие сигналы всех частотных подканалов (а точнее, функции, описывающие эти сигналы) ортогональны друг другу.

Важно, что хотя сами частотные подканалы могут частично перекрывать друг друга, ортогональность несущих сигналов гарантирует частотную независимость каналов друг от друга, а следовательно, и отсутствие межканальной интерференции (рис. 9.2).

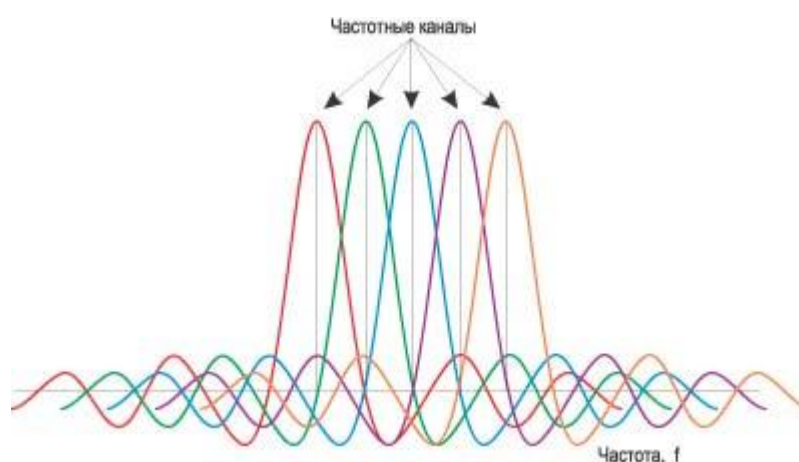


Рис. 9.2. Пример перекрывающихся частотных каналов с ортогональными несущими

Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется ортогональным частотным разделением с мультиплексированием (OFDM). Для его реализации в передающих устройствах используется обратное быстрое преобразование Фурье (IFFT), переводящее предварительно мультиплексированный на n -каналов сигнал из временного представления в частотное (рис. 9.3).

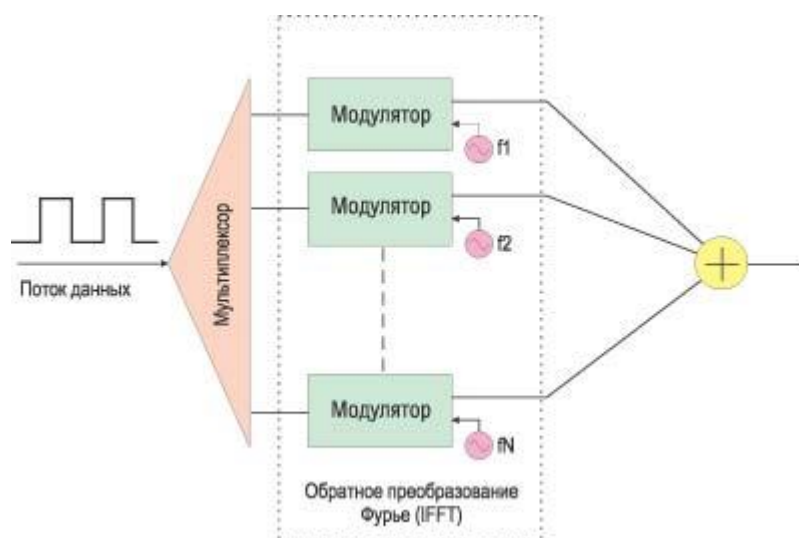


Рис. 9.3. Реализация метода OFDM

Каждый отсчет IFFT представляет собой поднесущую, которая подвергается фазовой (BPSK, QPSK) или квадратурно-амплитудной (QAM16 или QAM64) модуляции, что позволяет повысить информационную скорость передачи данных.

Группа поднесущих частот, которая в данный момент переносит битовые потоки, называется символом OFDM.

Технология OFDM находит применение не только в протоколе IEEE 802.16. К примеру, в протоколе IEEE 802.11g также используется технология OFDM, однако, в сравнении с протоколом IEEE 802.11g, в протоколе IEEE 802.16 предусмотрено более гибкое распределение полосы частот, используемых для передач данных. Причем это можно сделать как за счет уменьшения количества поднесущих, так и с помощью их сужения. Минимальная ширина сигнала, предусмотренная стандартом, составляет 1,25 МГц, а максимальная — 20 МГц. Естественно, что с уменьшением частотного ресурса скорость передачи уменьшается, но сама эта возможность позволяет использовать частотный спектр отдельными фрагментами, а не целиком, как это реализовано в протоколе IEEE 802.11g.

Для повышения помехоустойчивости при передаче данных в протоколе IEEE 802.16 предусмотрены такие традиционные технологии, как сверточное кодирование с декодированием по алгоритму Витерби, коды Рида-Соломона.

В итоге в стандарте IEEE 802.16a были выделены три типа физического уровня соединений, различающихся методом модуляции сигнала (табл. 9.1):

- WirelessMAN-SC — физический уровень с одной несущей частотой;
- WirelessMAN-OFDM — ортогональное частотное разделение на 256 каналов с мультиплексированием. Реализация множественного доступа к среде передачи данных происходит за счет технологии временного разделения (Time Division Multiple Access, TDMA);
- WirelessMAN-OFDMA — ортогональное масштабируемое частотное разделение каналов с мультиплексированием. Используется разделение на 2048 поднесущие частоты. Коллективный доступ к среде передачи данных реализуется за счет объединения нескольких поднесущих частот в один канал передачи и его выделения конкретному получателю (OFD Multiple Access, OFDMA).

Таблица 9.1. Характеристики стандартов IEEE 802.16

Стандарт	802.16	802.16a/d (802.16-2004)	802.16e
Частотный диапазон	10-66 ГГц	2-11 ГГц	2-6 ГГц
Тип сети	Стационарная	Стационарная	Подвижная
Зона покрытия	Зона прямой видимости	Вне зоны прямой видимости	
Радиус зоны покрытия	2-4 км	4-6 км (15-20 м на открытом пространстве)	4-6 км
Скорость передачи данных	32-134 Мбит/с при полосе 28 МГц	До 75 Мбит/с при полосе 20 МГц	До 15 Мбит/с при полосе 5 МГц
Модуляция	QPSK, 16 QAM, 64QAM	OFDM 256, OFDMA, BPSK, QPSK, 16QAM, 64QAM	
Ширина канала	20, 25 и 28 МГц	Избирательная ширина от 1,25 до 20 МГц	

Физический уровень WirelessMAN-SC предназначен для применения в зоне прямой видимости приемника и получателя сигналов. Остальные два уровня, основанные на ортогональном частотном разделении каналов, могут использоваться для построения сетей по топологии «точка-многоточие» в условиях отсутствия прямой видимости.

Из двух OFDM-уровней уровень WirelessMAN-OFDM несколько проще для реализации с технической точки зрения и потому пользуется большей поддержкой со стороны производителей оборудования.

В случае ортогонального частотного разделения на 256 каналов с мультиплексированием (WirelessMAN-OFDM) используется 256 отсчетов IFFT, из которых 192 поднесущие являются информационными, то есть применяются для передачи данных, 8 поднесущих предназначены для измерения характеристик канала связи и используются для передачи пилотных символов (pilot symbols), а остальные 56 поднесущих частот могут применяться для организации защитных интервалов, длительность которых составляет 1/4, 1/8, 1/16 или 1/32 длительности OFDM-сигнала.

Ширина канала связи может быть различной и изменяется от 1,25 до 20 МГц.

Ортогональное частотное разделение каналов с мультиплексированием типа WirelessMAN-OFDMA представляет собой масштабируемое частотное разделение каналов, то есть количество поднесущих в данном случае не фиксировано и может составлять 512, 1024 и 2048. В зависимости от количества поднесущих меняется и ширина канала, и количество подканалов (табл. 9.2).

Таблица 9.2. Характеристики OFDMA

Ширина канала	5 МГц	10 МГц	20 МГц
Количество поднесущих	512	1024	2048
Количество подканалов	32	64	128
Ширина подканала	156 кГц		
Длительность символа	101 мкс		
Расстояние между поднесущими	11,2 кГц		
Длительность циклического префикса	11,2 мкс		

Одной из особенностей стандарта IEEE 802.16 является его адаптивность к внешним помеховым условиям. Система подстраивается к характеристикам канала в каждый момент времени. Например, в идеальном по энергетике канале все поднесущие OFDM будут работать с модуляцией QAM64 и скоростью сверточного кодирования 3/4, обеспечивая максимальную скорость передачи 74,81 Мбит/с. В наихудших условиях передачи используются QPSK-модуляция для всех поднесущих и сверточное кодирование со скоростью 1/2. При этом скорость передачи составляет 1,04 Мбит/с. Всего протоколом предусмотрено семь различных комбинаций типов модуляции и скорости сверточного кодирования, в результате чего достигается требуемая помехоустойчивость протокола и большое разнообразие возможных скоростей передачи (табл. 9.3 и 9.4).

Таблица 9.3. Возможные режимы передачи

Тип модуляции	Скорость сверточного кодирования	Количество информационных бит на символ	Количество информационных бит в OFDM-символе
BPSK	1/2	0,5	88
QPSK	1/2	1	184
QPSK	3/4	1,5	280
QAM16	1/2	2	376
QAM16	3/4	3	568
QAM64	2/3	4	760
QAM64	3/4	4,5	856

Таблица 9.4. Зависимость скорости передачи от ширины канала связи и типа модуляции

Модуляция	QPSK	QPSK	QAM16	QAM16	QAM64	QAM64
Скорость сверточного кодирования	1/2	3/4	1/2	3/4	2/3	3/4
1,75 МГц	1,04	2,18	2,91	4,36	5,94	6,55
3,5 МГц	2,08	4,37	5,82	8,73	11,88	13,09
7,0 МГц	4,15	8,73	11,64	17,45	23,75	26,18
10 МГц	8,31	12,47	16,63	24,94	33,25	37,40
20 МГц	16,62	24,94	33,25	49,87	66,49	74,81

Существенным отличием стандарта IEEE 802.16 от IEEE 802.11 является возможность использования протокола с разрешением конфликтов. Устройства стандарта IEEE 802.11 работают по принципам Ethernet: все они имеют равные права на доступ к радиотракту, а попытавшись одновременно установить связь, разрешают конфликты, повторяя попытки захвата среды через случайное время. В сетях стандарта IEEE 802.16 имеется выделенное устройство — базовая станция оператора, которая раздает своим подчиненным права доступа к радиосреде. В результате имеется возможность более эффективно использовать радиочастотный ресурс и обеспечить эффективную передачу данных.

Базовые станции (Base Station, BS), как правило, применяют мультиплексирование с разделением по времени (TDM), при котором каждой абонентской станции (Subscriber Station, SS) последовательно выделяются временные слоты. Абоненты же разделяют общий канал посредством схемы множественного доступа с разделением по времени (Time Division Multiple Access, TDMA).

Для реализации дуплексного режима обмена данными используются две технологии: дуплексный режим с разделением по времени (TDD) нисходящего (DownLink) и восходящего (UpLink) потоков (при этом задействуется общий канал связи) и дуплексный режим с разделением по частотам (FDD), когда нисходящий и восходящий потоки оперируют на разных каналах и обмен данными может выполняться одновременно.

Сообщения управления MAC

Определен набор управляющих сообщений MAC. Эти сообщения транспортируются в блоках данных MAC PDU. Все управляющие сообщения MAC начинаются с поля тип сообщения и могут содержать дополнительные поля. Управляющие сообщения для базовых, ширококвещательных и исходных соединений (initial ranging) не могут быть фрагментированы или упакованы. Управляющие сообщения первичного соединения могут быть упакованы и/или фрагментированы. Значения поля тип сообщения представлены в табл. 9.5. Управляющие сообщения не могут передаваться через транспортные соединения.

Таблица 9.5. Значения поля тип

Тип	Имя сообщения	Описание сообщения	Соединение
0	UCD	Дескриптор восходящего канала	Широковещательное
1	DCD	Дескриптор нисходящего канала	Широковещательное
2	DL-MAP	Определение доступа к нисходящему каналу	Широковещательное
3	UL-MAP	Определение доступа к восходящему каналу	Широковещательное
4	RNG-REQ	Запрос диапазона	Исходное или базовое
5	RNG-RSP	Отклик диапазона	Исходное или базовое
6	REG-REQ	Запрос регистрации	Первичное управле-

			ние
7	REG-RSP	Отклик регистрации	Первичное управление
8	Зарезерв.		
9	PKM-REQ	Запрос управления ключом конфиденциальности	Первичное управление
10	PKM-RSP	Отклик на запрос управления ключом конфиденциальности	Первичное управление
11	DSA-REQ	Запрос добавления динамического сервиса	Первичное управление
12	DSA-RSP	Отклик добавления динамического сервиса	Первичное управление
13	DSA-ACK	Подтверждение добавления динамического сервиса	Первичное управление
14	DSC-REQ	Запрос изменения динамического сервиса	Первичное управление
15	DSC-RSP	Отклик изменения динамического сервиса	Первичное управление
16	DSC-ACK	Подтверждение изменения динамического сервиса	Первичное управление
17	DSD-REQ	Запрос аннулирования динамического сервиса	Первичное управление
18	DSD-RSP	Отклик аннулирования динамического сервиса	Первичное управление
19		Зарезервировано на будущее	
20		Зарезервировано на будущее	
21	MCA-REQ	Запрос мультикастингового присвоения	Базовое
22	MCA-RSP	Отклик мультикастингового присвоения	Базовое
23	DBPC-REQ	Запрос изменения профиля нисходящего канала	Базовое
24	DBPC-RSP	Отклик изменения профиля нисходящего канала	Базовое
25	RES-CMD	Команда сброса	Базовое
26	SBC-REQ	Запрос базовых возможностей SS	Базовое
27	SBC-RSP	Отклик базовых возможностей SS	Базовое
28	CLK-CMP	Сравнение показаний сетевых часов SS	Широковещательное
29	DREG-CMD	Команда регистрации или ее отмены	Базовое
30	DSX-RVD	Сообщение получения DSx	Первичное управление
31	TFTP-CPLT	Сообщение завершения конфигурационного файла TFTP	Первичное управление
32	TFTP-REP	Отклик завершения конфигурационного файла TFTP	Первичное управление

33-255		Зарезервировано на будущее	
--------	--	----------------------------	--

Сообщение дескриптора нисходящего канала (DCD)

DCD периодически передается BS, чтобы определить характеристики физического нисходящего канала. Параметры, следующие за ID канала, и число изменений конфигурации представляются в формате TLV, где поля типа и длины имеют длину один байт. Формат сообщения DCD описан в табл. 9.6.

Таблица 9.6. Формат сообщения DCD

Синтаксис	Размер	Описание
DCD_Message_Format () {		
Тип управляющего сообщения = 1	8 бит	
Идентификатор нисходящего канала	8 бит	
Число изменений конфигурации	8 бит	
Информация о канале в формате TLV	перем.	
Начало секции, специфической для PHY		
for(i=1; i<=n; i++)		Для каждого профиля нисходящего канала с 1 до n
Downlink_Burst_Profile }		Зависит от PHY

BS сформирует DCD в формате табл. 9.6, включая все перечисленные ниже параметры:

Число изменений конфигураций

Инкрементируется BS на 1 по модулю 256 для любого изменения параметра канала с заданным дескриптором. Если значение этого счетчика в последующем DCD остается тем же, SS может решить, что остальные поля не изменились и игнорировать оставшуюся часть сообщения.

Идентификатор нисходящего канала

Идентификатор нисходящего канала, к которому относится сообщение. Этот идентификатор произвольно выбирается BS и является уникальным для заданного домена подуровня MAC.

Параметры сообщения, которые следуют за числом изменений конфигурации, кодируются в формате TLV.

Downlink_Burst_Profile имеет комбинированную кодировку TLV, которая сопряжена с DIUC (Downlink Interval Usage Code) используемого физического канала. Каждый Downlink_Burst_Profile представляет собой неупорядоченный список атрибутов PHY, закодированных в формате TLV. Каждому интервалу с помощью сообщения DL-MAP ставится в соответствие DIUC.

Каждый Downlink_Burst_Profile в сообщении DCD содержит следующие параметры:

- Тип модуляции
- Тип кода FEC
- Длина последнего кода
- Порог обязательного выхода DIUC
- Порог минимальной записи DIUC
- Присутствие преамбулы

- Если тип кода FEC равен 1, 2 или 3 Downlink_Burst_Profile будет содержать также
- RS байты данных (K)
- RS байты четности (R)

Если тип кода FEC равен 2, то Downlink_Burst_Profile будет содержать тип кода BCC. Если же тип кода FEC равен 4, то Downlink_Burst_Profile будет содержать тип кода ряда BTC, тип кода колонки и тип интерливинга BTC.

Соответствие между профайлом кластера и DIUC представлено в табл. 9.7.

Таблица 9.7. Соответствие между профайлом кластера и DIUC

Профайл кластера (burst)	DIUC
Профайл DL 1	0
Профайл DL 2	1
Профайл DL 3	2
Профайл DL 4	3
Профайл DL 5	4
Профайл DL 6	5
Профайл DL 7	6
Профайл DL 8	7
Профайл DL 9	8
Профайл DL 10	9
Профайл DL 11	10
Профайл DL 12	11
Профайл DL 13	12
Зарезервировано	13
Зазор (Gap)	14
Конец таблицы DL-MAP	15

Конец таблицы DL-MAP указывает на первый PS после конца DL-субкадра. В табл. 6.3 представлен формат Downlink_Burst_Profile, который используется в сообщении DCD. Профайл кодируется с типом =1, 8-битовой длиной и 4-битовым DIUC.

Таблица 9.8. Формат Downlink_Burst_Profile

Синтаксис	Размер	Описание
Тип=1	8 бит	
Длина	перем.	
Зарезервировано	4 бита	Следует устанавливать в 0
DIUC	4 бита	

Информация в формате TLV	перем.	
--------------------------	--------	--

Секции данных нисходящего канала используются для передачи информационных и управляющих сообщений для станций клиентов. Для данных всегда используется FEC-кодирование. В режиме TDM данные передаются в порядке понижения трудоемкости профайлов. В случае режима TDMA данные группируются в кластеры (burst). Сообщение DL-MAP содержит карту соответствия, которая уведомляет, с какого PS начинаются изменения профайла. Если в пределах кластера данные (DL) не заполняют всего субкадра, передатчик прекращает работу.

Вообще число PS i , выделенное для конкретного кластера, может быть вычислено на основе DL-MAP. Пусть n - минимальное число PS, необходимое для одного кодового слова FEC данного профайла. Тогда $i = kn + j + q$, где k - число кодов FEC, которые относятся к данному кластеру, j - число PS, занятых наибольшим возможным укороченным кодовым словом, а q ($0 \leq q < n$) равно числу PS, занимаемых заполнителем в конце кластера, чтобы гарантировать целое i . Для операций с фиксированными кодами $j=0$. В конце кластера (когда нет следующего кодового слова) добавляются $4q$ символа, чтобы завершить PS. На рис. 9.4 показана схема привязки DL-MAP для варианта TDM, а на рис. 9.5 то же для варианта TDMA.

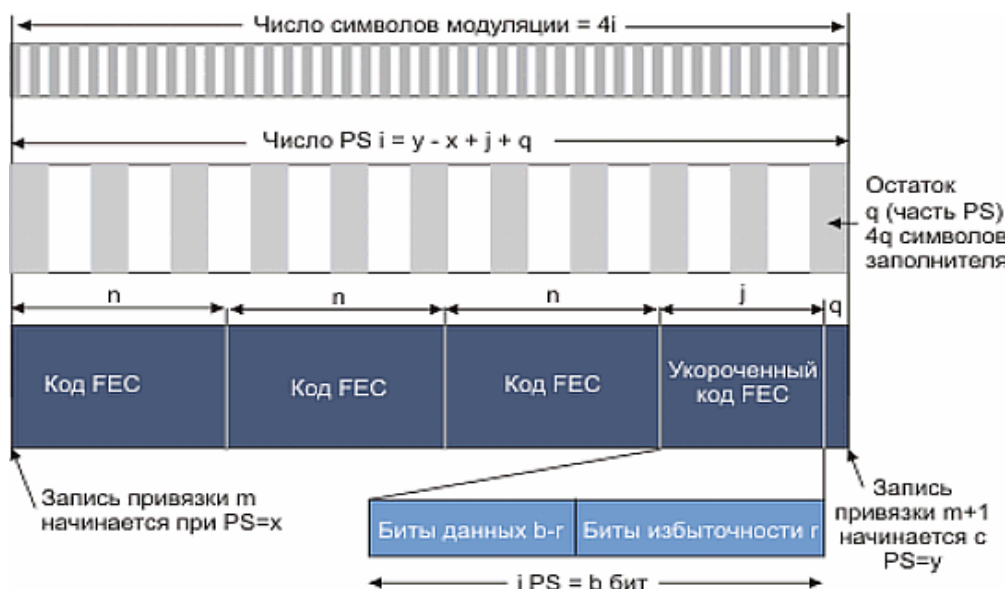


Рис. 9.4. Схема привязки DL-MAP, использующая укороченные блоки FEC - вариант TDM

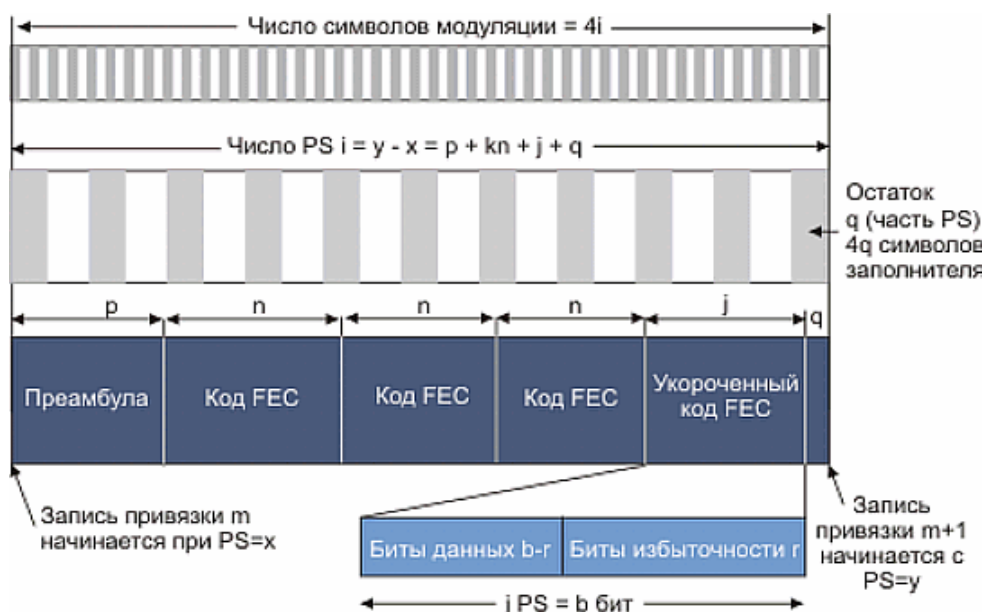


Рис. 9.5. Схема привязки DL-MAP, использующая укороченные блоки FEC - вариант TDMA

Поле данных для нисходящего канала разбивается на блоки, размер которых согласуется с размером кодов после добавления указателя CS. Заметим, что длина поля данных может варьироваться в зависимости от того разрешено ли использование укороченных кодов в профайле кластера. К каждому сегменту поля данных добавляется байт указателя. Это показано на рис. 9.6.



Рис. 9.6. Формат PDU при передаче по нисходящему каналу CS

Поле указателя определяет номер байта в пакете, который указывает либо на начало первого MAC PDU в пакете, либо на начало любого набора байт, который предшествует следующему MAC PDU. Если в CS-пакете нет MAC PDU или набора байт, тогда байт указателя устанавливается равным нулю. Когда имеются данные для передачи, `stuff_byte` равный `0xFF` будет использоваться в пределах поля данных для заполнения любых ниш между MAC PDU.

Кодирование и модуляция на физическом уровне нисходящего канала для данного режима отражены на рис. 9.7.



Рис. 9.7. Блок-схема подуровня PMD нисходящего канала

Нисходящий канал поддерживает адаптивное формирование профайлов кластеров для пользовательской части данных кадра. Может быть определено до 12 профайлов кластера. Параметры каждого передаются SS через MAC-сообщения в управляющей части нисходящего кадра. Использование DIUC определено в табл. 9.9.

Таблица 9.9. Значения DIUC

DIUC	Назначение
0	Управление кадром (не в сообщениях DCD)
1-6	Профайлы кластеров TMD (без преамбулы)
7-12	Профайлы кластеров TMDA (фиксированная преамбула)
13	Зарезервировано
14	Зазор (в сообщениях DCD)
15	Конец таблицы соответствия

Так как модуляция и схема FEC могут быть для SS опциональными, для BS предусмотрены механизмы идентификации возможностей SS. Эта информация передается от SS к BS при регистрации.

Сообщение дескриптора восходящего канала

Дескриптор восходящего канала (UCD) периодически передается BS, для того чтобы определить характеристики физического восходящего канала. Отдельное сообщение UCD передается для каждого восходящего канала. BS передает сообщения UCD в формате, показанном в таблице 9.10. Сообщение содержит следующие параметры:

Счетчик изменений конфигурации

Увеличивается BS на 1 (по модулю 256), всякий раз, когда производится изменение любого параметра канала с данным дескриптором. Если значение счетчика для очередного UCD остается тем же, SS решает, что остальные поля не изменены и можно игнорировать оставшуюся часть сообщения.

Размер минидомена

Размер n минидоменов для восходящего канала в единицах физических доменов. Допустимыми значениями являются $n=2^m$, где m равно целому из диапазона 0-7.

Идентификатор восходящего канала

Идентификатор канала, к которому относится сообщение. Идентификатор произвольно выбирается BS и является уникальным в пределах домена субуровня MAC.

Начало отсрочки передачи

Размер исходного окна отсрочки для исходного соперничества за диапазон, выраженный через степень 2. Значение n может лежать в интервале 0-15 (старшие биты могут не использоваться и приравняться нулю).

Конец отсрочки передачи

Размер конечного окна отсрочки передачи для исходного соперничества за диапазон, выраженный через степень 2. Значение n может лежать в интервале 0-15 (старшие биты могут не использоваться и приравняться нулю).

Запрос начала отсрочки

Запрос размера исходного окна отсрочки для данных исходного соперничества за диапазон, выраженный через степень 2. Значение n может лежать в интервале 0-15 (старшие биты могут не использоваться и приравняться нулю).

Конец отсрочки передачи

Запрос размера конечного окна отсрочки передачи для исходного соперничества за диапазон, выраженный через степень 2. Значение n может лежать в интервале 0-15 (старшие биты могут не использоваться и приравняться нулю).

Таблица 9.10. Формат сообщения UCD

Синтаксис	Размер	Описание
UCD_Message_Format		
Тип управляющего сообщения = 0	8 бит	
Идентификатор восходящего канала	8 бит	
Счетчик изменений конфигурации	8 бит	
Размер минидомена (minislot)	8 бит	
Начало отсрочки передачи	8 бит	
Конец отсрочки передачи	8 бит	
Запрос начала отсрочки	8 бит	
Запрос конца отсрочки	8 бит	
Информация о канале в кодировке TLV	перем.	
Начало секции, специфической для PHY		
for($i=1; i \leq n; i++$)		Для каждого профиля восходящего канала с 1 до n
Uplink_Burst_Profile }	перем.	

Чтобы обеспечить гибкость, остальные параметры сообщения кодируются в формате TLV.

Uplink_Burst_Profile имеет комбинированную кодировку TLV, которая сопряжена с UIUC (Uplink Interval Usage Code) используемого физического канала. Каждый Uplink_Burst_Profile представляет собой неупорядоченный список атрибутов PHY, зако-

дированных в формате TLV. Каждому интервалу с помощью сообщения UL-MAP ставится в соответствие UIUC.

Сообщение запроса диапазона (RNG-REQ)

Запрос RNG-REQ передается SS при инициализации и периодически по запросу BS, чтобы определить сетевую задержку и запросить мощность и/или изменение профайла нисходящего канала. Формат сообщения RNG-REQ описан в табл. 9.11.

Таблица 9.11. Формат сообщения RNG-REQ

Синтаксис	Размер	Описание
RNG-REQ_Message_Format() {		
Тип управляющего сообщения = 4	8 бит	
Идентификатор нисходящего канала	8 бит	
Ожидание до завершения	8 бит	
Данные, закодированные в форме TLV	перем.	

Поле CID в заголовке MAC предполагает наличие следующих значений в случае отправки в период управления инициализации.

- CID исходного диапазона, если SS осуществляется попытка подключения к сети.
- CID исходного диапазона, если SS еще не зарегистрирована и изменяет восходящий канал (или оба канала) согласно загруженному конфигурационному файлу.
- Базовый CID (присвоенный ранее посредством RNG-RSP), если SS еще не зарегистрирована и изменяет восходящий канал согласно загруженному конфигурационному файлу.
- Базовый CID (присвоенный ранее посредством RNG-RSP), если SS зарегистрирована и изменяет восходящий канал.
- Во всех прочих случаях используется базовый CID, как только он присвоен в сообщении RNG-RSP.

При посылке в период управления станции CID всегда равен базовому CID. Ниже описаны параметры, присутствующие в сообщении RNG-REQ. Заметим, что длина сообщения RNG-REQ, посланного в период управления инициализацией является фиксированной.

Идентификатор нисходящего канала

Идентификатор нисходящего канала, для которого SS получил UCD, описывающий восходящий канал, по которому должен быть передано сообщение запроса диапазона. Это поле содержит 8 бит.

Ожидание до завершения

Если это поле содержит код нуль, тогда все предыдущие атрибуты диапазонных откликов должны быть использованы до посылки данного запроса. В противном случае это предполагаемое время, необходимое для завершения восприятия параметров выделенного диапазона и выраженное в десятках миллисекунд.

Сообщение RNG-REQ должно содержать следующие параметры:

- Запрошенный профайл кластера нисходящего канала
- MAC-адрес SS
- Аномалии рабочего диапазона

Сообщение отклика на запрос диапазона (RNG-RSP)

Сообщение RNG-RSP передается BS в ответ на полученный запрос RNG-REQ или при необходимости скорректировать параметры канала по результатам измерения, которые были сделаны для других полученных данных или MAC-сообщений. SS готова получать сообщения RNG-RSP в любое время, а не только в ответ на RNG-REQ.

Исходное сообщение RNG-RSP должно передаваться, с использованием профайла нисходящего канала, который приемлем для обеспечения надежного приема. Для достижения гибкости параметры сообщения, следующие после ID восходящего канала, следует кодировать в формате TLV.

BS генерирует сообщения RNG-RSP в формате, показанном в табл. 9.12.

Таблица 9.12. Формат сообщения RNG-RSP

Синтаксис	Размер	Описание
RNG-RSP_Message_Format () {		
Тип управляющего сообщения = 5	8 бит	
Идентификатор восходящего канала	8 бит	
Данные, закодированные в форме TLV	перем.	

В сообщение RNG-RSP следует включить следующие параметры:

- Информация подстройки синхронизации
- Информация подстройки мощности
- Информация подстройки частоты
- Состояние диапазона

Следующие параметры могут быть включены в сообщение RNG-RSP:

- Новое значение частоты нисходящего канала
- Новое значение ID восходящего канала
- Рабочий профайл нисходящего канала
- Базовый CID

Обязательный параметр, если сообщение RNG-RSP послано на фазе инициализации в ответ на сообщение RNG-REQ.

CID первичного управления

Обязательный параметр, если сообщение RNG-RSP послано на фазе инициализации в ответ на сообщение RNG-REQ.

MAC-адрес SS (48 бит)

Обязательный параметр, когда CID в MAC-заголовке равен исходному CID диапазона.

Сообщение запроса регистрации (REG-REQ)

Сообщение REG-REQ посылается SS при инициализации, формат этого запроса описан в таблице 9.13.

Таблица 9.13. Формат сообщения REG-REQ

Синтаксис	Размер	Описание
-----------	--------	----------

REG- REQ_Message_Format() {		
Тип управляющего сообщения = 6	8 бит	
Данные, закодированные в форме TLV	перем.	

Сообщение REG-REQ включает в себя следующие параметры:

CID первичного управления (в общем MAC-заголовке)

Для SS CID в общем MAC-заголовке является CID первичного управления.

Все остальные параметры кодируются в формате TLV.

Сообщение REG-REQ содержит в себе следующие TLV:

- **Последовательность HMAC**
- **CID поддержки восходящего канала**

Сообщение REG-REQ может содержать следующие параметры TLV, формируемые SS:

- **Код ID производителя (SS)**
- **Код возможностей SS**

Сообщение отклика регистрации REG-RSP

Сообщение REG-RSP посылается BS в ответ на запрос REG-REQ, формат этого запроса описан в таблице 9.14.

Таблица 9.14. Формат сообщения REG-RSP

Синтаксис	Размер	Описание
REG-RSP_Message_Format		
Тип управляющего сообщения = 7	8 бит	
Отклик	8 бит	
Данные, закодированные в форме TLV	перем.	

BS генерирует REG-RSP, которые содержат в себе следующие параметры:

- **CID** (в общем заголовке MAC)

CID является в общем заголовке MAC является CID первичного управления для данной SS.

- **Отклик**

Однобайтовый код, принимающий значение:

0 = ok

1 = неудача аутентификации сообщения

В сообщении REG-RSP включаются следующие параметры:

- **Версия MAC**
- **Вторичный CID управления**
- **Последовательность (HMAC) кода аутентификации хэшированного сообщения**

Следующие параметры включаются в сообщение REG-RSP, если были обнаружены в REG-REQ или BS требует использования нестандартного значения параметра:

- Возможности SS
- BS откликается на возможности SS (только если они это отражено в REG-REQ). BS откликается на возможности SS для того чтобы уведомить о возможности их использования. Если BS не распознает возможность SS, она возвращает “off” в сообщении REG-RSP.
- Возможности возвращенные в REG-RSP не будут установлены на уровне выше, чем это указано в REG-REQ.

Следующие параметры могут быть включены в REG-RSP: расширения, специфические для производителя.

Сообщения управления ключами конфиденциальности (PKM-REQ/PKM-RSP)

Управление ключами конфиденциальности (**PKM**) использует два типа ключей, запрос PKM (PKM-REQ) и отклик PKM (PKM-RSP), как это видно из табл. 9.15.

Таблица 9.15. Формат сообщения PKM-REQ/PKM-RSP

Значение типа	Имя сообщения	Описание сообщения
9	PKM-REQ	Управляющий запрос ключа конфиденциальности [SS -> BS]
10	PKM-RSP	Отклик на запрос ключа конфиденциальности [SS -> BS]

Только одно сообщение PKM вкладывается в поле данных управляющего сообщения MAC. Протокольные сообщения PKM передаются от SS к BS с использованием формата, описанного в табл. 9.16. Они передаются SS в рамках первичной фазы управляющего соединения.

Таблица 9.16. Формат протокольных сообщений PKM

Синтаксис	Размер	Описание
PKM-REQ_Message_Format		
Тип управляющего сообщения = 9	8 бит	
Код	8 бит	
Идентификатор PKM	8 бит	
Атрибуты, закодированные в форме TLV	перем.	

Протокольные сообщения PKM передаются от BS к SS с использованием формата, описанного в табл. 9.17. Они передаются SS в рамках первичной фазы управляющего соединения.

Таблица 9.17. Формат сообщения PKM

Синтаксис	Размер	Описание
PKM-RSP_Message_Format		
Тип управляющего сообщения = 10	8 бит	

Код	8 бит	
Идентификатор РКМ	8 бит	
Атрибуты, закодированные в форме TLV	перем.	

Параметрами этих сообщений являются:

Код

Код содержит один октет и идентифицирует тип РКМ-пакета. Когда пакет приходит с неверным кодом, он молча отбрасывается. Значения кода определены в табл 9.18.

Идентификатор РКМ

Поле идентификатора содержит один октет. SS использует идентификатор при реагировании на запрос BS. SS инкрементирует поле идентификатора (по модулю 256) при отправке очередного (нового) РКМ-сообщения. Новым сообщением может быть запрос аутентификации или запрос ключа, которые не являются повторами передачи при таймауте. Поле идентификатора в информационных сообщениях аутентификации, которые не предполагают последующих откликов, устанавливается равным нулю.

Поле идентификатора в сообщении BS РКМ-RSP должно соответствовать значению идентификатора из РКМ-REQ, на которое BS реагирует. Поле идентификатора в сообщении ключа шифрования трафика (ТЕК), которое не посылается в ответ на РКМ-REQ, следует устанавливать равным нулю.

При получении сообщения РКМ-RSP SS ассоциирует сообщение с определенной машиной состояния (например, машиной состояния авторизации в случае отклика авторизации).

SS отслеживает идентификатор своего последнего отложенного запроса авторизации. SS отбрасывает отклики авторизации и отказы авторизации с полями идентификатора, которые не соответствуют заданному отложенному запросу авторизации.

SS отслеживает также идентификатор своего последнего отложенного запроса ключа для каждой ассоциации безопасности (SA). SS отбросит сообщение KEY Reply и Key Reject с не соответствующими запросу значениями идентификатора.

Атрибуты

РКМ-атрибуты несут в себе данные, специфические для обменов аутентификации, авторизации или управления ключами между клиентом и сервером. Каждый тип РКМ-пакета имеет свой собственный набор необходимых и опционных атрибутов. Если не указано явно, порядок атрибутов в сообщении произволен. Конец списка атрибутов определяется полем LEN заголовка MAC PDU.

Таблица 9.18. Коды сообщений

Код	Тип РКМ-сообщения	Имя управляющего сообщения MAC
0-2	зарезервировано	-
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP

9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Authent Info	PKM-REQ
13-255	зарезервировано	-

BS и SS молча отбрасывает запросы/отклики, которые не содержат полного списка необходимых атрибутов.

Сообщение добавления ассоциации безопасности (SA Add)

Это сообщение посылается BS -> SS для установления одной или более дополнительных SA. Код =3, атрибуты представлены в табл. 9.19.

Таблица 9.19. Формат сообщения SA Add

Атрибут	Содержимое
Порядковый номер ключа	Порядковый номер ключа авторизации
(один или более) дескрипторов SA	Каждый составной атрибут SA-дескриптора специфицирует идентификатор ассоциации SAID и дополнительные свойства SA

Сообщение запроса авторизации (Auth Request)

Код = 4

Атрибуты перечислены в табл. 9.20.

Таблица 9.20. Атрибуты сообщения Auth Request

Атрибут	Содержимое
SS-сертификат	Содержит сертификат X.509 SS
Возможности безопасности	Описывает запрашиваемые возможности безопасности SS
SAID	Первичный SAID для SS, равный базовому CID

Атрибут возможностей безопасности является составным атрибутом, описывающим запрашиваемые SS требования безопасности.

Атрибут SAID содержит SAID конфиденциальности. В этом случае предоставляемый SAID равен базовому CID SS.

Сообщение отклика авторизации (Auth Reply)

Отклик авторизации посылается BS клиенту SS в ответ на запрос авторизации, и содержит ключ авторизации, время жизни ключа и список дескрипторов SA, идентифицирующие первичный и статический SA. Эти данные определяют параметры доступа SS (тип, криптографический набор и т.д.). Ключ авторизации шифруется открытым ключом SS. Список дескрипторов SA включает в себя дескриптор для базового CID, сообщенный

BS в соответствующем Auth Request. Этот список может содержать также дескрипторы статических SAID, к которым разрешен доступ SS.

Код = 5

Атрибуты сообщения Auth Reply представлены в табл. 9.21.

Таблица 9.21. Атрибуты сообщения Auth Reply

Атрибут	Содержимое
Auth-Key	Ключ авторизации, зашифрованный общедоступным ключом клиента SS
Время жизни ключа	Время активной жизни ключа
Порядковый номер ключа	Порядковый номер ключа авторизации
Один или более дескрипторов SA	Каждый составной атрибут дескриптора SA специфицирует SAID и дополнительные свойства SA

Сообщение отклонения авторизации (Auth Reject)

BS реагирует на запрос авторизации SS, посылая сообщение Auth Reject, если базовая станция отклонила попытку авторизации SS.

Код = 6

Атрибуты сообщения Auth Reject представлены в табл. 9.22.

Таблица 9.22. Атрибуты сообщения Auth Reject

Атрибут	Содержимое
Код ошибки	Код ошибки, указывающий на причину отказа авторизации
Оptionная отображаемая строка	Текстовая строка, поясняющая причину отклонения авторизации

Сообщение запроса ключа

Код = 7

Атрибуты сообщения запроса ключа представлены в табл. 9.23.

Таблица 9.23. Атрибуты сообщения запроса ключа

Атрибут	Содержимое
Порядковый номер ключа	Порядковый номер ключа авторизации
SAID	ID ассоциации безопасности
Дайджест HMAC	Дайджест ключевого сообщения, полученный методом SHA

Атрибут дайджеста должен быть последним в списке атрибутов сообщения. Включение дайджеста позволяет BS аутентифицировать сообщения запроса ключа.

Сообщение отклика на запрос ключа

Код = 8

Атрибуты сообщения отклика на запрос ключа представлены в табл. 9.24.

Таблица 9.24. Атрибуты сообщения отклика на запрос ключа

Атрибут	Содержимое
Порядковый номер ключа	Порядковый номер ключа авторизации
SAID	ID ассоциации безопасности
ТЕК-параметры	Предшествующее поколение параметров ключа, соответствующих SAID
ТЕК-параметры	Новое поколение параметров ключа, соответствующих SAID
Дайджест HMAC	Дайджест ключевого сообщения, полученный методом SHA

Атрибут параметров ТЕК является составным атрибутом, содержащим все ключевые материалы, соответствующие определенному поколению ТЕК SAID. Сюда входит ТЕК, оставшееся время жизни ключа, его порядковый номер, инициализационный вектор блочного шифра CBC.

В любой момент времени BS поддерживает два набора активных поколений ключевого материала для каждого SAID. Один набор соответствует “старому”, второй набор соответствует “новому” поколению ключевого материала. Новое поколение имеет порядковый номер ключа на 1 больше (по модулю 4), чем старое. BS рассылает клиентам SS оба поколения активного ключевого материала. Таким образом, сообщения отклика на запрос ключа содержит два атрибута ТЕК-параметров, каждый из которых содержит ключевой материал для одного из активных наборов ключевого материала SAID.

Включение дайджеста позволяет клиенту-получателю аутентифицировать сообщение ключевого отклика и гарантировать синхронизацию наборов ключей у BS и SS.

Сообщение отклонение ключа

Получение сообщения отклонения ключа (KeyReject) указывает получившему клиенту SS, что для заданного SAID авторизация более недействительна.

Код =9

Атрибуты сообщения Key Reject представлены в табл. 9.25.

Таблица 9.25. Атрибуты сообщения KeyReject

Атрибут	Содержимое
Порядковый номер ключа	Порядковый номер ключа авторизации
SAID	ID ассоциации безопасности
Код ошибки	Код, указывающий причину отклонения запроса ключа
Текстовая строка (опционально)	Отображаемая строка, поясняющая отклонение запроса
Дайджест HMAC	Дайджест ключевого сообщения, полученный методом SHA

Атрибут дайджеста должен быть последним в списке атрибутов сообщения.

Сообщение недействительности авторизации

BS может послать сообщение о недействительности авторизации клиенту SS:

- по своей инициативе
- как отклик на сообщение, полученное от SS.

В обоих случаях такое сообщение предлагает SS предпринять повторную авторизацию в BS. BS посылает сообщение о недействительности авторизации, если BS не распознает SS в качестве авторизованного объекта, или по причине неудачной верификации дайджеста сообщения, что говорит об утрате синхронизации ключевых наборов BS и SS.

Код = 10

Атрибуты сообщения Authorization Invalid представлены в табл. 9.26.

Таблица 9.26. Атрибуты сообщения Authorization Invalid

Атрибут	Содержимое
Код ошибки	Код, указывающий причину сообщения о недействительности авторизации
Текстовая строка (опциона)	Отображаемая строка, поясняющая причину недействительности авторизации

Сообщение TEK Invalid

BS посылает клиенту (SS) сообщение TEK Invalid, если установлено, что зашифрованное PDU нисходящего канала содержит некорректное значение TEK в полученном заголовке MAC.

Код = 11

Атрибуты сообщения TEK Invalid представлены в табл. 9.27.

Таблица 9.27. Атрибуты сообщения TEK Invalid

Атрибут	Содержимое
Порядковый номер ключа	Порядковый номер ключа авторизации
SAID	ID ассоциации безопасности
Код ошибки	Код, указывающий причину сообщения TEK Invalid
Текстовая строка (опциона)	Отображаемая строка, поясняющая причину сообщения TEK Invalid
Дайджест HMAC	Дайджест сообщения, полученный методом SHA

Атрибут дайджеста должен быть последним в списке атрибутов сообщения.

Информационное сообщение аутентификации (Authent Info)

Сообщение Authent Info содержит один атрибут CA-Certificate формата X.509 производителя SS.

Код = 12

Атрибуты сообщения Authent Info представлены в табл. 9.28.

Таблица 9.28. Атрибуты сообщения Authent Info

Атрибут	Содержимое
CA-сертификат	Сертификат производителя SS

Сообщение сверки часов (CLK-CMP)

В сети с сервисными потоками, несущими данные, где требуется реконструирование сигналов часов (напр., DS1 и DS3) базовая станция периодически широковещательно посылает сообщения CLK-CMP. Если это предусмотрено, BS будет генерировать сообщение CLK-CMP с интервалом, определенным согласно формату, описанному в табл. 9.29.

Таблица 9.29. Формат сообщений CLK-CMP

Синтаксис	Размер	Описание
CLK-CMP_Message_Format() {		
Тип управляющего сообщения = 28	8 бит	
Счетчик синхротактов n	8 бит	
for(i=1; i<n; i++) {		
Clock ID(i)	8 бит	
Порядковый номер [i]	8 бит	
Результат сравнения[i] }	8 бит	

Сообщения CLK-CMP включают в себя следующие параметры: ID часов (ClockID), порядковый номер, и результат сравнения показаний часов CCV (Clock Comparison Value).

Порядковый номер

8-битовый код, инкрементируемый BS на 1 (по модулю 256) при формировании сообщения CLK-CMP. Этот параметр используется для детектирования потери пакетов.

Результат сверки часов

8-битовый код разности (по модулю 256) между следующими двумя эталонными сигналами: (1) 10МГц эталонная частота, синхронизованная с символьными часами радиоканала (например, GPS), и (2) эталонной частотой 8.192 МГц, синхронизованной с сетевыми часами.

Сообщение команды De/Re (DREG-CMD)

Сообщение DREG-CMD отправляется базовой станцией по базовом CID SS, чтобы изменить ее состояние доступа. По получении DREG-CMD SS выполнит операцию, предписываемую присланным кодом операции. Тип управления MAC для данного сообщения представлен в табл. 9.30.

Таблица 9.30. Формат сообщения DREG-CMD

Синтаксис	Размер	Описание
DREG-CMD_Message_Format() {		
Тип управляющего сообщения = 29	8 бит	
Код операции	8 бит	
Параметры, закодированные в форме TLV	перем.	

Коды операции и их значения представлены в табл. 9.31.

Таблица 9.31. Коды операций

Код операции	Операция
0x00	SS уходит с этого канала и пытается перейти на другой
0x01	SS прослушивает текущий канал, но не передает, пока не получит сообщение RES-CMD
0x02	SS прослушивает текущий канал, но только передает в режиме базового первичного управления и вторичных соединений управления.
0x03	SS возвращается к нормальной работе и может передавать, используя любые активные соединения.
0x04-0xFF	Зарезервировано

Сообщение о получении DSx (DSX-RVD)

Сообщение о получении пакетов динамических сервисов (DS) генерируется базовой станцией в ответ на первичный запрос DSx-REQ со стороны SS, чтобы проинформировать SS о том, что BS получила сообщение DSx-REQ в более приемлемое время, чем это может быть сделано с помощью DSx-RSP, которое может быть прислано только после DSx-REQ. Формат DSX-RVD представлен в табл. 9.32.

Таблица 9.32. Формат сообщений DSX-RVD

Синтаксис	Размер	Описание
DSX-RVD_Message_Format() {		
Тип управляющего сообщения = 30	8 бит	
ID транзакции	16 бит	
Код подтверждения	8 бит	

Сообщение завершения копирования посредством TFTP конфигурационного файла (TFTP-CPLT)

Сообщение TFTP-CPLT генерируется SS, когда ей удалось успешно получить конфигурационный файл из сервера. Формат сообщения TFTP-CPLT описан в табл. 9.33.

Таблица 9.33. Формат сообщения TFTP-CPLT

Синтаксис	Размер	Описание
TFTP-CPLT_Message_Format() {		
Тип управляющего сообщения = 31	8бит	
Данные, закодированные в форме TLV	перем.	

Сообщение отклика на уведомление о завершении копирования конфигурационного файла (TFTP-RSP)

Сообщение TFTP-RSP генерируется базовой станцией BS в ответ на сообщение TFTP-CPLT, присланное SS. Формат сообщения TFTP-RSP описан в таблице 9.34.

Таблица 9.34. Формат сообщения TFTP-RSP

Синтаксис	Размер	Описание
TFTP-CPLT_Message_Format() {		
Тип управляющего сообщения = 32	8 бит	
Данные, закодированные в форме TLV	перем.	

Несколько MAC-PDU могут быть переданы вместе как по восходящему, так по нисходящему каналу. MAC-PDU управляющих сообщений, пользовательских данных, запросов полосы могут быть пересланы за одну передачу. Схема объединения иллюстрируется на рис. 9.8.

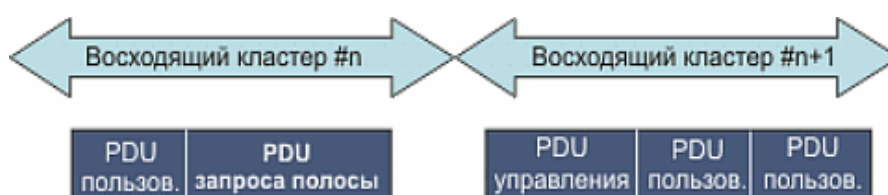


Рис. 9.8. Объединение MAC PDU (каждое из полей имеет свой уникальный CID)

MAC SDU может быть разделен между одним или более MAC PDU. Это позволяет более эффективно использовать доступную полосу пропускания с учетом требуемого уровня QoS. Фрагментация может быть реализована по инициативе BS или SS. Это определяется на базе формирования соединения. Значения поля FC описаны в табл. 9.35.

Таблица 9.35. Значения поля FC

Фрагмент	FC	FCN
Первый фрагмент	10	Инкрементируется по модулю 8
Промежуточный фрагмент	11	Инкрементируется по модулю 8
Последний фрагмент	01	Инкрементируется по модулю 8
Нефрагментировано	00	Инкрементируется по модулю 8

Порядковый номер позволяет SS воссоздать исходное поле данных и зарегистрировать потерю любого промежуточного пакета. При потере SS отбрасывает все MAC PDU до тех пор, пока не будет получен новый первый фрагмент или не будет получен нефрагментированный MAC PDU.

В случае включения режима упаковки, MAC может упаковывать по несколько MAC SDU в один MAC PDU. В режиме упаковки используется атрибут соединения, который говорит о том, используются пакеты постоянной длины или переменной. Схема упаковки для MAC-SDU постоянной длины показана на рис. 9.9, то же для переменной длины отображено на рис. 9.10.



Рис. 9.9. Упаковка MAC SDU постоянной длины



Рис. 9.10. Упаковка MAC SDU переменной длины

Для улучшения эффективности процесса запрос-предоставление предусмотрен механизм диспетчеризации. Путем задания параметров диспетчеризации и QoS BS может получить требующуюся пропускную способность и время отклика для восходящего канала.

Базовые виды услуг перечислены в таблице 9.36, это **UGS** (Unsolicited Grant Service), сервис запросов реального времени **rtPS** (Real-Time Polling Service), **nrtPS** (Non-Real-Time Polling Service) и сервис наилучшего возможного **BE** (Best Effort). Каждый вид сервиса приспособлен для определенного типа потока данных.

Таблица 9.36. Сервисы диспетчеризации и правила использования

Тип диспетчеризации	Комбинированный запрос	Изъятие полосы	Опрос (polling)
UGS	Не разрешен	Не разрешено	Для запроса уникастного опроса требуемой полосы для соединения не UGS используется бит PM
rtPS	Разрешен	Разрешено для GPSS	Диспетчеризация допускает только уникастный опрос
nrtPS	Разрешен	Разрешено для GPSS	Диспетчеризация может ограничить сервисный поток только уникастным опросом через политику передачи/ запросов; в противном случае разрешены все формы опроса
BE	Разрешен	Разрешено для GPSS	Разрешены все формы опроса

Заметим, что каждой SS приписано три CID для целей отправки и получения управляющих сообщений. Используется три соединения, чтобы обеспечить дифференцированные уровни QoS для разных соединений, транспортирующих управляющий трафик

MAC. Увеличение или уменьшение требований к полосе необходимо для всех сервисов кроме соединений с постоянной скоростью передачи (например, несжимаемый UGS). Полоса таких соединений не может быть изменена с момента формирования до ликвидации. Требования к сжимаемым UGS, таким как каналированным T1, могут варьироваться в зависимости от трафика.

Когда SS нужно запросить полосу для конкретного соединения с BE диспетчеризацией, она посылает сообщение BS, содержащее требование немедленного соединения **DAMA** (Demand Assigned Multiple Access). QoS соединения определяется в процессе формирования и обеспечивается BS.

Для получения нужной полосы восходящего канала SS использует запросы, направляемые ею к BS. Так как профайл восходящего канала может меняться динамически, все запросы полосы должны выражаться в байтах, которые необходимы для передачи MAC-заголовка и поля данных, но не должны учитывать издержки физического уровня. Такие запросы могут быть посланы в период запроса **IE** или любого кластера предоставления данных типа IE.

В зависимости от характера запроса полосы существует два режима работы SS: **GPC** (Grant per Connection) и **GPSS** (Grant per Subscriber Station). В первом случае BS предоставляет полосу конкретно каждому соединению, в то время как во втором случае полоса предоставляется всем соединениям SS. В последнем случае (GPSS) можно использовать меньшую суммарную полосу пропускания, а продвинутая SS может перераспределять полученную от BS полосу. Такой алгоритм удобен для решения задач реального времени, когда требуется более быстрый отклик.

Опрос (*polling*) является процессом, с помощью которого базовая станция резервирует SS полосу. Это резервирование может быть для отдельной SS или группы станций. Резервирование для группы соединений и/или SS в действительности определяет информационный элемент (IE) соединения при запросе полосы. Заметим, что опрос осуществляется для соединений или для SS. Полоса всегда запрашивается на основе CID, а резервирование полосы осуществляется для соединения (режим GPC) или для SS (режим GPSS).

Когда SS опрашиваются индивидуально, никакого сообщения не посылается, просто производится резервирование для SS в восходящем канале, достаточное для реагирования на запросы полосы. Если SS не нуждается в полосе, она возвращает байт 0xFF. Станции SS, работающие в режиме GPSS, при наличии активного UGS-соединения с достаточной полосой, индивидуально опрашиваться не будут, если только они не выставили бит PM (Poll Me) в заголовке пакета UGS-соединения. Это экономит полосу на опросе всех SS.

Если имеется недостаточная полоса пропускания для индивидуального опроса неактивных SS, некоторые SS могут опрашиваться в составе мультикаст-групп или с привлечением широковещательного опроса. Определенные CID зарезервированы для мультикаст-групп и для широковещательных сообщений.

MAC-протокол поддерживает несколько дуплексных технологий. Выбор дуплексной техники может повлиять на определенные параметры уровня PHY, а также на перечень поддерживаемых возможностей. На MAC-уровне поддерживаются кадровые и бескадровые спецификации PHY. Для бескадрового режима PHY интервала диспетчеризации выбираются MAC. При бескадровой FDD PHY восходящий и нисходящий каналы размещаются на разных частотах, так что каждая SS может осуществлять прием и передачу одновременно. Оба эти канала не используют фиксированной длины кадров. В такой системе нисходящий канал находится всегда во включенном состоянии, и все SS слушают его. Трафик передается широковещательно, используя мультиплексирование по времени (TDM). В восходящем канале применяется режим мультиплексирования **TDMA** (Time Division Multiple Access).

В кадровой (кластерной) системе **FDD** (Frequency Division Duplex) восходящий и нисходящий каналы размещаются на разных частотах, а нисходящие данные передаются в

виде кластеров (bursts). Для обоих направлений обмена используются кадры фиксированной длины. Это помогает использовать разные типы модуляции. При этом могут применяться полнодуплексные и полудуплексные SS.

В режиме **TDD** (Time Division Duplexing) восходящий и нисходящий каналы используют одну и ту же частоту. **TDD**-кадр имеет фиксированную длительность и содержит субкадры для восходящего и нисходящего каналов. Кадр делится на целое число физических доменов (PS-slots), которые помогают легко поделить полосу. Работа системы в режиме TDD и структура TDD-кадра показана на рис. 9.11.

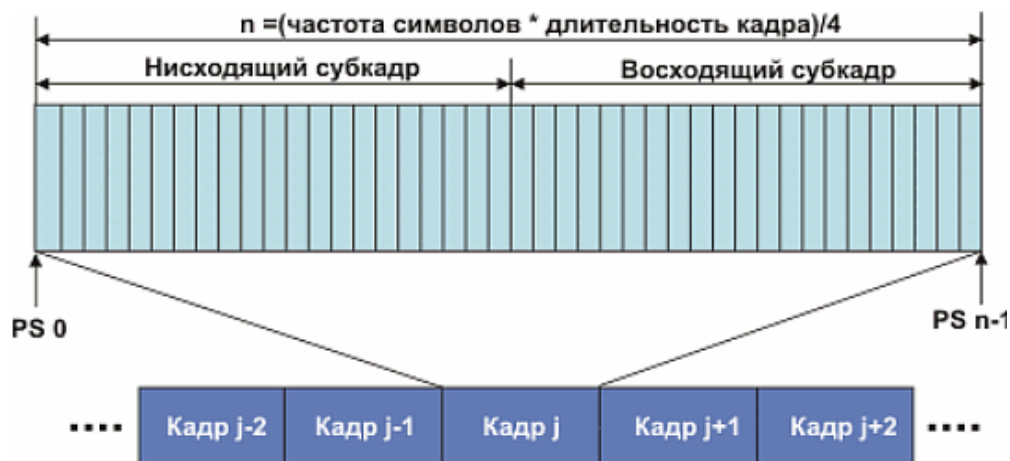


Рис. 9.11. Структура TDD кадра

Синхронизация восходящего канала базируется на эталонных временных метках восходящего канала, которые задаются счетчиком, инкрементируемым в 16 раз чаще, чем частота PS. Это позволяет часам SS быть хорошо синхронизованными с BS.

В случае бескадрового PHY сообщение привязки (DL-MAP) транслирует широко-вещательно временную метку всем SS. Эта метка BS используется для подстройки часов всех станций клиентов. После того как временная метка BS или SS достигает максимального значения $2^{29} - 1$, она принимает значение нуль и продолжает инкрементироваться.

Карта резервирования полосы восходящего канала использует в качестве модулей минидомены (minislot). Размер минидомены определяется как число физических доменов PHY PS и содержится в дескрипторе восходящего канала. Один минидомен содержит n PS, где n целое число из интервала 0-255.

Информация в DL-MAP относится к текущему кадру, то есть к кадру, в котором она доставлена. Информация, доставляемая в UL-MAP, относится к временному интервалу, начинающемуся в момент резервирования (измеряется от начала поученного кадра и до конца последнего зарезервированного минидомены). Пустые IE указывают на паузы в передаче по восходящему каналу. Станции SS не могут осуществлять передачу в это время. Данный вид синхронизации используется как для TDD, так и для FDD. Вариант TDD показан на рис. 9.12, а вариант FDD на рис. 9.13.

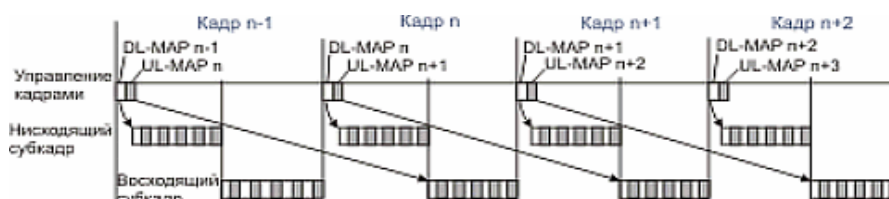


Рис. 9.12. Максимальное время релевантности управляющей информации PHY и MAC (TDD)

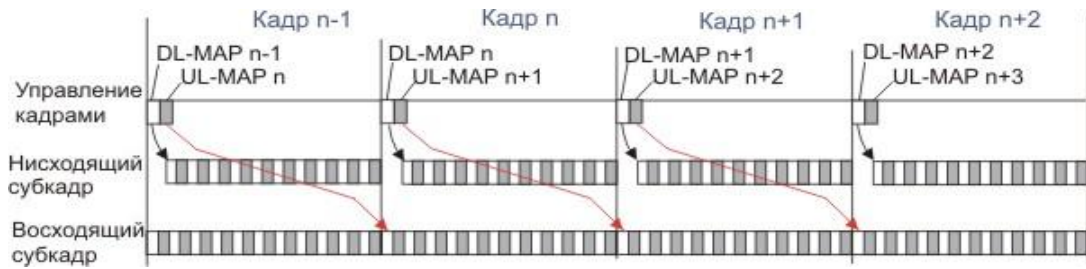


Рис. 9.13. Максимальное время релевантности управляющей информации PHY и MAC (FDD)

В бескадровых системах PHY DL-MAP содержит только временные метки восходящего канала и не определяет, какую информацию следует передавать. Все SS постоянно ищут нисходящий сигнал для любого сообщения, которое к ним адресовано. Сообщение UL-MAP содержит временную метку, которая указывает на первый минидомен, который определяет мэппинг. Задержка от конца UL-MAP до начала первого интервала в восходящем канале определенная таблицей соответствия, будет больше максимума RTT плюс время обработки, необходимое SS (см. рис. 9.14).

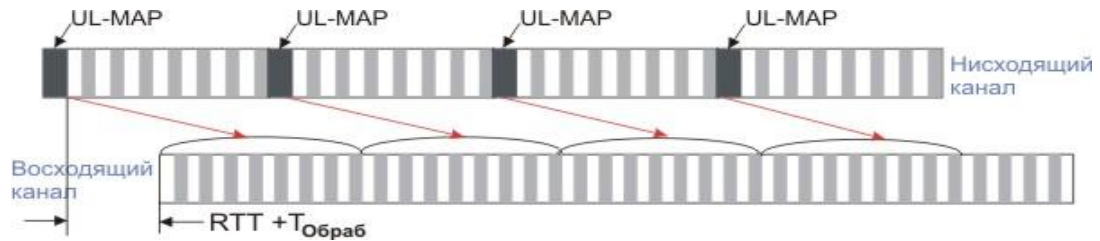


Рис. 9.14. Временная релевантность UL-MAP информации (бескадровое FDD)

Структура субкадра нисходящего канала для TDD показана на рис. 9.15, то же для FDD - на рис. 9.16.

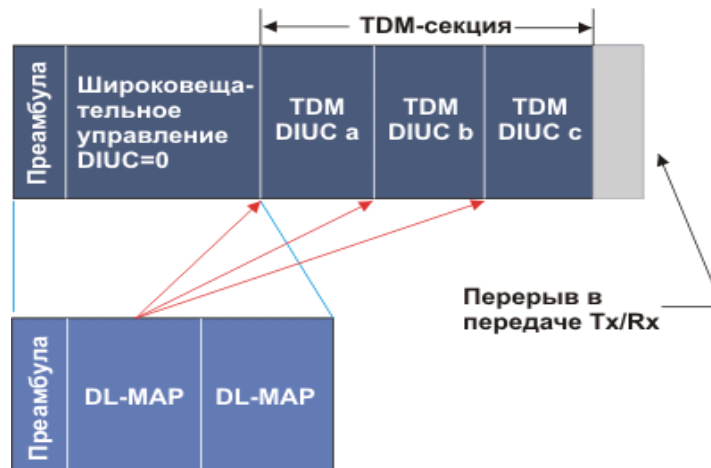


Рис. 9.15. Структура субкадра нисходящего канала для TDD

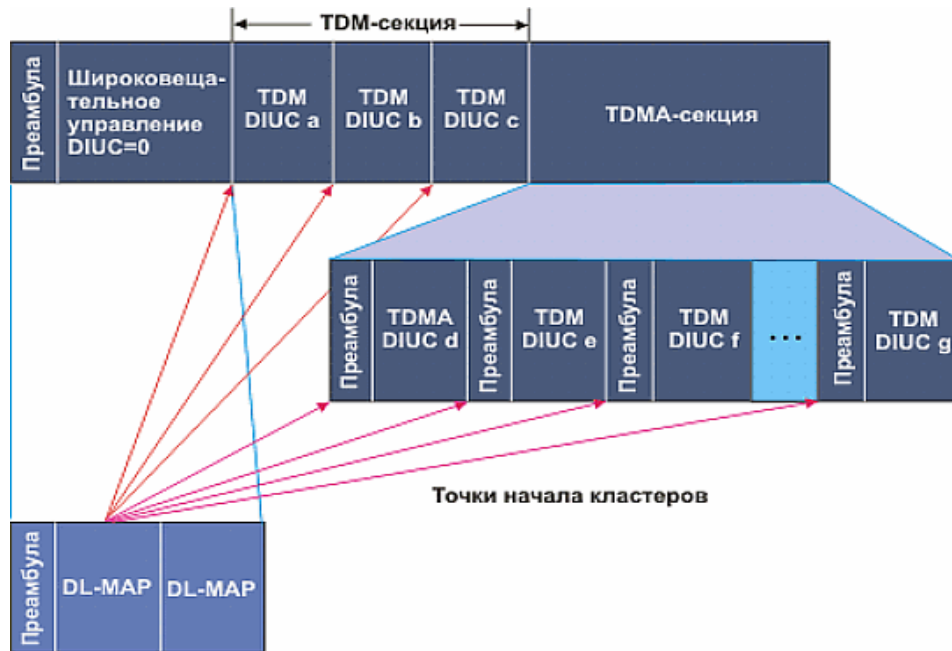


Рис. 9.16. Структура субкадра нисходящего канала для FDD



Рис. 9.17. Структура субкадра нисходящего канала для TDD

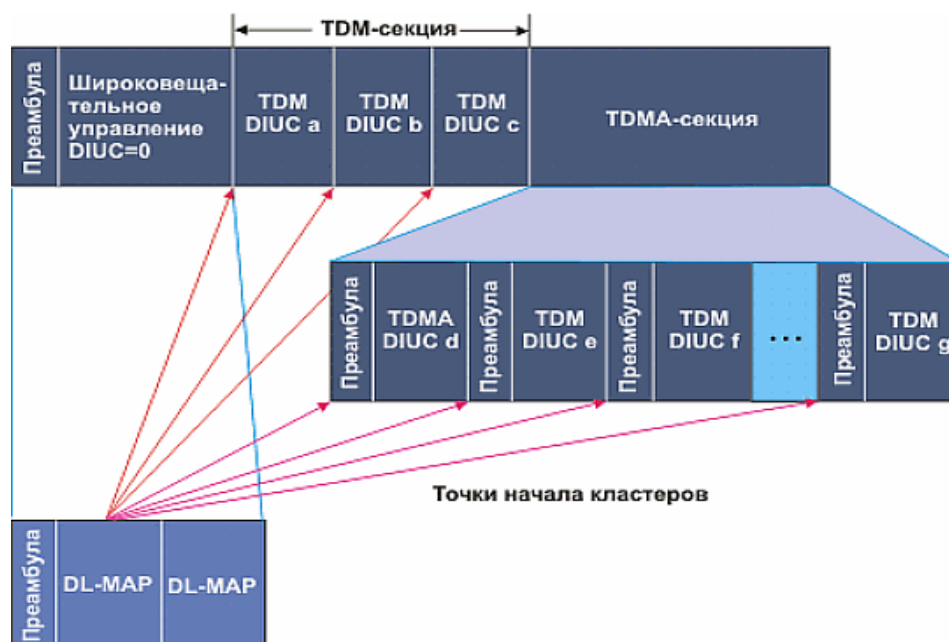


Рис. 9.18. Структура субкадра нисходящего канала для FDD

Возможность передачи определяется наличием свободного минидомена, который может быть использован SS для передачи сообщений или данных. Число возможностей передачи связано с конкретным информационным элементом (IE), размером интервала и объемом передачи.

BS контролирует восходящий канал с помощью сообщений UL-MAP и определяет, какие из минидоменов являются объектами столкновений. Столкновения могут произойти в периоды установления соединения и при запросах, определяемых их IE. Потенциальные столкновения при запросах зависят от CID в соответствующих IE.

Когда SS имеет данные для передачи и хочет войти в процесс разрешения конфликтов, она устанавливает исходное значение ширины окна отсрочки равным отсрочке начала запроса в сообщении UCD. SS случайным образом выбирает число в пределах окна отсрочки. Это случайное число указывает на разрешенное число попыток передачи, которые SS должна пропустить до начала посылки. SS рассматривает только допустимые возможности передачи, которые определяются IE запроса в сообщениях UL-MAP. Каждый IE может содержать много конфликтных возможностей передачи.

ID канала используется в процессе диспетчеризации для идентификации ресурсных запросов и откликов. Так как такие сообщения являются ширококестельными, узлы-получатели могут определить порядок использования как ID узла отправителя в сеточном подзаголовке, так и ID канала в поле MSH-DSCH. Структура ID соединения (CID) описана в таблице 9.37.

Таблица 9.37. Структура CID для сеточного режима

Синтаксис	Размер	Описание
CID { if(Xmt Link ID == 0xFF)		
{Logical Network ID}	8 бит	0x00: ширококестельно
else		
Type	2 бита	0x0 MAC управление 0x1 IP 0x2-0x3 зарезервировано

Надежность	1 бит	
Приоритет/Класс	3 бита	
Приоритет отбрасывания}	2 бита	
Xmt Link ID}	8 бит	0xFFF: широковещательное управление MAC

Поле *Приоритет/Класс* определяет класс сообщения.

Поле *Приоритет отбрасывания* определяет вероятность отбрасывания сообщения в случае перегрузки.

Значение поля Xmt Link ID присваивается узлом отправителем каналу до узла приемника.

Таблица 9.38. Кодирование поля Type

Бит поля Type	Назначение
5 (старший)	Сеточный подзаголовок. 1 = присутствует; 0= отсутствует
4	ARQ Feedback Payload (поле данных обратной связи)
3	Расширенный тип. 1 = расширенный; 0 = нерасширенный Указывает, являются ли расширенными данные подзаголовки упаковки или фрагментации
2	Подзаголовок фрагментации. 1=присутствует; 0=отсутствует.
1	Подзаголовок упаковки. 1=присутствует; 0=отсутствует.
0 (младший)	Подзаголовок управления предоставлением доступа. 1=присутствует; 0=отсутствует. Следует установить равным 0 для DL.

Может присутствовать четыре типа подзаголовков. Подзаголовки PDU (сеточный, фрагментации и управления предоставлением доступа) могут размещаться в PDU MAC сразу после общего заголовка MAC. Если присутствуют подзаголовки фрагментации и управления предоставлением доступа, последний должен быть первым. Если имеется сеточный заголовок, он всегда размещается первым. В таблице 9.38 представлен формат подзаголовка фрагментации.

Таблица 9.38. Структура подзаголовка фрагментации

Синтаксис	Размер	Пояснение
Подзаголовок фрагментации		
FC	2 бита	Индицирует состояние фрагментации поля данных: 00 = фрагментации нет 01 = последний фрагмент 10 = первый фрагмент 11 = промежуточный фрагмент
If(Type бит является Extended)		См. табл. 2
FSN	11 бит	Порядковый номер текущего SDU фрагмента. Это поле инкрементируется на 1 (по модулю 2048) для каждого фрагмента, содержащего SDU.
else		

FSN	3 бита	Порядковый номер текущего SDU фрагмента. Это поле инкрементируется на 1 (по модулю 2048) для каждого фрагмента, содержащего SDU.
Зарезервировано	3 бита	

Формат подзаголовка упаковки представлен в таблице 9.39.

Таблица 9.39 Формат подзаголовка упаковки

Синтаксис	Размер	Пояснения
Подзаголовок упаковки() {		
FC	2 бита	Индицирует состояние фрагментации поля данных: 00 = фрагментации нет 01 = последний фрагмент 10 = первый фрагмент 11 = промежуточный фрагмент
if(Type бит является Extended)		См.табл. 2
FSN	3 бита	Порядковый номер текущего SDU фрагмента. Это поле инкрементируется на 1 (по модулю 2048) для каждого фрагмента, содержащего SDU.
else		
FSN	3 бита	Порядковый номер текущего SDU фрагмента. Это поле инкрементируется на 1 (по модулю 2048) для каждого фрагмента, содержащего SDU.
Длина	11 бит	

Если бит ARQ обратной связи в поле *type* MAC-заголовка =1, в поле данных транспортируется ARQ-отклик. Если используется упаковка, то он является первым упакованным полем данных.

Формат сеточного подзаголовка представлен в таблице 9.40.

Таблица 9.40 Формат сеточного подзаголовка

Синтаксис	Размер	Пояснения
Подзаголовок сетки() {		
Xmt Node ID	16 бит	
}		

Таблица 9.41 Сообщения управления уровня MAC

Код типа	Название сообщения	Описание сообщения	Соединение
33	ARQ-Feedback	ARQ обратная связь для изолированной системы	Базовое
34	ARQ-Discard	Сообщение отмены ARQ	Базовое
35	ARQ-Reset	Сообщение сброса ARQ	Базовое
36	REP-REQ	Запрос канальных измерительных данных	Базовое1

37	REP-RSP	Отклик на запрос канальных измерительных данных	Базовое
39	MSH-NCFG	Конфигурации сети	Широковещательное
40	MSH-NENT	Вход в сеточную сеть	Базовое
41	MSH-DSCH	Распределенное расписание сетки	Широковещательное
42	MSH-CSCH	Централизованное расписание для сетки	Широковещательное
43	MSH-CSCF	Конфигурирование централизованного расписания для сетки	Широковещательное
44	AAS-FBCK-REQ	Запрос обратной связи AAS	Базовое
45	AAS-FBCK-RSP	Отклик обратной связи AAS	Базовое
38, 46-255	Зарезервировано		

Во время AAS части кадра сообщения DL-MAP, UL-MAP, DCD, UCD и CLK-CMP должны посылаться с использованием базового CID.

AAS - Adaptive Antenna System.

В сеточном (Mesh) режиме узел-кандидат на регистрацию генерирует сообщения **REG-RSP**, включающие следующие параметры:

SS MAC-адрес (SS - Subscriber Station)

Версия MAC (используемая в узле-кандидате)

HMAC Tuple (дайджест сообщения, вычисленный с помощью HMAC_KEY_U)

Сообщение **REG-REQ** может, кроме того, содержать следующие параметры:

IP-версия

Возможности кодирования SS

Идентификатор поставщика кодировщика

В сеточном режиме при регистрации узел генерирует **REG-RSP** сообщения, содержащие следующие параметры:

Node ID (идентификатор узла)

MAC Version (MAC-версия, используемая в сети)

HMAC Tuple (дайджест сообщения, вычисленный с помощью HMAC_KEY_D)

Сообщение **REG-RSP** может, кроме того, содержать следующие параметры:

IP-версия

Возможности кодирования SS. Возможности, указанные в **REG-RSP**, не устанавливаются выше того, что указано в **REG-REQ**.

Оборудование.

Здесь надо сразу сказать, что, т.к. стандарты 802.16 относительно молодые, ассортимент оборудования, представленного сегодня на рынке не так велик, как для стандарта 802.11. В России же, которую никак нельзя назвать передовой страной в этой области, дела обстоят ещё хуже.

К слову, первые образцы сертифицированного WiMAX-оборудования появились не в первой половине 2005 года, как ожидалось, а лишь к концу. Это произошло по двум причинам. Во-первых, некоторым производителям микросхем для оборудования, устанавливаемого в помещении пользователя, не удалось уложиться в намеченные сроки разработки. Во-вторых, WiMAX Forum потребовалось больше времени на оснащение лаборатории и формирование рабочей группы по тестированию оборудования.

Кроме того, как известно, российскими операторами беспроводных сетей передачи данных (БСПД) широко используется оборудование Wi-Fi, и никто не торопится его менять. Ускоренный вывод его из эксплуатации ожидается только в Москве и, возможно, в Петербурге, где бурный рост неофициальных сетей этого стандарта не позволяет предоставлять услуги даже с минимальным качеством. В остальных регионах диапазон 2,4 ГГц еще полностью или в основном свободен от неофициальных сетей, а по стоимости оборудование 802.11b остается вне всякой конкуренции и более того продолжает дешеветь.

В качестве примера рассмотрим систему MicroMAX SOC 5.8, предназначенную для построения базовых станций (БС) беспроводных сетей WiMAX в диапазоне частот 5250-5850 МГц. Оборудование работает в режиме Time Division Duplex и соответствует стандарту IEEE 802.16-2004.

Оборудование имеет архитектуру System On a Chip (SOC) на базе чипсета стандарта IEEE802.16-2004 производства Sequans.

Базовая станция состоит из внутреннего блока Small Data Adaptor SDA-4S (Release 3.0) или MicroMAX-SOC BSDU и внешнего блока Base Station Radio (BSR). Система MicroMAX в комплектации BSR - SDA является односекторной standalone БС малого класса и ориентирована на применение в пригородах и сельской местности в местах с невысокой плотностью абонентов, а также при построении корпоративных сетей. Система MicroMAX в комплектации BSR - BSDU является шести секторной БС среднего класса и ориентирована на применение в городах и пригородах.



Рис. 9.19. Внутренний блок Small Data Adaptor и внешний блок Base Station Radio

В БС Release 3.0 каждый BSR имеет собственный SDA. BSR имеет два варианта исполнения. В первом варианте BSR оснащается интегрированной 60 град секторной антенной. Во втором варианте BSR имеет разъем N-типа для подключения внешней секторной или всенаправленной антенны.

Внутренний блок SDA – 4S имеет четыре интерфейса 10/100 BT и DB-15 коннектор для подключения к BSR через адаптер DB-15- RJ-45.

Внутренний блок MicroMAX-SOC BSDU имеет интерфейс 100 BT и оснащен шестью радио интерфейсами для подключения шести BSR и соответственно 6 секторных антенн.

BSR также имеет DB-15 коннектор для подключения к SDA (BSDU) через адаптер DB-15- RJ-45.

Каждый блок BSR может одновременно обслуживать до 256 абонентов. Устройство MicroMAX SOC работает в качестве коммутатора (бриджа) 2-го уровня.

Управление устройством MicroMAX SOC осуществляется через Web браузер. Поддерживается SNMP v.2. Имеются WiMAX MIB draft 1, а также Airspan MIB.

Таблица 9.42. Характеристики MicroMAX SOC 5.8.

Спецификации радио		
Стандарт и совместимость	WiMAX Forum certified, IEEE 802.16-2004	
Поддержка дуплекса	TDD, OFDM 256FFT	
Частоты	5150-5350 МГц, 5470-5725 МГц, 5725-5850 МГц	
Ширина канала	10,20 МГц	
Выходная мощность	22 dBm	
Чувствительность при BER E10-6, требуемый уровень SNR		
QAM64	3/4 -77.4 dBm, SNR 21dB	
16QAM	1/2 -86.4 dBm, SNR 12 dB	
BPSK	-94.4 dBm, SNR 4 dB	
Bridging	IEEE 802.3d	
Поддерживаемые сервисы		
Качество обслуживания QoS	NRTPS ,BE, CIR, MIR, 8 уровней приоритизации трафика	
Максимальное кол-во абонентов	256	
Интерфейсы		
SDA-4S	4 x100 BT, DB15	
BSR	DB15, N-type antenna port	
Размеры	317x 400 x 65 мм.	
BSR	317x 400 x 65 мм.	
SDA	200 x150x40	
Вес		
BSR	3,8 кг.	
SDA	0.6 кг	
Питание	220 V	
Потребляемая мощность	30 Ватт	
Эксплуатационные условия	Indoor	Outdoor
Рабочая температура	0-40 C	-35+55 C
Влажность	80%	95%

Кроме того, рассмотрим пример абонентского оборудования: абонентские терминалы PocketMAX.

Устройства PacketMAX 100/200/300 Subscriber Unit предназначены для работы в качестве абонентских терминалов беспроводной сети WiMAX стандарта IEEE 8012.16-2004.

Абонентские терминалы PacketMAX 100/200/300 представляют собой комплект из внутреннего indoor и внешнего outdoor модулей. Outdoor модули могут оснащаться интегрированными в корпус антеннами или для достижения максимальной дальности связи иметь возможность подключения внешних антенн с высоким коэффициентом усиления.

Имеются как простые недорогие абонентские терминалы, ориентированные на предоставление доступа в Интернет, так и высокопроизводительные терминалы бизнес

класса с поддержкой качества обслуживания QoS, виртуальных сетей VPN, телефонии VoIP, TDM сервисов. Терминалы малого класса могут состоять только из внешнего модуля. Терминалы серии 100и 200 относятся к классу SOHO и Business. Серия 300 относится к классу Enterprise.

Установка абонентского терминала не требует наличия прямой видимости на базовую станцию при наличии требуемого уровня полезного сигнала, в том числе по отношению к уровню шума (помехи).

Таблица 9.43. Характеристики PocketMAX

Серия	380	320	300	290	220	200	100
Интерфейсы							
LAN 10/100 BT	1	1	1	1	1	1	1
POTS	8	2	0	0	2	0	0
E1	Да	-	-	-	-	-	-
Management	Да	Да	-	Да	Да	-	-
WLAN				Да			Да
Телефония							
VoIP	Да	Да			Да		Да
Fax support	Да	Да			Да		Да
IP networking							
IP routing	Да	Да	Да				Да
NAT	Да	Да	Да	Да	Да		
Bridging	Да						
PPPoE	Да	Да	Да	Да			
VLAN	Да						
DHCP	Да	Да	Да	Да			
OSPF	Да	Да	Да				
Мак кол-во хостов	250	250	250	5	5	5	5
QOS	CG, RT, NRT, BE						
безопасность	3DES, AES CCM 128&1024						
Спецификации радио							
Стандарт и совместимость	WiMAX Forum certified, IEEE 802.16-2004						
Поддержка дуплекса	TDD, OFDM 256FFT						
Частоты	5150-5359 МГц, 5425-5725 МГц, 5725-5925 МГц						
Ширина канала	7,10,20 МГц						
Выходная мощность	20 dBm						
Чувствительность BPSK	-100 dBm						
Управление							
Provisioning	MIB II (RFC 1213), WiMAX (MIB, Aperto Enterprise MIB , SNMP V2						
SNMP	IEE 802.16f MIB						
Питание	PoE						
Потребляемая мощность	40 Ватт						
Эксплуатационные условия	Indoor				Outdoor		
Рабочая температура	0-40 C				-40+65 C		
Влажность	80%				100%		

В заключение, подчеркнем некоторые наиболее существенные различия между стандартами IEEE 802.16a и IEEE 802.11x. Прежде всего, у WiMAX более интеллектуальный физический уровень. Важной особенностью здесь является возможность выбора ширины полосы пропускания канала и повторное использование каналов как способ увеличить емкость соты по мере роста сети. Стандарт предусматривает выбор ширины канала с шагом от 1,75 МГц до 20 МГц со множеством промежуточных вариантов. Дополнительными инструментами физического уровня для повышения эффективности использования радиоспектра служат измерение качества канала и автоматическое управление мощностью сигнала. Операторы могут перераспределять спектр посредством увеличения количества секторов антенны по мере роста числа абонентов.

Устройства IEEE 802.11 требуют по крайней мере 20 МГц для каждого канала (22 МГц в диапазоне частот 2,4 GHz для 802.11b) и оперируют только в полосах частот 2,4 GHz и 5 GHz. Далее, механизм управления доступом к среде базируется на протоколе CSMA/CA, который так же плохо масштабируется, как и протокол CSMA/CD. Аналогично проводной сети Ethernet увеличение числа одновременно работающих пользователей влечет экспоненциальное уменьшение эффективной полосы пропускания. В отличие от этого MAC-уровень в стандарте IEEE 802.16a способен без уменьшения пропускной способности обслуживать сотни пользователей.

Если Wi-Fi разрабатывалась как технология для локальных сетей, то WiMAX предназначена для сетей масштаба города. Несмотря на то что IEEE 802.11a и IEEE 802.11g используют для мультиплексирования тот же метод OFDM, что и IEEE 802.16a, реализованы они по-разному. Это и не столь жесткие требования по ограничению мощности сигнала позволяет WiMAX достигать радиуса действия в несколько десятков километров при пропускной способности до 70 Mbps в одном радиочастотном канале.

Безусловно, эти две беспроводные технологии предназначены для совершенно разных сегментов рынка и являются дополнительными. Так что данное сравнение преследовало цель лишь более четко определить их отличия.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. К. Феер: Беспроводная цифровая связь. Методы модуляции и расширения спектра. Пер. с англ. / Под ред. В.И. Журавлева – М.: Радио и связь, 2000. – 520 с.
2. Весоловский К. Системы подвижной радиосвязи / Пер. с польск. И.Д. Рудинского; под ред. А.И. Ледовского. – М.: Горячая линия – Телеком, 2006. – 536 с.
3. Системы мобильной связи: Учебное пособие для вузов / В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов; Под. ред. В.П. Ипатова. – М.: Горячая линия – Телеком, 2003. – 272 с.
4. Маковеева М. М., Шинаков Ю. С. Системы связи с подвижными объектами: Учеб. пособие для вузов – М.: Радио и связь, 2002 – 440 с.
5. Мордухович Л.Г., Степанов А.П. Системы радиосвязи. Курсовое проектирование: Учеб. пособие для вузов. – М.: Радио и связь, 1987. – 192с.
6. Проектирование радиорелейных линий прямой видимости: Ингвар Хенне, Пер Торвальдсен – Берген: Nera Telecommunications, 1994. -153 с.
7. Громаков Ю. А.. Стандарты и системы подвижной радиосвязи. – М.: ЭКО-ТРЭНДЗ, 1998. – 239 с.
8. Соколов А. В., Андрианов В. И. Альтернатива сотовой связи: транкинговые системы. – СПб.: БХВ-Петербург; Арлит, 2002. – 448 с.
9. Овчинников А.М., Воробьев С.В., Сергеев С.И. Открытые стандарты цифровой транкинговой радиосвязи. – М.: МЦНТИ, 2000. – 166 с.
10. Тамаркин В. М. Системы и стандарты транкинговой связи. – М.: Информационно-технический центр Мобильные телекоммуникации, 1998. – 131с.
11. Соловьёв А.А. Пейджинговая связь. – М.: Эко – Трендз, 2000. – 285 с.
12. Андрианов В.И., Соколов А.В. Сотовые, пейджинговые и спутниковые средства связи. – СПб.: БХВ-Петербург, Арлит. 2001. – 400 с.
13. Ратынский М.В. Основы сотовой связи / Под. ред. Д.Б. Зимины, 2-е изд. – М.: Радио и связь, 2000. – 248 с.
14. Карташевский В.Г., Семенов С.Н., Фирстова Т.В. Сети подвижной связи. – М.: Эко-Тренд, 2001. – 299 с.
15. Мобильная связь: технология DECT / С.И. Дингес – М.: СОЛОН-Пресс, 2003. – 272 с.
16. Спутниковые системы связи: Учеб. пособие / Камнев В.Е., Черкасов В.В., Чечин Г. Н – М.: «Альпина Паблицер», 2004. – 536 с.
17. Горностаев Ю.М., Соколов В.В., Невдяев Л.М. Перспективные спутниковые системы связи. – М.: Горячая линия – Телеком, 2000. – 132 с.
18. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.: Эко-Тренд, 2005. – 384 с.
19. Рошан П. Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11, пер. с англ. – М. Издательский дом “Вильямс”, 2004.-304с.
20. Столингс В. Беспроводные линии связи и сети. : Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 640 с.
21. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.

ИНТЕРНЕТ ССЫЛКИ

- к Главе 1

<http://www.kunegin.narod.ru>;
<http://www.micran.ru>;
<http://www.morion.ru>;
<http://www.nec.ru>;
<http://www.nera.com.ru>;
<http://www.rrl.newmail.ru>;
<http://www.saileks.spb.ru>;
<http://www.vlobatch.narod.ru>;
<http://www.rps2.ru> - RPS2: Radio Planning System 2
<http://www.loniir.ru> – Байкал РРЛ
<http://dsplab.uniyar.ac.ru> – ПИАР 4.53
<http://www.ctt-group.ru> – DRRL 3.1

- к Главе 2

<http://www.ericsson.com>
<http://www.electricrates.com>
<http://www.mot.com>
<http://www.tetramou.com>
<http://www.tetrapol.com>
<http://www.efjohnson.com>
<http://www.apcointl.org>
<http://www.transcrypt.com>

- к Главе 3

<http://www.protocols.ru/1251/protocols/GPRS.pdf>
http://www.sotovik.ru/analit_16.htm
<http://kunegin.narod.ru>

- к Главе 4

<http://sabitov.pochta.ru/html/glava2.htm>
<http://www.amobile.ru/opsos/standart/index.htm>
http://www.pbplib.com.ua/mobile/article_125.html
<http://sabitov.pochta.ru/html/vveden.htm>
<http://www.cwk.kazan.ru/1998/02/gigaset.htm>
<http://www.osp.ru/nets/1998/03/92.htm>
<http://www.informkom.ru/catalog/item.61.html>

- к Главе 5

<http://kunegin.narod.ru/ref/paging/index.htm>

- к Главе 6

<http://www.telemultimedia.ru>
<http://www.anitel.ru>
<http://www.satpro.ru>
<http://www.globaltel.ru>
<http://www.satinfo.RU>
<http://www.connect.ru>
<http://sputnik.alientelecom.ru>
<http://www.satellite.srd.mtuci.ru>

<http://www.alphatelecom.ru>
<http://www.tecckom.com>
<http://rol.ru>

- к Главе 7

<http://citforum.tomsk.ru/nets/wireless/>
<http://www.ixbt.com/comm/wireless/>
<http://www.comptek.ru/wireless/>
<http://www.nslabs.ru/software/security/nessus/>
<http://zyxel.ru/content/catalogue/classifier/48/6/21/>
<http://technograd.tomsk.ru>
<http://www.ixbt.com/comm/wrls-zyxel-g-560.shtml>
<http://www.mport.ru/news/3936/>

- к Главе 8

<http://microdom.by.com/articles/33obluetooth.htm>
<http://www.infosan.ru/articles/wireless/blue-faq.cfm>
<http://www.3dnews.ru/reviews/communication/bluetooth>
<http://www.ixbt.com/mobile/review/bluetooth-1.shtml>
<http://www.electronics.ru/showArticle.phtml?id=3634293>
<http://osp.ru/lan/2000/12/040.htm>
<http://opensystems.ru/os/2001/02/049.htm>
http://mo.com.ua/support/stand_and_tech/bluetooth.htm

- к Главе 9

http://pbxlib.com.ua/lan/article_90.html
<http://www.mobile-review.com/articles/2003/wimax.shtml>
<http://si.ibs.ru/content/si/102/1028-article.asp>
<http://www.wireless.ru/wireless/856>
http://www.telecomresearch.ru/docs/1_stand.doc
http://www.rasu.ru/new_site/docs/statia01.pdf
http://book.itep.ru/4/41/802_16.htm
<http://www.wireless.ru/wireless/858>
<http://grouper.ieee.org/groups/802/16/index.html>

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1 (к Главе 1)

Автоматизация проектирования цифровых радиорелейных линий

На данный момент существует необходимость быстро и точно рассчитывать качественные показатели цифровых радиорелейных линий в зависимости от окружающей их обстановки – этой цели как раз и служат программные комплексы по автоматизации проектирования РРЛ.

Существует несколько образцов данного ПО:

1. RPS2: Radio Planning System 2
2. Балтика-РРЛ
3. Проектирование и анализ радиосетей (ПИАР)
4. DRRL версия 3.1

RPS2: Radio Planning System 2

Универсальная Система RPS-2 предназначена для автоматизированного проектирования беспроводных сетей различной архитектуры (радиорелейных, транкинговых, сотовых), применяющих различные стандарты передачи данных. Использование системы позволяет в сжатые сроки разработать проект новой сети или расширить уже развернутую сеть, оценить ее достоинства и недостатки, проанализировать показатели электромагнитной совместимости проектируемой сети с другими сетями, работающими в той же местности, и оптимизировать характеристики с учетом конкретных географических условий местности при заданном распределении трафика и источников помех.

По своим функциональным возможностям, точности и полноте расчета характеристик сети, по удобству пользовательского интерфейса, программа RPS-2 не уступает наиболее известным зарубежным аналогам, выгодно отличаясь от них ценой, существенно более низкими требованиями к конфигурации компьютера, русским интерфейсом, доступностью технической поддержки и сопровождения.

Исходными данными являются:

- Цифровые карты местности. Они могут быть представлены в одном из стандартных форматов (“MapInfo”, “Planet” и т.д.) и с помощью прилагаемого конвертора преобразованы во внутренний формат программы, более экономный с точки зрения скорости проведения расчетов. При необходимости, не выходя из программы, картографические данные можно отредактировать, добавив новые объекты – препятствия и типы местности.
- База данных с характеристиками применяемого оборудования (частотный диапазон, диаграммы направленности и усиление антенн, частотные и энергетические характеристики приемопередатчиков, потери в фидерах и т.д.).

Программа позволяет:

- размещать радиостанции в заданном месте рассматриваемой территории, работающие в любом из применяемых в России и за рубежом стандартов (NMT-450, AMPS, D-AMPS, GSM, IS-95, SmartTrunk, TETRA, MPT 1327, EDACS и т.д.). Кроме того, пользователь имеет возможность определить свой стандарт проектируемой сети, введя его основные параметры: частотный диапазон, ширину канала и т.д.;
- определять для радиостанций оптимальный состав оборудования из базы данных, которая может пополняться и редактироваться пользователем;
- задавать и редактировать распределение плотности трафика в рассматриваемом регионе, что позволяет анализировать характеристики сотовых и транкинговых систем в условиях различной загрузки;
- рассчитывать, отображать на экране и выдавать на печать основные характеристики планируемой сети;
- рассчитывать показатели электромагнитной совместимости (уровень взаимных помех) планируемой сети с другими сетями;
- оптимизировать параметры планируемой сети путем изменения местоположения радиостанций, а также варьируя состав и технические характеристики размещаемого на них оборудования (программа снабжена удобным пользовательским интерфейсом, обеспечивающим возможность интерактивно проводить указанные изменения);
- отображать результаты измерений уровня принимаемого сигнала и сравнивать их с результатами расчета с последующей оптимизацией параметров применяемых математических моделей расчета.

Характеристики беспроводной сети, рассчитываемые с помощью программы RPS-2:

- область прямой видимости радиостанции;
- уровень сигнала (покрытие) в заданной окрестности указанной радиостанции с учетом диаграммы направленности излучающей антенны;
- требуемая мощность излучения абонента, достаточная для надежного приема его сигнала;
- помехи от близлежащих и удаленных радиостанций;
- профиль любой радиолинии;
- потери распространения между передающей и приемной антеннами;
- сигнал на входе приемной антенны абонента;
- отношение сигнал/шум в прямой и обратной линиях с учетом всех видов внутрисистемных и внешних помех;
- зоны, обслуживаемая секторами базовых станций в условиях помех и их реальная загруженность (трафик, приходящийся на каждый сектор);
- зоны, в которых происходит переключение абонентов с одной станции на другую, или с одного на другой их сектор (зоны hand-off);
- сбалансированность прямой и обратной линий базовых станций.

При расчете радиопокрытия пользователь имеет возможность выбрать одну из нескольких моделей распространения радиоволн. Все они рекомендованы к использованию МККР. В программе используются статистические модели распространения Хата и Уолфиш-Икегами, в которых грубо учитывается характер местности (сельская, пригород, городская, плотная городская), модель распространения МККР - рекомендация 370-5, в которой используются статистические данные профиля радиолинии. Кроме того, имеется возможность использовать модель, основанную на строгом анализе профиля радиолинии с выделением препятствий и учетом дифракционных потерь на них, поиском точек отражения и учетом соответствующих потерь. Здесь же имеется возможность учесть дополнительные потери в

листве деревьев, эффекты дифракции на крышах и экранировки в городской местности. Имея хорошую цифровую карту, можно с высокой точностью рассчитать покрытие и другие характеристики сети.

Программу RPS-2 можно использовать для планирования как макро-, так и микро-ячеек сотовых сетей, включая микросотовые системы, работающие внутри зданий. При расчете характеристик распространения сигналов внутри зданий использована оригинальная математическая модель.

RPS-2 состоит из следующих программных модулей:

- модуль расчета радиорелейных сетей;
- модуль расчета транкинговых и сотовых сетей всех стандартов;
- модуль расчета сетей в стандарте CDMA;
- модуль расчета сетей, работающих внутри зданий;
- модуль импорта результатов эксперимента, их отображения, сравнения с расчетом и корректировки параметров используемых моделей по результатам этого сравнения;
- модуль расчетов, связанных с разработкой санитарного паспорта места;
- автоматический конвертор цифровой карты из стандартного формата во внутренний формат представления картографических данных.

По желанию заказчика возможна поставка программы с любым набором указанных модулей.

Минимальные требования к конфигурации компьютера:

- Процессор Pentium II, 400 МГц или аналогичный;
- MS Windows 9x/Me/NT/2k/XP;
- 32 Мб ОЗУ;
- не менее 120 Мб свободного пространства на жестком диске;
- монитор с разрешением 800x600 High Color.

Оптимальные требования к конфигурации компьютера:

- процессор Pentium 4, 2 ГГц или аналогичный;
- 128 Мб ОЗУ;
- 200 Мб свободного места на жестком диске;
- монитор с разрешением 1280x1024 True Color.

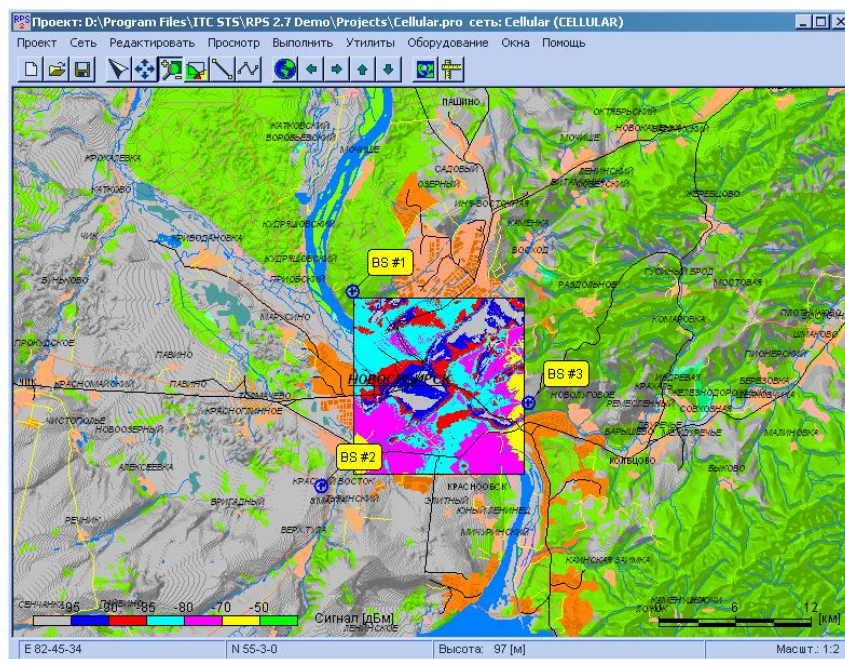


Рис. П1.1. Интерфейс программы RPS-2 с картой анализируемого региона

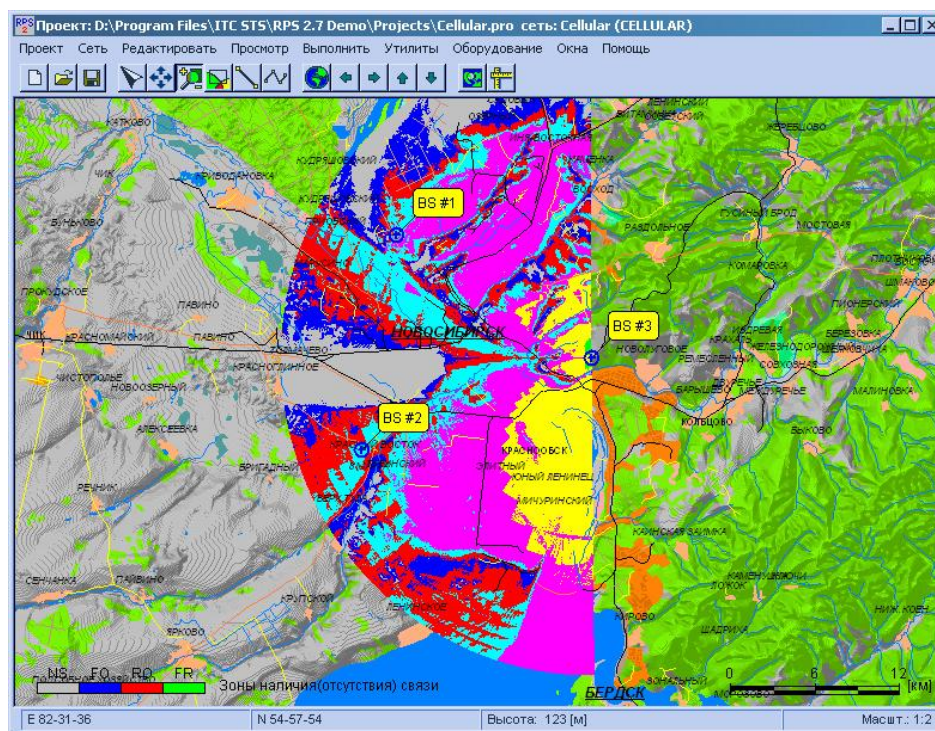


Рис. П1.2. Зоны покрытия

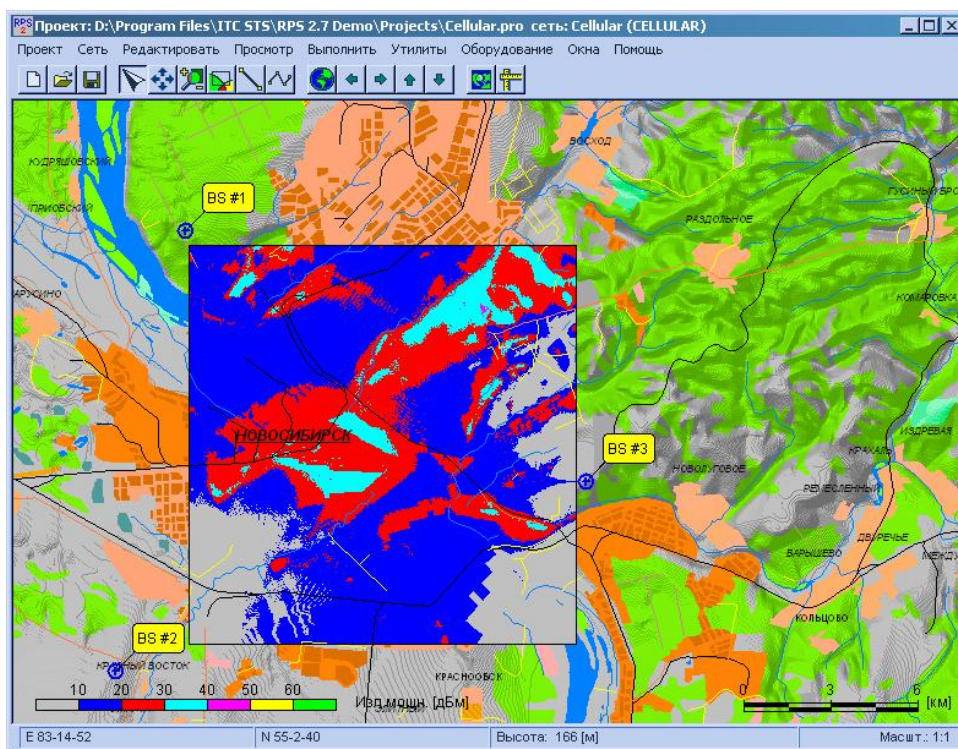


Рис. П1.3. Необходимая мощность абонентов

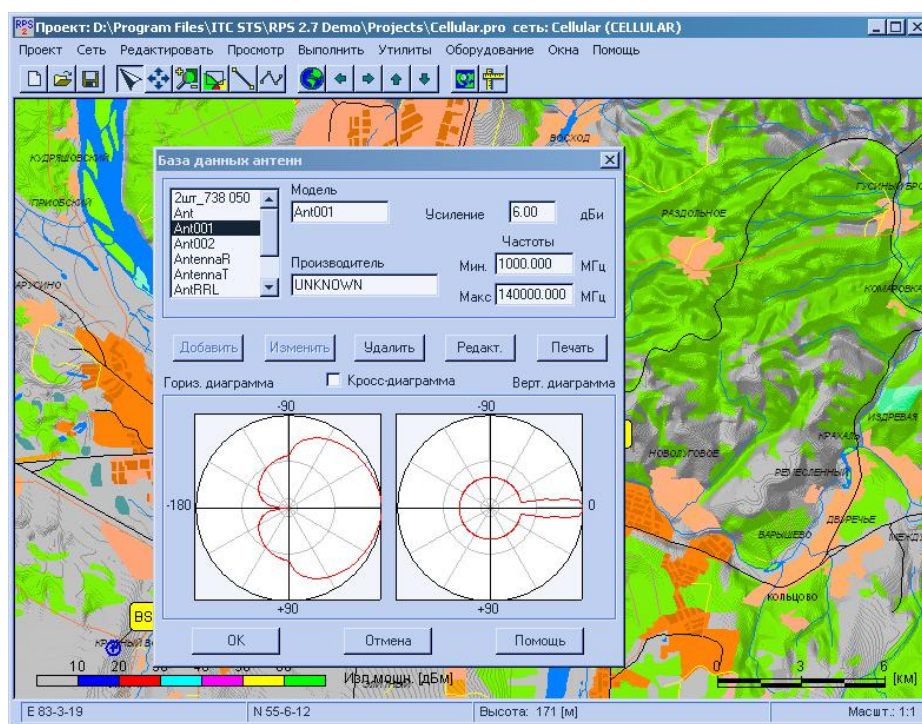


Рис. П1.4. Выбор антенн в базе данных программы

Балтика-РРЛ

Решаемые задачи:

- построение профиля трасс РРЛ;
- расчет потерь распространения радиоволн;
- расчет устойчивости связи;

- оптимизация высоты подвеса антенн.

Пользовательский интерфейс обеспечивает:

- ввод данных для построения профилей интервалов;
- ввод и редактирование исходных данных для расчетов;
- сохранение всех данных с целью их повторного использования;
- формирование и печать отчета.

При проведении расчетов учитывается:

- частота сигнала;
- поляризация;
- мощность передатчика;
- чувствительность приемника;
- потери в антенно-фидерных трактах передатчика и приемника;
- высоты подвеса и коэффициенты усиления антенн;
- параметры распределения градиента индекса рефракции;
- концентрация водяного пара в атмосфере;
- интенсивность выпадения осадков;
- профиль рельефа местности;
- характер местности.

Расчеты:

- потерь распространения с учетом дифракции на основе анализа профиля местности;
- ослабления в атмосферных газах;
- запаса на замирания;
- неустойчивости связи на интервале в условиях наихудшего месяца, в том числе:
 - составляющей неустойчивости связи при субрефракции;
 - составляющей неустойчивости связи, обусловленной влиянием дождей;
 - составляющей неустойчивости связи, обусловленной многолучевым распространением в атмосфере.

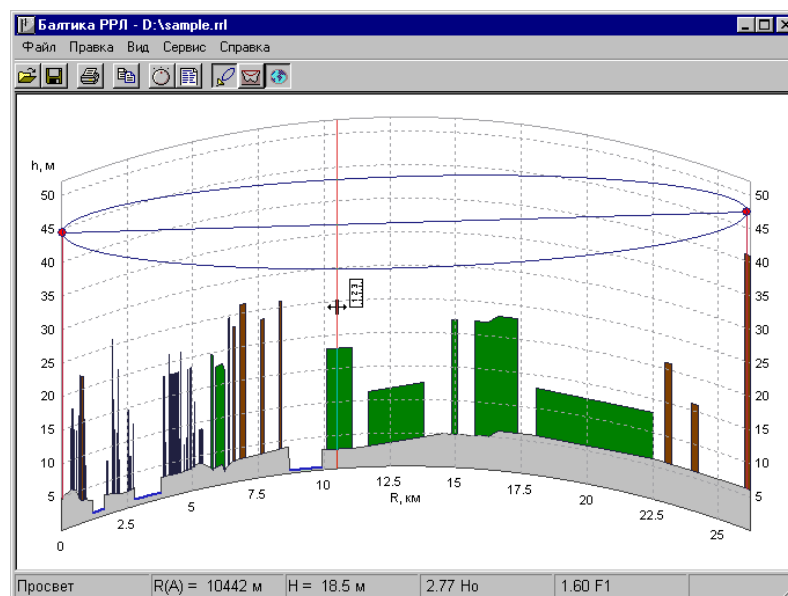


Рис. П1.5. Интерфейс программы

Отчет об интервале	
Основные параметры и результаты расчета интервала	
Уровень местности, м	Станция А 4.9
Направление передачи	А >> Б
Длина интервала, км	26.04
Частота, МГц	14000
Поляризация	вертикальная
Мощность передатчика, Вт	0.5
Высота подвеса передающей антенны, м	39.5
Усиление передающей антенны, дБи	30
Потери в передающем тракте, дБ	0
з.и.и.м., дБВт	26.99
Чувствительность приемника, дБВт	-125
Высота подвеса приемной антенны, м	41.4
Усиление приемной антенны, дБи	30
Потери в приемном тракте, дБ	0
Потери свободного пространства, дБ	143.74
Средние потери дифракции, дБ	0
Ослабление в атмосферных газах, дБ	0.64
Суммарные потери, дБ	144.38
Уровень сигнала на входе приемника, дБВт	-87.39
Запас на замирания, дБ	37.61
Составляющие неустойчивости сигнала	
(худший месяц):	
из-за дифракционных замираний, %	0
из-за атмосферной многолучевости, %	0.001861
из-за влияния дождей, %	0.022971

Рис. П1.6. Результаты расчетов

Расчеты основаны на рекомендациях МСЭ Р.530-7, Р.526-4, Р.676-3, Р.838 и "Методике расчета трасс аналоговых и цифровых РРЛ прямой видимости" (НИИР).

Проектирование и анализ радиосетей (ПИАР) версия 4.53

Технологии управления радиочастотным спектром включают в числе прочих следующие задачи:

- оценка электромагнитной обстановки (ЭМО) в местах предполагаемого размещения РЭС для обоснования решений о выделении полос, назначении радиочастот и принятия мер по повышению эффективности использования радиочастот, на основе оптимизации частотных присвоений, прогнозирования и измерения границ зон уверенного приема;
- анализ электромагнитной совместимости ЭМС РЭС (ВЧ устройств).

Для решения указанных задач в НПФ «ЯР» разработана система «Проектирование и анализа радиосетей» (ПИАР). Исходные данные для расчета ЭМО и ЭМС измеряются и прогнозируются по верифицированной методике, метрологически аттестованной в соответствии с ГОСТ Р8.563-96 (Свидетельство N 32/037-2002 от 19.03.2002 года), в связи с чем их достоверность гарантируется. В настоящее время ГИС ПИАР версии 4.53 находится в эксплуатации в 52 регионах России.

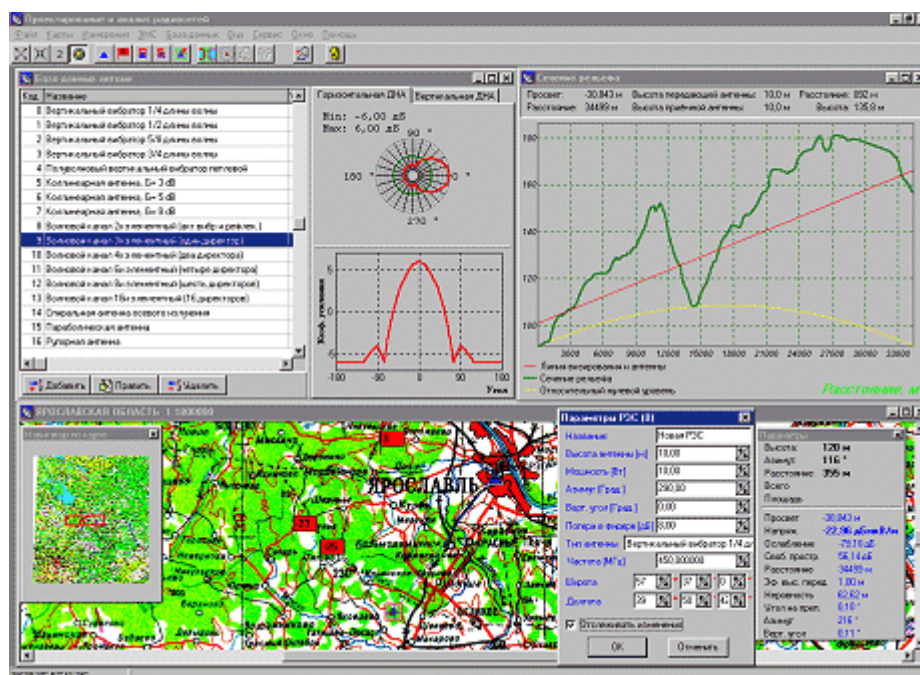
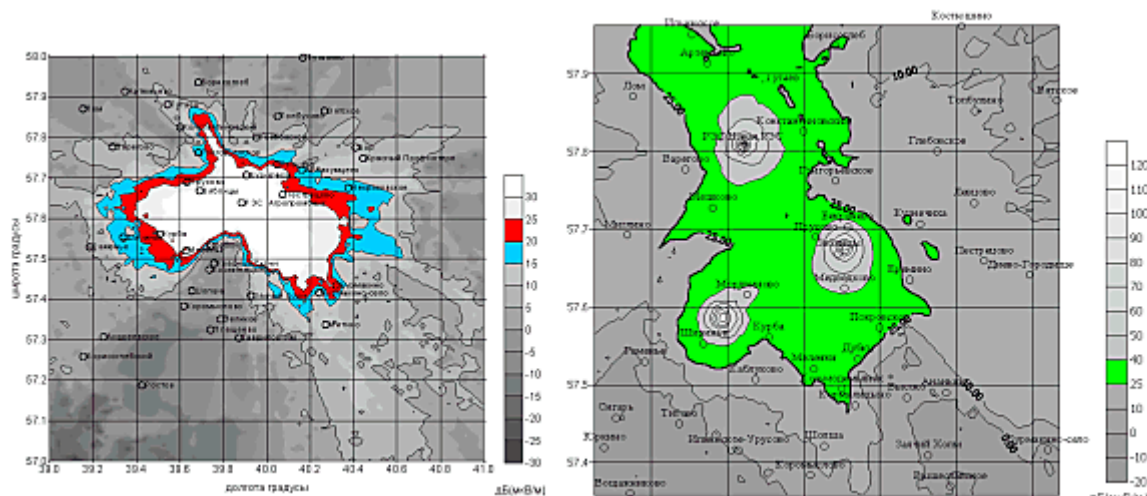


Рис. П1.7. Интерфейс программы ПИАР 4.53

ГИС ПИАР позволяет решать следующие основные задачи:

- производить анализ напряженности электромагнитных полей передатчиков,
- выполнять расчет карт напряженности поля,
- строить зоны уверенного радиоприема и радиосвязи,
- рассчитывать количество населения в зоне уверенного приема,
- анализировать ЭМС РЭС.

В пакет поставки входит утилита для математической обработки множества зон покрытия, позволяющая, например, строить пересечения, объединения зон и многое другое. Кроме того, Заказчику поставляются заполненные справочники типов РЭС (более тысячи наименований), антенн и классов излучений. Данные справочники постоянно пополняются фильтруемыми из множества источников достоверными сведениями.



Хочется отметить тот факт, что это единственный производитель который предоставил демоверсию своей программы для ознакомления. Программа обладает удобным

и понятным интерфейсом и позволяет выполнять все заявленные действия, в пределах доступных в демонстрационной версии.

DRRL версия 3.1

Программное обеспечение (ПО) DRRL версия 3.1 предназначено для автоматизации деятельности по проектированию цифровых радиорелейных линий (ЦРРЛ) и позволяет проводить расчеты качественных показателей ЦРРЛ в соответствии с рекомендациями Международного союза электросвязи (МСЭ).

При помощи программного обеспечения DRRL можно подобрать высоты подвеса антенн, характеристики антеннофидерного тракта линии, подобрать параметры или проверить пригодность того или иного типа оборудования для организации ЦРРЛ на заданном участке.

Расчет качественных показателей радиорелейной линии производится с учетом:

- замираний, вызванных многолучевым распространением радиоволн;
- замираний, вызванных влиянием субрефракции;
- влияния осадков на устойчивость работы РРЛ;
- ослабления сигнала в газах;
- эффективности частотного и пространственного разнесенного приема;
- внутрисистемных и внешних помех.

Ввод профиля интервала производится в табличной форме с удобным графическим интерфейсом, либо из любого текстового файла (опционально). Предусмотрен импорт высотных отметок профиля из таблиц MapInfo.

Принимая во внимание относительную сложность предмета, при создании данного программного обеспечения особое внимание уделялось простоте интерфейса пользователя, максимальной автоматизации вычислений, а также возможности получать отчеты о результатах вычислений в виде чертежей в соответствии с ГОСТ 21.101-97.

Необходимо отметить, что данное ПО, производимое в Новосибирске, наиболее популярно среди людей занимающихся непосредственным проектированием РРЛ. Но никакой демонстрационной версии фирма изготовитель в широкое пользование не предоставляет.

Цифровое радиорелейное оборудование в России.

Номенклатура продаваемых и производимых в России ЦРРС с кратким перечнем характеристик приведена в таблицах. Данные таблицы дают возможность оценить тенденции развития рынка ЦРРС в России.

ЦРПС зарубежных фирм, предлагаемые в России

Название	Завод, фирма.	Страна изготовитель	Сайт компании - изготовителя	Сигнал	Вых. мощность, дБм	Рабочие частоты, ГГц
9600LSY	Alcatel	Франция	http://www.alcatel.ru/	SDH 155 Мбит/с	30-35	3,6-11,7
9600LH						
9600USY						
MiniLink E	Ericsson	Швеция	http://www.ericsson.ru/	PDH 2,8,17,34 Мбит/с	17-26	7,1-39,5
Pasolink	Nec	Япония	http://www.nec.ru/	PDH 2 Мбит/с	12,5-26	5,9-40
Pasolink Plus				PDH 2 Мбит/с		
серия 3000				SDH 155 Мбит/с		
FlexLink	Nera	Норвегия	http://nera.com.ru/	PDH 2,34 Мбит/с	н/д	7,1-39,5
CompactLink				7,1-23,6		
InterLink				SDH 155 Мбит/с		3,6-11,7
CityLink				5,9-39,5		
EtherLink				12,5-26		5,9-39,5

ЦРПС российских производителей

Название	Завод, фирма	Город	Сайт компании - производителя	Сигнал	Вых. мощн, дБм	Рабочие частоты, ГГц
"БИСТ"	"Бист"	Чистополь	http://www.bist.ru/	PDH 2,8,34 Мбит/с	20-26	7,9-37
"БИСТ-8"						
"БИСТ-13"						
"БИСТ-23"						
Исеть	УПП "Вектор"	Свердловск	http://www.vektor.ru/	PDH 2,8,17,34 Мбит/с	20	14,4-15,2
Исеть-М				PDH 2,8,17,34 Мбит/с	20	
ВЭРТ-2РРС	Владимирский завод "Электроприбор"	Владимир	http://www.erlib.dials21.ru/	PDH 2,4,8 Мбит/с	30	1,7-2,1
WOCOM-E1,				PDH 2 Мбит/с	н/д	
WOCOM - 4E1				PDH 2,8 Мбит/с	н/д	

WOCCOM - Ethernet 10 Base T	"Вокком Системз"			10 Base T	н/ д	10,3-11,7
WOCCOM AS-40		Москва	http://wokkom.ru/	100 Base T	18	40-43
Перевал				PDH 2,8 Мбит/с	н/д	36-37
Кросс-8	"Импульс"	Москва	http://www.impuls.ru/	PDH 2,8 Мбит/с	20	37-39,5
Комплекс-5М1				10 Base T		
Комплекс-11	ЛЮНИИР	Санкт-Петербург	http://www.loniir.ru/	PDH 2,8 Мбит/с	27	10,7-11,7
Комплекс-15				PDH 2,8 Мбит/с	20	10,7-11,7
МИК-РЛ150М	"Микран"	Томск	http://www.mikran.ru/	PDH 2,8 Мбит/с	20	14,4-15,1
МИК-РЛ400М				256 Кбит/с	36	0,15-0,17
МИК-РЛ7 - МИК РЛ40Р				PDH 2 Мбит/с	36	0,39-0,45
МИК-РЛ4С - МИК-РЛ40С				PDH 2,8,34 Мбит/с	н/д	7-18
Радиус-7	Правдинский завод радиорелейной аппаратуры	Правдинск	http://www.pzra.nnov.ru/	PDH 2,8,34 Мбит/с	н/д	7,2-7,6
Радиус-15М				н/ д	14,4-15,4	
Радиус-ДС				н/д	7,9-8,4	
Радиан-8		Санкт-Петербург		PDH 2,8,17,34 Мбит/с	н/д	8
Радиан-15	"Радиан"		http://www.radian.spb.ru/			15
Радиан-23						23
"Эриком-11ЕЗ"	НПО "Радий"	Москва	http://www.radiy-niod.ru/	PDH 2,8,34 Мбит/с	24	10,7-11,7
"Эриком-11"				PDH 2,8 Мбит/с	17	10,7-11,7
"Эриком-13"						12,7-13,3
РЭСКОМ-15	"Росинтел"	Новомосковск	http://www.novomoskovsk.ru/	PDH 2,8,17,34 Мбит/с	22	14,5-15,35

АЗИД-5Ц				PDH 2,8,17,34 Мбит/с	38	
АЗИД-5ЦМ	Радиозавод им. А.С.Попова	Омск	http://www.relero.ru/	PDH 2,8,17,34 Мбит/с	37	0,39-0,45
Трасса-АЦ				PDH 2,8,17,34 Мбит/с	38	
MLink-G-L						
Mlink-G-M	Сеалтек	Москва	http://www.sealtek.ru/	PDH 2,34 Мбит/с	н/д	13-38
RadioRing				SDH 155 Мбит/с	н/ д	4-38
ФЛОКС				PDH 2,8,17,34 Мбит/с	30	1,4-2,7
ФЛОКС-4	МЦ "Фобос"	Москва	http://www.network-servise.ru/	PDH 2,8,34 Мбит/с	30	3,6-4,2
ФЛОКС-лайт				SDH 155 Мбит/с		
Просвет-18				Самарский "Экран"	з-д Самара	http://www.ekran.samara.ru/
				PDH 2,8,17,34 Мбит/с	20	17,7-19,7

TETRA в России

Стандарт TETRA (TETRA - Terrestrial Trunked Radio) - первый и пока единственный открытый общеевропейский стандарт цифровой транкинговой радиотелефонной связи - установлен ETSI (Европейским институтом по стандартизации в области телекоммуникаций), который координирует деятельность производителей оборудования, операторов сетей, национальных администраций и пользователей. Стандарт прошел через тщательную процедуру утверждения, что гарантирует TETRA высокое качество.

Наиболее крупные производители оборудования, операторы сетей, организации пользователей, тестирующие фирмы и разработчики программных приложений подписали в декабре 1994 года меморандум взаимопонимания (MoU) по продвижению технологии TETRA. В настоящий момент TETRA MoU объединяет более 97 компаний со всего мира. Прогноз перспектив развития стандарта TETRA показывает, что к 2010 году в сетях этого стандарта будет обслуживаться 5-10 миллионов пользователей.

С июня 2001 г. в России действует Некоммерческое Партнерство "TETRA-ФОРУМ", в которое вошли многие российские фирмы и организации, занимающиеся телекоммуникационным бизнесом. ЗАО "Компания "Информационная Индустрия" является членом Совета "TETRA-ФОРУМА". В 2002 году приказом Министра по связи и информатизации № 62 от 06.06.02 о реализации системного проекта "TETRAPUS" стандарт TETRA фактически выбран в качестве федерального стандарта для строительства сетей цифровой радиосвязи в России.

Она разработана для координации усилий российских ведомств и ведущих промышленных компаний по созданию сетей профессиональной радиосвязи на территории Российской Федерации. Программа реализуется под эгидой Мининформсвязи РФ. Ее целями являются объединение существующих и строящихся сетей профессиональной радиосвязи, гармонизация радиочастотного ресурса РФ и создание единой системы радиосвязи связи в интересах органов государственного управления, обороны, ведомств и крупных корпораций. В настоящее время в рамках программы «Тетрарус» построены фрагменты сети TETRA в Москве, Петербурге, Самаре, Калининграде, Курске, Казани, на Средней Волге (см., например, выпуск новостей nnIT.ru от 11 декабря 2006 г.).

Программа "Тетрарус"

Реализация программы "Тетрарус" способствует созданию системы профессиональной радиосвязи как необходимого элемента государственного управления, существенной экономии бюджетных средств, развитию высокотехнологичного производства и привлечению частных инвестиций.



Рис. П2.1. Развитие TETRA по программе Тетрарус на территории России

Цели программы:

- Объединение существующих и строящихся сетей профессиональной радиосвязи
- Гармонизация радиочастотного ресурса РФ
- Развитие отечественного производства оборудования TETRA и программных продуктов
- Создание единой системы радиосвязи связи в интересах органов гос. управления, обороны, ведомств и крупных корпораций



Рис. П2.2. Диаграмма пользователей сети TETRA

Связь для Олимпиады в Сочи: обязательные к выполнению строительство волоконно-оптических линий, наладка цифрового телерадиовещания, сети цифровой транкинговой связи стандарта TETRA на 10 тыс. пользователей и объектов электрической и почтовой связи обойдутся бюджету в 4 миллиарда рублей.

Мировые лидеры в области телекоммуникации, такие как Motorola, Nokia, OTE, Rohde&Schwarz BICK Mobilfunk, Teltronic S.A.U., DAMM Cellular Systems, Frequentis и др. продолжают работы по дальнейшему совершенствованию технологии TETRA, вводят в эксплуатацию сети связи TETRA в различных странах мира.



Рис. П2.3. Носимый абонентский терминал EADS Nokia THR-880i

Nokia THR880i предназначен для эксплуатации в системах TETRA, обеспечивающих связью службы общественной безопасности (милиция, скорая помощь, спасатели и др.) и имеет прочный корпус с алюминиевым шасси.

Функции: часы, будильник, календарь, калькулятор, журнал задач, лист напоминаний, предугадывающий ввод текста, 5 настроек профилей, записная книжка емкостью 255 номеров, концепция двухстороннего телефона, водонепроницаемый, пылезащитный и искробезопасный корпус, голосовые подсказки, кнопка экстренного вызова, управление громкостью, меню быстрого доступа, настройка нескольких пользователей и др. Функция позиционирования.

Полностью графический дисплей высокого разрешения (65536 цветов, 130x130 пикселей), ручная установка уровня контраста.

Клавиатура: алфавитно-цифровая, 10 функциональных клавиш, 10 кнопок быстрого доступа (menu + 0...9), аварийная кнопка, вращающиеся селекторы выбора групп и регулировки громкости (отдельная кнопка «вкл/выкл»), стрелочные кнопки выбора в меню и телефонной книжке, функция блокировки клавиатуры.

Типы вызовов:

Групповые;
 Экспресс-вызовы в системе TETRA;
 Телефонные внутри системы TETRA и в/из ТФОП и УАТС (дуплексные);
 Аварийные вызовы;
 Позднее подключение к разговору.

Групповые функции:

Присвоение номеров динамических групп;
 Сканирование групп, приоритеты;
 Поддержка до 1300 разговорных групп,
 Разбиение групп по блокам;
 Селектор выбора групп, кнопка выбора базовой группы;
 Голосовые подтверждения выбора групп.

Функции позиционирования:

Наличие встроенного GPS-приемника;

Вызов функции позиционирования возможен по запросу или при аварийных вызовах;

Вывод на дисплей терминала координат, высоты местоположения, а также направление и скорость движения;

Совместим с WAP и приложениями PC;

Передача данных по NMEA на порт RS-232.

Передача данных:

Статусные и короткие сообщения;

IP данные (single slot 7,2 кбит/с);

WAP 1.2.1;

XHTML браузер.

Вес 247 г.

THR880i имеет сертификат Ростеста и находится на сертификации в Министерстве связи РФ

Оборудование работающее на системе EDACS**Портативная радиостанция LPE Series**

Частотный диапазон - 806-825, 851-870 МГц

Мощность передатчика - 1- 3 Вт

Чувствительность приемника - 0,35 мкВ

Размеры - 144x58x35 мм

Время работы от батареи - 12 часов

Масса - 589 г

Напряжение питания - 7,5 В

Автомобильная/стационарная радиостанция EDACS-500M

Частотный диапазон - 806-825, 851-870 МГц

Мощность передатчика - 6-25 Вт

Чувствительность приемника - 0,35 мкВ

Размеры - 243x175x50 мм

Масса - 2,3 кг

Напряжение питания - 12 В

Рис. П2.4. Оборудование работающее на системе EDACS

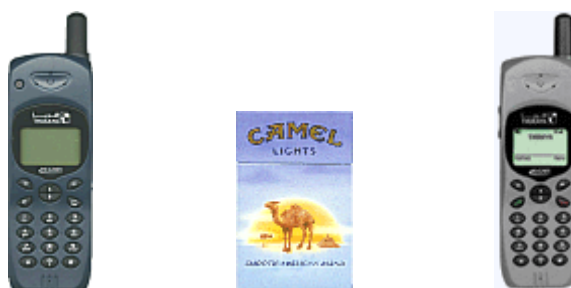
Модели спутниковых телефонов

Самые надежные спутниковые телефоны работают в сети **Инмарсат**. Проверенные временем и самыми жесткими условиями эксплуатации, они уже более 20 лет являются стандартом в мире систем спутниковой связи. Однако высокая цена, большие размеры и вес не позволяют их использовать их так же, как и сотовый телефон. Спутниковые телефоны системы Инмарсат представляют собой чемоданчик с откидной крышкой размером с первые портативные компьютеры. Крышка спутникового телефона по совместительству является и антенной, которую необходимо поворачивать по направлению на спутник (на дисплее телефона отображается уровень сигнала). В основном такие телефоны используются на судах, поездах или большегрузных автомобилях. Каждый раз, когда Вам необходимо позвонить или ответить на чей-то звонок, нужно будет устанавливать спутниковый телефон на какую-нибудь ровную поверхность, раскрывать крышку и крутить его, определяя направление максимального сигнала. Стоят такие спутниковые телефоны более 2500 долларов и весят от 2,2 кг. Минута разговора по такому спутниковому телефону обойдется Вам от 2,5 долларов США. Входящие звонки бесплатно, однако на Ваш спутниковый телефон не смогут позвонить с обычного телефона, а только с сотового или со специальной коммерческой линии (Совинтел, Комбеллга). Звонок с Билайна обойдется в 12 долларов за минуту, с коммерческой линии Комбеллги - в 7 долларов за минуту.



Система **Турайя** (Thuraya) - лакомая новинка на российском рынке спутниковой связи. Сама компания была образована еще в 1997 году, однако предоставление услуг на территории России началось только с этого года. Спутниковые телефоны этой системы позволяют разговаривать как в спутниковом, так и в сотовом режиме. Более того, для обоих режимов предусмотрен единый номер, которые остается постоянным даже при переключениях между режимами. Вы получаете возможность постоянно быть на связи и выбирать наиболее выгодные для Вас тарифы. О тарифах стоит сказать отдельное слово - они действительно самые низкие из всех российских операторов спутниковой связи. Часто, особенно в случае международных звонков, использование спутникового режима оборачивается реальной экономией: два абонента «Турайя», находясь на разных континентах, могут разговаривать за \$0,5 в минуту. Стоимость же разговора по наземному или сотовому телефону составит \$2-\$4 в минуту. Прочие достоинства спутниковых телефонов Турайя: бесплатные входящие звонки в спутниковом режиме, встроенный GPS-приемник с точностью до 100 метров (особенно полезно для тех, кто часто путешествует), гибкие тарифные планы (авансовые, кредитные). Однако, несмотря на столь низкие цены, компании удается обеспечивать достаточно хорошее качество услуг.

Сравнительные размеры мобильных спутниковых телефонов Турайя и пачки сигарет



Мобильные спутниковые телефоны Турайя (Thuraya)



Thuraya Ascom 21

- Телефонная связь по сети GSM и по спутниковой сети связи "Турайя"
- Передача данных и факсимильных сообщений со скоростью: 2.4, 4.8, 9.6 кбит/сек
- Определение местоположения (GPS) и сохранение 10 положений GPS



Thuraya Hughes 7100

- Телефонная связь по сети GSM и по спутниковой сети связи "Турайя"
- Передача данных и факсимильных сообщений со скоростью: 2.4, 4.8, 9.6 кбит/сек
- Определение местоположения (GPS) и сохранение 10 положений GPS

Спутниковые телефоны системы **Глобалстар** более подходят для использования в качестве дополнения к сотовому телефону. Трубки спутниковых телефонов Глобалстар - размером с первые сотовые, а весят они от 400 до 500 грамм. Некоторые модели позволяют работу в как в режиме спутникового, так и в режиме сотового. Вы можете настроить его так, чтобы он автоматически переключался между сотовой и спутниковой связью. Это позволяет не только экономить, но и избавляет Вас от основной проблемы всех спутниковых телефонов - требования прямой видимости спутника. Это требование распространяется на спутниковые телефоны всех существующих и всех будущих систем спутниковой связи, и связано в первую очередь с диапазоном частот, на которых они работают (в лучшем случае до ближайшего спутника 1500 километров). Спутниковые телефоны системы Глобалстар завоевали достаточно большую популярность не только благодаря малым размерам или возможности работать в сотовых сетях - их основное превосходство над конкурентами заключается в цене на оборудование и стоимости связи. Спутниковый телефон Telit SAT 550 стоит \$699 без НДС, а минута разговора обойдется Вам в 89 центов (65 центов при корпоративном тарифе). Входящие звонки еще дешевле - 69 центов (49 центов при корпоративном тарифе).

Подробнее о спутниковых телефонах Глобалстар:

Спутниковый телефон Telit SAT 550 - самый недорогой (\$699 без НДС), но может работать в двух режимах - спутниковом и сотовом. Переключение между режимами может быть автоматическим (при выходе из зоны покрытия сотовой связи телефон автоматически начинает искать спутник), либо ручным - через меню. Достаточно прочный спутниковый телефон, используется в основном при строительстве или разведке на неосвоенных территориях. Основные пользователи этого спутникового телефона -



строители, геолого-, нефте- и газоразведочные бригады, туристы. Телефон отлично себя зарекомендовал, батареи хватает на 1,5 часа разговора или 20 часов ожидания. Есть зарядное устройство от прикуривателя автомобиля. Недавно появился комплект для передачи данных, что позволяет организовать доступ в Интернет (при скорости в 9,6 кбит/с). Этой скорости вполне достаточно для проверки почты или передачи от 6 до 15 одностраничных документов в формате Microsoft Word без рисунков.

Спутниковый телефон Ericsson R-290 - средний по стоимости (\$899 без НДС), однако до последнего времени самый красивый из глобалстаровских телефонов. Также может работать как в режиме сотового, так и в режиме спутникового телефона. Можно использовать как "тонкие", так и "толстые" батареи. "Тонкой" батареи хватает на 1,5 часа разговора или 6 часов ожидания. Спутниковые телефоны этой модели часто возвращаются по гарантии, и к ним есть просто удивительно мало аксессуаров, так что мы Вам его не рекомендуем.



Спутниковый телефон Qualcomm GSP 1600 - до недавнего времени самый дорогой из спутниковых телефонов Глобалстар (\$1099 без НДС). Теоретически может работать в режиме сотовой связи, однако немногие российские операторы сотовой связи работают в поддерживаемых им режимах (AMPS, CDMA). Полезная для туристов функция - определение координат местоположения. Точность небольшая (погрешность может составлять сотни метров), однако чаще всего этого достаточно для ориентирования на местности. Меню на русском или английском языке. Этот спутниковый телефон поддерживает передачу данных - при покупке специального комплекта его можно использовать как модем (скорость передачи 9,6 кбит/с). Достаточно много аксессуаров, включая hands-free, адаптер для автомобильного прикуривателя, автомобильный комплект. Если Вы планируете большую часть времени находиться в автомобиле, Вам стоит купить автомобильный комплект - без него Вам придется при каждом разговоре выходить из машины. Автомобильный комплект для этого спутникового телефона представляет собой базу, в которой фиксируется телефон, и антенны, которая выносятся на крышу автомобиля. Стандартной батареи хватает на 3,5 часа разговора, или 9 часов ожидания, так что обычно покупается 2 батареи, одна из которых лежит "про запас".

Спутниковый телефон Telit SAT 600 - абсолютный "хит сезона". Самый красивый и современный спутниковый телефон из всех телефонов Глобалстар. Пока не продается, ожидаемая стоимость - от 1500 долларов. Никто им пока не пользовался, но фирма-изготовитель внушает доверие (выше мы уже описывали спутниковый телефон Telit SAT 550). Заявлено, что телефон будет поддерживать передачу данных со скоростью 9,6 кбит/с, работать в сотовых и спутниковых сетях, в него будет встроен блок определения местоположения. Батареи будет хватать на 3,5 часа разговора или 10 часов ожидания. Достаточно легкий телефон - 340 грамм. Интересный аксессуар - солнечная батарея. Есть автомобильный комплект.



Все вышеперечисленные спутниковые телефоны поддерживают работу с SMS (отправить SMS на спутниковый телефон Глобалстар можно с сайта или по электронной почте - этот сервис бесплатный). Если Вы приобретаете 10 или более спутниковых телефонов, Вы становитесь корпоративным клиентом. Основная выгода - отсутствие абонентской платы (экономия в 20 долларов на каждый аппарат) и примерно 15%-скидки на стоимость связи.

Если Вам не нужен мобильный спутниковый телефон, но Вы хотите обеспечить связь свой офис или дом в достаточно отдаленном месте, то Вам подойдет стационарный спутниковый телефон. Более точно будет назвать его "спутниковой базой", поскольку он представляет из себя электронный блок и выносную антенну. К электронному блоку можно подключать обычные телефоны/факсы/модемы/атс. Подключение оборудования не требует изменения настроек. В некоторых случаях использование стационарного комплекта даже выгоднее, так как тарифы на связь там равны корпоративным даже при малом количестве спутниковых телефонов.

Стационарный спутниковый телефон Ericsson EF-200 (\$1899 без НДС) - достаточно простая в установке модель, одна аналоговая телефонная линия позволяет параллельное подсоединение до 5 телефонных аппаратов. Питание спутникового телефона может осуществляться как от аккумулятора или сети, так и от солнечной батареи. Допустимый диапазон температур в рабочем режиме - от -30 до +60, в выключенном состоянии - от -40 до +85. Телефонные аппараты могут быть удалены от спутниковой базы на расстояние до 1600 метров.

Спутниковый таксофон Schlumberger Access - таксофон для работы в спутниковой сети Глобалстар. Как правило, такая модель устанавливается в местах, плохо защищенных от вандализма или плохих погодных условий. Оплата разговоров карточками, возможно сменять карточки без обрыва текущего разговора, защита от подделки (эмуляции) карточек.

Рассмотрим самые популярные модели спутниковых телефонов Инмарсат:

Портативный спутниковый телефон Thrane&Thrane TT-3060A - легкий, компактный и удобный спутниковый телефон для приема и передачи телефонных, факсимильных сообщений, данных и электронной почты в любой точке мира.



Портативный спутниковый телефон NERA WorldPhone Office - где бы Вы не находились, Вы всегда будете на связи с Nera WorldPhone Office. Идеальный помощник бизнесмена весом чуть больше 2 килограмм и размером с наколенный компьютер, Nera WorldPhone Office объединяет в одном корпусе телефонный аппарат, антенну (встроена в крышку), интерфейс к факсу и компьютеру.

Стационарный спутниковый телефон TT-3066A Capsat 'Big Dish' - реальная альтернатива прокладке телефонной линии связи и установке фиксированного аппарата. Теперь стало возможным практически из любого труднодоступного участка Земли мгновенно связаться по телефону с любым абонентом в мире, а также отправить факс, данные или электронную почту.



Стационарный спутниковый телефон Nera WorldPhone Provident - спутниковый телефон с увеличенной антенной, используется преимущественно в районах с небольшой плотностью услуг связи. 'Провидент' позволяет в кратчайшие сроки при небольших начальных инвестициях, по сравнению с другими системами связи, оснастить высококачественной связью территории, которые ранее не были доступны для наземных сетей связи.





Автомобильный спутниковый телефон TT-3062D - Благодаря компактному дизайну и крепкому корпусу, TT-3062A может быть легко установлен в большинстве современных автомобилей. Управляется с трубки, как обычный GSM-телефон, либо (через интерфейс данных) с компьютера. Возможно подключение обычного телефона (вместо трубки). Антенна и трубка могут быть удалены от основного блока на 70 метров.



Автомобильный спутниковый телефон Nera WorldPhone Liberator - жесткий алюминиевый корпус - гарантия функционирования телефона в любых, даже самых неблагоприятных условиях эксплуатации - на судах, поездах, автомобилях и самолетах. Работа телефона, в отличие от других телефонов серии Nera WorldPhone, полностью управляется с трубки. Малые размеры телефона дают возможность закрепить его в самых подходящих для этого местах - на приборной панели автомобиля, под сиденьем или на стене рубки яхты. Интерфейс к компьютеру - Ваша возможность отправлять и получать электронную почту, фотоснимки, факсы и документы.

Сравнение систем Globalstar и Iridium

Несмотря на общеизвестные финансовые проблемы Иридиум и Глобалстар в прошлом и настоящем, фактом является то, что обе компании продолжают эксплуатировать свои системы и предлагать услуги клиентам по всему миру. У тех потенциальных покупателей, которые задумываются о покупке спутникового телефона, возникает вопрос «который из них будет больше соответствовать моим нуждам?». Существует множество критериев, позволяющих ответить на этот вопрос; это такие критерии как плановое использование, стоимость трубки, поминутные расценки, качество услуг, и каждый потенциальный пользователь поставит свой приоритет по каждому из этих критериев.

Одной из характеристик спутниковых телефонов, задействованных в количественном исследовании, является «качество услуг». Группа по спутниковой коммуникации «Frost & Sullivan», международной консалтинговой компании исследования и роста рынка, в качестве конечного пользователя провела сравнение систем Иридиум и Глобалстар с целью определения их соответствующих качеств по критерию «качество услуг». Произведенные измерения, включая завершение вызова, качество речи, сброс вызова и скорость передачи данных, были статистически оценены в различных условиях с целью предоставления объективной оценки данного сравнительного критерия.

Исследование было задумано в первую очередь для того, чтобы изучить качество прохождения вызова и передачи данных этих двух спутниковых телефонов. Метод рассчитан на потенциального покупателя портативного спутникового телефона, которому необходимо совершать голосовые вызовы и передавать данные. Тестирование было задумано, чтобы определить, какая спутниковая телефонная система может предоставить превосходное качество вызова и передачи данных.

Таблица ПЗ.1 дает общее описание оборудования и ПО, использованного в настоящем сравнении продукции.

Таблица ПЗ.1. Общее описание трубок и пакета данных, использованных в исследовании

Иридиум	Глобалстар
Модель трубки: Портативный спутниковый телефон Моторола, серия 9500	Модель трубки: Трехмодовый портативный телефон Квалкомм GSP-1600
Версия ПО трубки: INC0620	Версия ПО трубки: 5.3.1.1.0
Комплект данных: Комплект данных для портативного телефона Моторола 9500	Комплект данных: GDC-1100
ПО: Всемирные услуги данных 15 июня 2001	ПО: Услуги данных в. 1.1

Последовательное сравнение голосовых вызовов

В общем, на обе системы пришлось более, чем 1.200 минут эфирного времени в сериях испытаний состоящих более, чем из 200 вызовов. Методика тестирования была поставлена так, чтобы можно было гарантировать, что какие-либо выявленные отклонения были вызваны только спутниковой телефонной системой. Таким образом, все вызовы спутникового телефона совершались на фиксированные линии в пределах Соединенных Штатов. Ни один из вызовов, использованных в целях исследования, не был сделан в зарубежные точки, а также на сотовые линии. Голосовые вызовы также совершались из двух географических различных точек, Техас и Калифорния.

Первоначальные измерения, взятые для голосовых вызовов, были следующие:

Доступность услуги

Завершение вызова (Происходит ли соединение вызова при завершении набора)

Качество речи (оценено по шкале от 1 до 5)

Длительность вызова (Длительность вызова в минутах и секундах)

Сброс вызова (Происходит ли прерывание вызова неожиданно)

Тестирование возможностей голосового вызова двух спутниковых телефонных систем было выполнено в два различных этапа. В первый этап оба телефона тестировались в идеальных условиях. Это предполагает абсолютно чистое небо, свободное от каких-либо препятствий выше 10 градусов над горизонтом. Тестирование также проводилось вдали от каких-либо возможных сигнальных помех, которые могли быть вызваны аэропортами, промышленными зонами или какими-либо другими действиями.

Результаты тестирования в идеальных условиях показали, что по большинству аспектов спутниковые телефоны продемонстрировали сходные результаты. У обоих телефонов не наблюдалось прерываний в работе, и первая попытка завершения вызова составила 97% у Иридиума и 100% у Глобалстар. Первая попытка завершения вызова является измерением частоты, с какой вызов был успешно сделан в первую попытку набора телефонного номера. Задача всех звонков заключалась в том, чтобы сохранить связь, по крайней мере, в течение 5 минут и продолжительность примерно 1/3 вызовов довести до 12 минут. Большая продолжительность вызова была желательна, чтобы сохранить связь в течение достаточно долгого срока для подтверждения, что передача вызова с одного спутника на другой происходит во время прохождения спутников в небе.

Таблица ПЗ.2 обобщает данные по голосовым вызовам, совершенным в идеальных условиях.

Таблица ПЗ.2. Сравнение голосовых вызовов в идеальных условиях

Средняя продолжительность вызова:	
Иридиум	8 минут 34 секунды
Глобалстар	8 минут 50 секунд
Процент соединения вызова при первой попытке:	
Иридиум	97%
Глобалстар	100%
Среднее качество речи (от 1 нечеткого до 5 идеального):	
Иридиум	3.1
Глобалстар	4.0
Среднее число сбросов вызова:	
Иридиум	18.4%
Глобалстар	2.6%

Система Глобалстар имела очень низкий уровень сброса, составляющий 2.6% при идеальных условиях. Система Иридиум не показала таких хороших результатов в этой оценке, ее процент сброса составил 18.4% при идеальных условиях. Наиболее сильное различие между двумя системами прослеживалось в качестве речи. В то время, как качество речи вызова может быть субъективной оценкой, во всех случаях отмечалось, что качество речи у Глобалстар было лучше чем у Иридиум. Ухудшение звукового сигнала и заметная задержка во времени стали причиной значительно более низкой оценки звонков Иридиум в этом испытании практически в каждом примере. Результат особенно был заметен на принимающем конце (т. е. для лица, принимающего звонок от кого-либо, говорящего по спутниковому телефону). Повторяющиеся замечания относительно частой потери слов или частей слов, скорее всего, были вызваны потерей пакетов данных. Также отмечалось характерное «замедление речи» у Иридиума, которое предавало звонящему со спутникового телефона лицу плавающий голос. При идеальном течении сценария, Иридиум набрал в среднем 3.1 балла по пятибалльной шкале от 1 (нечеткого) до 5 (идеального) с фактической оценкой от самого низкого 1 балла до высокого – 4 балла.

Разговоры по спутниковому телефону Глобалстар в целом показали лучшие результаты, чем Иридиум и могли быть даже охарактеризованы как близкие к сотовому телефону с хорошим качеством. В 23% случаев при идеальных условиях, качество речи у Глобалстар могло быть охарактеризовано как равное или лучше, чем у сотового телефона, в то время как Иридиум ни в одном случае не достиг качества сотового телефона в каких-либо из своих вызовов. Глобалстар был оценен на 4.5 балла или выше в речевом качестве. Рисунок ПЗ.1 показывает оценки речевого качества для обоих телефонов в различной среде вызовов.

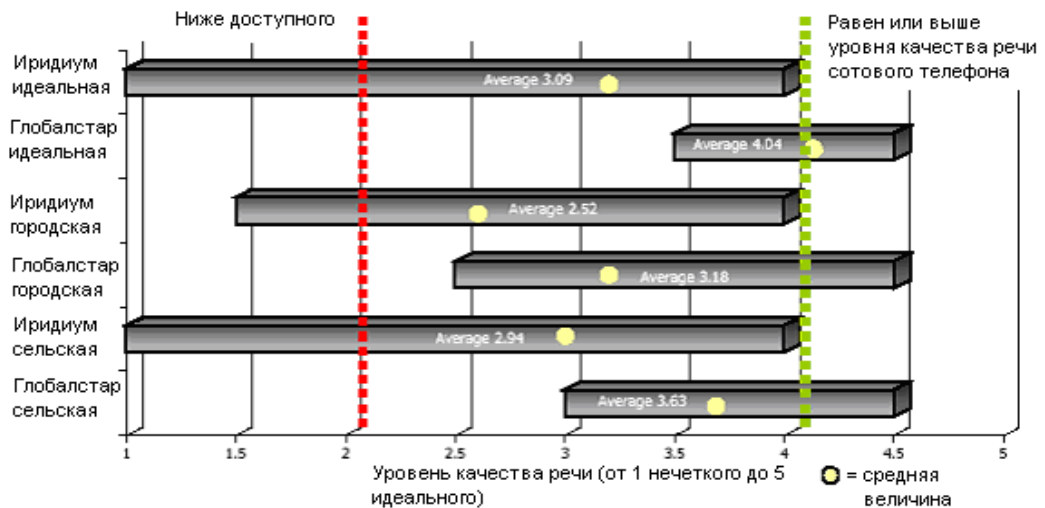


Рис. ПЗ.1. Сравнение речевого качества в различной среде

Следующий этап исследования заключался в проведении всестороннего тестирования двух спутниковых телефонных трубок в значительно более трудной среде. Две другие среды были городская или сельская. В обоих случаях были проделаны такие же тесты, какие перечислялись выше. Во многих случаях, тестирование подводило оба спутниковых телефона к их исчерпывающим возможностям. Методика была разделена таким образом, что каждый спутниковый телефон мог быть протестирован в условиях заметного ухудшения сигнала. Городское тестирование измерило результат общеизвестного «городского каньона», а сельское тестирование досконально исследовало такие факторы как лиственный покров и пересеченную местность.

Две системы работали, как и ожидалось в различных ситуациях: при больших физических сигнальных помехах, наблюдалось большее число сбросов вызовов и недоступность сервиса. Было ясно видно, что обе телефонные системы фактически могли работать в ситуациях, которые не рекомендуются поставщиками услуг.

В городской среде, завершение вызова для Иридиума составило 77% и 89% для Глобалстар. Это сопоставимо с 87% и 87% соответственно в сельской среде. (Эти цифры представляют завершение вызова в течение 4 попыток; завершение вызова с первой попытки показаны в графиках ниже.) В конечном счете, многочисленные успешные вызовы были сделаны в ситуациях довольно трудной среды. Также, большое различие между вызовами спутникового телефона Иридиум и Глобалстар было отмечено в том, что Иридиум значительно уступал в качестве речи. Шкала качества речи была сделана таким образом, что любое качество речи, оцененное на 2 балла или более низшую оценку (по шкале от 1 до 5 как описано выше), рассматривается как ниже минимума, необходимого для какой-либо деятельности.

Из всех вызовов, которые были завершены (т. е. соединение вызова было установлено) в городской среде, речевое качество Иридиум может быть рассмотрено как выше критического уровня только в 67% из всех завершённых вызовов в сравнении с 100% для Глобалстар. В сельской среде, Иридиум был оценен выше критического уровня на 85% из всех завершённых вызовов по сравнению с 100% для Глобалстар.

Другой основной фактор – сбросы вызовов. Здесь было отмечено схожее процентное соотношение сбросов вызовов. 70.4% в городских районах и 40.7% в сельских районах у Иридиум и 64.5% в городских районах и 37.0% в сельских районах у Глобалстар.

Более того, можно сказать, что блокировка сигнала остается блокировкой сигнала независимо от системы. При достаточно ясном небе, обе системы продемонстрировали свою функциональность, и основное отличие заключалось в качестве речи. Во всех условиях, система Глобалстар снова и снова показывала существенное и небольшое превосходство перед системой Иридиум в данном аспекте.

Таблицы ПЗ.4 и ПЗ.4 обобщают заключения по использованию двух спутниковых телефонных систем в сельской и городской среде.

Таблица ПЗ.3 Сравнение голосовых вызовов в сельской среде

Средняя продолжительность вызова:	
Иридиум	5 минут 03 секунды
Глобалстар	5 минут 51 секунда
Процентное соотношение соединения вызова с первой попытки:	
Иридиум	71%
Глобалстар	84%
Средняя оценка качества речи (от 1 нечеткого до 5 идеального)	
Иридиум	2.9
Глобалстар	3.6
Средняя оценка сброса вызова:	
Иридиум	40.7%
Глобалстар	37.0%

Таблица 2.4 Сравнение голосовых вызовов в городской среде

Средняя продолжительность вызова:	
Иридиум	3 минуты 35 секунд
Глобалстар	4 минуты 14 секунд
Процентное соотношение соединения вызова с первой попытки:	
Иридиум	74%
Глобалстар	83%
Средняя оценка речевого качества (от 1 нечеткого до 5 идеального):	
Иридиум	2.5
Глобалстар	3.2
Средняя оценка сбросов вызова:	
Иридиум	70.4%
Глобалстар	64.5%

Рисунки ПЗ.2 и ПЗ.3 показывают сравнительную оценку соединения и сброса вызова телефонов Иридиум и Глобалстар по вызовам, сделанным во всех типах среды, и демонстрируют преимущество Глобалстар в соединении и сбросе вызова.



Рис. ПЗ.2. Сравнение всех соединений вызовов Иридиум и Глобалстар при идеальной, городской и сельской среде

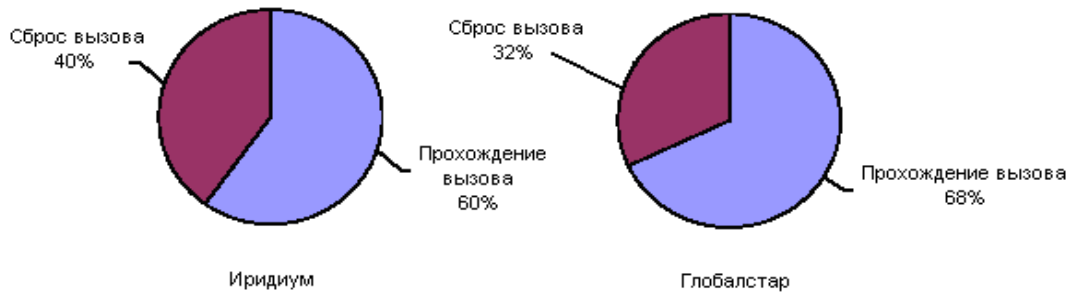


Рис. ПЗ.3. Сравнение всех сбросов вызова у Иридиум и Глобалстар в идеальной, городской и сельской среде

Биты и байты передачи данных

Стандартные приложения, рассмотренные в этой части исследования, касаются использования трубок Глобалстар и Иридиум, подсоединенных к портативному компьютеру, для e-mail доступа и загрузки простых данных. Часто для таких приложений требуется Интернет браузер http. Это создало проблему для нашего тестирования, поскольку не существует какой-либо простой методики, чтобы с легкостью можно было бы сравнить в количественном соотношении просмотр web страниц на двух спутниковых телефонных системах. Такие действия как скачивание, получение доступа, архитектура web страниц, утерянные пакеты и занятые серверы делают затруднительным установку анализа таким образом, чтобы какие-либо потенциальные проблемы могли быть изолированы от сети спутниковой системы. При возникновении сомнений, чем вызваны задержки, сложно сделать четкое количественное исследование.

По этой причине, эксперимент, затрагивающий сервис передачи данных, был разделен на две части. Сперва, для того, чтобы произвести количественные измерения, телефоны были протестированы с использованием протокола передачи файлов (ftp) с сервера, расположенного на высокоскоростном соединении с Интернетом. Были выбраны два файла и произведены многократные загрузки с тем, чтобы определить скорость передачи фактических данных. Вторая часть исследования представляла собой количественную оценку загрузки web в обеих системах. Эти результаты представлены в следующей секции.

Таблица ПЗ.5. Общий обзор деталей FTP данных

Информация по тестированию данных	
Использованный сайт	ftp.esr'l.com
Использованный клиент	WS_FTP LE32
Максимально сжатый файл:	aaa_win.apr
Размеры файла	151704 байта
Коэффициент потенциального сжатия	1 : 5.7
Минимально сжатый файл:	appatch_digu.tar.Z
Размеры файла	154290 байт
Коэффициент потенциального сжатия	1 : 1.1
Использованный коммутируемый сервис	Соединение 56K UUNet в Millbrae, CA

При загрузке данных, каждый файл был загружен 80 раз, что означает более, чем 20 МБ, загруженных через комбинированные системы. Это было сделано равно как через пакетные, так и коммутируемые режимы, предложенные каждым поставщиком услуг. Пакетный режим является режимом, через который Глобалстар и Иридиум предоставляют доступ в Интернет через свои соответствующие станции сопряжения, а режим коммутации

является режимом, в котором используется независимый поставщик услуг Интернет (ISP) для предоставления доступа в Интернет (в особенности коммутируемое соединение через спутник).

Потенциальное сжатие файлов важно, поскольку Иридиум предоставляет собственную технологию сжатия данных для увеличения скорости передачи данных при использовании своего пакетного сервиса. ПО автоматически сжимает файлы перед тем, как они проходят через спутниковую сеть. Конечно, некоторые файлы больше подвержены сжатию, чем другие. Поэтому, два файла, выбранные для этого исследования имеют различные коэффициенты потенциального сжатия и, как будет видно из данных ниже, это приводит к некоторым важным сведениям.

Таблица ПЗ.6 и Таблица ПЗ.7 показывают скорость передачи данных и время загрузки для максимально и минимально сжимаемых файлов, как в пакетных, так и коммутируемых сценариях. В дополнение ко всему приводится процент успешной загрузки.

Таблица ПЗ.6 Обзор детализации данных FTP

Использованный сайт	ftp.esr'l.com
Использованный клиент	WS_FTP LE32
Максимально сжимаемый файл:	aaa_win.apr
Размеры файла	151704 байта
Коэффициент потенциального сжатия	1 : 5.7
Минимально сжимаемый файл:	Appatch_digu.tar.Z
Размеры файла	154290 байт
Коэффициент потенциального сжатия	1 : 1.1
Использованная коммутируемая служба	Соединение 56K UUNet в Миллбрае, КА

Таблица ПЗ.7. Обзор детализации данных FTP

Сравнение загрузки данных при использовании служб коммутации

Средняя скорость передачи данных для максимально сжимаемых файлов:	
Иридиум	2.19 Кб/сек
Глобалстар	6.31 Кб/сек
Среднее время загрузки для максимально сжимаемых файлов:	
Иридиум	9.4 минуты
Глобалстар	3.2 минуты
Средняя скорость передачи данных для минимально сжимаемых файлов:	
Иридиум	2.21 Кб/сек
Глобалстар	6.02 Кб/сек
Среднее время загрузки для минимально сжимаемых файлов:	
Иридиум	9.4 минуты
Глобалстар	3.5 минуты
Процент успешных попыток загрузки:	
Иридиум	70%
Глобалстар	100%

Стоит заметить, что по сравнению со скоростью данных, к которой большинство конечных пользователей привыкло в рабочей и домашней обстановке, две системы работают

достаточно медленно. Это не удивительно, поскольку обе системы были спроектированы главным образом для предоставления голосовых вызовов. Тем не менее, исследование показывает, что Иридиум соизмерим с Глобалстар в единственной категории, относящейся к загрузке максимально сжимаемых файлов при использовании своего сервиса пакетных данных. Это происходит благодаря вышеупомянутому использованию технологии сжатия данных Иридиум. В любом другом случае, Глобалстар значительно опережает Иридиум.

В то время как обе системы ищут пути улучшения скорости передачи данных, для потенциальных пользователей сжатых данных скорость передачи данных от 2.28 до 7.62 Кб/сек, той и другой спутниковой телефонной системы, была бы не приемлема. Однако если требование конечных пользователей не выходит за рамки загрузки файлов или электронной почты, ограниченных несколькими 100 килобайтами, то сравнительное тестирование показывает, что система Глобалстар предлагает более высокую скорость передачи данных в сравнении с системой Иридиум во всех условиях. Это также неудивительно, при наличии основных технических различиях, которые присущи разработке каждой системы. Это также показывает, что в то время как Иридиум может достигать (и достигает) скорости до 8Кб/сек, обычная скорость передачи данных будет намного меньше, поскольку большинство файлов, использованных сегодня, в особенности те, которые содержатся на web страницах уже предлагаются сжатыми до определенного размера. Технология сжатия Иридиум выгодна только в немногих случаях.

Рисунки ПЗ.4, ПЗ.5, ПЗ.6 и ПЗ.7 демонстрируют графическую иллюстрацию сравнительной скорости передачи данных и время загрузки для различных изученных сценариев.

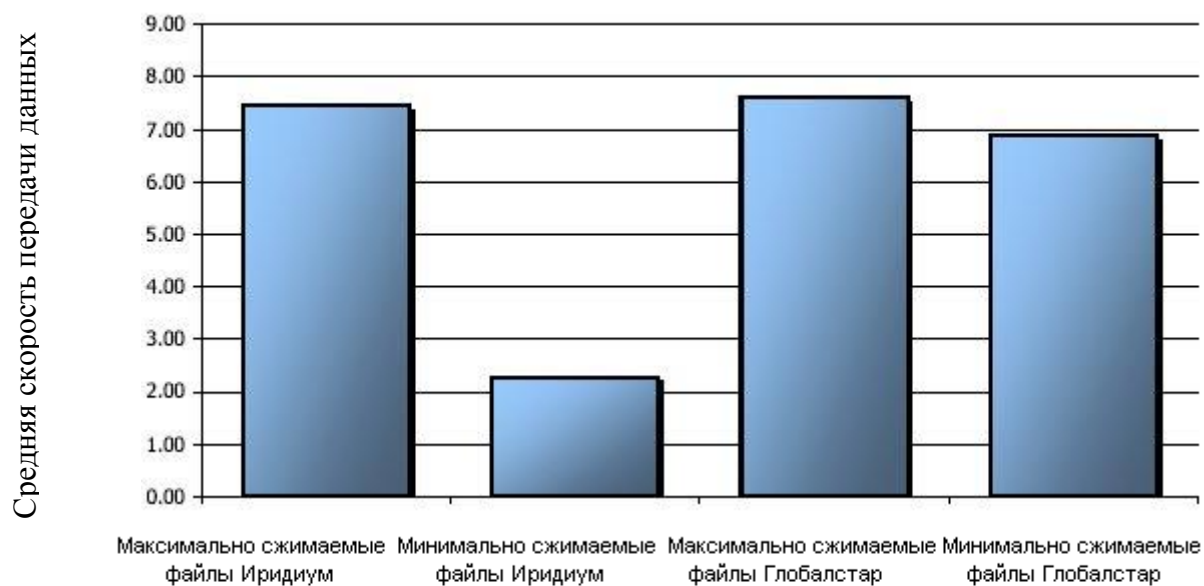


Рис. ПЗ.4. Средняя скорость передачи данных для режима передачи пакетных данных

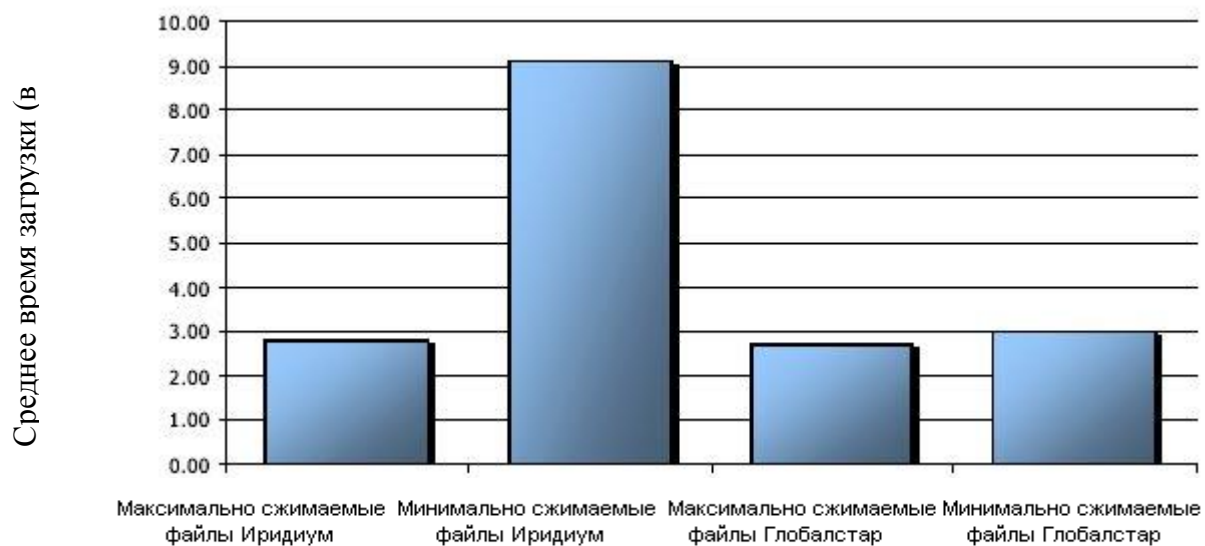


Рис. ПЗ.5. Среднее время загрузки для режима передачи пакетных данных

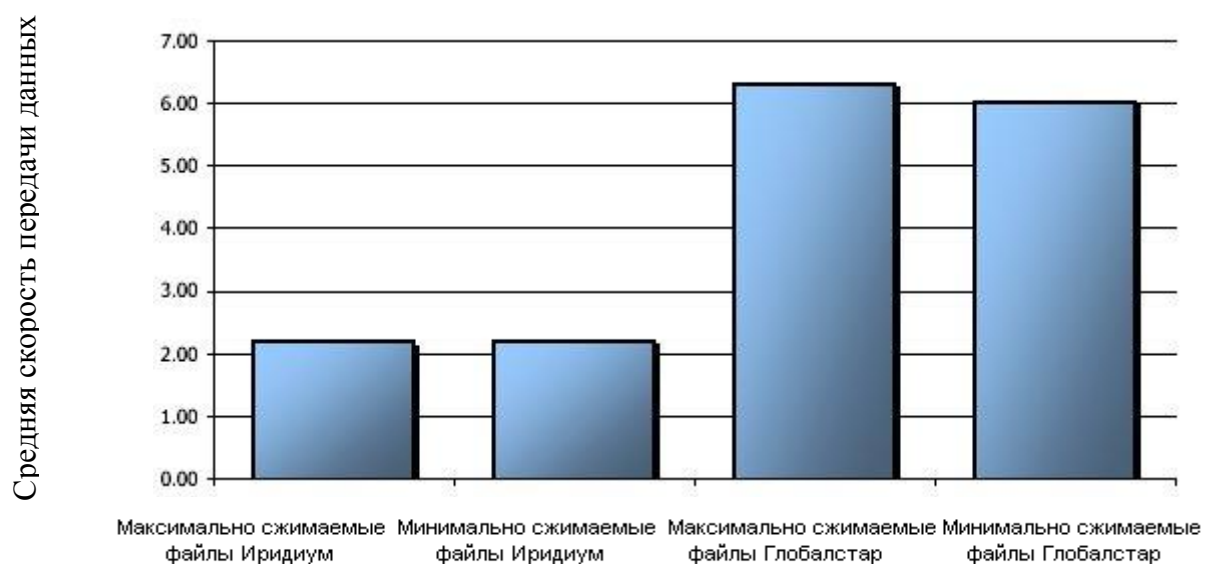


Рис. ПЗ.6. Средняя скорость передачи данных для режима коммутируемых данных

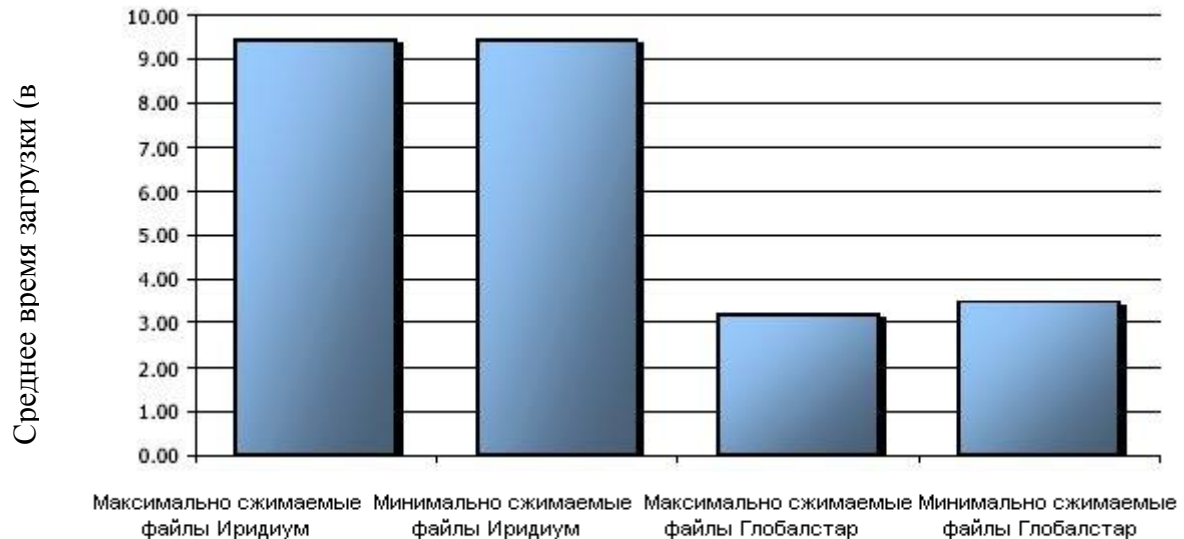


Рис. ПЗ.7. Среднее время загрузки для режима коммутируемых данных

Последний вопрос исследования, представляющий интерес, является скорость успешных загрузок. Значительное число загрузок Иридиум страдают от потери соединения, задержек и спуфинга, которые приводят к неудаче загрузок. Однако как видно ниже из рисунка 2.8, Глобалстар достиг 100% успеха в скорости. Эта скорость распространяется как на пакетную, так и коммутируемую передачу данных и насчитывает более, чем 80 попыток загрузки. С другой стороны, Иридиум имел 70% успеха в скорости загрузки для сценария коммутации и 88% для сценария пакетной передачи, достигнув средней скорости 79%.



Рис. ПЗ.8. Скорость успешной загрузки данных для коммутации и пакетной передачи

Спутниковый и Web телефон



Как было упомянуто выше, следующий этап этой части исследования заключался в исследовании применимости спутниковых телефонных систем в просмотре web страниц. Это было достигнуто с помощью доступа к различным web сайтам и просмотра каждого из них. Выбор сайтов был сделан по принципу от «легких», таких как www.Google.com, до «сложных», таких как www.NBC.com. В дополнение были просмотрены web страницы в США, Японии и Австралии для того, чтобы провести сравнение между сайтами, прямо связанными с центральным сервером США (к которому обе спутниковой телефонной станции также подсоединены) и удаленными от него.

Как Глобалстар, так и Иридиум настойчиво предупреждают конечного пользователя, что они не рассчитывают на то, что скорость соединения будет такой же, к какой мы привыкли в наших офисах и домах. Но, даже принимая эти предупреждения во внимание,

просмотр web страниц не становится развлекательным или приятным при использовании спутниковых телефонов. Для того чтобы ускорить просмотр, загрузка изображения и других мультимедийных средств были выключены в просмотре. И было быстро установлено, что при выполнении этой опции значительная часть содержания утрачивается. А поскольку web дизайн становится все более сложным, можно ожидать, что все меньше и меньше простых html текстов станут доступными для просмотра. Как только изображения были восстановлены, в обеих системах время загрузки значительно увеличилось.

Напрашивается вопрос, как могут Глобалстар и Иридиум быть сопоставлены в этом конкретном аспекте исследования? Совершенно очевидно, что относительно более высокая скорость передачи данных системы Глобалстар делает просмотр web страниц возможным, хотя и с достаточно низкой скоростью. Намного более низкая скорость передачи данных системы Иридиум делает этот просмотр занятием не из приятных. В дополнение к этому, при относительно большом числе сбросов и зависаний при загрузке просмотр web страниц становится более или менее непрактичным действием в системе Иридиум. К счастью, не предусматривается, что просмотр web страниц станет основным требованием для конечного пользователя, принимая во внимание стоимость спутникового телефона. Предполагается, что доступ к электронной почте и FTP будет более стандартным применением приложений данных, а как результаты выше показали, система Глобалстар превосходит Иридиум в большинстве измерений в рамках исследования.

Точки доступа Cisco Aironet для беспроводных сетей стандарта IEEE 802.11

Продукт	Функциональные характеристики/Преимущества
Точки доступа для офисных и сходных с ними условий	
<p>Точка доступа Cisco Aironet серии 1130AG</p>  <p>Двухдиапазонная "облегченная" или автономная точка доступа со встроенными антеннами, предназначенная для легкой установки в офисных и сходных с ними радиочастотных условиях</p>	<p>Два высокопроизводительных радиомодуля, поддерживающих стандарты IEEE 802.11a и 802.11g и обеспечивающих совокупную пропускную способность до 108 Мбит/с</p> <ul style="list-style-type: none"> • Встроенные разнесенные всенаправленные антенны, работающие в диапазонах 2.4 и 5 ГГц позволяют легко обойтись без внешних антенн <p>Данная точка поставляется либо в "облегченном" (lightweight), либо в автономном варианте. Во втором случае ее впоследствии можно будет модернизировать до "облегченного" варианта на месте.</p> <ul style="list-style-type: none"> • Низкопрофильный пластмассовый корпус • Объем памяти 32 Мбайт, из которых 16 Мбайт отведено под хранилище • Диапазон рабочих температур – от 32 до 104°F (от 0 до 40°C) • Поддержка inline-питания (реализация Cisco до принятия стандарта и действующий стандарт 802.3af) • Наличие консольного порта для управления • Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2 • Встроенная система монтажа с повышенной степенью защиты • Поддержка стандарта UL2043 для размещения в зонах повышенного давления
<p>Точка доступа Cisco Aironet серии 1100</p>  <p>Однодиапазонная автономная точка доступа со встроенными антеннами, предназначенная для легкой установки в офисных и близких к ним условиях</p>	<p>Один радиомодуль, поддерживающий стандарт 802.11g и обеспечивающий пропускную способность до 54 Мбит/с</p> <ul style="list-style-type: none"> • Встроенные разнесенные дипольные антенны, работающие в диапазоне 2.4 ГГц • Поставляется только в версии для автономной работы • Объем памяти 16 Мбайт, из которых 8 Мбайт отведено под хранилище • Диапазон рабочих температур – от 32 до 104°F (от 0 до 40°C) • Поддержка inline-питания (реализация Cisco до принятия стандарта) • Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2 • Встроенная система монтажа с повышенной степенью защиты • Поддержка стандарта UL2043 для размещения в зонах повышенного давления

"Облегченная" точка доступа Cisco Aironet серии 1000, модель 1010



Двухдиапазонная "облегченная" точка доступа со встроенными антеннами, предназначенная для легкой установки в офисных и сходных с ними радиочастотных условиях

Два радиомодуля, поддерживающих стандарты IEEE 802.11a и 802.11g и обеспечивающих совокупную пропускную способность до 108 Мбит/с

- Встроенные антенны, работающие в диапазонах 2.4 и 5 ГГц позволяют легко обойтись без внешних антенн
- Поставляется только в версии для работы в "облегченном" режиме
- Объем памяти 16 Мбайт, из которых 4 Мбайт отведено под хранилище
- Пластмассовый корпус
- Диапазон рабочих температур – от 32 до 104°F (от 0 до 40°C)
- Поддержка inline-питания (802.3af)
- Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2
- Поддержка стандарта UL2043 для размещения в зонах повышенного давления

Точки доступа, предназначенный для сложных радиочастотных сред внутри зданий

Точка доступа Cisco Aironet серии 1240AG



Двухдиапазонная "облегченная" или автономная точка доступа второго поколения с разъемами для антенн с двойным разнесением, предназначенная для установки в сложных радиочастотных средах

Два высокопроизводительных радиомодуля, поддерживающих стандарты IEEE 802.11a и 802.11g и обеспечивающих совокупную пропускную способность до 108 Мбит/с



- Разъемы RP-TNC для подключения внешних антенн с двойным разнесением, работающих в диапазонах 2.4 и 5 ГГц
- Данная точка поставляется либо в "облегченном" (lightweight), либо в автономном варианте. Во втором случае ее впоследствии можно будет модернизировать до "облегченного" варианта на месте.
- Защищенный металлический корпус
- Объем памяти 32 Мбайт, из которых 16 Мбайт отведено под хранилище
- Диапазон рабочих температур – от -4 до 131°F (от -20 до 55°C)
- Поддержка inline-питания (реализация Cisco до принятия стандарта и действующий стандарт 802.3af)
- Наличие консольного порта для управления
- Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2



Встроенная система монтажа с повышенной степенью защиты


- Поддержка стандарта UL2043 для размещения в зонах

Точка доступа Cisco Aironet серии 1230AG

Два высокопроизводительных радиомодуля, поддерживающих стандарты IEEE 802.11a и 802.11g и обеспечивающих

 <p>Двухдиапазонная "облегченная" или автономная точка доступа первого поколения с разъемами для антенн с двойным разнесением, предназначенная для установки в сложных радиочастотных средах</p>	<p>совокупную пропускную способность до 108 Мбит/с</p> <ul style="list-style-type: none"> • Разъемы RP-TNC для подключения внешних антенн с двойным разнесением, работающих в диапазонах 2.4 и 5 ГГц • Данная точка поставляется либо в "облегченном" (lightweight), либо в автономном варианте. Во втором случае ее впоследствии можно будет модернизировать до "облегченного" варианта на месте. • Защищенный металлический корпус • Объем памяти 16 Мбайт, из которых 8 Мбайт отведено под хранилище • Диапазон рабочих температур – от -4 до 131°F (от -20 до 55°C) • Поддержка inline-питания (реализация Cisco до принятия стандарта) • Наличие консольного порта для управления • Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2 <p>Встроенная система монтажа с повышенной степенью защиты</p> <ul style="list-style-type: none"> • Поддержка стандарта UL2043 для размещения в зонах повышенного давления
<p>Точка доступа Cisco Aironet серии 1200</p>  <p>Однодиапазонная "облегченная" или автономная точка доступа с разъемами для антенн с двойным разнесением, предназначенная для установки в сложных радиочастотных средах</p>	<p>Один высокопроизводительный радиомодуль, поддерживающий стандарт 802.11g и обеспечивающий пропускную способность до 54 Мбит/с</p> <ul style="list-style-type: none"> • Возможность модернизации до уровня стандарта 802.11a с помощью модуля аппаратной модернизации • Разъемы RP-TNC для подключения внешних антенн с двойным разнесением, работающих в диапазоне 2.4 ГГц • Данная точка поставляется либо в "облегченном" (lightweight), либо в автономном варианте. Во втором случае ее впоследствии можно будет модернизировать до "облегченного" варианта на месте. • Защищенный металлический корпус • Объем памяти 16 Мбайт, из которых 8 Мбайт отведено под хранилище • Диапазон рабочих температур – от -4 до 131°F (от -20 до 55°C) • Поддержка inline-питания (реализация Cisco до принятия стандарта) • Наличие консольного порта для управления • Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2 <p>Встроенная система монтажа с повышенной степенью защиты</p> <ul style="list-style-type: none"> • Поддержка стандарта UL2043 для размещения в зонах повышенного давления
<p>"Облегченная" точка доступа Cisco Aironet серии 1000, модель 1020</p>	<p>Два радиомодуля, поддерживающих стандарты IEEE 802.11a и 802.11g и обеспечивающих совокупную пропускную способность до 108 Мбит/с</p> <ul style="list-style-type: none"> • Разъемы RP-TNC для подключения внешних антенн с двойным разнесением, работающих в диапазоне 2.4 ГГц • Разъем RP-TNC для подключения внешней антенны без разнесения, работающей в диапазоне 5 ГГц • Поставляется только в версии для работы в "облегченном"

 <p>Двухдиапазонная "облегченная" точка доступа с разъемами для антенн, предназначенная для установки в сложных радиочастотных средах</p>	<p>режиме</p> <ul style="list-style-type: none"> • Металлический и пластмассовый корпуса • Объем памяти 16 Мбайт, из которых 8 Мбайт отведено под хранилище • Диапазон рабочих температур – от 32 до 104°F (от 0 до 40°C) • Поддержка inline-питания (802.3af) • Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2 • Поддержка стандарта UL2043 для размещения в зонах повышенного давления
<p>"Облегченная" наружная точка доступа/мост Cisco Aironet серии 1300</p>  <p>Однодиапазонная автономная точка доступа и беспроводной мост в корпусе, соответствующем стандарту NEMA-4, предназначенная для установки вне зданий</p>	<p>Один радиомодуль, поддерживающий стандарт 802.11g и обеспечивающий пропускную способность до 54 Мбит/с</p> <ul style="list-style-type: none"> • Разъемы RP-TNC для подключения внешних антенн с двойным разнесением, работающих в диапазоне 2.4 ГГц • Может быть сконфигурирована для работы в качестве автономной точки доступа, беспроводного моста или моста группы • Поддерживает конфигурации "точка-точка" и "точка-множество точек" • Водонепроницаемый корпус, соответствующий стандарту NEMA-4 • Возможность подключения входящих в комплект или дополнительно приобретаемых внешних антенн обуславливает гибкие возможности при внедрении • Объем памяти 16 Мбайт, из которых 8 Мбайт отведено под хранилище • Диапазон рабочих температур – от -22 до 131°F (от -30 до 55°C) • Поддержка inline-питания (реализация Cisco до принятия стандарта) • Наличие консольного порта для управления • Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2 • Встроенная система монтажа с повышенной степенью защиты • Поддержка стандарта UL2043 для размещения в зонах повышенного давления • Возможность подключения входящих в комплект или дополнительно приобретаемых внешних антенн обуславливает гибкие возможности при внедрении
<p>"Облегченная" наружная точка доступа Cisco Aironet серии 1500 для полностью связанных (mesh) сетей</p>	<p>Двойной радиомодуль 802.11a/g поддерживает скорость передачи данных до 54 Мбит/с</p> <ul style="list-style-type: none"> • Возможность использования стандарта 802.11b/g для организации доступа, а стандарта 802.11a – для подключения по обратному каналу • Поддержка конфигураций типа "точка-точка" и "точка-

 <p>"Облегченные" наружные точки доступа для полносвязанных (mesh) сетей позволяют строить экономичные, масштабируемые и защищенные беспроводные сети на открытом пространстве.</p>	<p>множество точек", а также полносвязанной (mesh) архитектуры</p> <ul style="list-style-type: none"> • Использование протокола Adaptive Wireless Path Protocol (на который оформлена патентная заявка) для интеллектуальной маршрутизации в беспроводных сетях • Водонепроницаемый корпус, соответствующий стандарту NEMA-4 • Диапазон рабочих температур – от -22 до 131°F (от -30 до 55°C) • Поддержка Cisco Self-Defending Network, NAC, WPA и 802.11i/WPA2
--	---

Использование сетей Bluetooth в современной радиоэлектронной аппаратуре

Несколько иллюстраций с прошедшей в ноябре 2000-го года выставки Comdex Fall:



Рис. П4.1. Toshiba. Мультимедийный ноутбук, проектор и цифровой фотоаппарат



Рис. П4.2. Коллекция полностью беспроводных PDA с расширенными коммуникационными возможностями



Рис. П4.3. Комплект оснащения киберпанка будущего - наушники, видеокамера, микрофон, внизу лежит коммуникатор в виде часов. Связь со станцией по протоколу Bluetooth на расстоянии до 100 метров

Радиомодули для сенсорных сетей на базе трансиверов стандарта IEEE 802.15.4

MICAz – радиомодули компании Crossbow с сетевым стеком протоколов ZigBee. Представляют собой трансиверы стандарта IEEE 802.15.4 компании Chipcon и аналогово-цифровой сенсорный интерфейс. Автоматически соединяются с соседним сетевым узлом, как маршрутизаторы. Радиомодули могут использоваться с датчиками температуры, освещённости, биомедицинскими, сейсмическими, акустическими и магнитными датчиками. Компания Crossbow выпускает также и другие модули для построения сенсорных сетей, которые в силу своего размера называют motes (пылинки). Большинство этих модулей предполагает использование сетевого протокола XMesh компании Crossbow.

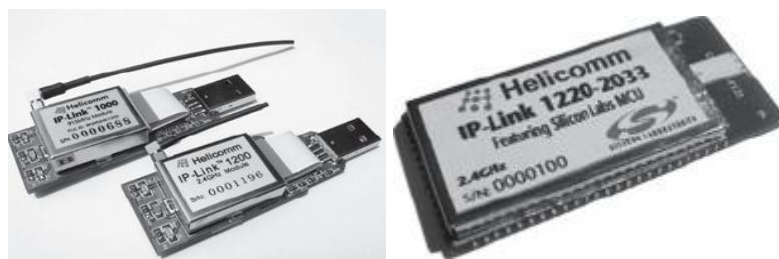
SmartMesh – радиомодули компании Dust Networks, использующие трансиверы стандарта IEEE 802.15.4 и аналогово-цифровой сенсорный интерфейс. Используют сетевой стек протоколов, отличный от ZigBee.

Радиомодули 802.15.4/ZigBee

XBee–радиомодули компании MaxStream. Представляют 802.15.4/ZigBee полностью автономные трансиверы и трансиверы и с последовательным интерфейсом RS_232 и USB интерфейсом. В диапазоне 2,4 ГГц при мощности излучения 100 (1) мВт дальность действия при прямой видимости до 1200 (100) м. Полная поддержка создания Ad-Hoc сетей.



IP_Link – радиомодули компании Helicomm. Представляют 802.15.4/ZigBee трансиверы для построения сети с топологией «звезда» с координированием от компьютера.



Модуль **ZigBee USB Dongle** компании Integration с USB интерфейсом. Представляет 802.15.4/ZigBee трансивер.

