**СТАВРОПОЛЬСКИЙ**

**ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**

**Кафедра Информационных систем**

для студентов направления подготовки для студентов направления подготовки 09.03.02.Информационные системы и технологии

Профиль «Информационные системы и технологии в бизнесе»

**Л Е К Ц И Я**

**по дисциплине «Технологии беспроводной связи»**

**Лекция №3: «ПРОТОКОЛЫ GSM И ПРЕОБРАЗОВАНИЕ РЕЧИ»**

Обсуждена на заседании кафедры

Протокол №\_\_\_ от « »\_\_\_\_\_\_\_\_2022 г.

Ставрополь

2022

**УЧЕБНЫЕ И ВОСПИТАТЕЛЬНЫЕ ЦЕЛИ:**

Сформировать у студентов представление о протоколах сети GSM и преобразованиях речи, а также знания по структуре кадров трафика и управления, принципах преобразования речи, кодированию, модуляции и демодуляции, шифрованию и дешифрованию.

**ВРЕМЯ** – 90 минут.

**УЧЕБНО-МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:**

1. Выставка литературы.
2. Образцы документов.
3. Плакаты.

**РАСПРЕДЕЛЕНИЕ ВРЕМЕНИ ЛЕКЦИИ:**

1. Вступительная часть – 5 минут;
2. Учебные вопросы лекции:

1) Протоколы сети GSM  – 35 минут.

2) Частотный план в стандарте GSM - 20 минут.

3) Преобразование речи в стандарте GSM - 25 минут.

1. Заключение – 5минут.

Задание студентам для самостоятельной работы

**СОДЕРЖАНИЕ ЛЕКЦИИ:**

**Вступительная часть**

 В лекции описаны: общая структура протоколов и сигнальные протоколы, частотный план в стандарте GSM, структура кадров трафика и управления. Показаны принципы преобразования речи, кодирование, модуляция и демодуляция, шифрование и дешифрование.

**1 Протоколы сети GSM**

Основное описание протоколов сети GSM дано в документах ETSI. Эти документы представляют некоторые группы, расположенные по версиям.

Рассмотренные функции регистрации (registration), аутентификации (authentication), маршрутизации вызова (call routing) и обновление координат местоположения, механизм передачи соединения (handover) выполняются подсистемой сети главным образом с использованием протоколов системы мобильной связи, основанных на протоколах системы ОКС № 7. Структура этих протоколов показана на [рис. 1](https://intuit.ru/studies/courses/551/407/lecture/9334?page=1#image.2.1).

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

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

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

**Сигнальный протокол в GSM** разделен на три уровня в зависимости от интерфейса, как показано на [рис. 1](https://intuit.ru/studies/courses/551/407/lecture/9334?page=1#image.2.1).

Участок "мобильная станция — базовая станция" работает со следующими уровнями.

Уровень 1 — физический уровень, который использует структуры канала, рассмотренные выше, по воздушному интерфейсу.

Уровень 2 — уровень звена передачи данных по Um интерфейсу, уровень звена передачи данных — это модифицированная версия LAPD-протокола, используемого в ISDN; она называется LAPDm.

Уровень 3 — сигнальный протокол из GSM, использующий также модифицированную версию LAPD; самостоятельно разделен на 3 подслоя.



Рисунок 1 - Структура протоколов GSM

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

Передача сигналов между различными объектами в фиксированной части сети (интерфейс A) использует протоколы на уровне 1 MTP1 (Message Transfer Part — подсистема передачи сообщений) на уровне 1 и на уровне 2 — SCCP (Signaling Connection Control Part — система управления соединением каналов сигнализации), принадлежащие системе сигнализации ОКС № 7.

На уровне 3 применяют перечисленные выше протоколы GSM — MM и CM.

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

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

**Система управления соединением канала сигнализации (SCCP — Signaling Connection Control Part)** управляет логическими соединениями в сети ОКС для передачи блоков данных сигнализации. Она выполняет функции третьего уровня (сетевой уровень) модели взаимодействия протоколов ОКС.

SCCP предоставляет возможность осуществлять по сети ОКС передачу данных для управления соединением и при техническом обслуживании, непосредственно не связанную с конкретным каналом речи или передачи данных.

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

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

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

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

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

Последнее сообщение содержит следующие параметры ([рис. 2](https://intuit.ru/studies/courses/551/407/lecture/9334?page=1#image.2.2)).



Рисунок 2 - Сообщения "разрешенная подсистема"

Одна из пользовательских функций подсистемы управления соединением канала сигнализации SCCP (Signaling Connection Control Part) — прикладная часть системы базовой станции (BSSAP — Base Station System Part). Она предназначена для обслуживания взаимодействия BSS и MSC (см. [рис. 1](https://intuit.ru/studies/courses/551/407/lecture/9334?page=1#image.2.1)). В случае соединения типа "точка — точка" BSSAP использует сигнальное соединение с активной мобильной станцией, имеющей один или более активизированных процессов для передачи сообщений уровня 3. В случае конференц-связи или широковещательного вызова имеется всегда одно соединение в соте, связанное с данным вызовом, и одно дополнительное соединение в системе базовой станции (BSS — Base Station System) для передачи сообщений уровня 3. Есть дополнительное соединение для "главного абонента" при широковещательном вызове или конференц-связи. Дополнительные соединения могут также потребоваться для любых мобильных станций при конференц-связи группы или широковещательном вызове, при которой сеть решает разместить выделенные или временно закрепленные каналы.

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

1. прикладная часть для прямой передачи (DTAP — Direct Transfer Application Part), называемая также GSM L3, используется для передачи транзитных сообщений между MSC и MS. Информация уровня 3 в этих сообщениях не интерпретируется BSS (Base Station System);
2. основная прикладная часть системы базовой станции (BSSMAP — Base Station System Management Application Part) поддерживает другие процедуры между MSC и BSS (Base Station System), связанные с MS управлением ресурсами, управлением передачей соединения (хэндовером), или в данной соте, или в пределах всей BSS (Base Station System). Описание протокола для обмена информацией BSSMAP (Base Station Management Application Part) на уровне 3 содержится в Рекомендации ETSI GSM 08.08.

**Уровень управления радиоресурсами (RRM — Radio Resource Management)** наблюдает за установлением соединения по радио и фиксированной сети между подвижной станцией и центром коммутации подвижной связи (MSC). Главные функциональные компоненты этого уровня — подвижная станция и подсистема базовых станций, центр коммутации подвижной связи (MSC).

Уровень RRM предназначен для управления радиосеансом. Сеанс — это время, которое мобильная станция находится в режиме соединения и управляет конфигурацией радиоканалов, включая распределение специализированных каналов.

Радиосеанс всегда инициализируется подвижной станцией с помощью процедуры доступа, либо для исходящего вызова, либо в ответ на широковещательный вызов при входящем вызове. Уже рассмотренные выше процедуры исходящего вызова и широковещательного вызова, такие как назначение выделенного канала для сигнализации мобильной станции, и структура широковещательного подканала, устанавливаются на уровне RRM.

Кроме того, уровень RRM осуществляет управление радиохарактеристиками, такими как управление мощностью, прерывистая передача и прием.

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

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

**Виды сообщений и составы сигналов 3-го уровня**

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

Обмен сигнальной информацией по протоколу LAPD производится в виде сообщений, каждое из которых имеет следующий вид ([рис. 3](https://intuit.ru/studies/courses/551/407/lecture/9334?page=2#image.2.7)).



Рисунок 3 - Вид сообщения протоколов LAPD 3-его уровня

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

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

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

**2 Частотный план в стандарте GSM**

На [рис. 4](https://intuit.ru/studies/courses/551/407/lecture/9334?page=4#image.2.10) показан принцип образования каналов в системе GSM.

Для радиодоступа GSM 900 выделены две полосы частот:

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



Рисунок 4 - Образование каналов в системе GSM

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

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

Многостанционный доступ с временным разделением (TDMA — Time Division Multiple ACCESS), содержащий 8 слотов и 248 физических полудуплексных каналов, составляет группу из 1984 полудуплексных каналов. При размере кластера 7 (см. повторное использование частот) число каналов в одной соте равно примерно 283 (1984 / 7) полудуплексных каналов. Как было показано ранее, разбиение, содержащее семь наборов частот, достаточно, чтобы охватить произвольно большую область, используя повторное применение частот с учетом допустимого расстояния между сотами.

Каналы трафика (TCH) используются для доставки данных и речи. Структура образования кадров трафика (TCH) показана на [рис. 5](https://intuit.ru/studies/courses/551/407/lecture/9334?page=4#image.2.11).



Рисунок 5 - Структура кадров трафика радио доступа системы GSM

Мультикадр трафика содержит 26 кадров временного доступа (TDMA), каждый из которых состоит из 8 пакетов ( burst1 ) трафика. Длительность мультикадра трафика — 120 мс. Поэтому длительность кадров временного доступа 120 мс / 26 = 4,615 мс, а длительность временного положения (слота) трафика равна 120/(26 x 8)=15/26=0,577 мкс. Из 26 кадров 24 используются для трафика, один (12-й кадр) — как низкоскоростной выделенный канал управления (SACCH — Slow Associated Control Channel) и один (25-й) в настоящее время не используется.

Пакет содержит:

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

TCH прямого и обратного направления разделены во времени на 3 периода передачи пакета. Поэтому мобильная станция не может одновременно получать и принимать один и тот же канал, что упрощает ее электронное устройство.

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

В дополнение к каналам THC's с полной скоростью могут применяться каналы THC's с полускоростью. THC's с полускоростью фактически могут удвоить емкость системы, так как в них предусматривается кодирование речи в пределах 11,4 Кбит/с вместо 22,8 Кбит/с. Полускоростные THC's каналы также используются для передачи сигналов управления. В рекомендациях они названы автономными специализированными каналами управления (SDCCH — Stand-alone Dedicated Control Channels) [[81](https://intuit.ru/studies/courses/551/407/literature#literature.81)].

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

Структура кадров и мультикадров управления показана на [рис.6](https://intuit.ru/studies/courses/551/407/lecture/9334?page=5#image.2.12). По сравнению с приведенными на [рис. 5](https://intuit.ru/studies/courses/551/407/lecture/9334?page=4#image.2.11) кадрами, мультикадр состоит из 51 кадра TDMA, каждый из которых содержит 8 слотов.



Рисунок 6 - Структура кадров управления

Содержания слотов управления и защитный интервал зависят от их назначения и указаны на [рис. 7](https://intuit.ru/studies/courses/551/407/lecture/9334?page=5#image.2.13).



Рисунок 7 - Структуры слотов управления

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

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

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

Слот доступа (AB — Access Burst) предназначен для разрешения доступа MS к BSS, передается по каналу права доступа (RACH — Random Access Channel). Этот слот передается в качестве первого запроса, когда станции еще не вошли в синхронный режим и неизвестно время прохождения сигнала. Он содержит концевую комбинацию (TB) — в данном случае она состоит из 3 бит; последовательность синхронизации для базовой станции — 41 бит, что позволяет базовой станции начать процесс синхронизации и обеспечить правильный прием последующих 36 бит. Большой защитный интервал (68,25 бит длительностью 252 мкс) обеспечивает максимальное время для защиты кадров от эффекта межсимвольного искажения.

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

На [рис. 8](https://intuit.ru/studies/courses/551/407/lecture/9334?page=5#image.2.14) показано объединение информации управления и трафика в единый поток.



Рисунок 8 - Объединение мультикадров трафика и управления в единый поток

**3 Преобразование речи в стандарте GSM**

На [рис.](https://intuit.ru/studies/courses/551/407/lecture/9334?page=5#image.2.16) 9 показана последовательность действий при преобразовании речи в радиоволны и обратном преобразовании.



Рисунок 9 - Последовательность действий при преобразовании речи в радиоволны и обратном преобразовании

На основании субъективных показателей качества речи и сложности реализации (которая связана со стоимостью, задержкой обработки и потребляемой мощностью) для GSM выбрано долговременное линейное предсказание с возбуждением регулярной импульсной последовательностью (RPE — LPC). В основе этого метода положен принцип предсказания, когда информация от предыдущих временных отсчетов используется, чтобы предсказать текущий временной отсчет. Коэффициенты линейной комбинации предыдущих временных отсчетов, плюс, закодированная форма остаточных, разность между предсказанным и фактическим временным отсчетом, представляют сигнал. Речь разделена на 20 временных отсчетов в миллисекунду, каждый из которых закодирован как 260 битов, что составляет полную скорость передачи информации 13 Кбит/с. Это так называемое кодирование речи на полной скорости (Full Rate). В настоящее время в системе GSM используются усовершенствованные кодеры GSM 06.10 и GSM 06.20. Основная блок-схема таких кодеров приведена на [рис. 10](https://intuit.ru/studies/courses/551/407/lecture/9334?page=5#image.2.17). Она отличается наличием двух устройств: медленного анализатора (синтезатора) и быстрого анализатора, улучшающих систему предсказания.



Рисунок 10 - Основная блок-схема кодеров GSM 06.10 и GSM 06.20

Некоторыми североамериканскими операторами GSM1900 был реализован алгоритм преобразования речи "усовершенствованная полная скорость" (EFR — Enhanced Full-Rate). Он обеспечивает улучшенное речевое качество, используя существующую скорость 13 Кбит/c.

Из-за влияния естественных или искусственных электромагнитных помех закодированная речь или сигналы данных, передаваемые по радиоинтерфейсу, должны быть защищены от ошибок. GSM использует сверточное кодирование (convolution encoding) и чередование блоков (block interleaving). Конкретные алгоритмы для речи и для различных скоростей передачи данных отличаются между собой. Метод, используемый для речевых блоков, описан ниже.

Рассмотрим речевой кодер-декодер, который производит блок на 260 битов для каждых 20 временных отсчетов речи каждые 20 мс ([рис. 11](https://intuit.ru/studies/courses/551/407/lecture/9334?page=6#image.2.18)).



Рисунок 11 - Один отсчет речевого сигнала: 1блок = 260 бит (20мс)

Субъективные испытания показали, что которые некоторые биты этого блока были более важны для качества речевого восприятия, чем другие. Поэтому биты разделены на три класса:

* Класс Ia, 50 битов — наиболее чувствительные к ошибкам;
* Класс Ib, 132 бита — умеренно чувствительные к ошибкам;
* Класс II, 78 битов — наименее чувствительные к ошибкам.

Классу Ia биты добавлен циклический избыточный код на 3 бита для обнаружения ошибок. Если ошибка обнаружена, кадр оценивается как значительно поврежденный и удаляется. Он может быть заменен немного уменьшенной версией предыдущего правильно полученного кадра. Это 53 бита, вместе с 132 битами класса Ib и конечной последовательностью (TB — Tail Bit) на 4 бита (всего 189 битов).

Напомним, что сверточное кодирование (convolution coding) — это метод передачи с исправлением ошибок, при котором каждое поле входной последовательности длины K преобразуется в канальный поток данных длины n. Здесь K — длина кодового ограничения (constrain length); она указывает длину регистра сдвига, запоминающего поле входного потока. Каждый бит выходной последовательности получается как результат суммирования по модулю 2 нескольких последовательно передаваемых K символов входной последовательности. Отношение длины исходной информационной последовательности к длине кодированной последовательности называется скоростью кодирования (code rate) и обозначается r.

В стандарте GSM используется сверточный кодер с кодовым ограничением K=5. Каждый входной бит закодирован двумя битами выходного потока (r=1/2), базируясь на комбинации предыдущих 5 входных битов. Таким образом, сверточный кодер передает на выход 378 битов, к которым добавляются 78 остающихся бит класса II биты, которые являются незащищенными. Следовательно, каждые 20-миллисекундные временные отсчеты речи закодированы в виде 456 битов ([рис. 12](https://intuit.ru/studies/courses/551/407/lecture/9334?page=6#image.2.20)) и требуют скорости передачи информации в битах 22,8 Кбит/с.



Рисунок 12 - Принцип кодирования пакета трафика

Перестановка (перемежение) информации — это изменение позиций блоков информации относительно друг друга, которое позволяет разнести стоящие рядом символы, принадлежащие одному и тому же сообщению. При этом групповые ошибки преобразуются в одиночные и эффективно исправляются, например, сверточным декодером. Имеется несколько алгоритмов перестановки (перемежения), например, перестановка блоков информации в соответствии с таблицей (табличное перемещение), диагональное перемещение и т. д. Ниже рассмотрен один, наиболее простой алгоритм, который используется чаще всего в сочетании с другими.

Принцип перестановки в данном случае заключается в том, что временные отсчеты GSM величиной 456 бит (для полной скорости передачи речи) разбиваются на 8 групп по 57 бит. Каждая такая группа передается в различных пакетах трафика и в различных кадрах. Биты в каждом пакете пронумерованы и разделены на четные и нечетные, и в соответствии с этим включаются в различные пакеты трафика. Принцип перестановки информации показан на [рис. 13](https://intuit.ru/studies/courses/551/407/lecture/9334?page=6#image.2.21).



Рисунок 13 - Принцип перестановки информации

Основной недостаток принципа перестановки — это вносимая задержка из-за накопления пакетов информации, их перестановки и передачи.

В GSM защита информации представлена средствами шифрования передачи. Метод шифрования не зависит от типа передаваемых данных (речь, пользовательские данные или сообщения сигнализации). Оно применяется только к нормальным пакетам (normal burst).

Шифрование достигается преобразованием с помощью операции "исключающее ИЛИ". Эта операция проводится между псевдослучайной многоразрядной последовательностью и 114 полезными битами нормального пакета (все информационные биты кроме 2 контрольных флагов). Псевдослучайная последовательность получается на основе номера пакета и сеансового ключа (session key). Ключ устанавливается в начале сеанса путем обмена сигналами между приемником и передатчиком, используется только в течение одного сеанса связи. После окончания сеанса ключ автоматически стирается.

Расшифровка использует тот же самый ключ шифрования. Более детально процесс шифрования и дешифрования дан в курсе лекций "Криптография и безопасность сетей".

**Выводы:**

Функции, которые выполняются подсистемой сети, главным образом используют протоколы системы мобильной связи, основанные на протоколах системы ОКС № 7.

Радиоинтерфейс между MS BSC уровня 3 из GSM использует сигнальный протокол, который представляет собой модифицированную версию LAPD, разделенную на 3 подслоя: управление радиоресурсами (RRM — Radio Resources Management), управление передвижением (MM — Mobility Management) и управление соединением (Connection Management).

Для передачи сигнальных сообщений между центром коммутации мобильной связи (MSC) и системой базовой станции (Base Station System) используются MTP (Message Transfer Part) и подсистемы управления соединением канала сигнализации SCCP (Signaling Connection Control Part), которые являются частями системы ОКС.

Прикладная часть системы базовой станции (BSSAP — Base Station System Part) предназначена для обслуживания взаимодействия BSS — MSC. Она подразделяется на две отдельных функции: прикладная часть для прямой передачи (DTAP — Direct Transfer Application Part), используется для передачи транзитных сообщений между MSC и MS; и основная прикладная часть системы базовой станции (BSSMAP — Base Station System Management Application Part), которая поддерживает другие процедуры между MSC и BSS (Base Station System), связанные с MS управлением ресурсами, управлением передачей соединения (хэндовером), или в данной соте, или в пределах всей BSS (Base Station System).

Уровень управления радиоресурсами (RRM) наблюдает за установлением соединения по радио и фиксированной сети между подвижной станцией и центром коммутации подвижной связи (MSC).

Уровень управления мобильностью (ММ — Mobility Management) выполняет функции, которые связаны с передвижением абонента, а также функции защиты и аутентификации.

Уровень управления соединением (СМ) отвечает за управление вызовом, дополнительными видами услуг и службой передачи коротких сообщений.

Для радиодоступа GSM 900 выделены две полосы частот:

890–915 МГц для канала связи от абонента к станции (направление MS к BS);

935–960 МГц для исходящего канала от станции к абоненту (направления BS к MS).

Полосы по 25 МГц разделены на 124 пары каналов. Они работают в дуплексном режиме с интервалом несущей частоты по 200 кГц, используя многостанционный доступ с частотным разделением каналов (FDMA — Frequency Division Multiple Access). Каждый радиоканал с шириной полосы 200 кГц разделен на временные соты, которые создают 8 логических каналов. При этом применяется методика, известная как многостанционный доступ с временным разделением (TDMA — TIME DEVISION MULTIPLE ACCESS).

Мультикадр трафика содержит 26 кадров временного доступа (TDMA), каждый из которых состоит из 8 пакетов трафика. Из 26 кадров 24 используются для трафика, один (12-й кадр) — как низкоскоростной выделенный канал управления (SACCH — Slow Associated Control Channel) и один (25-й) в настоящее время не задействован.

Пакет трафика содержит два поля данных по 57 бит, поле обучающей последовательности и ";хвостовые биты" (tail bits). Каналы трафика прямого и обратного направления разделены во времени на 3 периода передачи пакета. Поэтому мобильная станция не может одновременно получать и принимать один и тот же канал, что упрощает ее электронное устройство.

В дополнение к каналам трафика с полной скоростью могут применяться каналы THC's с полускоростью. Канал трафика с полускоростью фактически может удвоить емкость системы, так как в нем предусматривается кодирование речи в пределах 11,4 Кбит/с вместо 22,8 Кбит/с.

Мультикадр управления состоит из 51 кадра TDMA, каждый из которых содержит 8 слотов.

Содержания слотов управления и защитный интервал зависит от их назначения. Используются слоты: подстройки частоты, синхронизации, пустой, доступа.

Для передачи быстродействующего объединенного канала управления (FACCH — Fast Associated Control Channel) и низкоскоростного выделенного канала управления (SACCH — Slow Associated Control Channel) применяются каналы трафика. Остальные каналы управления передаются в мультикадре управления, содержащем 51 кадр и имеющем специальную структуру.

На основании субъективных показателей качества речи и сложности реализации (которая связана со стоимостью, задержкой обработки и потребляемой мощностью) для GSM выбрано долговременное линейное предсказание с возбуждением регулярной импульсной последовательностью (RPE — LPC).

GSM использует сверточное кодирование (convolution encoding) и чередование блоков (block interleaving). Цифровой сигнал модулируется на аналоговую несущую частоту, используя гауссовскую манипуляцию с минимальным частотным сдвигом (GMSK — Gaussian-filtered Minimum Shift Keying).

Для защиты информации от помех применяется перестановка (перемежение) информации. Она представляет собой изменение позиций блоков информации относительно друг друга, которое позволяет разнести стоящие рядом символы, принадлежащие одному и тому же сообщению. При этом групповые ошибки преобразуются в одиночные и эффективно исправляются, например, сверточным декодером.

В GSM защита информации представлена средствами шифрования передачи. Шифрование достигается преобразованием с помощью "исключающее ИЛИ". Эта операция проводится между псевдослучайной многоразрядной последовательностью и 114 полезными битами нормального пакета (все информационные биты кроме 2 контрольных флагов).

Подавление искажений, вызванных замиранием из-за многолучевого распространения, производится с помощью обучающей последовательности, передаваемой в середине каждого временного интервала пакета, а также с помощью медленных скачков частоты.

Уменьшение межканальных помех достигается прерывистой передачей (DTX — Discontinuous transmission mode), а сохранение энергии в подвижной станции — прерывистым приемом.

Существует пять классов определенных подвижных станций согласно их пиковой мощности передатчика, с номиналами, равными 20, 8, 5, 2, и 0,8 ваттам. Чтобы снизить межканальные помехи и сохранить мощность, приемопередатчики мобильных станций и базовые станции работают на самой низкой мощности, которую выбирают, чтобы поддержать приемлемое качество сигнала.

**Контрольные вопросы**

1. Приведите структуру протоколов сети GSM.
2. Охарактеризуйте сигнальные протоколы сети GSM.
3. Охарактеризуйтесистему управления соединением канала сигнализации (SCCP — Signaling Connection Control Part).
4. Охарактеризуйте уровень управления радиоресурсами (RRM — Radio Resource Management).
5. Опишите принцип образования каналов в сети GSM.
6. Опишите структуру кадров трафика радио доступа сети GSM.
7. Опишите структуру кадров управления сети GSM.
8. Опишите структуру слотов управления сети GSM.
9. Опишите последовательность действий при преобразовании речи в радиоволны и обратном преобразовании в сети GSM..
10. Принцип кодирования пакета трафика в сети GSM.
11. Принцип перестановки информации в сети GSM.

По материалам профессора А.П. Жук

\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.