Стандарт DECT. Принцип работы. Безопасность.

Эссе по курсу «Защита информации»
Выполнил студент 4-го курса ФРТК
Чутчев Марк Владимирович
Группа 914

Долгопрудный, 2003

Содержание

Историческая справка

Стандарт DECT (Digital European Cordless Telecommunications) был опубликован Европейским институтом стандартизации электросвязи (European Telecommunications Standards Institute - ETSI) в 1992 г., а первые коммерческие продукты, соответствующие этому стандарту, появились в 1993 г. Первоначально они представляли собой в основном средства для построения беспроводных учрежденческих автоматических телефонных станций (УАТС), пользователи которых могли связываться между собой в пределах учреждения с помощью переносных телефонов, а также обычные домашние бесшнуровые телефонные аппараты. Некоторые производители создали оборудование для беспроводных ЛВС, поддерживающее DECT.

Позднее появились другие приложения DECT, которые начали разрабатываться еще в процессе определения стандарта. В их состав вошли: средства RLL; системы, обеспечивающие беспроводный доступ к ресурсам сетей общего пользования для абонентов с ограниченной мобильностью (Cordless Terminal Mobility - CTM); средства, позволяющие аппаратуре DECT работать с сотовыми сетями (например, GSM). Эти приложения открыли широкие возможности перед операторами как проводных, так и беспроводных сетей связи.

Краткое описание стандарта DECT

DECT является стандартом радиодоступа, поддерживающим широкий набор экономичных средств предоставления коммуникационных услуг. Данный стандарт разрабатывался в соответствии с семиуровневой моделью взаимодействия открытых систем (OSI/ISO) и состоит из девяти частей, описывающих его обязательные и факультативные элементы. Обязательные элементы стандарта гарантируют возможность "сосуществования" систем связи на одной территории при отсутствии координации их работы и позволяют избежать планирования частот, что необходимо в обычных сотовых сетях.

По своему желанию производители могут поддерживать отдельные факультативные элементы стандарта DECT для построения систем голосовой телефонии, доступа к сети ISDN и передачи данных. В целях обеспечения взаимодействия различных приложений DECT Институтом ETSI стандартизуется ряд совокупностей параметров, так называемых профилей (profiles). Одним из подобных профилей является унифицированный профиль доступа (Generic Access Profile - GAP), определяющий функционирование портативных телефонных аппаратов и базовых станций DECT для всех приложений голосовой связи. Другой профиль - профиль интерфейса GSM (GSM Interface Profile - GIP) определяет взаимодействие аппаратуры DECT и сетей GSM. По существу, GIP - это профиль GAP с небольшими дополнениями по взаимодействию с GSM.

Стандарт DECT разрабатывался для удовлетворения потребностей сложной системы радиосвязи - беспроводной АТС. Среда беспроводной АТС характеризуется высокой плотностью трафика и строгими требованиями пользователей к качеству и конфиденциальности (для чего необходимо шифрование радиосигнала) связи. Беспроводные телефонные системы DECT осуществляют кодирование речи методом адаптивной дифференциальной импульсно-кодовой модуляции (Adaptive Differential Pulse Code Modulation - ADPCM), позволяющим передавать оцифрованную речь на скорости 32 Кбит/с. Это значительно большая частота следования битов, чем, например, аналогичная частота, предусмотренная в любом из мировых стандартов цифровой сотовой связи. Она обеспечивает качество передачи речи такое же, как у обычного телефона. Системы DECT реализуют незаметное (автоматическое) переключение абонента на ближайшую базовую станцию при его перемещении из зоны обслуживания одной базовой станции в зону обслуживания другой, что позволяет избежать разрывов связи.

Разрабатывавшийся для беспроводных АТС, DECT оказался подходящим и для домашних, а также местных локальных телефонных систем. Стандарт поддерживает также различные службы передачи данных и обеспечивает взаимодействие с сетью связи фактически любого другого типа.

Системы DECT работают в частотном диапазоне 1880/1900 МГц, который разбит на десять частотных каналов, и, следовательно, являются мультичастотными (МС). В каждом частотном канале данные передаются в 24 циклически повторяющихся временных интервалах или тайм-слотах (множественный доступ с разделением времени - TDMA). В первой половине этих тайм-слотов осуществляется передача информации от базовой станции к портативным устройствам, а во второй половине - в обратном направлении (дуплекс с разделением времени - TDD). Система DECT, таким образом, может быть определена как МС/TDMA/TDD. Каждый из речевых каналов использует пару тайм-слотов, что означает возможность применения 120 (10 несущих частот х 12 тайм-слотов) речевых каналов.

Механизм выбора каналов, известный как непрерывный динамический выбор канала (Continuous Dynamic Channel Selection - CDCS), позволяет системам функционировать "бок о бок" при отсутствии координирования их работы. Любое из портативных устройств стандарта DECT в принципе имеет доступ к любому каналу (как к частотному, так и к временному). Когда необходимо установить соединение, портативное устройство связи DECT выбирает канал, обеспечивающий наиболее качественную связь. После того как соединение установлено, данное устройство продолжает анализировать диапазон, и если обнаруживается канал, гарантирующий лучшее качество связи, то переключает соединение на него. Старое и новое соединения перекрываются во времени, что обеспечивает возможность незаметного переключения.

Благодаря применению CDCS в системах DECT не требуется планирования частот: решение этой проблемы, фактически, перекладывается на портативное устройство связи. Данное обстоятельство делает инсталляцию систем простой процедурой, а также позволяет увеличивать общее число каналов путем простого добавления, где это необходимо, новых базовых станций.

Стандарт DECT предусматривает ряд функций защиты, включая шифрование радиосигнала и аутентификацию портативных устройств связи. Система идентификации устройств DECT позволяет одному и тому же устройству связи осуществлять доступ к нескольким различным системам (например, к базовой станции обычного домашнего телефона, АТС и к системе общего доступа), а также одной базовой станции обеспечивать доступ к различным системам связи. При подобной организации несколько служб могут совместно использовать одну и ту же инфраструктуру связи, что весьма привлекательно с экономической точки зрения.

В Европе DECT является обязательным стандартом - частотный диапазон DECT во всех странах-участницах Европейской конференции администраций почт и электросвязи (CEPT) зарезервирован исключительно для систем поддерживающих этот стандарт. Он имеет также широкую поддержку в промышленности: все основные поставщики беспроводных офисных телефонных систем, работающие на европейском рынке, либо уже предлагают системы DECT, либо объявили о намерениях выпускать такие продукты. Первые коммерческие системы DECT появились на рынке в 1993 г., а некоторые производители уже продают системы DECT второго поколения.

Растет интерес к стандарту DECT и за пределами европейского континента. В США на основе DECT создается стандарт на средства связи, работающие на частотах 1850/1990 МГц, выделенных Федеральной комиссией по связи (Federal Communications Comission - FCC) для систем персональной связи (Personal Communications Services - PCS). Частоты PCS делятся на несколько диапазонов для лицензируемых систем и диапазон для нелицензируемых приложений (1910/1930 МГц). Нелицензируемый диапазон будет использоваться такими системами, как беспроводные УАТС. Подгруппой TR41.6 Института ANSI для подобных приложений был разработан стандарт WCPE, который в основном повторяет стандарт DECT, за исключением физического уровня, приведенного в соответствие с требованиями FCC. Механизм CDCS, предусмотренный стандартом DECT, позволяет системам WCPE "сосуществовать" с другими системами, работающими в том же диапазоне: система просто не будет использовать радиоканал, если определит, что он уже занят.

В настоящее время стандарт WCPE адаптируется также для приложений (например, систем общего доступа), функционирующих на лицензируемых частотах PCS. В

лицензируемых сетях PCS эта технология будет применяться в системах нижнего уровня, обеспечивая высококачественную связь для пользователей с ограниченной мобильностью в условиях большой плотности абонентов. Вероятно, системы нижнего уровня будут использоваться совместно с системами более высокого уровня, базирующимися на обычной цифровой сотовой технологии.

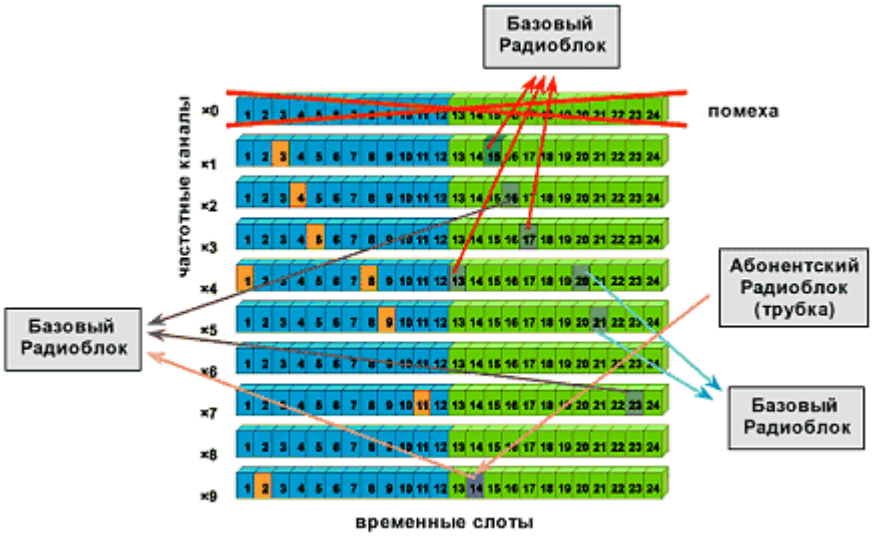
Принцип работы систем стандарта DECT

Принцип MC/TDMA/TDD

Радиоинтерфейс DECT основывается на методологии радиодоступа с использованием нескольких несущих, принципа множественного доступа с разделением времени, дуплекса сразделением времени (MC/TDMA/TDD). Выделение базовой частоты DECT использует 10 частотных каналов (MC - Multi Carrier) в диапазоне 1880-1990 МГц. Временной спектр для DECT подразделяется на временные фреймы, повторяющиеся каждые 10 мс. Фрейм состоит из 24 временных слотов, каждый из которых индивидуально доступен (TDMA - Time Division Multiple Access), слоты могут использоваться либо для передачи либо для приема.

В базовой речевой услуге DECT два временных слота - с разделением в 5 мс - образуют пару для обеспечения поддерживающей емкости обычно для полных дуплексных 32 kbit/s соединений (ADPCM - адаптивная дифференциальная импульсно-кодовая модуляция - G.726 кодированная речь). Для облегчения реализаций базового стандарта DECT временной фрейм в 10 мс разделяется на две половины (TDD - Time Division Duplex); первые 12 временных слота используются для передачи фиксированной части ("связь вниз"), а остальные 12 - для передачи носимой части ("связь вверх").

Структурой TDMA обеспечивается до 12 одновременных голосовых соединений DECT (полный дуплекс) на каждый трансивер, что дает значительные ценовые преимущества по сравнению с технологиями, позволяющими только одно соединение на трансивер (например, CT2). Благодаря усовершенствованному радиопротоколу, DECT может предлагать полосы частот различной ширины, соединяя несколько каналов в одну несущую. Для целей передачи данных достигаются защищенные от ошибок чистые скорости в n x 24 kbit/s максимально до 552 kbit/s, при этом, как оговорено стандартом DECT, обеспечивается полная безопасность.



Использование радиоспектра

При использовании принципа MC/TDMA/TDD для базового DECT (частотные и временные измерения), устройству DECT в любой момент доступен общий спектр из 120 дуплексных каналов. При добавлении третьего измерения (пространства) - при условии, что емкость DECT ограничивается помехами от сопряженных сот и достигается соотношение C/I (Carrier-to-Interface) = 10 дБ - можно получить очень низкий коэффициент повторного использования канала. Различные каналы связи в прилегающих сотах могут использовать тот же канал (комбинация частота/временной слот). Следовательно, при высокой плотности установки базовых станций DECT (например, на расстоянии 25 м в идеальной модели покрытия в форме шестиугольника) можно достичь емкости трафика для базовой технологии DECT приблизительно до 10 000 Эрланг/кв.км./этаж при отсутствии необходимости частотного планирования. Инсталляция оборудования DECT упрощена, так как необходимо учитывать только требования к покрытию и трафику. Эрланг равен средней нагрузке трафика, вызываемой одним речевым соединением DECT - с использованием одной пары "частота/временной слот" - 100% времени.

Непрерывная передача сигнала

Базовая станция (базовый радиоблок - БРБ) DECT постоянно передает сигнал, по крайней мере, по одному каналу, таким образом выступая в качестве маяка для соединения с мобильными DECT-трубками (абонентскими радиоблоками - АРБ). Передача может быть частью активной связи, а может быть холостой. Передача маяка БРБ содержит служебную информацию - в многофреймовой мультиплексной структуре - об идентификации базовой станции, возможностях системы, статусе БРБ и пейджинговую информацию для установления входящей связи. АРБ, подключенные к передаче маяка, проанализируют передаваемую информацию и определят, есть ли у АРБ права доступа к системе (только те АРБ, у которых есть права доступа, могут установить связь), соответствуют ли возможности системы услугам, требующимся АРБ и - в том случае, если связь необходима - есть ли у БРБ свободная емкость для установления радиосвязи с АРБ.

Динамический выбор и динамическое выделение канала

DECT определяет постоянный динамический выбор канала и динамическое выделение канала. Все оборудование DECT обязано регулярно сканировать свое локальное радиоокружение - по крайней мере один раз каждые 30 секунд. Сканирование означает получение и измерение силы местного радиочастотного сигнала по всем свободным каналам. Сканирование осуществляется как фоновый процесс и представляет список свободных и занятых каналов (список RSSI: Received Signal Strength Indication - Индикация мощности полученного сигнала), один для каждой комбинации "временной слот/несущая", который будет использоваться в процессе выбора канала.

Свободный временной слот не используется (временно) для передачи или приема. В списке RSSI низкие значения мощности сигнала означают свободные каналы без помех, а высокие значения означают занятые каналы или каналы с помехами. С помощью информации RSSI, DECT-АРБ или DECT-БРБ может выбрать оптимальный (с наименьшими помехами) канал для установления новой линии связи. Каналы с самыми высокими значениями RSSI постоянно анализируются в DECT-АРБ для того, чтобы

проверить, что передача исходит от базовой станции, к которой у носимой части есть права доступа. АРБ засинхронизируется с БРБ, имеющей самый мощный сигнал, как определено стандартом DECT. Каналы с самыми низкими значениями RSSI используются для установления радиосвязи с БРБ, если пользователь АРБ решит установить связь, или в случае, когда мобильной DECT-трубке передается сигнал о входящем звонке через прием пейджингового сообщения.

В базовой станции DECT каналы с низкими значениями RSSI используются при выборе канала для установления передачи маяку (холостой передачи).Механизм динамического выбора и выделения канала гарантирует, что связь всегда устанавливается на самом чистом из доступных каналов.

Установление связи

Установление связи, инициируемое пользователем (исходящая связь)Инициатива установления радиоканала в базовых приложениях DECT всегда принадлежит АРБ. АРБ выбирает (используя динамический выбор канала) наилучший из доступных каналов и связывается по нему с БРБ. Чтобы обнаружить попытки установления связи со стороны АРБ, БРБ должен принимать на этом канале, когда АРБ передает свой запрос на доступ. Чтобы АРБ могли использовать все 10 радиочастотных несущих DECT, БРБ постоянно последовательно сканирует свои незанятые принимающие каналы в поисках попыток АРБ установить связь. АРБ синхронизируются с этой последовательностью с помощью постоянно передаваемой базовой станцией служебной информации. На основе этой информации АРБ могут определять точный момент, когда возможен успешный доступ к БРБ на выбранном канале. Установление связи, инициируемое сетью (входящая связь)При поступлении входящего вызова на DECT-АРБ, сеть доступа информирует об этом АРБ, отправив соответствующий идентификатор об этом АРБ по пейджинговому каналу. АРБ, приняв пейджинговое сообщение со своим идентификатором, устанавливает радиоканал для обслуживания входящего вызова, используя ту же процедуру, которая применяется при установлении исходящей связи.

Handover

Благодаря мощному динамическому выбору и выделению канала и возможностям DECT, обеспечивающим handover без прерывания связи, АРБ могут уходить от соединения, содержащего помехи, устанавливая второе соединение - на вновь выбранном канале - либо с той же базовой станцией (внутрисотовый handover) либо с другой базовой станцией (handover между сотами). Эти два радиосоединения временно поддерживаются параллельно, при этом передается идентичная речевая информация, и в то же время анализируется качество соединений. По прошествии некоторого времени базовая станция определяет, у какого радиосоединения лучше качество, и освобождает другой канал. Если DECT-АРБ перемещается из одной соты в другую, мощность получаемого сигнала БРБ-измеряемая с помощью динамического выбора и выделения канала носимой частью - будет постепенно уменьшаться. Мощность сигнала БРБ, обслуживающей соту, в направлении которой движется АРБ, будет постепенно возрастать. В тот момент, когда сигнал нового БРБ становится сильнее сигнала старого БРБ, происходит handover без прерывания связи (как описано выше) к новому БРБ. Хэндовер без прерывания связи, совершенно независимо инициируемый мобильной DECT-трубкой, остается незамеченным для пользователя. Хотя handover всегда инициируется DECT-АРБ, возможны ситуации, в которых линия связи "АРБ-БРБ" не обеспечивает требуемого

качества. На этот случай в DECT предусмотрены протоколы оповещения, которые позволяют БРБ передать сообщение о воспринимаемом качестве соединения АРБ, который может затем инициировать handover. Хэндовер в DECT - это механизм ухода от каналов, подверженных воздействию помех, или каналов с низким уровнем сигнала. Однако handover происходит недостаточно быстро, чтобы противодействовать ситуациям быстрого замирания. Для этой цели DECT-БРБ может быть оборудована разнесенными антеннами. Стандартом предусмотрен протокол сигнализации для контроля за выбором антенны БРБ с мобильной DECT-трубки. Благодаря тому, что радиолиния между БРБ и АРБ имеет природу дуплекса с временным разделением (симметрии), выбор лучшей антенны БРБ улучшает не только качество "восходящей линии связи", но и качество "нисходящей линии связи", на низкой скорости.

Совместимость

Свойства совместимости технологии радиодоступа в основном базируются на возможности ухода (handovera) - в частотной области - от зашумленной радиолинии, не полагаясь на информацию, переданную по первоначальному каналу (подверженному воздействию). MC/TDMA/TDD, постоянный динамический выбор и выделение канала и процедуры handovera в стандарте DECT демонстрируют отличные возможности совместимости даже в условиях сильной интерференции

Защищённость

Использование технологии радиодоступа, предоставляющей мобильность, подразумевает значительный риск в отношении защищенности. Стандарт DECT предусматривает меры противодействия естественным дефектам защищенности, свойственным бесшнуровой связи.Для предотвращения несанкционированного доступа были введены эффективные протоколы прописки и аутентификации, а концепция усовершенствованного кодирования обеспечивает защиту от прослушивания.

Прописка

Прописка - это процесс, благодаря которому система допускает конкретную мобильную DECT-трубку к обслуживанию. Оператор сети или сервис-провайдер обеспечивает пользователя АРБ секретным ключом прописки (PIN-кодом), который должен быть введен как в БРБ, так и в АРБ до начала процедуры. До того, как трубка инициирует процедуру фактической прописки, она должна также знать идентификацию БРБ, в которой она должна прописаться (из соображений защищенности область прописки может быть ограничена даже одной выделенной (маломощной) БРБ системы). Время проведения процедуры обычно ограничено, и ключ прописки может быть применен только один раз, это делается специально для того, чтобы минимизировать риск несанкционированного использования. Прописка в DECT может осуществляться "по эфиру", после установления радиосвязи с двух сторон происходит верификация того, что используется один и тот же ключ прописки. Происходит обмен идентификационной информацией, и обе стороны просчитывают секретный аутентификационный ключ, который используется для аутентификации при каждом установлении связи. Секретный ключ аутентификации не передается по эфиру. Мобильная DECT-трубка может быть прописана на нескольких базовых станциях. При каждом сеансе прописки, АРБ просчитывает новый ключ аутентификации, привязанный к сети, в которую он прописывается. Новые ключи и новая

информация идентификации сети добавляются к списку, хранящемуся в АРБ, который используется в процессе соединения.Трубки могут подключиться только к той сети, в которую у них есть права доступа (информация идентификации сети содержится в списке.

Аутентификация и шифрование

Аутентификация трубки может осуществляться как стандартная процедура при каждом установлении связи. Во время сеанса аутентификации базовая станция проверяет аутентификационный ключ, не передавая его по эфиру. Принцип нераскрытия идентификационной информации по эфиру заключается в следующем: БРБ посылает трубке случайное число, которое называется "запрос". Трубка рассчитывает "ответ", комбинируя аутентификационный ключ с полученным случайным числом, и передает "ответ" базовой станции. БРБ также просчитывает ожидаемый "ответ" и сравнивает его с полученным "ответом". В результате сравнения происходит либо продолжение установления связи либо разъединение. Если кто-то подслушивает по эфирному интерфейсу, для того чтобы украсть аутентификационный ключ, ему необходимо знать алгоритм для выявления ключа из "запроса" и "ответа". Этот "обратный" алгоритм требует огромной компьютерной мощности.Поэтому стоимость извлечения ключа подслушиванием процедуры аутентификации невероятно высока. Процесс аутентификации использует алгоритм для вычисления "ответа" из "запроса" и аутентификационный ключ в трубке и на базовой станции. Он представляет собой способ отправки идентификационной информации пользователя в зашифрованной форме по эфиру для предотвращения кражи идентификационной информации. Этот же принцип может быть применен для данных пользователя (например, для передачи речи). Во время аутентификации обе стороны также просчитывают ключ шифрования. Этот ключ используется для шифрования данных, передаваемых по эфиру. Получающая сторона использует тот же ключ для расшифровки информации. В DECT процесс шифрования является частью стандарта (хотя и необязательной).

Спецификация DECT

Диапазон частот	1880-1900 МГц
Метод доступа	MCT/TDMA/TDD
Разделение несущих	1,728МГц
Число несущих	10
Число временных интервалов	24
Число дуплексных речевых каналов на несущую	12
Длительность цикла	10 мсек
Полная скорость	1152 кбит/сек
Модуляция	GFSK
Кодирование речи	32 бит/сек
Номинальная мощность	10 мВт
Метод кодирования речи	ADPCM
Выбор канала	CDCS

DECT и безопасность

Завершая описание DECT, рассмотрим особенности защиты от несанкционированного доступа, вопросы организации связи и способы интеграции с другими телекоммуникационными системами.
Стандарт DECT имеет неоспоримые преимущества в области качества связи и обеспечивает (по сравнению с другими стандартами) наиболее низкий уровень излучения радиотелефонов. Что же касается его коммерческого успеха, этим он во многом обязан высокой степени защищенности DECT-связи от несанкционированного доступа.

Обеспечение безопасности

Вопросы защиты крайне важны для сетей радиосвязи, где информация передается по эфиру и теоретически не существует проблем ее перехвата и дальнейшего использования. И здесь высокий потенциал стандарта DECT определяется тем комплексом мер, которые прописаны как дополнительные требования в разных профилях доступа.

Виды угроз

Для систем беспроводного доступа существуют три основных вида угроз: нелегальное использование средств связи, несанкционированный перехват информации и преднамеренное воздействие на нее с целью нарушения нормального функционирования системы. В зависимости от профиля доступа сценарии воздействия и способы защиты от угроз могут быть разными, как и степень чувствительности самой системы DECT к этим воздействиям.
Большинство видов угроз и методов воздействия на систему связано с попытками тем или иным способом уклониться от оплаты эфирного времени. Чаще всего для данных целей используются станции-двойники или похищенные станции (табл. 1). Степень защищенности сети определяется эффективностью применяемой системы паролей, способом аутентификации мобильных станций и абонентов, а также организационно-административными мерами, например созданием "черного списка" сети.
Другой вероятный вид угроз связан с перехватом информации. В DECT предусмотрена защита от активного и пассивного перехвата. В первом случае создается ложная базовая станция (БС) для перехвата информации или перенаправления ее другому адресату, во втором осуществляется пиратское подключение к радиоканалам.
Заметим, что в коммерческих сетях ущерб от такого вида угроз может быть весьма значительным, и он отнюдь не сводится к оплате счетов несанкционированных пользователей. Для защиты от этого вида угроз в DECT применяются шифрование информации и взаимная аутентификация работающих станций. Существуют и другие, более изощренные, методы воздействия, которые "не вписываются" в рамки данной статьи.

Табл. 1 Возможные виды угроз и способы обеспечения безопасности

Вид угрозы	Средства воздействия	Способы защиты
Нелегальное использование средств связи с целью избежать оплаты или обеспечить анонимность	Станции-двойники, похищенные станции	Аутентификация по паролю, создание "черного списка"
Несанкционированный пе-	Активный перехват (ложная	Аутентификация на мобиль-

рехват с целью получения доступа к конфиденциальной информации	БС) Пассивный перехват	ной станции. Периодическое обновление ключей шифрования
Преднамеренное воздействие с целью нарушения правильного функционирования системы	Создание радиопомех Программные способы	Активные (пеленгация источников помех) Пассивные (помехозащита, кодирование)

Аутентификация оборудования

Для того чтобы исключить появление двойников, способных посылать и принимать вызовы с использованием идентификатора законного абонента, в стандарте DECT введена процедура установления подлинности. Проверка основана на аутентификационном ключе, который хранится как в контроллере базовой станции (RFP), так и на абонентском терминале (PP).

Операция аутентификации абонентской станции (АС) выполняется по инициативе БС при каждой новой попытке установления соединения - независимо от того, является ли вызов входящим или исходящим. Применяется также аутентификация в процессе сеанса связи.

Процесс начинается, когда БС формирует и передает запрос. Этот запрос содержит некоторый постоянный или редко меняющийся параметр RS (64 бита) и случайное число RAND F (64 бита), генерируемое для данного сеанса. В ПЗУ абонентской станции "зашит" алгоритм аутентификации A12, с помощью которого по ключу UAK и случайному числу RAND F формируется ответ на запрос RES1 (так называемая цифровая подпись). На базовой станции ожидаемый ответ сравнивается с принятым значением RES1, и при их совпадении аутентификация считается успешной.

Основное требование к алгоритму аутентификации - его необратимость, т.е. невозможность однозначного восстановления абонентского ключа и ответа RES в случае их перехвата по радиоканалу даже при известности алгоритма шифрования.
Схема аутентификации, принята в DECT, во многом схожа с той, которая используется в GSM. Однако разработчики стандарта DECT пошли еще дальше, предусмотрев аутентификацию не только абонентского оборудования, но и базовой станции по запросу абонентской.

Аутентификация БС проводится, чтобы исключить возможность ее неправомочного использования; в частности, блокируется угроза перенаправления вызовов абонентов с целью их перехвата. В целом алгоритм аутентификации БС аналогичен применяемому для АС , только роли базовой и абонентской станций меняются: АС вычисляет обратный аутентификационный код со значением FP, принятым от базовой станции, а случайный код RAND P передается на БС, где с помощью алгоритма аутентификации A22 вычисляется ответный сигнал RES2, который и отправляется на АС в качестве квитанции.
Взаимная аутентификация БС и АС может осуществляться тремя способами - прямым и двумя косвенными. Прямой способ состоит в последовательном выполнении процедур аутентификации АС и БС (порядок - любой).

Первый из косвенных способов подразумевает проведение двух процедур аутентификации АС с шифрованием данных. При этом АС по полученным данным вычисляет ключ шифра и использует его для шифрования всей информации. Если БС не владеет точным ключом аутентификации K, то вычисленный ею ключ CK будет неверным и не позволит ей правильно принять данные, переданные АС, что и станет причиной

разрыва соединения. Аутентификация завершится успешно только тогда, когда БС правильно расшифрует данные и ответит на запрос.

Второй косвенный способ основан на использовании статического ключа SCK. В этом случае процедура аутентификации осуществляется за один цикл обмена сигналами, поскольку ключ SCK известен обеим станциям.

Аутентификация абонентов

Каждая мобильная станция должна пройти процедуру аутентификации в сети DECT, во время которой выявляется, знает ли абонент свой персональный идентификатор и не является ли станция украденной. Такая процедура проводится каждый раз перед началом работы и предусматривает введение абонентом своего персонального номера. Функции контроля номера в системе DECT выполняет встроенный в абонентскую станцию аутентификационный модуль DAM (DECT Authentication Module), в котором записаны международный код опознания абонента (IPUI - International Portable User Identity) и ключ аутентификации K.
Если станция уже активизирована, то процедура аутентификации абонента может быть проведена в любой момент (во время сеанса связи) и по запросу БС. После набора персонального идентификатора UPI базовая станция вычисляет по нему ключ K и инициирует процедуру аутентификации AC.

В стандарте DECT определены четыре категории прав доступа (PARK-Portable Access Right Key), зависящие от размера систем:
* A - с малым числом сот;
* B - офисные со сложной коммутацией и наличием связи с локальными сетями;
* C - сопряженные с сетями общего пользования;
* D - сопряженные с сетями GSM.
Каждый международный индивидуальный код IPUI, который может быть использован с разными PARK, состоит из двух частей: типа абонента (PUT - Portable User Type) и его номера (PUN - Portable User Number). Для указания типа используется поле фиксированного размера (4 бита), а длина номера зависит от его типа. В стандарте DECT определены семь типов номеров PUN для различных профилей доступа (табл. 2).

Наряду с идентификационным международным кодом IPUI в DECT используется временный телефонный идентификатор (TPUI-Temporary Portable User Identity), который позволяет защитить код IPUI от перехвата. Он состоит из 20 бит или имеет ту же структуру, что и IPUI N типа (см. табл. 2); в нем первые 16 бит повторяют последнюю часть кода IPUI, а оставшиеся 20 являются собственно кодом TPUI.

Шифрование

Криптографическая защита в стандарте DECT обеспечивается с помощью общего ключа шифрования CK (Cipher Key), который позволяет формировать сегментированную шифрующую последовательность KSS - Key Stream Segments. Такая последовательность "накладывается" на поток данных на передающей стороне и "снимается" на приемной. Строится KSS в соответствии со стандартными алгоритмами шифрования, разрабатываемыми и поставляемыми ETSI.

В зависимости от условий применения системы DECT в ней используются ключи разных типов: производные (DCK - Derived Chipher Key) и статические (SCK - Static Cipher Key). Криптографический ключ первого типа получается путем логического преобразования

общего ключа, например путем сложения его с серийным номером абонентского терминала. Такой ключ обновляется в начале каждого сеанса связи. Статический ключ вводится абонентом вручную и обычно используется в домашних системах связи, где он является уникальным для каждой пары АС-БС. Этот ключ хранится в ЗУ мобильной станции, и менять его рекомендуется не реже одного раза в месяц, иначе возрастает риск нарушения защиты информации.
Очевидно, что степень безопасности системы, в которой используется процедура аутентификации, определяется способом реализации процедур генерации, распределения и хранения ключей аутентификации.

Стандарт DECT допускает несколько способов загрузки ключей: по радиоканалу, с помощью DAM-карточки или вручную (UPI-код). Первый из них наиболее удобен с точки зрения оперативной смены ключей, однако связан с риском для безопасности системы. Достаточно эффективным средством хранения ключей является карточка DAM, используемая в терминалах DECT/GSM.

Таблица 2. Структура международного кода опознавания абонента IPUI

Тип кода	**PUT**	**PUN**	**Тип сети**
N	4	36 (IPUI)	Домашняя
S	4	60 (номер абонента ISDN)	ISDN
O	4	60 (номер абонента ТФОП)	Офисная на базе УПАТС
T	4	16 (EIC)+44 (доп. номер)	Сеть с филиалами
P	4	16 (POC)+80 (ACC)	Telepoint RLL
Q	4	80 (BACN)	Telepoint
R	4	60 (IMSI)	GSM

Обозначения: ACC - учетный номер сети Telepoint; BACN - двоично-десятичный банковский учетный номер; EIC - код установленного оборудования; IMSI - международный идентификационный номер АС; POC - код оператора сети общего пользования.
Telepoint - сеть DECT, в которой допускаются только исходящие вызовы. Она подключена к сети общего пользования с помощью БС, устанавливаемых в местах концентрации людей

Приложения DECT

Деловые беспроводные телефонные системы

Деловая беспроводная телефония (business cordless telephony - BCT) была первым приложением стандарта DECT, предложенным производителями. Системы, продаваемые сегодня, являются либо полностью интегрированными беспроводными УАТС, включающими коммутирующие системы, либо добавочными системами, которые могут быть подключены к существующим телефонным станциям, формируя, таким образом, гибридную систему, поддерживающую как кабельные, так и беспроводные соединения.

К системам BCT предъявляются бочльшие, чем к прочим приложениям DECT, требования по объему поддерживаемого трафика - порядка 10 000 Эрл/кв. км/этаж. Эти потребности могут быть удовлетворены при использовании пикосотовых систем (с миниячейками), размер которых внутри помещений (в горизонтальной плоскости) составляет 30-70 м и один этаж вверх или вниз, а вне зданий - 100-300 м.

Рыночный потенциал систем BCT огромен: эксперты предполагают, что к 2000 г. треть телефонных аппаратов, используемых в деловых целях, будут беспроводными.

Средства BCT не обязательно должны работать через УАТС. Аппаратура DECT может непосредственно взаимодействовать с сетями связи общего пользования, обеспечивая выполнение функций системы Centrex. Данное обстоятельство является чрезвычайно привлекательным для операторов сетей общего пользования, особенно если эти операторы могут обеспечить связь как в здании учреждения, так и вне его. Один из сетевых операторов в Финляндии уже начал опытную эксплуатацию подобной системы, которая демонстрирует многообещающие результаты.

Местная радиосвязь (RLL)

Использование радио в качестве альтернативы медному кабелю для доступа к сети обретает все большую популярность. Первые системы, основанные на сотовой технологии, начали эксплуатироваться в начале 90-х годов. Сегодня всем очевидны преимущества этого вида связи в отношении быстроты подключения абонентов, а также низкой стоимости установки и функционирования соответствующих систем. Похоже, в ближайшее время системы местной радиосвязи (Radio in the local loop - RLL) получат широкое распространение, особенно в странах Восточной Европы и Азии, где и политические, и финансовые условия предполагают бурное развитие сетей электросвязи.

Системы RLL привлекательны как для относительно давно действующих операторов кабельных сетей, так и для новых конкурирующих с ними компаний, которые предоставляют услуги сетей связи.

Там, где кабельные сети не получили большого распространения, системы RLL могут быть использованы для подключения к глобальным сетям большого числа новых абонентов за значительно более короткое время по сравнению со временем, необходимым для развертывания кабельной сети. Но в то же время местная радиосвязь может играть значительную роль и в местах с развитой кабельной инфраструктурой связи. Давно действующие операторы кабельных сетей могут использовать системы RLL для предоставления своим абонентам дополнительных линий передачи данных, например для факсимильной или модемной связи, без наращивания кабельной системы связи.

Конкурирующие с ними новые поставщики услуг сетей связи также могли бы использовать технологию RLL для подключения абонентов. Основное преимущество здесь в том, что оператору нет необходимости знать, где будут находиться его клиенты. Недавно появившийся оператор может ожидать, что, скажем, 10-15% абонентов телефонных сетей, находящихся на данной территории, перейдут на новое обслуживание, однако точно определить их он не в состоянии. Используя технологию RLL, оператор способен минимизировать предварительные затраты на обеспечение обслуживания потенциальных абонентов. Весомая часть сетевой инфраструктуры может быть установлена (и оплачена) при подключении абонента к сети. В этой ситуации система RLL - наиболее экономичное средство, обеспечивающее обслуживание абонентов.

Большинство существующих сегодня систем RLL основаны на сотовой технологии и используют при этом один из сотовых стандартов, таких как NMT, а также цифровой AMPS или GSM. Подобно породившим их сотовым системам, эти системы RLL оптимизированы для большой зоны обслуживания и, таким образом, лучше подходят для обеспечения обслуживания абонентов в условиях небольшой плотности их расположения. Например, системы RLL, базирующиеся на стандарте NMT- 450, позволяют обслуживать абонентов, находящихся в 40 км от ближайшей базовой станции.

В противоположность им, системы RLL, соответствующие стандарту DECT, оптимизированы для городских и пригородных территорий, где плотность абонентов довольно высока. При использовании направленных антенн (на обоих концах радиоканала. - Прим. ред.) эффективная дальность действия базовой станции увеличивается до 5 км. Узел доступа DECT (базовая станция RLL) содержит некоторое число направленных антенн обычно расположеных таким образом, чтобы охватить все направления (в горизонтальной плоскости). Вместо бесшнуровых телефонов абоненты системы RLL применяют стационарные устройства доступа, которые оснащены направленными антеннами, наведенными на ближайший узел доступа DECT. К стационарному устройству доступа могут быть подключены телефоны, факсимильные аппараты, модемы и другие средства.

Недавно ETSI были определены дополнения к стандарту DECT, включающие увеличенную преамбулу и улучшенный механизм синхронизации, благодаря которым повысится стабильность параметров сигналов DECT при их распространении на большие расстояния и при отражениях. Эти дополнения призваны сделать стандарт DECT более подходящим для систем связи, работающих вне помещений, включая средства RLL.

Судя по всему, в условиях средней и большой плотности абонентов системы RLL, соответствующие стандарту DECT, становятся более экономически выгодными, чем сотовые. "Критической" точкой здесь является плотность 20 абонентов на 1 кв. км. Одна из причин этого кроется в формате TDMA, использованном в DECT, который позволяет одному радиопередатчику поддерживать одновременно до 12 соединений. Такого не предусматривает ни одна другая цифровая сотовая или бесшнуровая технология связи.

В целом можно сказать, что системы RLL, соответствующие стандарту DECT, лучше других подходят для работы в условиях средней или высокой плотности абонентов - либо в городах, либо в сельской местности, где число абонентов может быть и невелико, однако плотность их размещения довольно высока. Эти системы подойдут также абонентам, которые сейчас или в будущем захотят использовать линии связи для передачи данных или для работы с сетью ISDN.

Связь с мобильными объектами

Архитектура системы RLL стандарта DECT, описанная выше, подходит только для связи со стационарными устройствами доступа, имеющими направленные антенны с большим коэффициентом усиления, которые необходимы для обмена информацией между узлом доступа DECT и стационарным устройством доступа на расстоянии до 5 км. Однако данная архитектура в любой момент может быть модифицирована для связи с мобильными терминалами с помощью радиоретрансляционных станций (Wireless Relay Stations - WRS). Функционирование WRS в настоящее время стандартизовано ETSI как часть общего стандарта DECT.

WRS может быть использована различными способами. В одном случае, будучи оснащенной двумяітремя направленными антеннами, она может обеспечить передачу сигнала на территории, "затененные" различными неровностями рельефа. В другом случае, имея одну направленную антенну для связи с узлом доступа DECT, с помощью второй ненаправленной антенны вокруг станции-повторителя может быть создана миниячейка радиусом 100/300 м. В любой конфигурации WRS поддерживает до шести речевых каналов одновременно.

При достаточном числе радиоретрансляционных станций, обеспечивающих перекрытие миниячеек, можно организовать связь с мобильными абонентами на большой территории. При этом абоненты, используя бесшнуровые телефонные аппараты, могут осуществлять вызовы и принимать звонки на всей этой территории. К тому же им гарантируется незаметное переключение на ближайший ретранслятор (так, как это происходит в системах сотовой связи) при перемещении от одной миниячейки к другой.

Ближайшее настоящее и будущее DECT

В Европе DECT является обязательным стандартом - частотный диапазон DECT во всех странах-участницах Европейской конференции администраций почт и электросвязи (CEPT) зарезервирован исключительно для систем поддерживающих этот стандарт. Он имеет также широкую поддержку в промышленности: все основные поставщики беспроводных офисных телефонных систем, работающие на европейском рынке, либо уже предлагают системы DECT, либо объявили о намерениях выпускать такие продукты. Первые коммерческие системы DECT появились на рынке в 1993 г., а некоторые производители уже продают системы DECT второго поколения.

Растет интерес к стандарту DECT и за пределами европейского континента. В США на основе DECT создается стандарт на средства связи, работающие на частотах 1850/1990 МГц, выделенных Федеральной комиссией по связи (Federal Communications Comission - FCC) для систем персональной связи (Personal Communications Services - PCS). Частоты PCS делятся на несколько диапазонов для лицензируемых систем и диапазон для нелицензируемых приложений (1910/1930 МГц). Нелицензируемый диапазон будет использоваться такими системами, как беспроводные УАТС. Подгруппой TR41.6 Института ANSI для подобных приложений был разработан стандарт WCPE, который в основном повторяет стандарт DECT, за исключением физического уровня, приведенного в соответствие с требованиями FCC. Механизм CDCS, предусмотренный стандартом DECT, позволяет системам WCPE "сосуществовать" с другими системами, работающими в том же диапазоне: система просто не будет использовать радиоканал, если определит, что он уже занят.

В настоящее время стандарт WCPE адаптируется также для приложений (например, систем общего доступа), функционирующих на лицензируемых частотах PCS. В лицензируемых сетях PCS эта технология будет применяться в системах нижнего уровня, обеспечивая высококачественную связь для пользователей с ограниченной мобильностью в условиях большой плотности абонентов. Вероятно, системы нижнего уровня будут использоваться совместно с системами более высокого уровня, базирующимися на обычной цифровой сотовой технологии.

В настоящее время усилия разработчиков технологии DECT направлены на расширение услуг передачи данных и увеличение пропускной способности каналов до 2,304 и 3,456 Мбит/с. Как следствие, наиболее востребованными оказались профили доступа, связанные с пакетной передачей (DPRS), мультимедиа (DMAP) и доступом в сеть Internet. Особенности систем на базе этих профилей пока активно исследуются, но в ближайшее время их аппаратные реализации должны появиться на телекоммуникационном рынке.

Список использованных материалов

1. DECT TECHNICAL SPECIFICATION
   http://www.netser.com.tr/dectspe.htm
2. DECT Forum
   http://www.dect.ch
3. Cordless Digital Telephony
   http://www.gare.co.uk/technology_watch/cordless.htm
4. Стандарт DECT. Описание.
   http://www.aist.net.ru/standart/tech/dect/description