**Кодирование речевой информации**

Вступление

Необходимость кодирования речевой информации возникла не так давно, но на сегодняшний момент, в связи с бурным развитием техники связи, особенно мобильной связи, решение этой проблемы имеет большое значение при разработке систем связи.

Огромное распространение в наше время получили бытовые радиотелефоны. Они позволяют пользователю не быть привязанным к одному месту в течении телефонного разговора, нет необходимости стремглав мчаться к телефону, услышав звонок (если, конечно, вы вообще его звонок услышите). К тому же во многих моделях существуют различные удобства для пользователя: связь между трубкой и базовым аппаратом, громкая связь (хороша в случае, когда “сели” аккумуляторы в трубке). По всем вышеперечисленным преимуществам эти аппараты завоевали большую популярность и получили большое распространение.

Но поскольку аппаратов стало много, то возникла проблема определения “свой-чужой”, а поскольку обмен данными между трубкой и базовым аппаратом ведется на радиочастотах (27 МГц, 900 МГц),разговор по радиотелефону можно легко подслушать, появилась необходимость кодирования (или шифрования) речевой информации.

Сразу необходимо оговориться, что речевая информация принципиально отличается от другого вида - текстов (рукописных и в электронном виде). При шифровании текста мы имеем дело с ограниченным и определенно известным нам набором символов. Поэтому при работе с текстом можно использовать такие шифры, как шифры перестановки, шифры замены, шифры взбивания и т.д. Речь же нельзя (во всяком случае на сегодняшнем уровне развития технологи распознавания речи)представить таким набором каких-либо знаков или символов. Поэтому применяются другие методы, которые, в свою очередь, делятся на аналоговые и цифровые. В настоящее время больше распространены цифровые методы, на них- то мы и остановимся.

Принцип цифрового кодирования заключается в следующем: аналоговый сигнал от микрофона подается на АЦП, на выходе которого имеем n-разрядный код (при подборе хорошей частоты дискретизации пользователь на другом конце линии может и не догадаться, что голос его собеседника оцифровали, а потом (на базовом аппарате) перевели обратно в аналоговую форму). Затем этот код шифруется с помощью всевозможных алгоритмов, переносится в диапазон радиочастот, модулируется и передается в эфир.

Злоумышленник в своем “шпионском” приемнике услышит просто шум (при хорошем кодировании). Правда, из опыта подслушивания (случайного) радиопереговоров людей, пользующихся скремблерами можно без труда определить, что этот шум имеет совсем не естественное происхождение, поскольку после нажатия тангетты шум исчезал, а затем снова появлялся. Но определить, о чем говорили эти люди, было невозможно без серьезных знаний в области криптологии и соответствующей аппаратуры. В телефонных переговорах этой проблемы нет, поскольку канал дуплексный, и необходимость в тангетте отпадает, а шифрование происходит непрерывно в течении всего разговора.

Систем шифрования, разумеется, великое множество, но для бытовых (а, следовательно, максимально дешевых) радиотелефонов применимы лишь некоторые, простые, но в то же время достаточно надежные.

# Система кодирования речи

Предлагаемая система кодирования речи удовлетворяет двум основным требованиям: она дешева в исполнении и обладает достаточной надежностью от взлома (взломать можно любую, даже самую стойкую криптографическую систему).

## Обоснование выбора метода кодирования

В основе техники шумоподобных сигналов лежит использование в канале связи для переноса информации нескольких реализаций этих сигналов, разделение которых на приеме осуществляется с помощью селекции их по форме. При этом уверенное разделение сигналов может быть получено при введении частотной избыточности, т.е. при использовании для передачи сообщений полосы частот, существенно более широкой, чем занимает передаваемое сообщение.

Селекция сигналов по форме является видом селекции, обобщающим амплитудную, частотную, фазовую и импульсную селекции.

**Преимущества:**

Шумоподобный сигнал позволяет применять новый вид селекции - по форме. Это значит, что появляется новая возможность разделять сигналы, действующие в одной и той же полосе частот и в одни и те же промежутки времени. Принципиально можно отказаться от метода разделения рабочих частот данного диапазона между работающими радиостанциями и селекцией их на приеме с помощью частотных фильтров.

Интересной особенностью системы связи с шумоподобными сигналами являются ее адаптивные свойства - с уменьшением числа работающих станций помехоустойчивость действующих автоматически возрастает.

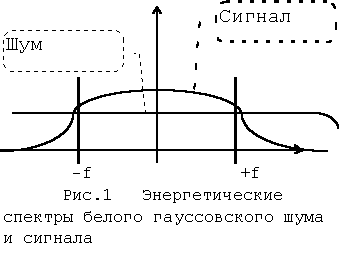
**Недостатки:**

переход к более сложному носителю информации приводит, естественно, к известному усложнению систем связи.

Теоретические и экспериментальные исследования показывают, что исключение более половины полосы частот6 занимаемой шумоподобным сигналом, не нарушают нормальной работы системы. Естественно, что при этом имеет место снижение помехоустойчивости, пропорциональное ширине полосы вырезаемого участка спектра. Следовательно, рассматриваемый метод передачи позволяет решить задачу нормального приема сигналов при наличии весьма мощных мешающих станций в полосе пропускания. Тем самым может быть решена задача, с которой метод частотной селекции принципиально не может справиться.

## Описание метода кодирования

Слабое место многих систем кодирования - это статистическая слабость кода, то есть , анализируя статистику за некоторый период, можно составить мнение о том, что это за система и тогда действовать более направлено. То есть резко сокращается время поиска ключа. Данная система оперирует шумоподобными сигналами, которые по своим свойствам, в том числе и статистическим, практически идентична белому гауссовскому шуму.



Немного проясним ситуацию. По определению сложности закона генерации ряда чисел, если сложность последовательности {gi} равна m, то любые m+1 последовательные ее значения зависимы. Если же эта зависимость представима линейной, то получается реккурентное соотношение следующего вида:

c0gi+c1gi-1+...+cmgi-m=0

При этом c0 c0 обязаны быть ненулевыми. Каждый последующий член последовательности определяется из m предыдущих. Простой их вид реализации получается, когда все составные принимают лишь значения 0 и 1, что делает их очень удобно представляемыми на ЭВМ.

Поля бит можно представить как вектора, каждая компонента которых принимает значения из GF(2). Такие вектора удобно рассматривать как многочлены:

(10010101)=x7+x4+x2+1.

Неразложимость многочлена: над полем комплексных чисел любой многочлен разложим на линейные множители или, по-другому имеет столько корней, какова его степень. Однако это не так для других полей - в полях действительных или рациональных чисел многочлен x2+x+1 корней не имеет. Аналогично, в поле GF(2) многочлен x2+x+1 тоже не имеет корней.

Генератор псевдослучайных чисел

В данном случае можно воспользоваться относительно простым методом генерации псевдослучайной последовательности: а именно - анализом тепловых шумов стабилитрона, работающего в режиме пробоя. Шумы усиливаются и подаются на триггер Шмидта, а затем передавая полученные биты в регистр сдвига. Поскольку тепловые шумы имеют достаточно случайный характер, то и последовательность будет случайной.

# Формирование кода

Для формирования кода используется 5-разрядный первичный ключ, получаемый из генератора псевдослучайных чисел. Таким образом, на начальном этапе формирования ключа мы имеем количество комбинаций 25-2=30 (-2 поскольку комбинация 00000 является недопустимой). Потом первичный ключ подается на два генератора (два для увеличения количества кодов - см. ниже), вырабатывающие по этому ключу 31-разрядные м-последовательности. Эти последовательности перемножаются по модулю 2, циклически сдвигаясь, и образуя два вложенных цикла, выдают 312 вариантов ключа. Итого, общее число допустимых комбинаций составляет 30\*312 .

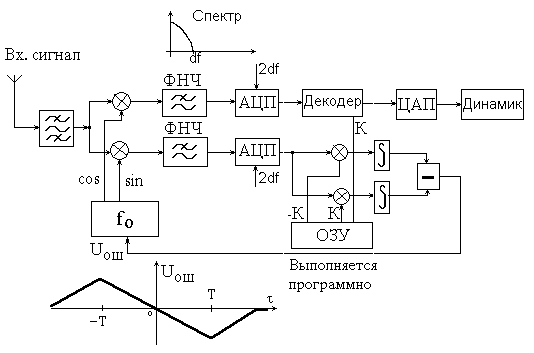
Эти 312 вариантов хранятся в ОЗУ базового аппарата. Выбор одного ключа осуществляется путем повторного обращения к генератору псевдослучайных чисел. Итого, получаем неплохую для данных условий криптографической защиты цифру 30\*313=~900000 комбинаций, не говоря о том, что надо еще догадаться, какой метод применяется для кодирования. При этом статистические свойства данной последовательности практически не отличаются от м-последовательности.

Также возможна аппаратная реализация схемы формирования кода, но принципиального значения это не имеет, поскольку быстродействие здесь роли не играет - код формируется при положенной трубке, а это время больше минуты.

Программа составлена для процессора i80386 и оперирует расширенными (32-разрядными) регистрами. Можно, конечно, реализовать ее на более дешевом процессоре (из семейства SISC - это i8086, i8080, i80186 или i80286), но программа усложнится, к тому же увеличится время выполнения программы, но это не главное; самое главное, что кодирование речи также осуществляется программно, и здесь время выполнения программы критично. Также можно реализовать программу на RISC-процессоре. Этот способ более перспективный.

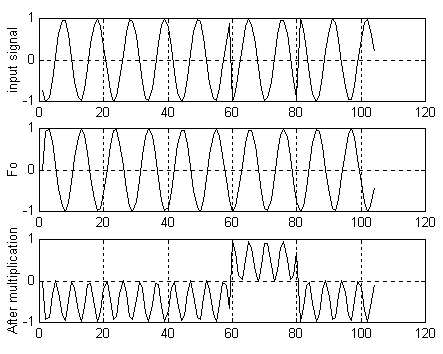
# Структурная схема приема сигнала

На представленной схеме приемника отражены основные, принципиальные моменты приема сигнала.



Итак, фазоманипулированный сигнал (см. диаграмму внизу) приходит с высокочастотной части приемника (здесь не изображена) и попадает на полосовой фильтр, пропускающий конкретный диапазон частот. Таким образом устраняются помехи , имеющие частоту вне пропускаемого диапазона.

Затем сигнал идет на блоки умножения, на которые также подается с опорного кварцевого термостатированного генератора . Сигналов два, они сдвинуты по фазе относительно друг друга на 180 градусов. Это необходимо для последующего сравнения. Итак, цепь разветвилась. После умножения получается сигнал, изображенный на диаграмме. (моделирование в Matlab 4.2c)

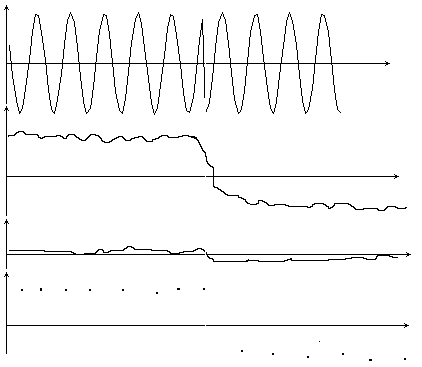


После сигнал подается на фильтр нижних частот, сглаживающих сигнал (см. диаграмму 2 и 3 ниже). Если фаза сигнала опорного генератора совпадает с пришедшим сигналом, мы имеем нечто похожее на

Затем сигнал подается на АЦП, причем частота дискретизации выбрана таким образом, что на каждый элемент приходится два отсчета (см. диаграмму 4 ниже). Это необходимо для надежного декодирования сигнала.

Декодирование выполняется путем умножения (программного) оцифрованных отсчетов на ключ. Сигнал свертывается, и из 31-разрядного кода получается один бит полезной информации, которая затем по уровню анализируется и делается вывод о пришедшей информации: это 1 или 0.

Вторая ветвь схемы служит для фазовой автоподстройки во время разговора. Сигнал умножается (программно) на ключ и инверсное значение ключа, затем сглаживается в интеграторе. Далее формируется сигнал ошибки, который, будучи поданным на опорный генератор, подстраивает его фазу по максимальному абсолютному значению напряжения ошибки.



# Заключение

Представленная система кодирования речи для бытовых радиотелефонов не претендует на какую-то особую оригинальность. Здесь использовались идеи, которые появились еще в 50-е годы с работами К. Шеннона, развившего идею А.В.Котельникова о том, что потенциальная помехоустойчивость системы связи при действии гауссовых помех инвариантна по отношению к ширине полосы частот. Долгое время (до 80-х годов) эти идеи не находили применения из-за несовершенства технической базы, прежде всего регистров и микропроцессоров. Сейчас многие новые разработки в области связи используют эти идеи из-за их очевидных преимуществ: простоты реализации, низкой стоимости и хорошей устойчивости таких кодов к помехам. Можно привести пример одной из первых систем, использовавшей шумоподобные сигналы - это система “RAKE”. После нее началось широкое применение шумоподобных сигналов в наземной и космической связи.

Применение помехоустойчивого и в то же время защищенного (в достаточной степени) от несанкционированного прослушивания кодирования, на взгляд автора этих строк, очень хороший вариант для бытовых применений.