Обзор современных устройств скремлирования

**Аналоговые скремблеры:**

* речевые скремблеры простейших типов на базе временных и/или частотных перестановок отрезков речи,
* комбинированные речевые скремблеры на основе частотно-временных перестановок отрезков речи, представленные конкретнымн отсчетами, с применением цифровой обработки сигналов(В).

**Цифровые системы сокрытия речи:**

* широкополосные (С)
* узкополосные (D)

Системы типа С и D (см. рис. 3) не передают какой-либо части исходного речевого сигнала. Речевые компоненты кодируются в цифровой поток данных, который смешивается с псевдослучайной последовательностью, вырабатываемой ключевым генератором по одному из криптографических алгоритмов, и полученное таким образом закрытое речевое сообщение передается при помощи модема в канал связи, на приемном конце которого производятся обратные преобразования с целью получения открытого речевого сигнала.  
Технология изготовления широкополосных систем закрытия речи типа С хорошо известна, не представляет особых трудностей техническая реализация используемых для этих целей способов кодирования речи типа АДИКМ (адаптивной дифференциальной импульсно-кодовой модуляции), ДМ (дельта-модуляции) и т.п.

Но представленная такими способами дискретизированная речь может передаваться лишь по специально выделенным широкополосным каналам связи с полосой пропускания, обычно лежащей в диапазоне 4.8-19.2 кГц, и не пригодна для передачи по линиям телефонной сети общего пользования, где требуемая скорость передачи данных должна составлять 2400 бит/с. В таких случаях используются узкополосные системы закрытия типа D (см. рис. 3), главной трудностью при реализации которых является высокая сложность алгоритмов сжатия речевых сигналов, осуществляемых в вокодерных устройствах.

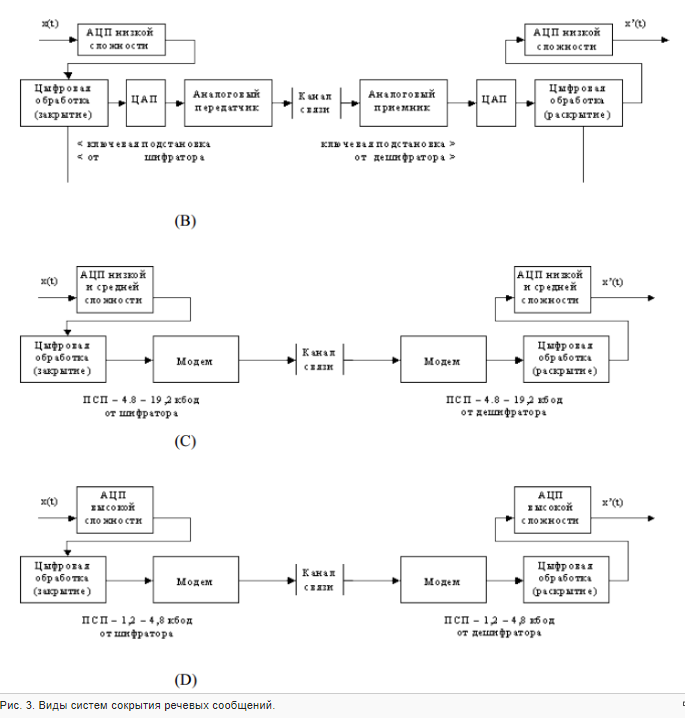
Посредством дискретного кодирования речи с последующим шифрованием всегда достигалась высокая степень закрытия, но в прошлом этот метод не находил широкого распространения в повсеместно имеющихся узкополосных каналах связи из-за низкого качества восстановления передаваемой речи.

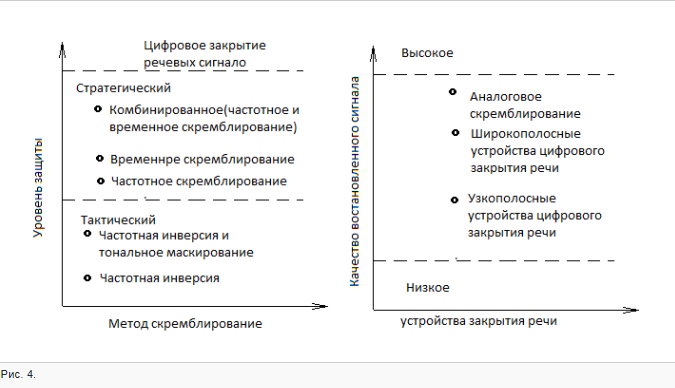
Последние достижения в развитии низкоскоростных дискретных кодеров позволили значительно улучшить качество речи без снижения надежности закрытия.

Говоря об уровне, или степени секретности систем закрытия речи, следует отметим, что эти понятия весьма условные. К настоящему времени не выработано на этот счет четких стандартов или правил. Однако в ряде источников основные уровни защиты определяют как тактический и стратегический, что в некотором смысле пересекается с понятиями практической и теоретической стойкости криптографических систем закрытия данных:

* тактический, или низкий, уровень используется для защиты информации от подслушивания посторонними лицами на период времени, измеряемый минутами или днями. Существует большое количество простых методов, способных обеспечить такой уровень защиты при приемлемой стоимости;
* стратегический, или высокий, уровень защиты информации от перехвата используется в ситуациях, подразумевающих, что высоко квалифицированному, технически хорошо оснащенному специалисту потребуется для дешифрования перехваченного сообщения период времени от нескольких месяцев до многих и многих лет.

Часто используется и понятие средней степени защиты, занимающее промежуточное положение между тактическим и стратегическим уровнем закрытия. Можно составить диаграмму (рис. 4), показывающую связь между различными методами закрытия речевых сигналов, степенью секретности и качеством восстановленной речи. Понятие "качество речи", используемое на диаграмме, весьма условно. Под ним, как правило, понимают узнаваемость абонента и разборчивость принимаемого речевого сигнала.





**Аналоговое скремблировани**

Наибольшая часть аппаратуры засекречивания речевых сигналов использует в настоящее время метод аналогового скремблирования, поскольку, во-первых, это дешевле, во-вторых, эта аппаратура применяется в большинстве случаев в стандартных телефонных каналах с полосой 3 кГц, в-третьих, обеспечивается коммерческое качество дешифрованной речи и, в-четвертых, гарантируется достаточно высокая стойкость закрытия, Аналоговые скремблеры преобразуют исходный речевой сигнал посредством изменения его амплитудных, частотных и временных параметров в различны комбинациях. Скремблированный сигнал может затем быть передан по каналу связи в той же полосе частот, как и исходный, открытый. В аппаратах такого типа используется один или несколько принципов аналогового скремблирования из числа указанных ранее.

а)Скремблирование в частотной области:

* частотная инверсия (преобразование спектра сигнала с помощью гетеродина и фильтра),
* частотная инверсия и смещение (частотная инверсия с меняющимся скачкообразно смещением несущей частоты), разделение полосы частот речевого сигнала на ряд поддиапазонов с последующей их перестановкой и инверсией.

в)Скремблирование во временной области (разбиение блоков или частей речи на сегменты с перемешиванием их во времени с последующим прямым и/или реверсивным считыванием);

с )Комбинация временного и частотного скремблирования.

Как правило, все перестановки каким-либо образом выделенных сегментов или участков речи во временной и/или в частотной областях осуществляются по закону псевдослучайной последовательности, вырабатываемой шифратором по ключу, меняющемуся от одного сообщения к другому. На стороне приемника выполняется дешифрование цифровых кодов, полученных из канала связи, и преобразование в аналоговую форму. Системы, работа которых основана на таком методе, являются достаточно сложными, поскольку для обеспечения высокого качества передаваемой речи требуется высокая частота дискретизации входного аналогового сигнала и соответственно высокая скорость передачи данных но каналу связи. Каналы связи, которые обеспечивают скорость передачи данных только 2400 бод, называются узкополосными, в то время, как другие, обеспечивающие скорость передачи свыше 2400 бод, относятся к широкополосным. По этому же принципу можно разделять и устройства дискретизации речи с последующим шифрованием. Несмотря на всю свою сложность, аппаратура данного типа представлена на коммерческом рынке рядом моделей, большинство из которых передает данные по каналу связи со скоростями модуляции от 2.4 до 19.2 кбит/с, обеспечивая при этом несколько худшее качество воспроизведения речи по сравнению с обычным телефоном. Основным же преимуществом таких цифровых систем кодирования и шифрования остается высокая степень закрытия речи, получаемая посредством использования широкого набора криптографических методов, применяемых для защиты передачи данных по каналам связи.

Аналоговые скремблеры, по их режиму работы, можно разбить на два следующих класса:

* статические системы, схема кодирования которых остается неизменной в течение всей передачи речевого сообщения;
* динамические системы, постоянно генерирующие кодовые подстановки в ходе передачи (код может быть изменен в процессе передачи несколько раз в течение каждой секунды).

Очевидно, что динамические системы обеспечивают более высокую степень защиты, поскольку резко ограничивают возможность легкого прослушивания переговоров посторонними лицами.  
Процесс аналогового скремблирования представляет собой сложное преобразование речевого сигнала с его последующим восстановлением (с сохранением разборчивости речи) после прохождения преобразованного сигнала по узкополосному каналу связи, подверженному воздействию шумов. Возможно преобразование речевого сигнала по трем параметрам: амплитуде, частоте и времени. Считается, что использовать амплитуду нецелесообразно, так как изменяющиеся во времени затухание канала и отношение сигнал/шум делают чрезвычайно сложным точное восстановление амплитуды переданного сигнала. Практическое применение получило только частотное и временное скремблирование и их комбинации. Как вторичные ступени скремблирования в этих системах могут использоваться ограниченные виды амплитудного скремблирования.

#### Частотные скремблеры

Как уже отмечалось выше, существует два основных вида частотных скремблеров инверсный и полосовой. Оба основаны на преобразованиях спектра исходного речевого сигнала для скрытия передаваемой информации и восстановлении полученного речевого сообщения путем обратных преобразований. Инверсный скремблер осуществляет преобразование речевого спектра, равносильное повороту частотной полосы речевого сигнала вокруг некоторой средней точки. При этом достигается эффект преобразования низких частот в высокие частоты, и наоборот.

Данный способ обеспечивает невысокий уровень закрытия, так как при перехвате легко устанавливается величина частоты, соответствующая средней точке инверсии в полосе спектра речевого сигнала. Некоторое повышение уровня закрытия обеспечивает полосносдвиговый инвертор, осуществляющий разделение полосы на две субполосы, при этом точка разбиения выступает в роли некоторого ключа системы. В дальнейшем каждая субполоса инвертируется вокруг своей средней частоты. Этот вид скремблирования, однако, также слишком прост для вскрытия при перехвате и не обеспечивает надежного закрытия. Повысить уровень закрытия можно путем изменения по некоторому закону частоты, соответствующей точке разбиения полосы речевого сигнала (ключа системы).

#### Временные скремблеры

Временные скремблеры основаны на двух основных способах закрытия: инверсии по времени сегментов речи и их временной перестановке. По сравнению с частотными скремблерами задержка у временных скремблеров намного больше, но существуют различные методы ее уменьшения. В скремблерах с временной инверсией речевой сигнал делится на последовательность временных сегментов и каждый из них передается инверсно во времени - с конца. Такие скремблеры обеспечивают ограниченный уровень закрытия, зависящий от длительности сегментов. Для достижения неразборчивости медленной речи необходимо, чтобы длина сегмента составляла около 250 мс. Это означает, что задержка системы будет равна примерно 500 мс, что может оказаться неприемлемым для некоторых приложений.  
Для повышения уровня закрытия прибегают к способу перестановки временных от- резков речевого сигнала в пределах фиксированного кадра. Правило перестановок является ключом системы, изменением которого можно существенно повысить степень закрытия речи. Остаточная разборчивость зависит от длительностей отрезков сигнала и кадра и с увеличением последнего уменьшается.

Главным недостатком скремблера с фиксированным кадром является большая величина времени задержки системы, равная удвоенной длительности кадра. Этот недостаток устраняется в скремблере с перестановкой временных отрезков речевого сигнала со скользящим окном. В нем число комбинаций возможных перестановок ограничено таким образом, что задержка любого отрезка не превосходит установленного максимального значения. Каждый отрезок исходного речевого сигнала как бы имеет временное окно, внутри которого он может занимать произвольное место при скремблировании. Это окно скользит во времени по мере поступления в него каждого нового отрезка сигнала. Задержка при этом снижается до длительности окна.

### Комбинированное скремблировани

Используя комбинацию временного и частотного скремблирования, можно значитель- но повысить степень закрытия речи. Комбинированный скремблер намного сложнее обычного и требует компромиссного решения по выбору уровня закрытия, остаточной разборчивости, времени задержки, сложности системы и степени искажений в восстанов- ленном сигнале. Количество же всевозможных систем, работающих по такому принципу, ограничено лишь человеческим воображением

### Дискретизация сигнала с последующим шифрованием (цифровое скремблирование)

Альтернативным аналоговому скремблированию методом передачи речи в закрытом виде является шифрование речевых сигналов, преобразованных в цифровую форму, перед их передачей. Этот метод обеспечивает более высокий уровень закрытия по сравнению с описанными выше аналоговыми методами.

В основе устройств работающих по такому принципу, лежит представление речевого сигнала в виде цифровой последовательности, закрываемой по одному из криптографических алгоритмов. Передача данных, представляющих дискретизированные отсчеты речевого сигнала или его параметры, по телефонным сетям, как и в случае29 устройств шифрования алфавитно-цифровой и графической информации, осуществляется через устройства, называемые модемами.  
Основной целью при разработке устройств цифрового закрытия речи является сохранение тех ее характеристик, которые наиболее важны для восприятия слушателем. Одним из путей является сохранение формы речевого сигнала. Это направление применяется в широкополосных цифровых системах закрытия речи. Однако использование свойств избыточности информации, содержащейся в человеческой речи, более эффективно. Это направление разрабатывается в узкополосных цифровых системах закрытия речи.

Ширину спектра речевого сигнала можно считать приблизительно равной 3,3 кГц, а для достижения хорошего качества восприятия необходимое соотношение сигнал/шум должно составлять 30 дБ. Тогда, согласно теории Шеннона, требуемая скорость передачи дискретизированной речи будет соответствовать величине 33 кбит/с.

С другой стороны, структура речевого сигнала представляет собой последовательность звуков (фонем), передающих информацию. Поскольку в английском языке около 40 фонем, а в немецком – 70, то для представления фонетического алфавита потребуется 6-7 бит. Максимальная скорость произношения не превышает 10 фонем в секунду. Следовательно, минимальная скорость передачи основной технической информации речи не ниже 60-70 бит/с.

Основной особенностью использования систем цифрового закрытия речевых сигналов является необходимость использования модемов. В принципе возможны следующие подходы при проектировании систем цифрового закрытия речевых сигналов:

1)цифровая последовательность параметров речи с выхода вокодерного устройства подается на вход шифратора, где подвергается преобразованию по одному из криптог- рафических алгоритмов, затем поступает через модем в канал связи, на приемной стороне которого осуществляются обратные операции по восстановлению речевого сигнала, в которых задействованы модем и дешифратор (см. рис.1.D). Шифрующие/дешифрующие функции обеспечиваются либо в отдельных устройствах, либо в программно-аппаратной реализации самого вокодера;  
2) шифрующие/дешифрующие функции обеспечиваются самим модемом (так называемый засекречивающий модем) обычно по известным криптографическим алгоритмам типа DES и другим. Цифровой поток, несущий информацию о параметрах речи, с выхода вокодера непосредственно поступает на такой модем. Организация связи по каналу аналогична вышеприведенной.