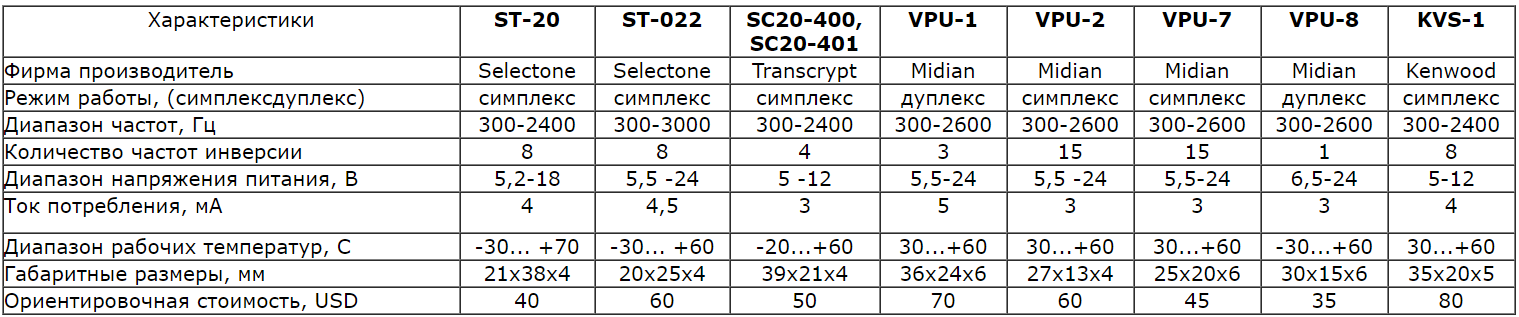
Существуют два основных метода закрытия речевых сигналов: аналоговое скремблирование и дискретизация речи с последующим шифрованием. Аналоговые скремблеры преобразуют исходный речевой сигнал (без перевода его в цифровую форму) таким образом, чтобы при прослушивании канала с помощью радиостанции, не оснащенной подобным устройством, были созданы существенные затруднения для разборчивости передаваемой информации. При этом при скремблировании преобразованный речевой сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный сигнал. В цифровых устройствах защиты информации (УЗИ) речевые компоненты преобразуются в цифровой поток данных и смешиваются с некоторой псевдослучайной последовательностью, вырабатываемой ключевым генератором. Полученное таким образом закрытое речевое сообщение передается в канал связи, на приемном конце которого производятся обратные преобразования с целью получения открытого речевого сигнала.  
  
 Основными техническими характеристиками скремблеров, которые необходимо оценивать при выборе конкретного типа устройства защиты информации, являются уровень закрытия информации, остаточная разборчивость, качество восстановления сигнала, влияние на параметры радиостанций, уровень технического исполнения (габариты, потребление, возможность установки в различные типы станций и т.п.).  
  
 Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является уровень закрытия информации. Следует отметить, что данное понятие носит условный характер, т.к. к настоящему времени на этот счет не выработано четких стандартов или правил. Вместе с тем, условно можно разделить все УЗИ на средства защиты информации от непреднамеренного перехвата (т.е. от прослушивания лицами, не использующими специальные средства перехвата чужих переговоров) и средства защиты информации от несанкционированного доступа (т.е. от прослушивания возможными конкурентами, целью которых является именно перехват чужих переговоров, и оснащенных для этого специальными техническими средствами). Естественно, что средства защиты информации от несанкционированного доступа, в свою очередь, можно разделить на несколько уровней, обеспечивающих различный уровень закрытия переговоров в зависимости от степени оснащенности конкурента. В литературе часто встречается классификация УЗИ по времени дешифрования информации после ее записи. Однако такая классификация больше применима для сложных криптографических систем военного назначения, а не для сетей УКВ радиосвязи, где ценность передаваемой информации не так велика, и опасность представляет, как правило, только перехват переговоров в реальном масштабе времени. Поэтому в качестве критерия уровня закрытия информации для средств УКВ радиосвязи более целесообразно использовать стоимость технических средств, обеспечивающих перехват сообщений в реальном масштабе времени.  
  
 Под остаточной разборчивостью понимают степень возможности восстановления речевого сообщения при прослушивании его с помощью технических средств, не оснащенных данным типом УЗИ. В какой-то мере остаточная разборчивость является составной частью характеристики уровня закрытия информации, однако, остаточная разборчивость характеризует степень неразборчивости сообщений при их прослушивании без применения специальных средств, а уровень закрытия информации показывает защищенность переговоров и при преднамеренном перехвате с использованием специальной аппаратуры. Количественно остаточная разборчивость может быть оценена процентом восстановленных фрагментов сообщения при прослушивании переговоров с помощью радиосредств, не оснащенных данным типом УЗИ. (Часто требования к остаточной разборчивости задаются как максимально допустимый класс разборчивости речи по ГОСТ 16600-72.) Естественно, что наибольшую степень защиты информации обеспечивают скремблеры с минимальной остаточной разборчивостью. Следует, однако, отметить, что практически все известные аналоговые речевые скремблеры в той или иной мере сохраняют остаточную разборчивость. В прослушиваемом речевом сигнале, защищенном скремблером, сохраняется информация о темпе речи, улавливаются паузы. При несложных способах защиты опытный оператор может разобрать (в зависимости от наличия сведений о тематике ведущихся переговоров) от 10 до 50 % передаваемой информации.  
  
 Качество восстановления сигнала является важнейшей эксплуатационной характеристикой скремблеров. Оно определяется искажениями сигнала при его частотных или временных преобразованиях. Может быть выражено разборчивостью (не путать с остаточной разборчивостью!) и узнаваемостью восстановленной речи. Приемлемым или коммерческим качеством восстановленной на приемном конце речи считается такое, когда слушатель без усилий может определить голос говорящего и смысл произносимого сообщения. Точную количественную оценку разборчивости речи можно получить путем измерения процента правильно переданных тестовых сообщений при проведении длительных и трудоемких артикуляционных испытаний.  
  
 Влияние скремблеров на параметры радиостанций проявляется, прежде всего, в ухудшении их чувствительности за счет уменьшения соотношения сигнал/шум на входе приемника. Кроме этого, при преобразованиях сигнала, связанных с изменением любых параметров преобразования во времени, требуется некоторый временной интервал для синхронизации таймерных устройств передающей и приемной стороны. Это заставляет оператора выдерживать паузу между нажатием тангенты “передача” на радиостанции и началом речи.  
  
 Как правило, уменьшение остаточной разборчивости сопровождается ухудшением, как качества восстановления сигнала, так и параметров радиостанций. Это объясняется тем, что, желая увеличить степень защиты информации, разработчики идут на различные ухищрения, приводящие к дополнительным искажениям либо спектра, либо временных параметров сигнала.  
  
 Для пользователей средств УКВ радиосвязи крайне важен уровень технического исполнения скремблеров. Т.к. конструктивно скремблеры представляют собой малогабаритные микроэлектронные узлы, которые устанавливаются внутрь корпуса радиостанции, предпочтителен выбор аналоговых УЗИ с минимальными габаритами и энергопотреблением. Естественно, что минимизация габаритов позволяет расширить применимость скремблеров, т.к. обеспечивается возможность их установки в большее количество радиосредств.  
  
 Большинство структур безопасности оснащено профессиональными средствами УКВ радиосвязи зарубежных фирм таких, как Motorola, Kenwood, Yaesu, Standard, Alinco, Icom и др., использующими аналоговые виды модуляции сигнала (частотный или фазовый). Для подобного рода радиосредств в подавляющем большинстве в качестве устройств защиты информации применяются аналоговые речевые скремблеры.

Наибольшее количество известных моделей скремблеров реализуют частотную инверсию сигнала. Все они имеют близкие параметры. Одними из первых на отечественном рынке появились модели скремблеров фирмы Selectone (ST-20 и ST-022), работающие в диапазоне частот 300-2400 Гц и обеспечивающие инверсию сигнала относительно 8 возможных номиналов частот в диапазоне от 2,6 до 3,7 КГц (частота инверсии устанавливается программно).

Простейшие модели скремблеров фирмы Transcrypt SC20-400 и SC20-401 обладают характеристиками, аналогичными ST-20 и ST-022; речевой диапазон частот, 4 варианта частоты инверсии.

Сравнительная характеристика скремблеров по основным параметрам приведена в табл.

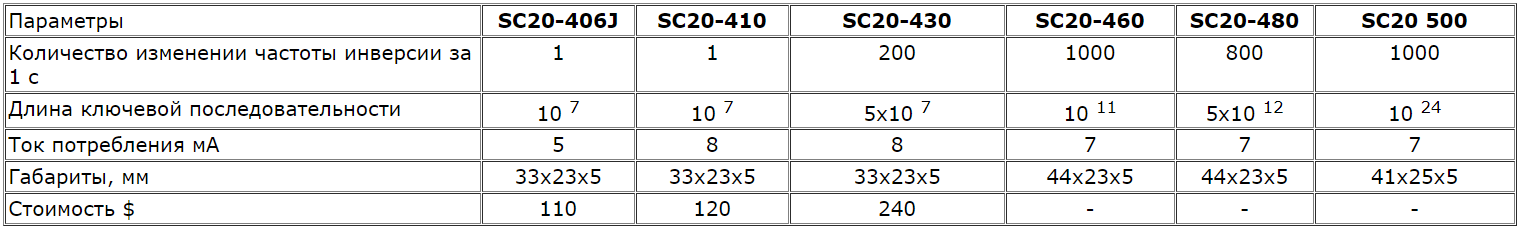
Более сложное преобразование сигнала предлагают полосно- сдвиговые инверторы, разработанные НТЦ "ИНТЕР-ВОК" Принцип работы микросборок 04ХК011 ("Сонет"), 04ХК012, 04ХК014А, 04ХК015А, 04ХК017А состоит в разделении речевого спектра на две части, низкочастотную и высокочастотную, каждая из которых разворачивается вокруг своих средних частот. Все они работают в диапазоне речевых частот - 300-3400 Гц. Указанные скремблеры обладают повышенной по сравнению с частотными инверторами степенью закрытия информации. В технических данных указывается, что скремблеры обеспечивают остаточную разборчивость речи не более 10%. В то же время гарантируется сохранение высокого качества речи при прослушивании с помощью радиостанции, оснащенной аналогичным скремблером.



Большая номенклатура динамических скремблеров выпускается фирмой Tramscrypt. Принцип их работы аналогичен частотным инверторам с изменением частоты инверсии сигнала во времени Число возможных частот инверсии - 16. Различные модели скремблеров этой фирмы отличаются скоростью изменения переменного параметра: от 1 раза в секунду для SC20-406J и SC20-410 до 1000 раз в секунду для SC20-460 и SC20-500. Параметры скремблеров представлены в таблице.

Несмотря на большую длину ключевой последовательности (псевдослучайной последовательности изменения частоты разбиения полосы сигнала), числовое значение переменного параметра невелико (16) и не обеспечивает надежного закрытия. Как показали исследования радиосредств, оснащенных скремблерами, модели SC20-410 при прослушивании переговоров с помощью радиостанции с установленным частотным инвертором с фиксированной частотой инверсии сигнала можно разобрать от 50 до 80 % передаваемой информации.

Принцип работы скремблеров требует синхронизации передающих и приемных радиосредств, что требует от оператора делать паузу после нажатия тангенты "передача" на радиостанции. Для модулей фирмы Transcrypt время синхронизации составляет 300 500 мс.

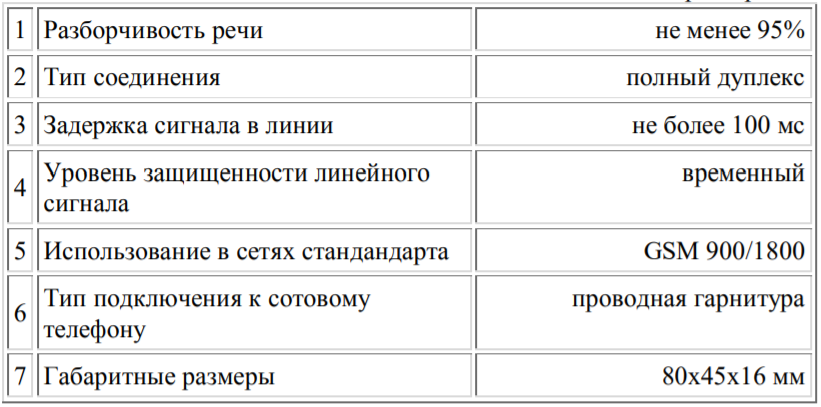


Временные преобразования осуществляет скремблер, разработанный НИИ микроэлектронной аппаратуры (НИИМА) "Прогресс". Он выполнен в виде бескорпусного микромодуля на керамической подложке с использованием специализированных БИС дельта-кодера и дельта-декодера, устройства шифрования и памяти. Речевой сигнал, поступающий на вход, преобразуется кодером адаптивного дельта-кодека в цифровую форму и записывается в память в виде последовательности речевых сегментов. Из 32 сегментов образуется кадр. В соответствии с записанным кодом устройство шифрования создает псевдослучайную последовательность перестановок этих сегментов в кадре. После временных преобразований декодер адаптивного дельта кодека восстанавливает на выходе скремблера исходный речевой сигнал внутри каждого сегмента. В режиме приема по синхросигналу производятся кадровая синхронизация и обратные преобразования для восстановления исходного сигнала.

Использование специализированных БИС позволяет при энергопотреблении 75 мВт обеспечить удовлетворительное качество восстановления речевого сигнала и малую (3-5 %) остаточную разборчивость

Как видно из приведенного обзора, пользователи средств УКВ радиосвязи имеют широкий выбор средств защиты информации для своих радиостанций и локальных сетей радиосвязи. Кроме этого, как видно из обзора представленных моделей, следует учитывать, что аналоговые скремблеры никогда не обеспечат защиту от преднамеренного прослушивания ваших переговоров. Для надежной защиты передаваемой информации необходимо использовать радиостанции с передачей сигнала в цифровой форме с определенным алгоритмом маскировки. Такую защиту может обеспечить применение существенно более дорогих цифровых радиостанций.

Известны скремблеры для эффективной защиты телефонных переговоров в сетях, работающих по GSM стандарту. Специально разработанный скремблер GUARD GSM, будучи эконом-вариантом, отлично маскирует речь, передаваемую по каналам GSM связи. Данное устройство соединяется с сотовым телефоном по проводной гарнитуре и имеет небольшие размеры. Скремблер GUARD GSM имеет тридцать два режима скремблирования, основные характеристики приведены в табл.



Принцип работы данного скремблера основан на первоначальном разрушении и временной перестановки звука на передающей стороне с его последующим восстановлением на принимающей стороне. Этот процесс дуплексный. Начало разговора, как правило, начинается в открытом режиме и далее по обоюдной команде устройства, переключаются в режим скремблирования.

Как видно из обзора представленных моделей, следует учитывать, что аналоговые скремблеры никогда не обеспечат защиту от преднамеренного прослушивания ваших переговоров. При этом финансовые затраты лиц, планирующих перехват ваших переговоров, не будут являться для них препятствием. Для надежной защиты передаваемой информации необходимо использовать радиостанции с передачей сигнала в цифровой форме с определенным алгоритмом маскировки. Такую защиту может обеспечить применение существенно более дорогих цифровых радиостанций или использование цифровых УЗИ для аналоговых радиосредств, разработки которых проводятся рядом организаций.