# Современные устройства скремблирования

Среди различных систем передачи речи особое место занимают узкополосные системы связи. За счет узкой полосы каждого канала в отдельности (3,1–4 кГц) достигается рациональное использование радиочастотного ресурса. Данные системы характеризуются низкими требованиями к стабильности характеристик канала связи и малой стоимостью оборудования. Примерами узкополосных систем связи являются проводные телефонные линии общего и специального назначения, системы специальной, оперативно-технологической и любительской радиосвязи вплоть до диапазона ОВЧ (VHF). В подобных системах наряду с требованиями надежности и оперативности, важны также вопросы обеспечения безопасности передаваемой информации. Устройства скремблирования по-прежнему остаются основным средством обеспечения безопасности в таких системах из-за их узкой полосы и низкого рабочего соотношения сигнал/шум. Согласно выделяют следующие основные принципы скремблирования: скремблирование в частотной области, скремблирование во временной области, а также двухмерное или комбинированное скремблирование, реализующее одновременно два приведенных выше преобразования речевого сигнала. Для передачи информации по каналу связи в масштабе реального времени,скремблирование в частотной области является более предпочтительным, чем во временной. Это обусловлено тем, что полосовые скремблеры более устойчивы к неравномерности амплитудно-частотной характеристики канала, что позволяет получить минимальные искажения сигнала при дескремблировании. В то же время основным недостатком полосовых скремблеров является то, что скремблированный сигнал характеризуется присущим речи ритмом и сравнительно высоким уровнем остаточной разборчивости.Как правило, основуполосовых скремблеров составляет банк частотно-избирательных фильтров, реализованных в аналоговом, либо в цифровом виде. Реализация банка фильтров в цифровом виде и применение алгоритма быстрого преобразования Фурье (БПФ) позволяет значительно увеличить количество полос, на которые разбивается спектр исходного сигнала. За счет этого возрастает количество возможных вариантов перестановок полос, приводящее к повышению степени закрытия речи. Однако при использовании алгоритма, работающего по принципу поблочного накопления и обработки отсчетов, для корректного дескремблирования речевой информации необходимо обеспечение синхронизации между скремблером и дескремблером. Отсутствие синхронизации приводит к появлению в дескремблированном сигнале «щелчков», следующих с периодом, равным длительности окна БПФ.

## FSM-U1



Принцип скремблирования

Динамическое формирование ключа (новый ключ на каждый сеанс)

Принцип кодирования – многократная динамическая обработка фазы

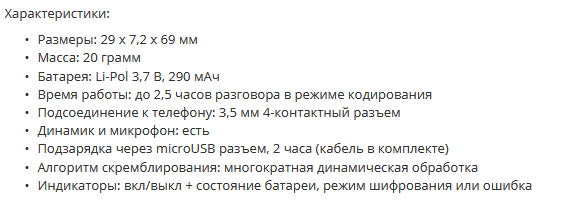
Двухэтапное преобразование речевого потока

Динамическое деление на интервалы. В то время, как у «классического» скремблера интервал статический, FSM-U1 делит речевой поток на участки переменной длины. Первичная разбивка создает от 20 до 50 интервалов с секунду, затем каждый интервал разбивается на изменяющееся количество участков различной длины. Общее количество комбинаций первой стадии обработки ― 1015

Изменение фазы каждого динамического участка в пределах от 0 до 180° (количество комбинаций ― 180)

Общее количество комбинаций алгоритма ― 103,4\*1015

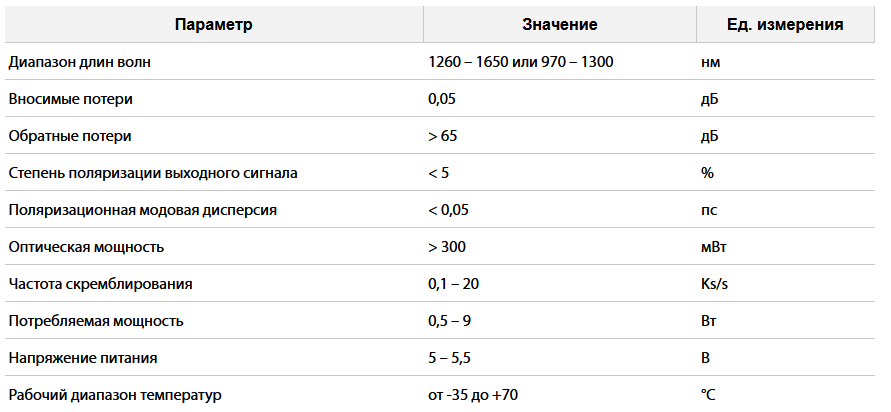
Генерация и обмен ключами на основе технологии Voiceprint



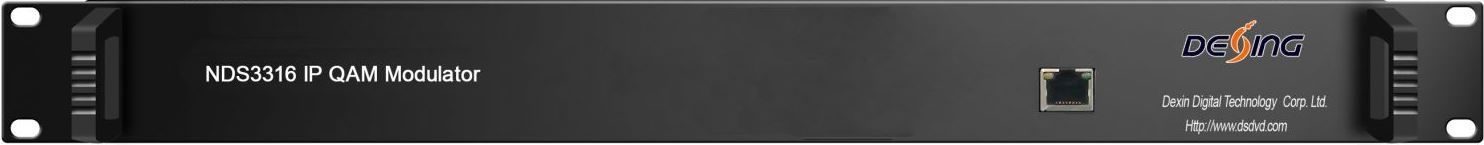
## PSM-002

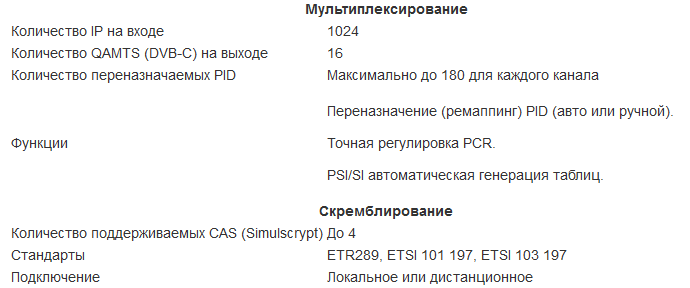


Поляризационный скремблер PSM-002 специально разработан для применения в сенсорных системах и системах связи и телекоммуникаций, что предусматривает использование в экстремальных условиях окружающей среды. Скорость скремблирования регулируется пользователем по средствам интерфейса RS-232. Функция скремблирования может быть отключена по команде. Модуль может быть реализован как для лабораторного, так и для наружного применения, со стандартным и расширенным температурным диапазоном.



## NDS3316 16xIP-QAM



P-QAM модулятор со встроенным мультиплексором и скремблером. Устройство является оборудованием последнего поколения, спроектированное и произведенное по принципу «all-in-one» (все-в-одном). На входе (2xGbE SFP) устройство принимает до 1024 IP TS, ремультиплексирует и мультиплексирует контент, на выходе QAM-модулятор выдает до 16 несмежных DVB-C в диапазоне 50-960 MHz, которые могут быть закрыты simulscrypt CAS. Соотношение цена/качество позволяет использовать данное оборудование как в крупных кабельных сетях, так в относительно небольших региональных сетях.

Выбор методов закрытия зависит от вида конкретного применения и технических характеристик канала передачи. Как отмечалось во введении, в речевых системах связи известны два основных метода закрытия речевых сигналов, разделяющихся по способу передачи по каналам связи: аналоговое скремблирование и дискретизация речи с последующим шифрованием (цифровое скремблирование). Под скремблированием понимают изменение характеристик речевого сигнала таким образом, чтобы полученный сигнал, становился неразборчивым и неузнаваемым, занимая ту же полосу спектра, что и исходный.

При использовании скремблера обеспечивается защита переговоров от любых средств съема информации.

Каждый из этих двух методов имеет свои достоинства и недостатки. Так, например, в первых двух системах, представленных на рис. 3, в канале связи при передаче присутствуют кусочки исходного, открытого речевого сообщения, преобразованные в частотной и/или временной областях. Это означает, что эти системы, могут быть атакованы криптоаналитиком противника на уровне анализа звуковых сигналов. Поэтому ранее считалось, что наряду с высоким качеством и разборчивостью восстановленной речи аналоговые скремблеры могут обеспечить лишь низкую или среднюю, по сравнению с системами цифрового кодирования и шифрования, степень закрытия (секретности). Однако новейшие (разработанные в последние годы) алгоритмы способны обеспечить не только средний, но иногда и очень высокий уровень секретности в системах типа В.