**Обзор современный устройств скремблирования**

Скремблирование — обратимое преобразование цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности.

Защита телефонных переговоров

Скремблеры активно применяются для защиты телефонных переговоров. При скремблировании возможно преобразование речевого сигнала по трём параметрам: амплитуде, частоте и времени. Однако в системах подвижной радиосвязи практическое применение нашли в основном частотные и временные преобразования сигнала, а также их комбинации. Возможные помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, в связи с чем амплитудные преобразования при скремблировании практически не применяются.

Основные методы преобразования речевого сигнала:

* Частотные преобразования
* Частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра)
* Разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра в каждом относительно средней частоты поддиапазоне
* Разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки
* Временные преобразования
* Инверсия по времени сегментов речи
* Временные перестановки сегментов речевого сигнала
* Комбинированные методы

Мобильный Скремблер Avantalk

Мобильный скремблер Avantalk обеспечивает защиту информации, передаваемой мобильным телефоном. Нужно учитывать, чтобы у абонента на другой стороне был аналогичный прибор. Коды шифрования информации у обоих приборов должны совпадать.

Технические характеристики:

1. Максимальная дальность связи между блоком MS и телефоном до 3 метров

2. Минимальное расстояние между блоком MS и мобильным телефоном от 0,5 метра

3. Максимальное время заряда LI-ION аккумулятора…………………………до 10 часов 4. Время работы блока MS с полностью заряженным аккумулятором…… до 8 часов

Скремблер Avantalk реализован в виде Bluetooth-гарнитуры и подключается к соответствующему смартфону посредством Bluetooth. При подключенном скремблере разговор ведется через встроенный микрофон. Когда вы дозвонились Вашему собеседнику, один из вас включает режим кодирования. В течение нескольких секунд Ваши устройства будут обмениваться первичными данными и устанавливать связь. После установки связи загорится соответствующий светодиод, подтверждающий вхождение в «защищенные режим». Голос собеседника в режиме скремблирования несколько искажается.

Скремблер для защиты от прослушки мобильного телефона и смартфона FSM-U1

FSM-U1 — новое устройство кодирования разговоров для мобильного телефона-смартфона. В скремблере реализован новый мощный алгоритм «закрытия» разговора с помощью технологии «многократной динамической обработки фазы».

Скремблер реализован в виде гарнитуры и подключается к соответствующему разъему смартфона. При подключенном скремблере разговор ведется через него. FSM-U1 имеет встроенный динамик и микрофон.

Устройство питается от встроенного Li-Pol аккумулятора 3.7В емкостью 290 мАч. Ресурс аккумулятора – до 2.5 часов разговора в режиме скремблирования. Время перезаряда – 2 часа, от USB.

Методика применения:

При выключенном скремблировании FSM-U1 может работать как гарнитура. Когда вы дозвонились Вашему собеседнику, один из вас включает режим кодирования. В течение нескольких секунд Ваши устройства будут обмениваться первичными данными и устанавливать связь. После установки связи Вы услышите звуковой сигнал, подтверждающий вхождение в «защищенные режим». Загорится соответствующий светодиод. Простое отсоединение гарнитуры при включенном скремблировании позволяет оценить степень защищенности звукового потока.

Принцип скремблирования:

- Общее количество комбинаций алгоритма — 103,4⋅1015

- Динамическое формирование ключа (новый ключ на каждый сеанс)

- Принцип кодирования – многократная динамическая обработка фазы

- Двухэтапное преобразование речевого потока:

1. 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

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

- Генерация и обмен ключами на основе технологии Voiceprint

Скремблер «Guard Bluetooth» с 4-мя режимами шифрования и беспроводным подключением

Беспроводной скремблер «Guard Bluetooth» предназначен для защиты переговоров во время разговора по сотовому телефону. Подключение скремблера к телефону происходит по радиоканалу через «bluetooth». При работе скремблер изменяет выходящий звуковой сигнал по принципу частотной инверсии. Закодированный сигнал передаётся на мобильный телефон, и потом по сотовой связи к вашему собеседнику. Для декодирования сигнала собеседнику необходимо иметь аналогичный прибор. При перехвате сигнала третьими лицами его будет практически невозможно разобрать, либо дешифровать. Разборчивость перехваченного сигнала может максимально составлять 5%.

Особенности Разборчивость скремблированной речи не более 3-5% слов. Это означает что при прослушивании зашифрованной речи при несанкционированном перехвате беседы во время переговоров, вероятность разобрать суть беседы возможно максимум на 3-5%.

4 режима шифрования на выбор. Скремблер «Guard Bluetooth» имеет 4 программных режимов работы. Во время переговоров по сотовому телефону, собеседники могут переключаться с режима на режим, тем самым наиболее эффективно защищая себя от прослушивания третьими лицами.

«Bluetooth» соединение телефона со скремблером. Беспроводная связь устройства с мобильным телефоном более комфортна для использования устройства защиты разговора через сотовый телефон.

В кодировании скремблера используется частотная инверсия. При скремблировании во время переговоров, происходит частотный сдвиг на 6 децибел в различных направлениях, чем достигается зашифрованность речи собеседников.

Технические характеристики

Принцип кодирования: инверсия звукового спектра;

Беспроводное соединение: Bluetooth;

Формирование ключа: статическое;

Общее количество комбинаций алгоритма: 4 комбинации;

Количество изменений частоты инверсии: 4 частоты;

Длина ключевой последовательности: 16 бит; Канал связи: полный дуплекс; Разборчивость дескремблированной речи: 95%;

Полоса звуковой инверсии: с 280 Hz до 3140Hz;

Наклон предискажений во время скремблирования звукового потока 6dB на октаву;

Диапазон частот инверсии: с 44.336kHz до 184.734kHz;

Выходной импеданс: с 300 по 500 кОм;

Питание: 9В (крона);

Ток потребления мА: 70 мА; Индикация: светодиодная;