**Обзор современных устройств скремлирования**

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.

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.

**Скремблер для смартфона FSM-U1**

|  |  |
| --- | --- |
| Размеры | 29×7,2×69 мм |
| Масса | 20 г |
| Батарея | Li-Pol 3,7 В, 290 мАч |
| Время работы | 2,5 ч. разговора |
| Подсоединение к телефону | 3,5 мм 4-контактный разъем |
| Динамик и микрофон | да |
| Подзарядка | microUSB разъем, около 2 ч. |
| Алгоритм скремблирования | неоднократная динамическая обработка фазы |
| Индикаторы | вкл/выкл + состояние батареи, режим шифрования или ошибка |

**Мобильный скремблер MS** обеспечивает защиту информации, передаваемой мобильным телефоном. Скремблеры активно применяются для защиты телефонных переговоров, не позволяя системам радиомониторинга мобильной связи осуществлять «прослушку» по ключевым словам и характерным изменениям интонации голоса.

При использовании скремблера MS подслушивание разговора, который ведется по вашему телефону, становится полностью невозможным, независимо от методики перехвата. Подразумеваются любые методы, включая такие, как контроль «у оператора», пассивный перехват в зоне телефона, активный перехват с переключением телефона на «ложную» базу и т.д. Все эти способы прослушивания будут бесполезны, если вы и ваш собеседник включили режим кодирования.  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](https://radio-security.com.ua/g2424615-akkumulyatory)…………………………до 10 часов  
4. Время работы блока MS с полностью заряженным аккумулятором…… до 8 часов

Достаточно невысокая стоимость скремблера позволяет создать «сеть» среди постоянных партнеров или внутри корпоративной «верхушки» для ведения полностью «закрытых» переговоров в пределах этой сети.

**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». После этого Вы можете спокойно беседовать на секретные темы.

Голос собеседника в режиме скремблирования несколько искажается. Это нормально, так как сигнал проходит многократную обработку и затем передается по относительно низкокачественному GSM-каналу. Создаваемый дискомфорт не соизмерим с важностью обеспечения конфиденциальности. Для улучшения понимания говорите медленно и разборчиво, а также используйте наушники.

**"ОРЕХ-А"**

Для защиты от преднамеренного прослушивания речевой информации, передаваемой по телефонным каналам как городской, так и междугородной телефонной сети.

Обеспечивает дуплексный режим, адаптирован к отечественным телефонным линиям. Криптографическая стойкость обеспечивается трехуровневой ключевой системой. Обмен сеансовыми ключами реализован по методу открытого распределения ключей для каждого сеанса связи.

Ключ генерируется самим аппаратом и сохраняется в нем только на время данного сеанса связи. Закрытие речевой информации достигается методами: временных перестановок, инверсии спектра сигнала, инверсии времени, преобразования временного масштаба, разрушающего непрерывность речевого сигнала.

**ТЕХНИЧЕСКИЕ ХАРРАКТЕРИСТИКИ**

* метод шифрования: мозаичный IDEA;
* количество комбинаций ключей: 1036;
* режим работы: дуплексный;
* время установки связи: 1-7 с;
* словесная разборчивость: не менее 90%;
* задержка речевого сигнала в тракте: не более 0,32 с;
* питание: 220 В, 50 Гц;
* потребляемая мощность: не более 6 Вт;
* габариты: 190х300х40 мм;