**Скремблер** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *scramble* — *шифровать*, *перемешивать*) — программное или [аппаратное](https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) устройство ([алгоритм](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC)), выполняющее **скремблирование** — обратимое преобразование [цифрового потока](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%82%D0%BE%D0%BA_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) без изменения [скорости передачи](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D0%BE%D1%80%D0%BE%D1%81%D1%82%D1%8C_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) с целью получения свойств [случайной](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D0%B0%D1%8F_%D0%B2%D0%B5%D0%BB%D0%B8%D1%87%D0%B8%D0%BD%D0%B0) [последовательности](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C). После скремблирования появление «1» и «0» в выходной последовательности равновероятны. Скремблирование — обратимый процесс, то есть исходное сообщение можно восстановить, применив обратный алгоритм.

Методы скремблирования можно разделить на аналоговые и цифровые, на статистические и динамические (роллинговые скремблеры), на с частотным и временным преобразованием, на полосные и инверсные методы, так же есть комбинированные методы.

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

**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». При использовании FSM-U1 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.

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

Скремблер реализован в виде гарнитуры и подключается к соответствующему разъему смартфона. При подключенном скремблере разговор ведется через него или наушники. 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 (компьютер, сетевое з/у или разъем в автомобиле).

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. 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 (поставляются в комплекте).

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

**Avantalk**



Мобильный скремблер Avantalk 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 Avantalk 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…………………………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.

**GUARD Bluetooth**

**Скремблер GUARD-Bluetooth** - это прибор с высоким  уровнем скремблирования. Он предназначен для шифрования разговоров, ведущихся по сотовой связи. Защита информации передаваемая по каналам сотовой связи обеспечивается за счет первоначального разрушения спектра речи и ее временной перестановки на передающей стороне (у того абонента, который говорит).

**Инверсионный беспроводной скремблер «Guard Bluetooth»**предназначен для защиты переговоров по сотовому телефону. Подключение скремблера к телефону происходит на частоте «bluetooth» 2,4Ггц. Беспроводная связь обеспечивает удобство в использовании устройства. При работе скремблер изменяет выходящий звуковой сигнал по принципу частотной инверсии. Закодированный сигнал передаётся на сотовый телефон, и далее по сотовой связи он приходит к вашему собеседнику. Для декодирования сигнала собеседнику необходимо иметь аналогичный аппарат с верными настройками. Устройство имеет 4 заранее заданных режима кодирования, которые можно переключать прямо во время разговора.

При перехвате сигнала третьими лицами его будет практически невозможно разобрать, либо дешифровать. Разборчивость перехваченного сигнала может максимально составлять 5% из общего разговора, и это будут бессвязные узнаваемые слова. Скремблер «Guard Bluetooth» работает от стандартной батареи 9 вольт формата «Крона». Передняя панель снабжена 2 переключателями кодирования, сверху располагается кнопка подключения «bluetooth». Устройство имеет малый вес и небольшие габариты, благодаря чему может свободно поместиться, например, во внутренний карман пиджака, либо в небольшую барсетку.

**Область применения**

Беспроводной скремблер «Guard Bluetooth» применяется в области цифровой безопасности при переговорах по сотовой связи частными лицами. Простота использования даёт возможность успешно применять скремблер людям без специальных навыков и технического образования. Небольшие размеры и работа от сменной батареи позволяет транспортировать скремблер и работать с устройством практически в любой обстановке.

**Технические характеристики**

|  |  |
| --- | --- |
| Принцип кодирования | Инверсия звукового спектра |
| Формирование ключа | Статическое |
| Общее количество комбинаций алгоритма | 4 комбинации |
| Количество изменении 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 |
| Максимальная дальность связи Bluetooth | 10 метров |
| Выходная мощность передатчика | 1 мВатт |
| Питание | 9В (крона) |
| Ток потребления мА | 70 мА |
| Индикация | Светодиодная |
| Материал корпуса | Пластик, алюминий |
| Габариты | 134х70х24 мм |
| Вес | 100 грамм |