### Огляд сучасних пристроїв скремблювання

На сьогодні можна виділити два напрямки шифрування мовних сигналів – це скремблювання аналогових сигналів та перетворення мовного повідомлення в дискретний вигляд з подальшим шифруванням.

Скремблювання — шифрування потоку даних, в результаті якої він виглядає як потік випадкових бітів.

Склемблери перетворюють вихідний мовний сигнал, змінюючи його амплітудні, частотні і часові параметри у різних комбінаціях. Потім скрембльований сигнал може передаватись по каналу зв'язку в тій самій смузі частот, що і вихідний, відкритий. Засоби мовного скремблювання вперше з'явились під час другої світової війни. Серед останніх досягнень в цій області слід відзначити широке використання інтегральних схем, зокрема процесорів цифрової обробки сигналів. Все це забезпечило високу надійність пристроїв закриття мови зі зменшенням їхнього розміру і вартості.Склемблери перетворюють вихідний мовний сигнал, змінюючи його амплітудні, частотні і часові параметри у різних комбінаціях. Потім скрембльований сигнал може передаватись по каналу зв'язку в тій самій смузі частот, що і вихідний, відкритий.

Оскільки скрембльовані мовні сигнали в аналоговій формі лежать в тій же смузі частот, що і вихідні відкриті, це значить, що їх можна передавати по звичайних каналах зв'язку, що використовуються для передачі мовної інформації, без потреби застосування якого-небудь спеціального обладнання, такого, як, наприклад, модеми. Тому пристрої мовного скремблювання не такі дорогі і значно простіші, ніж пристрої кодування з наступним цифровим шифруванням (вокодери).

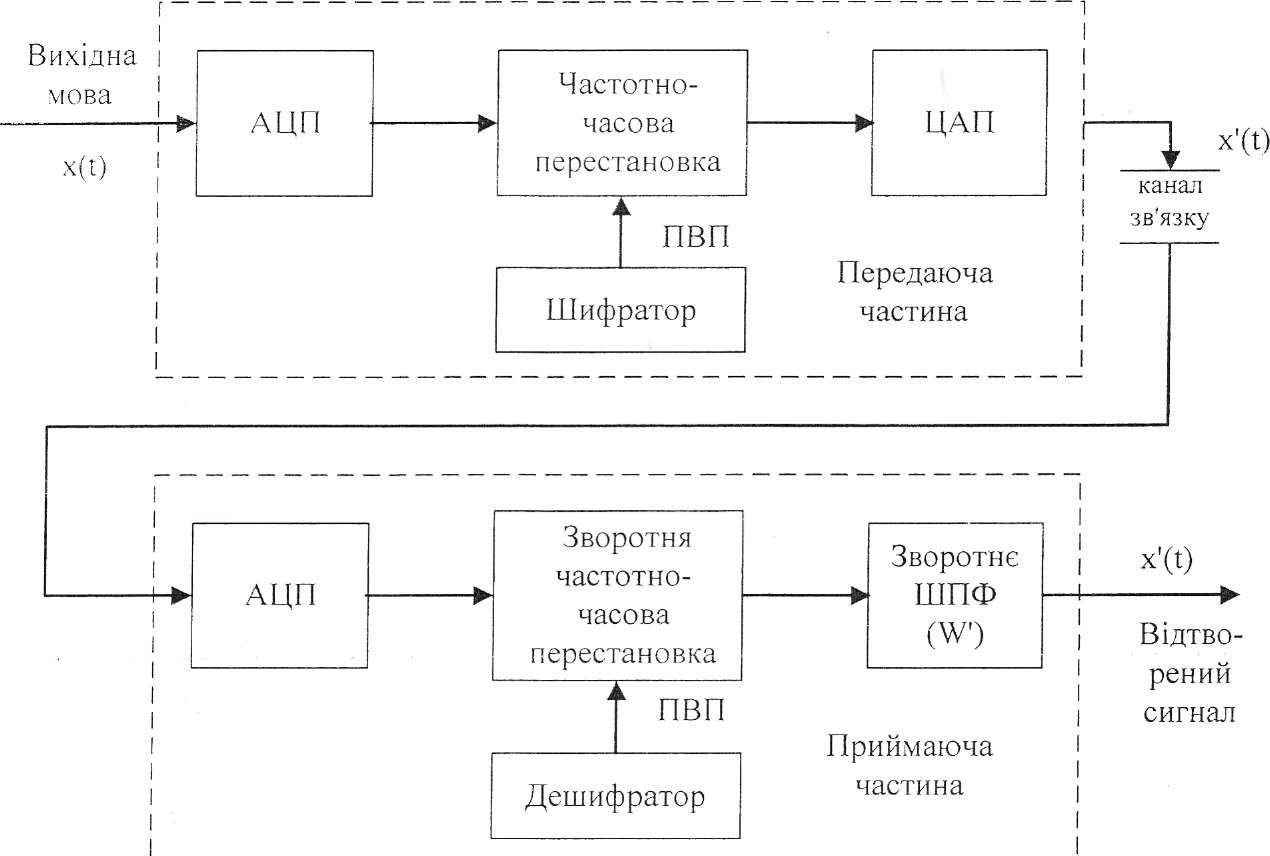
Телефонні скремблери*,* за їх режимом роботи, можна розбити на два наступні класи:

- статичні системи, схема кодування яких залишається незмінною на протязі передачі мовного повідомлення;

- динамічні системи, які постійно генерують кодові підстановки в ході передачі (код може змінюватись в процесі передачі декілька разів на протязі кожної секунди).

Використовуючи комбінацію часового і частотного скремблювання, можна значно підвищити степінь закриття мови. Комбінований скремблер набагато складніший, ніж звичайний і потребує компромісного рішення із вибору рівня закриття, кінцевої розбірливості, часу затримки, складності системи і рівня спотворень у відновленому сигналі.

Як приклад такої системи розглянемо скремблер, схема якого наведена на рисунку де операція частотно-часових перестановок дискретизованих відрізків мовного сигналу здійснюється з допомогою кількох процесорів цифрової обробки сигналу, один з яких може реалізовувати функцію генератора випадкової послідовності (ключа системи закриття)



(ПВП - псевдовипадкова послідовність)

В такому скремблері спектр оцифрованого аналого-цифровим перетворювачем (АЦП) мовного сигналу внаслідок використання алгоритмів цифрової обробки сигналів розбрівається на частотно-часові елементи, які потім змішуються на частотно-часовій площині у відповідності з одним із криптографічних алгоритмів і підсумовуються, не виходячи за межі частотного діапазону вихідного сигналу. Отриманий таким чином закритий сигнал з допомогою цифроаналогового перетворювача (ЦАП) переводиться в аналогову форму і подається в канал зв'язку. На приймальній стороні здійснюються зворотні операції із відновлення отриманого закритого мовного повідомлення. Стійкість представленого алгоритму можна прирівняти до стійкості систем цифрового закриття мови (на основі вокодерів).

Телефонний скремблер "Орех-ІІ" виконаний у вигляді підставки під телефон. Пристрій побудований на основі високопродуктивного цифрового процесора оброблення сигналів, що здійснює закриття мовної інформації. Працює із будь яким телефонним апаратом. Скремблер має просте управління, практично всі операції із закриття інформації здійснюються автоматично.

Закриття мовної інформації досягається такими методами:

1. Часових перестановок.
2. Інверсії спектра.
3. Перетворення часового масштабу, що руйнує неперервність мовного сигналу.

Телефонний скремблер "Орех-ІІ" має такі основні технічні характеристики:

1. Якість розмови у повнодуплексному режимі - не гірше 90 %.
2. Затримка мовного сигналу в тракті передача прийом - не більше 0,32 с.
3. Пригнічення скрембльованого сигналу на передавальній стороні не менше 40 дБ.
4. Час встановлення закритого зв'язку - не більше 10 с.
5. Використовується найсучасніша ключова система кодування- декодування за методом відкритих ключів.
6. Забезпечується гальванічне розділення від абонентської лінії та від підключеного телефонного апарату.
7. Електроживлення від мережі змінного струму 220 В.
8. Споживана потужність - не більше 1 Вт.
9. Габарити - 200x280440 мм.
10. Маса- не більше 1,5 кг.

На стенді телефонний апарат вилкою підключається в стандартну телефонну розетку скремблера, а скремблер - в розетку абонентської телефонної лінії. Крім того скремблер підключається до телефонної лінії. В режим захисту скремблер переводиться після того як встановлене з'єднання між двома абонентами, що мають однотипні скремблери. Для встановлення режиму захисту необхідно попередити про це абонента, із яким установлене з'єднання, і потім натиснути кнопку на передній панелі телефонної приставки.

Можливі два режими захисту мовної інформації:

1. з автоматично сформованим ключем;
2. з додатково введеним паролем.

У режимі з автоматичним сформованим ключем необхідно натиснути на кнопку на передній панелі приставки повторно. При встановленні захисту мовний інформатор видає в трубку повідомлення "Захист установлений" і індикатор "Зв'язок" постійно світить. Мінімальна структура з закриттям мовної інформації на основі даного засобу захисту повинна складатися з двох приставок, включених відповідно до рисунку



Відомі скремблери для ефективного захисту телефонних переговорів в мережах, що працюють по GSM стандарту. Спеціально розроблений скремблер **GUARD GSM**, будучи економ-варіантом, відмінно маскує мову, передану по каналах GSM зв'язку. Цей пристрій з'єднується зі стільниковим телефоном по провідній гарнітурі і має невеликі розміри. Скремблер GUARD GSM має тридцять два режими скремблювання, основні характеристики наведені нижче:

1. розбірливість мови. – не менше ніж 95%
2. тип з’єднання – повний дуплекс
3. затримка сигналу в лінії – не більше 100мс
4. рівень захищеності лінійного сигналу – тимчасовий
5. використання в мережах стандарту -GSM 900/1800
6. тип підключення до мобільного телефону – провідна гарнітура
7. габаритні розміри – 80

Початок розмови, як правило, починається в відкритому режимі і далі за обопільною команді пристрою перемикаються в режим скремблювання.

**Скремблер GUARD Bluetooth**

|  |  |
| --- | --- |
| Принцип кодування - інверсія звукового спектру | инверсия звукового спектра; |
| Безпровідне з’єднання - bluetooth | Bluetooth; |
| Формування ключа - статичне | статическое; |
| Загальна кількість комбінацій алгоритму - 4 | 4 комбинации; |
| Кількість змін частоти інверсії – 4 частоти | 4 частоты; |
| Довжина ключової послідовності – 16 біт | 16 бит; |
| Канал зв’язку – повний дуплекс | полный дуплекс; |
| Розбірливість дескремблированної мови – 95% | 95%; |
| Смуга звукової інверсії - 280 Гц- 3140 Гц | с 280 Hz до 3140Hz; |
| Діапазон частот інверсії - з 44.336 кГц до 184.734 кГц | 6dB на октаву; |
| Вихідний імпеданс - з 300 до 500 кОм | с 44.336kHz до 184.734kHz; |
| Живлення - 9В | с 300 по 500 кОм; |
| Струм мА – 70 | 9В (крона); |
| Індикація - світлодіодна | 70 мА; |
| Материал корпусу – пластик+алюміній | светодиодная; |
| Габарити – 100гр. | пластик, алюминий; |
| Вес | 134x70x24 мм; |
|  | 100 грамм. |