***Скремблювання*** – це таке перетворення бінарного цифрового сигналу, внаслідок якого без зміни швидкості передачі сигнал набуває якостей випадкової послідовності символів 1 та 0 незалежно від статистичних властивостей джерела повідомлення.

Оскільки скрембльовані мовні сигнали в аналоговій формі лежать в тій самій смузі частот, що й вихідні відкриті, це означає, що їх можна передавати по звичайним каналам зв’язку, що використовуються для передачі мови, без якогось спеціального приладу (модему).

Суть генерації кодової підстановки полягає в побітній зміні потоку даних, що проходять через систему. Практично єдиною операцією, що використовується в скремблерах є «XOR» — побітне виключне АБО. Паралельно проходженню інформаційного потоку в скремблері за визначеним правилом генерується кодуючий потік біт. Як пряме, так і зворотне шифрування здійснюється накладанням «XOR» на вхідну послідовність. Кодуюча послідовність біт генерується циклічно з невеликого початкового об’єму інформації — ключа за наступним алгоритмом. З поточного набору біт видираються  значення визначених розрядів і складаються по «XOR» між собою. Усі розряди зсуваються на 1 біт, а тільки що отримане значення («0» або «1») поміщається в самий молодший розряд, що звільнився. Серед сучасних пристроїв закриття мовних сигналів найбільше поширення здобули пристрої, що використовують метод аналогового скремблювання.

Для **аналогових скремблерів** характерна присутність під час передавання в каналі зв'язку фрагментів початкового відкритого мовного повідомлення, перетвореного в частотній і (або) часовій області. Це означає, що зловмисники можуть спробувати перехопити і проаналізувати передавану інформацію, на рівні звукових сигналів. Досвід свідчить, що новітні алгоритми аналогового скремблювання здатні забезпечити дуже високий рівень утаємничення.

**Цифрові скрмблери** не передбачають передачі якої-небудь частини початкового мовного сигналу. Мовні компоненти кодуються в цифровий потік даних, який змішується з псевдовипадковою послідовністю, що виробляється ключовим генератором по одному з криптографічних алгоритмів. Підготовлене таким чином повідомлення передається за допомогою модему в канал зв'язку, на приймальному кінці якого проводяться зворотні перетворення з метою отримання відкритого мовного сигналу.

Технологія створення широкосмугових систем, призначених для утаємничення мови, добре відома, а її реалізація не уявляє особливих труднощів. При цьому використовуються такі методи кодування мови,

як АДІКМ (адаптивна диференціальна імпульсно-кодова модуляція), ДМ (дельта-модуляція) і т.ін. Але представлена таким чином дискретизована мова може передаватися лише по спеціально виділеним широкосмуговим каналам зв'язку із смугою пропускання 4,8–19,2 кГц. Це означає, що вона не придатна для передачі по лініях телефонної мережі загального користування, де необхідна швидкість передавання даних повинна складати не менше 2400 бит/с. У таких випадках використовуються вузькосмугові системи, головною проблемою при реалізації яких є висока складність алгоритмів зняття мовних сигналів, здійснюваних у **вокодерних пристроях**.

За допомогою дискретного кодування мови з подальшим шифруванням завжди досягався високий ступінь утаємничення. Раніше цей метод мав обмежене застосування в наявних вузькосмугових каналах із-за низької якості відновлення передаваної мови. Досягнення в розвитку технологій низькошвидкісних дискретних кодерів дозволили значно поліпшити якість мови без зниження надійності утаємничення.

***Аналогові скремблери*** підрозділяються на:

* + мовні скремблери простих типів на базі часових і (або)

частотних перестановок мовного сигналу (рис. 1);

* + комбіновані мовні скремблери на основі частотно-часових перестановок відрізків мови, представлених дискретними відліками, із застосуванням цифрової обробки сигналів (рис. 2).

***Цифрові системи утаємничення мови*** підрозділяються на широкосмугові (рис. 3) і вузькосмугові (рис. 4).

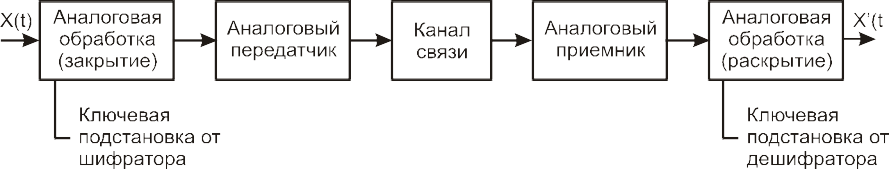


Рисунок 3.1- Схема простого мовного скремблеру

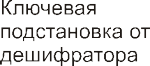
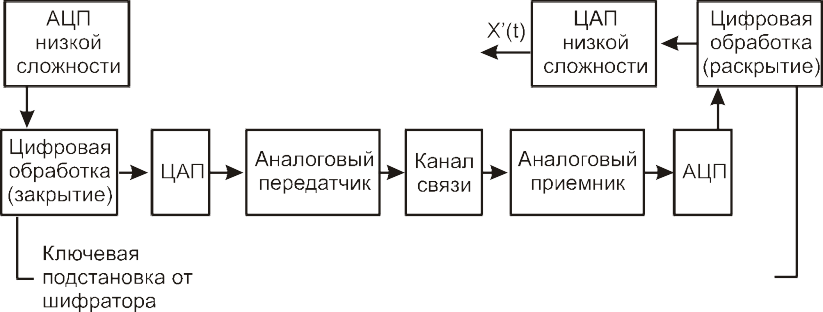


Рисунок 2- Схема комбінованого мовного скремблеру

Оцінюючи рівень захисту систем закриття мови, слід зазначити, що це поняття вельми умовне. При цьому слід констатувати, що у ряді виробів основні рівні захисту визначаються, як **тактичний** і **стратегічний*,*** що в деякому розумінні перекликається з поняттями практичної *і* теоретичної *стійкості криптосистем утаємниченняя даних.*

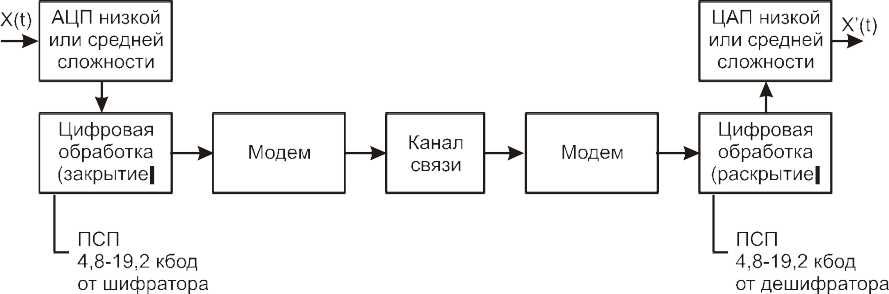


Рисунок 3.3. Схема широкосмугової системи утаємничення мови

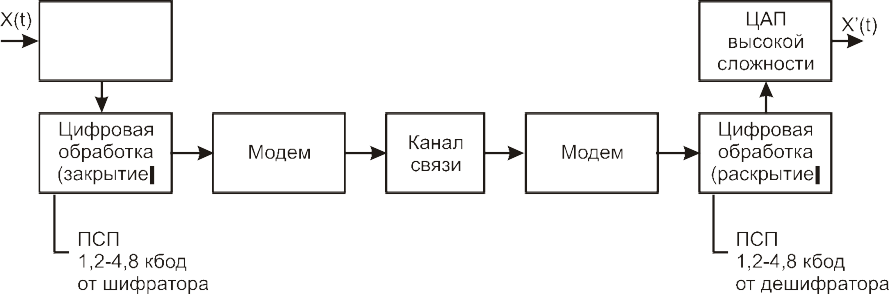


Рисунок 4. Схема вузькосмугової системи утаємничення мови

***Тактичний***, або низький, рівень використовується для захисту інформації від прослуховування сторонніми особами на період, вимірюваний від хвилин до днів. Існує багато простих методів і способів забезпечення такого рівня захисту з прийнятною стійкістю.

***Стратегічний***, або високий, рівень захисту інформації від перехоплення використовується в ситуаціях, які мають на увазі, що висококваліфікованому, технічно добре оснащеному фахівцю буде потрібно для дешифрування перехопленого повідомлення період часу від декількох місяців до декількох років.

Слід зазначити, що таке поняття, як *якість відновленої мови*, є достатньо умовним, оскільки під ним звичайно розуміють факт пізнання абонента і розбірливість сигналу, що приймається.

Висновок: Реалізація такого алгоритму можлива як програмно, так і на радіоелектронних елементах, що й забезпечило його широке застосування.

Декодування заскрембльованих послідовностей відбувається по тій ж самій схемі, що і кодування. Саме для цього в алгоритмах застосовується результуюче кодування по «виключному АБО» — схема, однозначно відновлювана при розкодуванні без яких-небудь додаткових обчислювальних витрат.

Залежність кожного біта вихідної послідовності тільки від одного вхідного біта, ще більш поширило використання скремблерів у захисті передачі даних. Це зв’язано з виникаючими у каналі передачі завадами, що можуть внести спотворення, в цьому випадку тільки на ті біти, на які вони проходяться, а не на зв’язану з ними групу байт, як це має місце в блокових шифрах.