**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**

**ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

Фізико-технічний інститут

**Реферат**

з дисципліни: «Системи технічного захисту інфромацій»

на тему: «Захист телефонних ліній з використанням скремблерів»

**Виконав:**

Студент 4 курсу ФТІ

групи ФБ-62

Бублик О.О.

**Перевірив:**

Прогонов Д.О.

Київ

2020

**Зміст**

Вступ

1. Аналогове скремблювання

2. Основні характеристики

3. Частотні перетворення

4. Часові перетворення

5. Порівняння

Висновки

**Вступ**

Кожен, хто користується якими-небудь засобами зв'язку, хоче обмежити можливості доступу сторонніх людей до інформації, яка передається. Надійний захист інформації може бути забезпечений в системах цифрового радіозв'язку, де застосовані методи криптографії. Криптографічні алгоритми отримали широке поширення цифрових стандартів стільникового зв'язку, забезпечуючи досить високий ступінь захисту інформації від несанкціонованого доступу.

У вітчизняних системах конвенційного та транкінгового радіозв'язку цифрові технології поки ще не знайшли такого широкого застосування. У порівнянні з аналоговими радіостанціями вартість цифрових радіозасобів помітно вище.

Тим не менш, бажання обмежити доступ до своєї інформації від цього не стає менше. Як правило, більшості користувачів не потрібно гарантований захист інформації, досить забезпечити нерозбірливість переданої інформації при прослуховуванні її сторонніми особами за допомогою звичайних аналогових радіостанцій або скануючих приймачів. Оптимальним вирішенням цього завдання є використання аналогових скремблерів.

Одним з найуразливіших каналів просочування інформації є телефонні лінії загального користування, за допомогою яких здійснюється велика кількість конфіденційних і секретних переговорів. Сучасна апаратура знімання інформації дозволяє легко прослуховувати ці канали. Найбільш простий спосіб отримання інформації - безпосереднє підключення до лінії в будь-якій точці від абонентського закінчення (телефонного апарату) до входу в АТС, включаючи розподільні щити і комунікаційні колодязі. При використанні апаратури знімання високого класу - практично неможливо визначити несанкціоноване підключення до лінії. У такому разі єдиним способом захисту інформації є перетворення її до такого виду, з якого зловмисник не зможе зрозуміти її зміст протягом якогось певного часу.

Відомі три основні методи захисту від перехоплення телефонних повідомлень усього телефонного тракту:

*1. Одностороннє маскування* накладанням на телефонне повідомлення з боку одержувача маскувальних перешкод із подальшою їх компенсацією;

*2. Скремблювання*(часочастотні перетворення) мовних сигналів;

*3. Дискретизація мови з подальшим шифруванням*.

Кожен із цих методів має свої переваги і недоліки. Так, методи маскування і скремблювання забезпечують захист телефонних повідомлень на нижньому сигнальному рівні, тоді як шифрування пов'язане із криптографічними перетвореннями мовної інформації, представленої у формі даних на вищому рівні інтерполяції.

*Метод маскування* передбачає адитивне накладання на аналоговий телефонний сигнал спеціальних перешкод, рівень яких забезпечує надійне енергетичне маскування телефонних повідомлень упродовж усього телефонного тракту. Отже йдеться про зниження відношення "сигнал/шум" до значень, за яких стає вже неможливим виділення зловмисником інформаційного сигналу засобами технічної розвідки.

Під *скремблюванням* розуміється зміна характеристик мовного сигналу таким чином, що отриманий модульований сигнал, маючи властивості нерозбірливості і невпізнання, займає таку ж смугу частот спектру, як і початковий відкритий. Якою б складною не була процедура скремблювання, найменший елемент, з яким вона оперує, - це перетворений фрагмент мовного сигналу, який не можна зробити коротше певного інтервалу через інтерференційні явища при передачі в каналі.

Основними властивостями скремблерів є:

1) досить висока якість відновленої мови;

2) невисока складність реалізації;

3) наявність залишкової інформації в закритому сигналі, яка може бути використана нападаючою стороною.

**1. Аналогове скремблювання**

У мовних системах зв'язку відомі два основних методи закриття мовних сигналів, що розділяються за способом передачі каналами зв'язку: аналогове скремблювання і дискретизація мови з наступним шифруванням (цифрове скремблювання). Кожний з цих двох методів має свої переваги та недоліки. Раніше вважалося, що поряд з високою якістю і розбірливістю відновленої мови аналогові скремблери можуть забезпечити лише низьку або середню, у порівнянні із системами цифрового кодування та шифрування, ступінь закриття (таємності). Однак новітні (розроблені в останні роки) алгоритми здатні забезпечити не тільки середній, але іноді, навіть, дуже високий рівень таємності.

Під *аналоговим скремблюванням* мається на увазі перетворення вихідного мовного сигналу з метою мінімізації ознак мовного повідомлення, в результаті якого цей сигнал стає нерозбірливим і невпізнанним. При цьому він займає таку ж смугу частот спектру, як і вихідний сигнал. Необхідною властивістю такого перетворення є можливість зворотного перетворення для відновлення мовного сигналу на приймальній стороні.

Найбільша частина апаратури засекречування мовних сигналів використовує в наш час метод аналогового скремблювання, оскільки: по-перше, це дешевше; по-друге, ця апаратура застосовується в більшості випадків у стандартних телефонних каналах зі смугою 3 кГц; по-третє, забезпечується комерційна якість дешифрованої мови; по-четверте, гарантується досить висока стійкість закриття інформації.

Аналогові скремблери перетворюють вихідний мовний сигнал за допомогою зміни його амплітудних, частотних і тимчасових параметрів у різних комбінаціях. Скрембльований сигнал може потім бути переданий каналами зв'язку в тій же смузі частот, що і вихідний - відкритий. В апаратах такого типу використовується один або кілька принципів аналогового скремблювання з числа перерахованих нижче:

*1) скремблювання в частотній області*:

· частотна інверсія (перетворення спектру сигналу за допомогою гетеродину і фільтру) ;

· розбиття смуги частот мовного сигналу на декілька піддіапазонів і частотна інверсія спектра в кожному щодо середньої частоти піддіапазону;

· розбиття смуги частоти мовного сигналу на кілька піддіапазонів та їх частотні перестановки.

*2) скремблювання в часовій області* (розбивка блоків або частин мови на сегменти з перемішуванням їх у часі з наступним прямим і/або реверсивним зчитуванням):

· інверсія за часом сегментів мовлення;

· тимчасові перестановки сегментів мовного сигналу.

3) Комбіновані методи перетворення сигналу припускають використання одночасно декількох різних способів скремблювання (як частотних, так і тимчасових), число яких обмежується, як правило, можливостями технічної реалізації аналогових скремблерів.

Аналогові скремблери за режимами роботи, можна розбити на такі класи:

1) статичні системи, схема кодування яких залишається незмінною протягом всієї передачі мовного повідомлення;

2) динамічні системи, що постійно генерують кодові підстановки в ході передачі (код може бути змінений у процесі передачі кілька разів протягом кожної секунди).

Очевидно, що динамічні системи забезпечують більш високий ступінь захисту, оскільки різко обмежують можливість легкого прослуховування переговорів сторонніми особами.

Аналоговим скремблерам вдалося уникнути багатьох труднощів, пов'язаних з передачею мовного сигналу і/або його параметрів, властивим цифровим системам закриття мови, і в той же час досягти певного рівня розвитку, що забезпечує середній та високий ступінь захисту мовних повідомлень. Оскільки скрембльовані мовні сигнали в аналоговій формі лежать у тій же смузі частот, що і вихідні відкриті, це означає, що їх можна передавати звичайними комерційними каналами зв'язку, що використовуються для передачі мови, без застосування будь-якого спеціального устаткування, такого, як, наприклад, модеми.

Можливе перетворення мовного сигналу за трьома основними параметрами: за амплітудою, за частотою і за часом. Вважається, що використовувати амплітуду недоцільно, тому що, змінюються в часі загасання каналу та відношення сигнал/шум, що роблять надзвичайно складним точне відновлення амплітуди переданого сигналу на приймальній стороні. Практичне застосування одержало тільки частотне та часове скремблювання, а також їх комбінації. Як вторинні способи скремблювання в цих системах можуть використовуватися обмежені види амплітудного скремблювання.

**2. Основні характеристики**

Основними технічними характеристиками аналогових скремблерів є рівень закриття інформації, залишкова розбірливість і якість відновлення сигналу.

Найбільш важливою характеристикою скремблера для користувача, що бажає забезпечити захист інформації в своїх каналах зв'язку, є рівень закриття інформації. Слід зазначити, що, якщо для складних цифрових систем передачі мови і даних поняття рівня закриття суворо регламентується і визначається криптографічного стійкістю інформації, то для аналогових скремблерів (особливо в системах рухомого радіозв'язку) дане поняття носить умовний характер, так як до теперішнього часу на цей рахунок не вироблено чітких стандартів чи правил.

У ряді випадків в якості критеріїв рівень закриття інформації при порівнянні різних засобів рухомого радіозв'язку з аналоговим скремблювання можна використовувати кількість ключових параметрів і кількість можливих ключів скремблера.

Під ключовим параметром аналогового скремблера звичайно розуміють будь-який параметр перетворення мовного сигналу, значення якого необхідно знати для здійснення зворотного перетворення сигналу на приймальній стороні.

Ключем аналогового скремблера (за аналогією з цифровими системами шифрування), як правило, називають конкретно секретний стан деяких параметрів перетворення мовного сигналу. Кількість ключів скремблера визначається безліччю всіляких значень ключа. Для скремблерів з одним ключовим параметром воно визначається числом можливих станів цього параметра, для скремблерів з кількома ключовими параметрами - кількістю можливих комбінацій значень цих параметрів (як правило, твором чисел станів всіх ключових параметрів).

Якість відновлення сигналу визначається спотвореннями сигналу при його частотних або часових перетвореннях. Фактично, ця характеристика відображає розбірливість і впізнаваність відновленої мови. Прийнятним або комерційним якістю відновленої на приймальному кінці промови вважається таке, коли слухач без зусиль може визначити голос мовця і сенс сказаного повідомлення.

Найкращою якістю відновлення сигналу володіють частотні інвертори, які практично не погіршують розбірливість і впізнаваність мови при правильній реалізації . Більш складні методи частотних перетворень можуть вносити деякі спотворення в мовний сигнал. Реалізація високої якості відновлення мови при тимчасових перетвореннях вимагає досить складної обробки.

Під залишкової розбірливістю розуміють відсоток відновлених фрагментів скрембльованого мовного сигналу при прослуховуванні переговорів за допомогою звичайних УКХ - приймачів або радіостанцій, не оснащених аналогічним скремблером.

Слід зазначити, що переважна більшість відомих аналогових мовних скремблерів в тій чи іншій мірі зберігають залишкову розбірливість. У прослуховуючому мовному сигналі, захищеному скремблером, зберігається інформація про темпі мови, уловлюються паузи. При нескладних способах захисту досвідчений оператор може розібрати (залежно від наявності відомостей про тематику ведуться переговорів) від 10 до 50 % переданої інформації.

Основними технічними характеристиками аналогових скремблерів є рівень закриття інформації, залишкова розбірливість і якість відновлення сигналу.

Для користувачів засобів УКХ - радіозв'язку вкрай важливий рівень технічного виконання скремблерів. Так як конструктивно частіше всього скремблери являють собою малогабаритні мікроелектронні вузли, які встановлюються всередину корпусу радіостанції, переважний вибір скремблювання пристроїв з мінімальними габаритами. Природно, що мінімізація габаритів дозволяє розширити застосування скремблерів, оскільки забезпечується можливість їх встановлення в більшу кількість радіозасобів. Для користувачів, що бажають забезпечити захист інформації для вже наявних радіостанцій, цілком може підійти варіант із зовнішнім підключенням скремблера.

Встановлення скремблерів в радіостанції може призвести до певних обмежень на використання інших модулів або вбудованих функцій радіостанцій, таких як тональна (DTMF) або підтональна (CTCSS) сигналізація. Часто це відбувається через неможливості одночасного конструктивного розміщення всередині станції, проте іноді такі обмеження можуть пояснюватися несумісними з DTMF або CTCSS спектральними або тимчасовими перетвореннями сигналу.

При встановленні скремблерів бажано звертати увагу на додатковий струм споживання, який вносять ці модулі. Значний струм споживання може впливати на тривалість роботи станцій без заміни акумулятора.

Зручність використання скремблерів, багато в чому, залежить від тих коштів, які передбачені для установки ключа. У даному випадку, вибір доцільно здійснювати, виходячи з умов експлуатації радіозасобів. Для одних користувачів необхідна оперативна заміна ключа з клавіатури безпосередньо в процесі роботи, для інших - більш важливим є вимога по незмінності ключа і неможливості перевстановити його без використання спеціальних программаторів.

Відмінною особливістю системи тимчасового скремблювання/ дескремблювання є елемент пам'яті, який повинен зберігати інформацію про прибутті в нього сигналі протягом деякого часу. На дескремблер відбувається операція "зшивання" назад в вихідний сигнал (можливо з деякими спотвореннями). Основні проблеми при відновленні сигналу відбуваються в місцях "зшивок" через власне неідеальності розбиття на відрізки. Тому що, з одного боку, чим більше число частин, на який ми розбиваємо вхідний сигнал, для того, щоб їх потім перемішати - тим складніше його буде потім зібрати тим людям, які займаються перехопленням і розшифровкою. Але як показує практика - занадто маленькі відрізки призводять до того, що перешкоди, що додаються в сигнал у місцях "зшивок " будуть надавати помітний вплив на сам сигнал, і його розпізнавання після проходження дескремблера буде достатньо ускладнене.

Таким чином в реальній системі довжина відрізка розбиття обмежена величиною порядку 15-20 мілісекунд. Ще одна негативна сторона - затримка інформації, так як сигнал затримується в блоці пам'яті для подальшого скремблювання/дескремблювання. Таким чином при оцінці допустимого часу затримки в розмові - порядку 0.3-0.5 секунд (при величині затримки порядку секунди - розмова стає практично неможливий) - оцінка кількості відрізків дає 16-64 елементарних фрагментів мови. Також до недоліків відноситься необхідність синхронізації передавача і приймача, і як наслідок - можливість зриву цієї синхронізації, що буде вимагати додаткових тимчасових витрат.

Якість відновлення сигналу є найважливішою експлуатаційної характеристикою скремблерів. Вона визначається спотвореннями сигналу при його частотних або тимчасових перетвореннях. Може бути виражене розбірливістю і впізнаваністю відновленої мови. Прийнятним або комерційним якістю відновленої на приймальному кінці промови вважається таке, коли слухач без зусиль може визначити голос мовця і сенс сказаного повідомлення. Точну кількісну оцінку розбірливості мови можна отримати шляхом вимірювання відсотка правильно переданих тестових повідомлень при проведенні тривалих і трудомістких артикуляційних випробувань.

Вплив скремблерів на параметри радіостанцій проявляється, перш всього, в погіршенні їх чутливості за рахунок зменшення співвідношення сигнал/шум на вході приймача. Крім цього, при перетвореннях сигналу, пов'язаних із зміною будь-яких параметрів перетворення в часі, потрібно певний часовий інтервал для синхронізації таймерних пристроїв передавальної і приймальні сторони. Це змушує оператора витримувати паузу між натисканням тангенти " передача" на радіостанції і початком мовлення. Як правило, зменшення залишкової розбірливості супроводжується погіршенням, як якості відновлення сигналу, так і параметрів радіостанцій. Це пояснюється тим, що, бажаючи збільшити ступінь захисту інформації, розробники йдуть на різні хитрощі, що призводять дододатковим спотворень або спектру, або часових параметрів сигналу. Для користувачів засобів УКХ радіозв'язку вкрай важливий рівень технічного виконання скремблерів. Т.я. конструктивно скремблери являють собою малогабаритні мікроелектронні вузли, які встановлюються всередину корпусу радіостанції, переважний вибір аналогових засобів з мінімальними габаритами і енергоспоживанням.

**3. Частотні перетворення**

При частотній інверсії перетворення спектру мовного сигналу еквівалентно повороту частотної смуги сигналу навколо деякої середньої частоти. Інвертор - балансний змішувач з частотою на передавальному і приймальному тракті - частота

Спектр сигналу на виході мікрофону інверсується частотою 3700 Гц в інверсний спектр, де маємо нижню і верхню бокову інвертовані з спектральними складовими. На приймальній інвертор спектру на тій же частоті здійснює повторну інверсію і графік (В) інтерпретує вихідний сигнал з прямим спектром в діапазоні 300-3400.

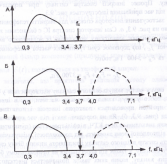
Якість відновленої мови залежить від:

- типу змішувачів,

- фільтрів, які обмежують смугу частот (нижню бокову)

- корекції на приймальній стороні

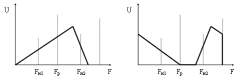
Принцип даного перетворення сигналу показаний на рис.1. При цьому досягається ефект перетворення низьких частот у високі частоти, і навпаки.



*Рис. 1. Принцип роботи частотного інвертора мовного сигналу*

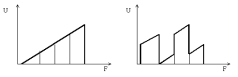
Даний спосіб забезпечує невисокий рівень закриття, тому що при перехопленні легко встановлюється величина частоти, що відповідає середній точці інверсії в смузі спектру мовного сигналу.

Більш складний у порівнянні з частотної інверсією спосіб перетворення сигналу забезпечує скремблер з розбиттям смуги мовного сигналу на піддіапазони з частотної інверсією сигналу в кожному піддіапазоні (смугозсувний інвертор) . Зазвичай використовується розбиття смуги на 2 піддіапазони. Принцип такого частотного перетворення для 2- х піддіапазонів зображений на рис. 2, де а) - вихідний спектр сигналу, б) - спектр сигналу після перетворення, Fр - частота розбиття спектра сигналу; Fі1, Fі2 - частоти інверсії 1- го і 2- го піддіапазонів.



*Рис. 2. Принцип роботи смугово-зсувного інвертора мовного сигналу при розбитті спектру сигналу на 2 піддіапазони.*

Мовний спектр можна також розділити на кілька частотних смуг рівної ширини і провести їх перемішування і інверсію по деякому правилу (ключ системи). Так функціонує смуговий скремблер (рис. 3).



*Рис. 3. Принцип роботи чотирьох смугового скремблера*

Зміна ключа системи дозволяє підвищити ступінь закриття, але вимагає введення синхронізації на прийомній стороні системи. Основна частина енергії мовного сигналу зосереджена в невеликій області низькочастотного спектру, тому вибір варіантів перемішування обмежений і такі системи характеризуються високою залишковою розбірливістю інформації.

Істотне підвищення ступеня закриття мови може бути досягнуте шляхом реалізації в смуговому скремблері швидкого перетворення Фур'є (ШПФ)(рис.4).



*Рис. 4. Схема частотних перестановок телефонного сигналу на основі ШПФ*

При цьому кількість припустимих перемішувань частотних смуг значно збільшується, що забезпечує високий ступінь закриття без погіршення якості мови. Можна додатково підвищити ступінь закриття шляхом здійснення затримок різних частотних компонентів сигналу на різну величину.

Головним недоліком використання ШПФ є виникнення в системі великої затримки сигналу (до 300 мс), обумовленою необхідністю використання вагових функцій. Це призводить до ускладнень у роботі дуплексних систем зв'язку.

**4. Часові перетворення**

Найпростішим видом тимчасового перетворення є часова інверсія, при якій вихідний сигнал ділиться на послідовність часових сегментів і кожен з них передається інверсно в часі - з кінця до початку. Такі скремблери забезпечують обмежений рівень закриття, що залежить від тривалості сегментів. Для досягнення нерозбірливості повільної мови необхідно, щоб довжина сегменту становила близько 250 мс. Це означає, що затримка системи буде дорівнювати приблизно 500 мс, що може виявитися неприйнятним для деяких застосувань. Принцип роботи та структурна схема часового інвертора зображений на рис. 5,6.

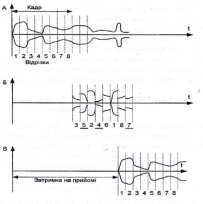


*Рис. 5. Структурна схема телефонного каналу із часовим скремблюванням*



*Рис. 6. Принцип роботи часового інвертора*

У скремблер з часовими перестановками мовний сигнал ділиться на часові кадри, кожен з яких у свою чергу підрозділяється на сегменти, а потім сегменти мовного сигналу піддаються перестановці. Принцип роботи такого скремблера з фіксованим вікном і числом часових сегментів у кадрі зображено на рис. 7.



*Рис. 7. Принцип роботи скремблера з часовими перестановками*

Головним недоліком скремблера з фіксованим кадром є збільшена величина часу затримки системи, що дорівнює подвоєній тривалості кадру. Цей недолік усувається в скремблерах з перестановкою часових відрізків мовного сигналу з "назкрізним вікном". У ньому число комбінацій можливих перестановок обмежено таким чином, що затримка будь-якого відрізка не перевершує встановленого максимального значення. Кожний відрізок вихідного мовного сигналу як би має тимчасове вікно, у середині якого він може займати довільне місце під час скремблювання. Це вікно рухається в часі в міру надходження в нього кожного нового відрізка сигналу. Затримка при цьому знижується до тривалості вікна.

**5. Порівняння**

Для частотного інвертора єдиним ключовим параметром є значення частоти інверсії сигналу. Розмірність цього параметра, тобто число можливих значень частот інверсії (число ключів) з відчутними спотвореннями, що виникають при прослуховуванні на сусідній частоті, не перевищує 20-30. Для перехоплення переговорів, що ведуться за допомогою радіозасобів, оснащених частотним інвертором, достатньо мати аналогічну радіостанцію або скануючий приймач з можливістю підбору частоти інверсії.

У смугово-зсувних інверторах в якості основного ключового параметра виступає частота розбиття смуги мовного сигналу Fр, розмірність якої порівнянна з розмірністю ключового параметра частотного інвертора. Якщо частота розбиття є єдиним ключовим параметром, то даний спосіб аналогового скремблювання забезпечує закриття мовної інформації, порівнянне з частотної інверсією. У разі коли можуть змінюватися і частоти інверсії в кожній з смуг, число ключів, відповідно і рівень закриття інформації, збільшуються.

У смугових скремблерів ключовими параметрами системи є число частотних смуг і кодова комбінація їх перестановки. Реально число смуг не перевищує 4 - х, тому число можливих комбінацій - 24 (одна з них не є перестановкою).

Скремблери з часовими перестановками мають кілька ключових параметрів: тривалість сегмента мови, тривалість тимчасового відрізка і правило перестановки часових відрізків в сегменті. Різні поєднання значень цих параметрів можуть дати можливість реалізації кількох сотень ключів.

***Приклад:*** Телефонна приставка (скремблер) Орех - А (виробництва зеленоградської компанії АНКАД)

Технічні характеристики:

\* закриття мовної інформації досягається за допомогою часових перестановок і інверсії спектра сигналу;

\* перестановки виробляються відповідно до сеансового ключа (128 біт), який виробляється автоматично при вході в захищений режим;

\* ключ в приставці зберігається тільки на час сеансу зв'язку;

\* для ідентифікації абонентів, що входять у зв'язок, може бути використаний 4 - значний десятковий пароль;

\* час встановлення захищеного зв'язку від 1 до 7 секунд;

\* словесна розбірливість - не менше 90%;

\* затримка мовного сигналу - не більше 0.32 с;

\* конструктивно Орех - А виконаний у вигляді підставки під телефонний апарат;

\* маса приставки - не більше 2 кг.

**Висновки**

Скремблери всіх типів, за винятком найпростішого (із частотною інверсією), вносять перекручування у відновлений мовний сигнал. Межі тимчасових сегментів порушують цілісність сигналу, що неминуче приводить до появи позасмугових складових. Небажаний вплив роблять і групові затримки позасмугового мовного сигналу в каналі зв'язку. Результатом перекручувань є збільшення мінімально припустимого відношення сигнал/шум, при якому може здійснюватися надійний зв'язок. Але, не зважаючи на це найбільш надійними, з точки зору ступеня закриття мови, є скремблери з "назкрізним вікном", а для більшого рівня закриття слід застосовувати комбіновані скремблери.

На сьогодні, разом з усіма недоліками та перевагами, методи тимчасового і частотного скремблювання, а також комбіновані методи успішно використовуються в комерційних каналах зв'язку для захисту конфіденційної інформації.