МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 «Кібербезпека»

на тему: **ЗАХИСТ МОВНОЇ ІНФОРМАЦІЇ В ТЕЛЕФОННІЙ ЛІНІЇ МЕТОДОМ СКРЕМБЛЮВАННЯ**

Студент групи СЗЗ-51 Підлісний Ярослав Олегович _____
(підпис)

Науковий керівник: ст.викл. Гребенніков Асаді Болдхоягович _____
(підпис)

Нормоконтроль ст. викл. Гребенніков Асаді Болдхоягович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н., доц. Г.В. Шуклін
«_____»_____ 2022р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Підлісному Ярославу Олеговичу

1. Тема роботи: Захист мовної інформації в телефонній лінії методом скремблювання

Затверджена наказом по університету від «____»_____ 2022 р. № ___

2. Термін здачі студентом оформленої роботи «____» _____ 2022 р.

3. Об’єкт дослідження: є захист мовної інформації від витоку по телефонним каналам зв`язку на об'єкті інформаційної діяльності.

4. Предмет дослідження: є методи та засоби захисту мовної інформації на об'єкті інформаційної діяльності.

5. Мета роботи: розробка системи захисту мовної інформації при проведенні телефонних розмов на об’єкті інформаційної діяльності.

6. Перелік питань, які мають бути розроблені:

1. Аналіз існуючих підходів до захисту мовної інформації від витоку в телефонній лінії.

2. Вимоги до захисту мовної інформації в телефонній лінії на об’єкті інформаційної діяльності.

3.Засоби несанкціонованого отримання мовної інформації в телефонних лініях.

4. Методи захисту мовної інформації.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____2022 р.

Науковий керівник _____ Гребенніков А.Б.

Завдання прийняв до виконання _____ Підлісний Я.О.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз існуючих підходів до захисту мовної інформації від витоку в телефонній лінії	До 04.04.2022	Виконано
2	Вимоги до захисту мовної інформації в телефонній лінії на об'єкті інформаційної діяльності.	04.04.22-25.04.22	Виконано
3	Засоби несанкціонованого отримання мовної інформації в телефонних лініях	25.04.22-06.05.22	Виконано
4	Методи захисту мовної інформації	06.05.22-13.05.22	Виконано
5	Перевірка роботи на плагіат, передзахист	16.05.22-01.06.22	Виконано
6	Підготовка презентації до захисту, захист	02.06.22-21.06.22	

Студент _____ Підлісний Я.О.

(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи _____ Гребенніков А.Б.

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 71 сторінка, 34 рисунки, 28 джерел.

Об’єкт дослідження – захист мовної інформації від витоку по телефонним каналам зв`язку на об'єкті інформаційної діяльності.

Предмет дослідження – методи та засоби захисту мовної інформації на об'єкті інформаційної діяльності.

Мета роботи – розробка системи захисту мовної інформації при проведенні телефонних розмов на об’єкті інформаційної діяльності.

Методи дослідження – теорія електрозв’язку, теорія інформації, системний аналіз.

У роботі розглянуті основні принципи захисту мовної інформації в процесі спілкування засобами телефонії.

Сформульовані та визначені основні завдання щодо захисту мовної інформації при використанні телефонних ліній на об’єктах інформаційної діяльності. Здійснено аналіз основних методів захисту мовної інформації при використанні телефонії. Здійснено аналіз сучасних засобів захисту мовної інформації. На підставі проведених досліджень розроблено систему захисту мовної інформації інформації в телефонній лінії на об’єкті інформаційної діяльності методом скремблювання.

Галузь використання – інформаційна безпека.

ОБЛАДНАННЯ:

КРИПТО-ТЕЛЕФОННА СИСТЕМА SCR-M12, ПРИСТАВКА ДО ТЕЛЕФОННОГО АПАРАТУ СТА 1000, ТЕЛЕФОННА ПРИСТАВКА «ОРЕХ»,

АВТОНОМНИЙ КОДУЮЧИЙ ПРИСТРІЙ ASC-2, АБОНЕНТСЬКИЙ ТЕЛЕФОННИЙ ПРИСТРІЙ ДЛЯ МАСКУВАННЯ «РАЗБЕГ-К», СКРЕМБЛЕР Р-117Л.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АТС – автоматична телефонна станція

АЦП – аналогово-цифровий перетворювач

ВЧН – високочастотне нав`язування

ДТЗС – допоміжні технічні засоби і системи

ЕМПШ – електромагнітне поле шуму

ЗІ – захист інформації

ЗЗІ – засоби захисту інформації

ІзОД - інформація з обмеженим доступом

НЧ – низькочастотні

ОІД – об’єкт інформаційної діяльності

ПНЧ – перетворювачі низьких частота

ПЕОМ – персональна електронно-обчислювальна машина

ПЕМІН – побічні електромагнітні випромінювання

ТЗПІ – технічні засоби приймання інформації

ЦАП – цифрово-аналоговий перетворювач

УКХ – ультро-короткі хвилі

ШПФ – швидке перетворення Фур'є

ВСТУП

У зв`язку з розвитком телефонізації виникає проблема захисту мовної інформації в процесі спілкування за допомогою засобів телефонії. Підслуховування переговорів є однією із завдань зловмисників. Існують різні способи здійснення даного злочину, але найбільше поширення отримав використання телефонного радіо закладного пристрою, який вмонтовується або в саму телефонну лінію, або в приміщення, де розташована дана телефонна лінія. Крім того, даний закладний пристрій можна сховати і в самі АТС. Тому завдання сховати мовну інформацію, яка передається по каналам телефонної лінії на теперішній час стає достатньо актуальною.

Мета роботи – розробка системи захисту мовної інформації при проведенні телефонних розмов на об’єкті інформаційної діяльності.

Об’єкт дослідження – захист мовної інформації від витоку по телефонним каналам зв`язку на об'єкті інформаційної діяльності.

Предмет дослідження – методи та засоби захисту мовної інформації на об'єкті інформаційної діяльності.

Галузь застосування – інформаційна безпека.

1. КАНАЛИ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ В ТЕЛЕФОННИХ ЛІНІЯХ ЗВ`ЯЗКУ

1.1. Засоби безпеки мовної інформації

Для створення засобів безпеки мовної інформації при проведенні телефонних перемовин в першу чергу необхідно розуміти яким чином можна здійснити підслуховування. На рисунку 1.1. представлено способи здійснення підслуховування.

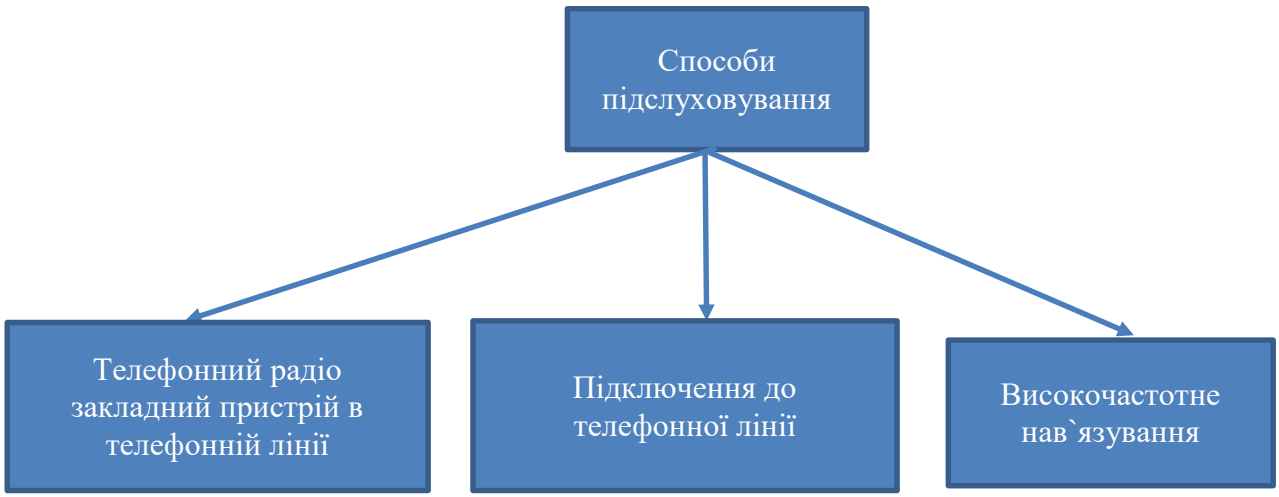


Рисунок. 1.1. Способи підслуховування

Найбільш поширеним способом підслуховування є використання телефонного радіо закладного пристрою. Даний пристрій можна вмонтувати не тільки в телефон, телефонну лінію, але і в приміщенні, де даний апарат знаходиться. Крім того, даний пристрій можна розмістити і за межами приміщення. Також є загроза, якщо засіб негласного отримання інформації розміщено на АТС. Даний пристрій уявляє собою мініатюрний передавач, який підключено контактно, дальність дії 200 метрів в діапазоні 400 – 500 МГц. Також, даний мініатюрний передавач може мати форму конденсатора з дальністю дії 500-800 метрів з діапазоном 139 МГц. Також даний передавач може мати форму мініатюрного мікрофону з дальністю дії не більше 100 метрів і діапазоном 107-115 МГц.

Кількість існуючих способів втручання в конфіденційні телефонні перемовини породжують і кількість різних заходів протидії цьому. Здійснення

протидії прослуховуванню є насправді достатньо складною задачею і при цьому для її реалізації необхідно виділяти достатньо багато коштів. Більш дешевше є використання спеціального обладнання, яке спроможне маскувати повідомлення, передача яких здійснюється по телефонним каналам або проводити відповідні правові та організаційні заходи по забезпеченню конфіденційності перемов.

Для цього варто здійснювати монтаж телефонних кабелів в приміщенні таким чином, щоб можна було контролювати кожну ділянку прокладки і щоб при цьому було б складно сховати радіо закладний пристрій прослуховування. Крім того, при проведенні перемовин варто відключати телефони, які з'єднані дротами. При цьому відсутнє джерело прослуховування. Дуже ефективним способом забезпечення захисту телефонних перемовин є використання засобів, які здійснюють маскування мови або скремблерів. На теперішній час технічний прогрес в засобах шифрування досяг достатньо великого рівня і алгоритми шифрування достатньо стійкі.

Скремблер – це спеціальний пристрій, який або автоматично шифрує інформацію при перемовинах, або ставиться в телефонну апаратуру для здійснення шифрування мовної інформації, яка передається по каналам зв'язку. В таблиці 1.1 представлено технічні характеристики існуючих скремлерів.

Таблиця 1.1. Технічні характеристики скремблерів

п/п	Тип	Структура	Виробник	Особливості в експлуатації
1	SCR-M12	Крипто-телефонна станція	Маском	Приставка, яка захищає телефони та факсимільні апарати
2	СТА-1000	Спеціальна приставка до телефону	Маском	Захист мовної інформації по телефонним каналам зв'язку
3	"Орех"	Приставка до телефону	Анкад	Захист мовної інформації по телефонним каналам зв'язку
4	ASC-2	Кодуючий пристрій, який кодує інформацію в автономному режимі	"REI" (США)	Універсальний засіб захисту від прямого прослуховування та і виявляє наявність закладних пристроїв прослуховування
5	"Разбег-К"	Маскиратор абонентських телефонних пристроїв	пниеи	Захист мовної інформації. Має ступінь RS-232. Захищено від мікрофонного ефекту та ВЧН

6	"Уэа"	Телефонний маскуватор	пниеи	Має розташування в кейсі. Подключа ється до лінії прямим шляхом або через акустичний дротовий канал.
7	Р-117Л	Скремблер	Маском	Захист перемовин, які проводяться по радіоканалам. Може сумісно використовуватись з різноманітними портативними радіостанціями
8	"Туман"	Маскиратор	Маском	Метою пристрою є маскування телефон них перемовин по абонентським лініям зв'язку. Прилад приєднується до розриву дротів, які напрвлені від телефонного апарату до телефонної трубки
9	"Селена"	Маскиратор	Маском	Пристрій має маленькі розміри і дуже легко підключається до довільної телефонної лінії.
10	Е-24	Аппаратура закрытия речевой информации	"Алмаз"	Застосовується разом з радіостанціями Р-159
11	Е-9к	Аппаратура закрытия речевой и цифровой информации	"Прогресс"	Застосовується разом з радіостанціями Р-159
12	АТ-2400	Аппаратура ведения конфиденциальных телефонных переговоров	Анкорт	Має вид приставного пристрою до телефону
13	"Voice changer"	Изменитель голоса	Анкорт	Здійснює зміну голосу при проведенні телефонних перемовин. Дає можливість в великому діапазоні змінювати тембр голосу та мову при цьому неможливо виявити
14	Линия-1	Устройство конфиденциальной связи	Елерон	Дає можливість здійснювати захист мовної інформації в лініях телефонного зв'язку. Фізичний принцип - метод інверсії спектру
15	"Туман"	Маскиратор телефонных переговоров	Елерон	Приєднується в розрив дротів
16	"Угра"	Телефонный скремблер	пниэи	Приєднується в розрив дротів

В залежності від ситуації використовується той чи інший пристрій. На рисунку 1.2. преставлено три можливі ситуації.

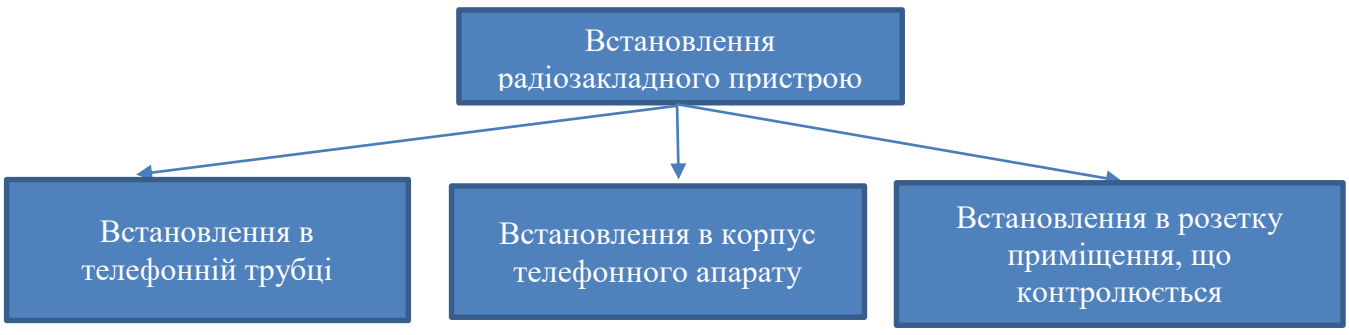


Рисунок 1.2. Місця встановлення радіо закладного пристрою.

Якщо пристрій сховано в телефонну трубку, то для захисту мовної інформації використовується тільки скремблер. Якщо ж засіб негласного отримання інформації встановлено в телефонний корпус, то в цьому випадку необхідно приєднувати скремблер до розриву дротів між телефонною трубкою та телефонним апаратом. І якщо радіо закладний пристрій встановлено в розетку, то скремблер приєднується в розрив дротів між телефонним апаратом і телефонною розеткою.

1.2. Засоби протидії витоку мовної інформації

На теперішній час надійним способом забезпечення конфіденційної інформації при проведенні перемовин є цифровий спосіб радіо зв'язку, де використовуються криптографічні алгоритми. Ці алгоритми є достатньо надійними та стійкими в забезпечені конфіденційності перемовин. В таблиці 1.2 представлено способи протидії підслуховуванню телефонних перемовин.

Таблиця 1.2. Способи протидії підслуховуванню телефонних перемовин

Спосіб підслуховування телефонних перемовин	Метод виявлення способу підслуховування	Засоби протидії
Мікрофонний ефект	Метрологічні вимірювання на наявність мікрофонного ефекту	1. Вилучення телефонного апарату і заміна його на новий. 2. Засоби спеціального захисту
Контактне або безконтактне підключення до телефонної лінії	Моніторинг телефонних ліній на наявність підключення або зміну електричних параметрів самої лінії, включаючи зміну напруги, струмів. Виявлення індукованих датчиків	Прокладка телефонного дроту в комунікаціях, які захищенні. Неперервне вимірювання електричних параметрів. Вилучення електричного обладнання, яке не використовується. Використання скремблерів. Використання екранованих дротів. Зашумлення ліній зв'язку.

В багатьох випадках при захисту витоку інформації по технічним каналам використовують засоби ультро-коротких хвиль (УКХ) для здійснення

функціонування диспетчерського зв'язку між співробітниками в процесі забезпечення захисту інформації на об'єктах інформаційної діяльності. Це пов'язано з тим, що при спілкуванні використовують локальні мережі радіозв'язку. На рисунку 1.3 представлено два основних метода захисту мовної інформації.

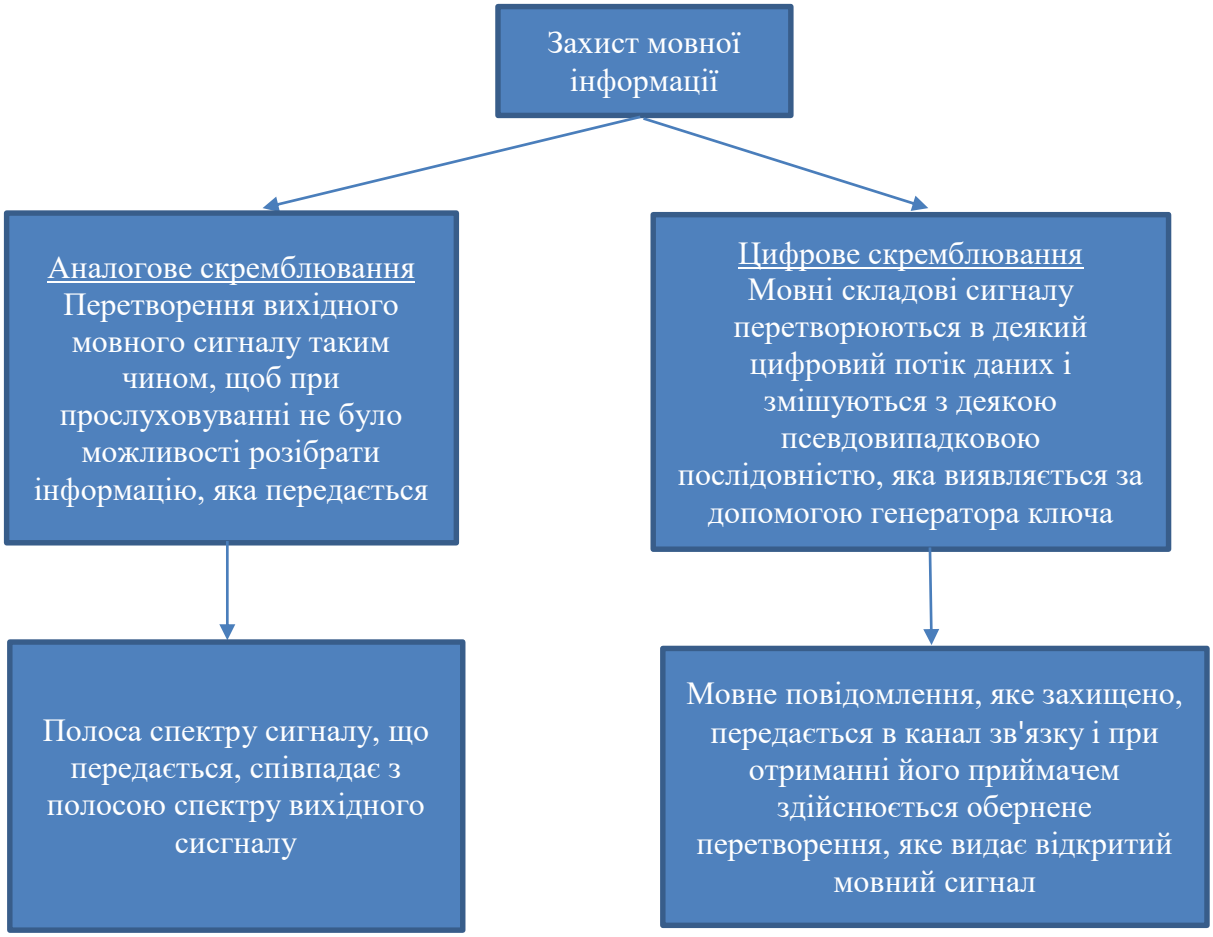


Рисунок 1.3. Методи захисту мовної інформації.

Основними параметрами, які характеризують якість захисту мовної інформації скремблером є рівень закриття інформації, граничне спроможність розпізнавання, якість відновлення сигналу, вплив на параметр радіостанцій, рівень технічного виконання. Однак, найголовнішим параметром є рівень закриття інформації. Крім того, ЗЗІ можна розглядати одні, як засоби захисту інформації від неумисного витоку – прослуховування відбувається особами, які не використовують спеціальні засоби перехоплення конфіденційних перемовин, та засоби від несанкціонованого доступу до конфіденційної інформації – прослуховування здійснюється зацікавленими особами, яких цікавить саме конфіденційна інформація перемовин і

які використовують для цього спеціальні засоби. Засоби захисту інформації від несанкціонованого доступу залежать від того, якими засобами відбувається перехоплення. Чим рівень засобів перехоплення інформації вищий, тим вищим повинен бути і рівень засобів захисту інформації від несанкціонованого втручання. В загальному, основним показником класифікації обладнання, яке використовується для захисту конфіденційної інформації від несанкціонованого втручання, є час дешифрування інформації після її запису. Такий показник залежить від криптографічного алгоритму, який перетворює інформацію в зашифрований вид, потім виконує обернене пертворення.

На рисунку 1.4 представлено схему підслуховування за допомогою вищих гармонік

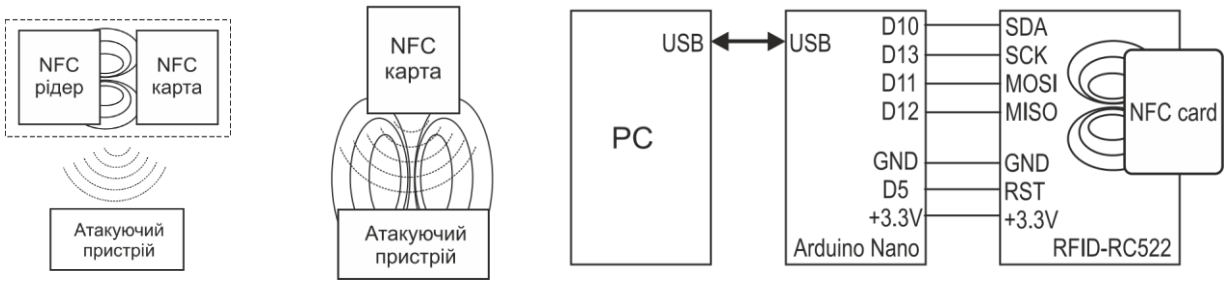


Рисунок 1.4. Схема підслуховування при наявності вищих гармонік.

Таблиця 1.3. Вимірювання гармонік

Спектр	1 гармоника, dBm	2 гармоника, dBm	3 гармоника, dBm
Без відповідного засобу	-32,4	-63,04	-74,07
З відповідним засобом	-32,41	-67,02	-63,07

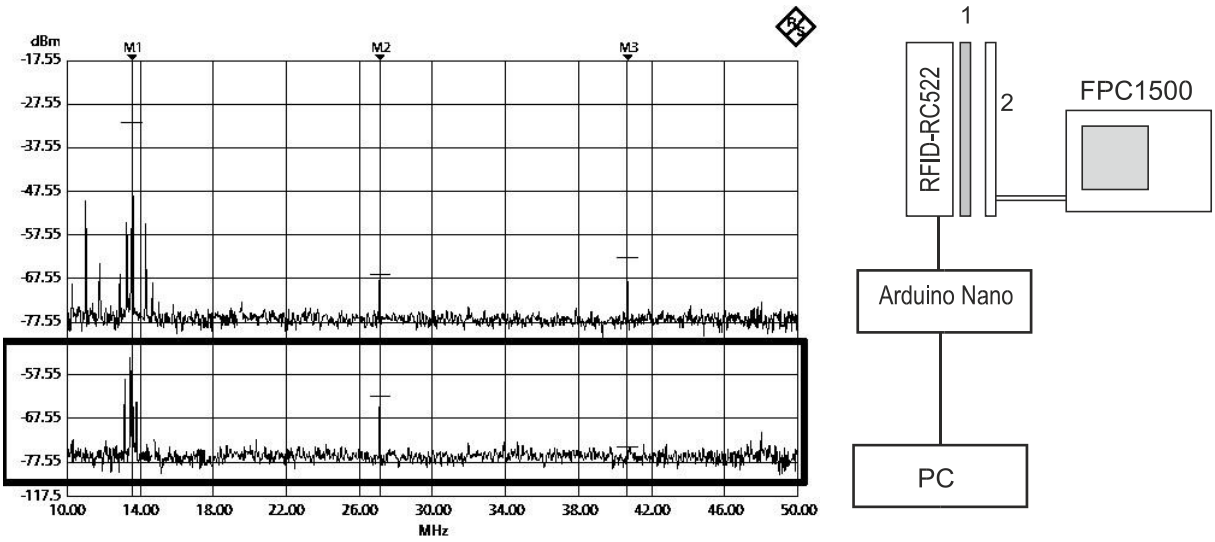


Рисунок 1.5. Спектр сигналу при використанні засобу захисту від несанкціонованого перехоплення мовної інформації.

1.3. Скремблювання

В залежності від способу передачі інформації існують два основних методи закриття інформації. Одним таким методом є аналогове скремблювання, а другим є метод, який здійснює дискретизацію мовної інформації з подальшим її шифруванням. Процес скремблювання - це зміна параметрів мовного сигналу в такий модульований сигнал, щоб при цьому його не можна було розпізнати і не можна при цьому було перехопити і щоб при цьому він займав ту ж саму полосу частот, який займає і початковий сигнал.

В аналогових скремблерах передається інформація у вигляді відкритого мовного повідомлення по каналам зв'язку. Це повідомлення перетворюється по частотній або часовій зоні. На теперішній час існують новітні алгоритми, які забезпечують великий рівень закритості.

На відміну від аналогових скремблерів, цифрові не передають мовний сигнал у відкритому вигляді. Мовні складові кодують в цифровий потік даних, який потім змішується з псевдовипадковою послідовністю, яка породжується ключовим генератором по одному з криптографічних алгоритмів. Отримане повідомлення передається за допомогою модема в канал зв'язку. Приймач, отримавши дане зашифроване повідомлення, здійснює обернене перетворення, що дає можливість отримати відкритий мовний сигнал.

Аналогові скремблери за своїм принципом роботи мають наступні види:

- мовні скремблери найпростіших видів, які базуються на часових та частотних перестановок мовного сигналу (рис.1.6);
- комбіновані мовні скремблери, які базуються на частотно-часових перестановок інтервалів мовного повідомлення.

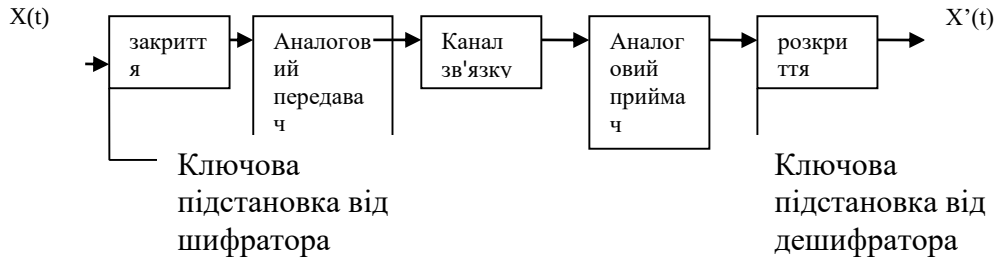


Рисунок 1.6. Простіша схема мовного скремблера

Цифрові засоби закриття мовної інформації бувають широко смугові – аналогово-цифрові перетворювачі (АЦП) та цифрово-аналогові перетворювачі (ЦАП), які мають низьку та середню складність та вузько смугові - аналогово-цифрові перетворювачі (АЦП) та цифрово-аналогові перетворювачі (ЦАП) високої складності.

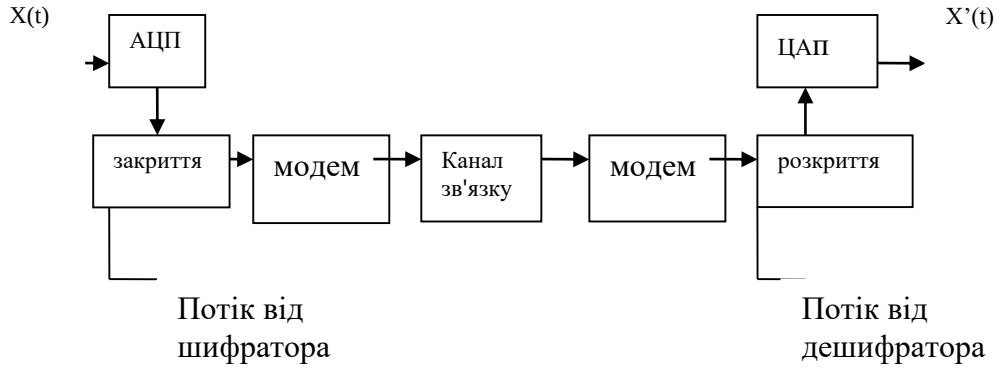


Рисунок 1.7. Схема закриття мовної інформації

При використанні АЦП и ЦАП низької або середньої складності, виникає широко смугова система, а при використанні АЦП та ЦАП високої складності – вузько смугова.

Основними рівнями захисту мовної інформації є тактичний та стратегічний. Тактичний, тобто низький рівень, використовується для захисту інформації від прослуховування сторонніми особами на період, який вимірюється хвилинами, часами або днями. Що стосується стратегічного, тобто високого рівня захисту мовної інформації від перехоплення, використовується тоді, коли висококваліфікованому фахівцю в галузі технічного захисту, необхідно для дешифрування перехопленого повідомлення період часу вимірюється в місяцях або роках. Варто відмітити, що параметр, який носить назву якість відновлення мовної

інформації є умовним. Даний параметр характеризує здібність пізнати абонента та можливість розібрати сигнал, який приймається.

Вплив скремлерів на характеристики радіостанцій має велику залежність в якості їх чутливості. Це пов'язано з тим, що зменшується співвідношення f/η, де f - сигнал, а η- шум на вході приймача. Крім того, перетворення сигналів, які пов'язані з параметрами, які є функціями від часу, необхідно визначити деякий інтервал часу для синхронізації таймерних приладів, які присутні як стороною, що передає інформацію так і стороною, яка її приймає. Даний процес є обов'язковим і він створює ефект запізнення між вмиканням команди передача радіостанції і початком передачі мовної інформації.

При удосконаленні систем захисту інформації, розробникам відповідного обладнання необхідно створювати новації. Однак, ці новації призводять до додаткових параметрів, які характеризують більш глибокі пошкодження спектрів сигналів, а також створювати біль складні залежності параметрів від часу, які характеризують радіостанції.

Користувачі радіостанцій постійно шукають технічний рівень скремлерів. Скремблери мають не великі розміри мікроелектронних вузлів, які встановлюються всередині корпусу радіостанції.

1.4. Скремблюючі технічні засоби

Достатня кількість існуючих моделей скремблерів здійснюють реалізацію частотної інверсії сигналу. Однак за параметрами вони мало чим відрізняються один від одного. Одними з перших, які з'явились на ринку України появились були моделі скремлерів компанії Selectone. Це в першу чергу скремблери ST-20 , а пізніше з'явилась модель ST-022. Діапазон частот моделі ST-20 від 300Гц до 2400 Гц. Дана модель забезпечує інверсію сигналу відносно восьми можливих номіналів частот в діапазоні від 2,6 Кгц до 3,7 Кгц і при цьому частота інверсії встановлюється за допомогою програмного забезпечення. Також дана модель працює в діапазоні напруг живлення від 5,2 В до 18 В, при цьому струм споживання

не перевищує 4 мА. Крім того, діапазон робочих температур коливається від - 30 до +70 С. Сам розмір корпусу прилада – 20.96 на 38.20 на 3. 81 мм.

Модель ST-022 відрізняється від ST-20 тим, що має більш розширений діапазон частот - до 3000 Гц та напруга живлення досягає 24 В, і при цьому має більш менші розміри – 20 на 25 на 4 мм. Вартість скремблерів компанії Selectone від сорка до шістдесят долларів США.

Існуючі моделі скремблерів компанії Transcrypt SC20-400 і SC20-401 мають характеристики такі, як і ST-20 та ST-022. Мовний діапазон частот, чотирир варіанта частоти інверсії, напруга живлення від 5 В до 12 В, струм споживання - 3 мА, діапазон робочих температур - від - 20 до +60 С, при цьому розміри – 39 на 21 на 4 мм. Вартість скремблерів в околі п'ятдесят доларів США.

Група частотних інверторів компанії Midian дає широкий спектр в залежності від тих засобів, якими володіє споживач. Моделі VPU-1 и VPU-8 використовуються в дуплексних радіостанціях і в залежності від модифікації мають різні частоти інверсії. Вони відрізняються один від одного тільки розмірами. Прилад VPU-2 має 15 частот інверсії, які задаються за допомогою програмного забезпечення, а прилад VPU-7 має одну фіксовану частоту інверсії. Дані скремблери мають дуже маленькі розміри і забезпечують тільки симплексний режим функціонування. Вартість скремблерів від 35 долларів США до 70 долларів США. Параметри цих скремблерів представлено в таблиці 1.4.

Таблиця 1.4. Режими функціонування скремлерів

Параметри	**ST-20**	**ST-022**	**SC20-400, SC20-401**	**VPU-1**	**VPU-2**	**VPU-7**	**VPU-8**	**KVS-1**
Компанія-виробник	Selectone	Selectone	Transcrypt	Midian	Midian	Midian	Midian	Kenwood
Режим функціонуван	симплекс	симплекс	симплекс	дуплекс	симплекс	симплекс	дуплекс	симплекс

ня, (симплекс дуплекс)								
Діапазон частот, Гц	300-2400	300-3000	300-2400	300-2600	300-2600	300-2600	300-2600	300-2400
Кількість частот інверсії	8	8	4	3	15	15	1	8
Діапазон напруг живлення, В	5,2-18	5,5 -24	5 -12	5,5-24	5,5 -24	5,5-24	6,5-24	5-12
Струм споживання, мА	4	4,5	3	5	3	3	3	4
Діапазон робочих температур, С	-30...+70	-30...+60	-20...+60	30...+60	30...+60	30...+60	-30...+60	30...+60
Розміри, мм	21x38x4	20x25x4	39x21x4	36x24x6	27x13x4	25x20x6	30x15x6	35x20x5
Вартість в долларах США	40	60	50	70	60	45	35	80

Існує група скремблерів, які реалізують більш складний принцип перетворення сигналу, а саме смугові зсувні інвертори, які були розроблені НВП “ЛУЧ”. Мікро системи 03ІЛ001, 03ІЛ002, 03ІЛ003А, 03ІЛ004А, 03ІЛ005А працюють по принципу розпадання мовного спектру сигналу на дві складові-складова низької частоти та складова високої частоти. Кожна з цих складових обмежується в околі власних середніх частот. Обидві складові працюють в діапазоні мовних частот від 300 Гц до 3400 Гц, при цьому вони мають маленькі

розміри та малий струм споживання – одиниці міліампер. Також дане обладнання дає можливість змінювати частоти розбиття смуги мовного сигналу 03ІЛ014 -1 , 03ІЛ015 - 2, 03ІЛ016А - 3, 03ІЛ017 та 03ІЛ018А - 4, 03ІЛ011 та 03ІЛ012 - 32 . Всі вказані структури працюють від джерела живлення з напругою +5 В, за виннятком 03ІЛ001, яка спроможна працювати в діапазоні від 6В до 13В

Розглянуті скремблери дають можливість значно підвищувати ступінь закриття інформації. Крім того, данні скремблери дають можливість спостерігати існування розуміння мови особами, які здійснюють несанкціоноване прослуховування, не більше ніж на 10 % . Крім того, при цьому зберігається висока якість мовної інформації між особами, які ведуть телефонні перемовини.

Дані скремблери мають маленькі габарити – 15 на 15 на 6,5 мм і встановлюються всередині корпусу довільних радіостанцій. Вартість таких скремблерів з урахванням їх монтажу становлять від 50 долларів США до 80 долларів .

Найбільш популярними в Україні обладнання класу смугових скремблерів є скремблер типу CVS-240 марки Standard, який встановлюється в засіб радіозв'язку, виробником якого є концерн Marantz. Дане обладнання працює за принципом розділення смуги мовного сигналу на чотири складові самого діапазону та здісненні перестановок елементів множини, яка складається з цих складових. Код перестановки здійснюється за допомогою спеціальних контактів. Розглянутий скремблер дає можливість отримувати високий ступінь закриття інформації, яку можна порівняти зі смуговим зсувним інвертором.

Існують крім розглянутих скремблерів і динамічні скремблери, виробником яких є компанія Tramscrypt. По принципу своєї роботи вони аналогічні частотним інверторам з можливістю змінювати частоти інверсії сигналу з часом. Він має шістнадцять можливих частот інверсії. Різні моделі скремблерів даної компанії відрізняються між собою швидкістю зміни варіативного параметру: від одного разу в секунду для SC20-406J та SC20-410 до тисячі разів в секунду для

SC20-460 та SC20-500. Характеристики скремблерів представлено в таблиці 1.5. Крім спроможності самостійно перетворювати сигнали, існують додаткові модулі Transcrypt, які реалізують додаткові функції такі, як вибіркові та аварійні виклики, селективний доступ, спроможність дистанційно керувати радіостанцією по каналам радіозв'язку. Дані модулі можна встановлювати в радіостанціях виробників різних компаній, наприклад таких як Motorola, Standard, Johnson. При цьому скремблери гарантовано працюють в діапазоні робочих температур від -30 градусів Цельсія до +60 градусів Цельсія

Таблиця 1.5. Характеристики скремблерів

Характеристики	**SC20-406J**	**SC20-410**	**SC20-430**	**SC20-460**	**SC20-480**	**SC20 500**
Кількість зміни частоти інверсії за 1 с	1	1	200	1000	800	1000
Довжина ключової послідовності	10 7	10 7	5x10 7	10 11	5x10 12	10 24
Струм споживання мА	5	8	8	7	7	7
Розміри, мм	33x23x5	33x23x5	33x23x5	44x23x5	44x23x5	41x25x5
Вартість в долларах США	110	120	240	-	-	-

Розглянуті скремблери забезпечують високий рівень закриття інформації. Це підштовхує користувачів засобів радіозв'язку купувати модулі саме компанії Transcrypt, незважаючи на їх достатньо не низьку ціну. Однак існує обмеження: Незважаючи на те, що псевдовипадкова послідовність зміни частоти розбиття смуги сигналу, число значень варіативного параметру не перевищує шістнадцяти, що в свою чергу не забезпечує необхідного закриття. Дослідження засобів радіозв'язку, в які було вмонтовано скремблери моделі SC20-410, прослуховування

перемовин за допомогою радіостанцій, в яких було встановлено частотний інвертор з фіксованою частотою інверсії сигналу, можна було розібрати від 50% до 80 % інформації, що передавалась.

Сам принцип функціонування скремблерів потребує синхронізації радіо засобів, які здійснюють передачу та прийом сигналу. Це вимушує оператора робити паузу після натиснення кнопки передати на радіостанції. Для складових компанії Transcrypt час синхронізації складає від 300 мс до 500 мс.

Існує інша група динамічних скремблерів, а саме MOT-TVS/VPU-10, виробником яких є компанія Midian. Характеристики скремблера VPU-10 ідентичні характеристикам SC20-406J та SC20-410 і при цьому зміна частоти інверсії здійснюється оди раз в секунду. Скремблери TVS-1 та TVS-2 мають властивість швидкої дії і при цьому існують додаткові сервісні функції такі, які мають і скремблери компанії Transcrypt.

Відчизняними розробниками реалізовано скремблери, які здійснюють часові перетворення сигналів. Дане обладнання має форму відкритого малогабаритного модуля, який має керамічну основу і використовується спеціальний дельта-кодер та дельта-декодер, засіб шифрування та реєстри пам'яті. Мовний сигнал, який надходить на вхід, перетворюється кодером адаптивного дельта-кодера в цифровий вид та при цьому відбувається запис в пам'ять у вигляді послідовності мовних кластерів. Зі тридцяти двох кластерів формується кадр. У відповідності інформації, яка записана у вигляді коду, відповідний засіб шифрування створює псевдовипадкову послідовність перестановок цих кластерів в кадрі. При завершення часових перетворень декодер адаптивного дельта кодера відновлює на виході скремблера початковий мовний сигнал всередині кожного кластера. В режимі прийому сигналу завдяки синхронізації здійснюється кадрова синхронізація з одночасним оберненим перетворенням для відновлення початкового сигналу.

Завдяки використанню такого модуля споживання енергії дорівнює 75 мВт, що в свою чергу забезпечує відповідну якість мовного сигналу, що відновлюється, а також при цьому можливість розібрати сигнал становить від трьох до п'яти відсотків. Розміри даного скремблера становлять сорок два на п'ятнадцят на три міліметри.

Висновки до розділу 1

Із вищевикладеного можна зробити висновок, що при використанні засобів радіозв'язку є достатньо великий вибір засобів захисту мовної інформації для власних радіостанцій та локальних мереж радіозв'язку.

Також при розгляданні відповідного засобу, необхідно враховувати те, що аналогові скремблери не дають можливість забезпечити захист мовної інформації від несанкціонованого прослуховування перемовин. Крім того грошові витрати осіб, які зацікавлені в несанкціонованому перехопленні мовної інформації, не є значно великими, можна сказати що вони дуже малі.

Щоб надійно захистити мовну інформацію, яка передається необхідно використовувати такі радіостанції, які спроможні передавти сигна в цифровій формі і з певним визначеним крипто алгоритмом.

2. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ РАДІОЗВ'ЯЗКУ

2.1. Класифікація методів скремблювання

При використанні засобів передачі інформації в першу чергу необхідно обмежити доступ сторонніх осіб до ОІД, де відбуваються перемовини.

На теперішній час самим надійним захистом є такі системи зв'язку, які дають можливість перетворювати аналогові сигнали в цифрові з подальшим використанням криптографічних перетворень, які дають можливість шифрувати інформацію, яка передається, а потім здійснювати процес дешифрування.

Сучасні системи конвенціонального та транкінкого радіозв'язку, які використовуються в вітчизняних системах не досягли широкого використання в технології цифрової передачі інформації. Це пов'язано з тим, що вартість цифрових систем значно вища, за вартість аналогових.

Однак, доступ до конфіденційної інформації потребує свого попиту. Для достатньо великої кількості споживачів поняття гарантованого захисту конфіденційної інформації не є суттєвим і вони залишаються на тому, що достатньо їм, щоб інформація, яка прослуховується є незрозумілою. В цьому випадку, використання аналогових скремблерів є оптимальним як економічно так і технічно.

2.1.1. Аналогове скремблювання

Принцип аналогового скремблювання полягає в перетворенні вхідного мовного сигналу, метою якого є мінімізація ознак мовного повідомлення. Іншими словами це претворення повинно бути здійснено таким чином, щоб слова, які передаються, не можливо було б розібрати. Однак, даний сигнал повинен займати таку ж саму полосу частот спектру, як і вхідний сигнал. Необхідною і достатньою умовою такого принципу перетворення є обов'язкова спроможність оберненого перетворення такого, щоб можна було б в повному об'ємі відновити мовний сигнал на тій стороні, що його приймає.

Такими аналоговими технічними засобами, які забезпечують захист інформації і є скремблери. Вони також носять назву маскуватори мови. Однак, при використанні скремблерів для закриття мовної інформації все ж таки присутні ознаки частково відкритого мовного повідомлення.

Незважаючи на те, що аналогові методи захисту інформації не дають достатню ступінь закриття мовних сигналів, на відміну цифровим, вони достатньо прості, не є дорогими і мають властивість високої якості відновлення мовного сигналу.

Сам процес скремблювання можливий по одному з трьох параметрів: параметром є амплітуда, або частота, або часу. При використанні мобільних

радіостанцій широке використання отримало перетворення сигналів по частоті, або часі, або комбінації цих двох параметрів. Так як, при передачі сигнала, який є носієм мовного повідомлення постійно присутні завади, то при використанні амплітудного перетворення сигналу виникають великі трудності по відновленню мовного повідомлення. З цих причин аиплітудне перетворення в сучасних системах радіозв'язку не використовується.

На рисунку 1.8. представлено найпростішу електронну схему аналогового методу, яким є скремблер.

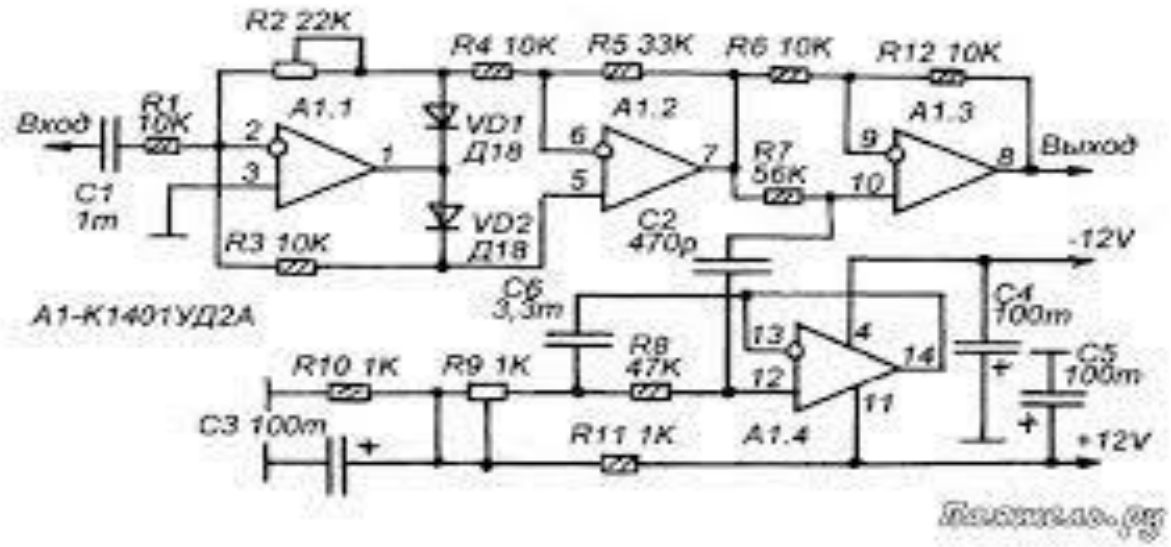


Рисунок 1.8. Електронна схема скремблера.

Крім того, існують методи шифрування голосу, а також мови. На рисунку 1.9 представлено електронну схему скремблера для шифрування голосу.

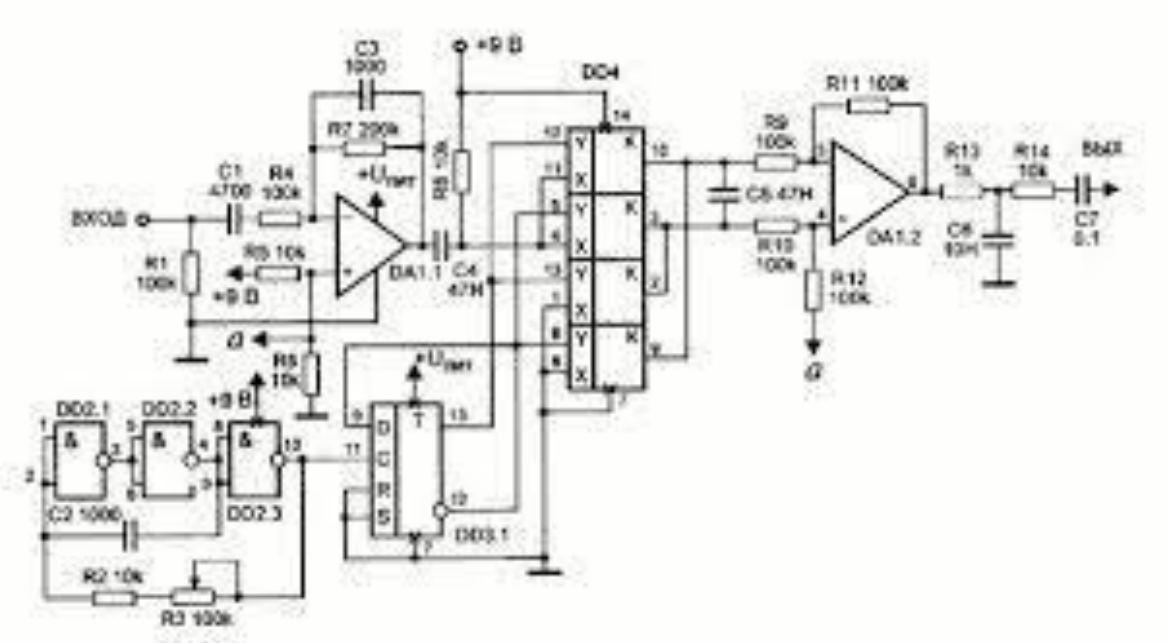


Рисунок 1.9. Схема скремблера на мікросхемах для шифрування голосу

На рисунку 1.10 представлено електронну схему скремблера шифрування мови.

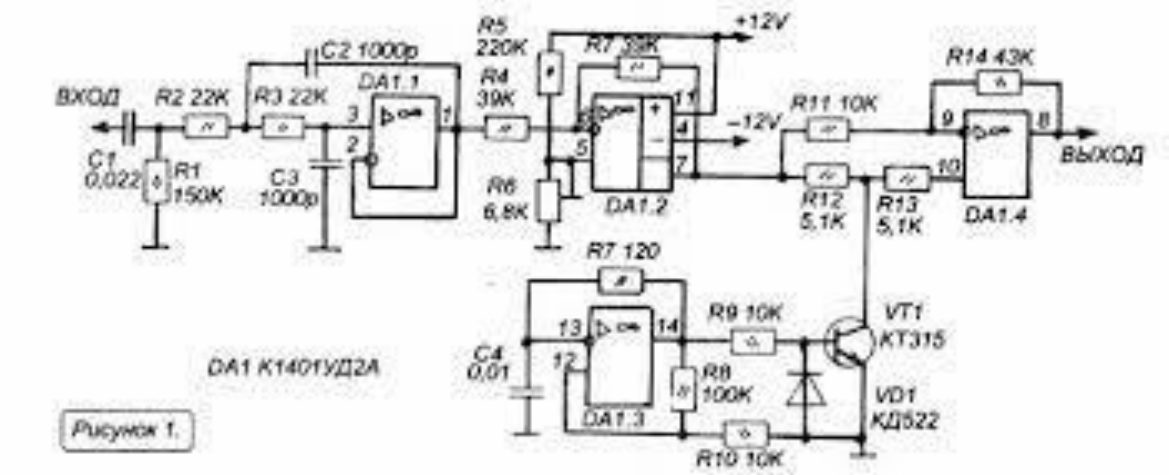


Рисунок 1.10. Схема скремблера на мікросхемах для шифрування мови

Найголовнішою технічною характеристикою аналогових скремблерів є значення рівня закриття інформації, гранична розбірливість та показник якості відновлення сигналу.

Однак серед вказаних трьох характеристик, найбільш важливим параметром скремблера для системи захисту інформації в каналах зв'язку, є значення рівня закриття інформації. Однак, так як на теперішній час не створено зрозумілих стандартів та правил поняття закриття інформації, то для аналогових скремблерів це поняття є умовним. На відміну від аналогових методів, в цифрових системах передачі інформації поняття значення рівня закриття інформації є криптографічна стійкість передачі інформації.

І все ж таки, в якості критерія значення рівня закриття інформації в порівнянні з різними видами мобільного радіозв'язку з аналоговим скремблюванням варто використовувати мінімальну кількість основних характеристик та певна кількість доступних ключів скремблера.

Під основною характеристикою аналогового скремблера в загальному розглядається інформативний параметр перетворення мовного сигналу, значення якого слід задавати для спроможності здійснювати обернене перетворення сигналу на тій стороні, яка приймає цей сигнал.

Ключом аналогового скремблера, що для цифрових аналогом є шифрування, розуміють детермінований скритий від сторонніх стан мінімальних характеристик перетворення мовного сигналу. Кількість ключів скремблера визначається множиною, елементами якої є всі можливі значення ключа. Для скремблерів з одним ключовою характеристикою ця кількість визначається кількістю існуючих станів цієї характеристики. Якщо скремблери мають декілька ключових характеристик, то числом можливих комбінацій значень цих характеристик є за правилом множення в комбінаториці попарний добуток станів.

Показний якості відновлення сигналу обчислюється за вразливістю сигналу при його частотних або/і часових перетвореннях. В дійсності цей параметр є індикатором для розбірливості та в пізнаванні мови, яка відновлюється.

Дійсним інтервалом значення показника якості відновлення мовної інформації приймачем вважається такий інтервал, що при довільному значенні

показника якості, який належить цьому інтервалу, особа, яка є учасником перемовин, може розібрати мовну інформацію, яка до нього надходить.

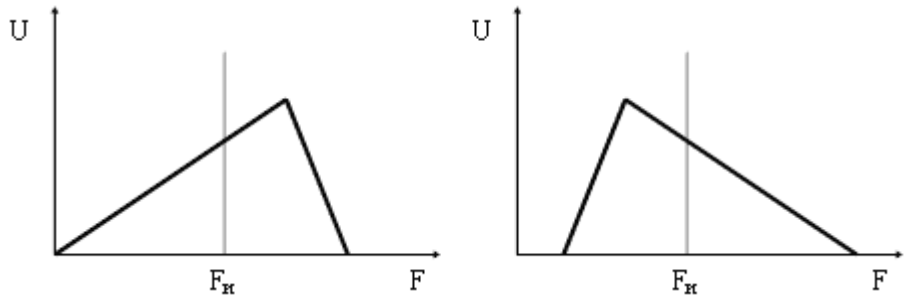
Прилади, які дають такий показник якості називаються частотними інверторами. При достовірній реалізації вони не погіршують розбірливість та можливість впізнати мову. Якщо використовувати більш складні методи частотних перетворень, то виникає проблема пошкодження в мовний сигнал. Що стосується часових перетворень, то для досягнення достовірного значення якості відновлення мови виникає проблема складності в обробці сигналу в приймачі.

Параметр, який носить назву граничної розбірливості, уявляє собою значення відсотка відновлених фрагментів скрембльованого мовного сигналу при прослуховуванні перемовин з використанням ультра коротких хвильових приймачів чи радіостанцій в яких відсутні аналогові скремблери.

Сучасні аналогові скремблери зберігають остаточну розбірливість. Якщо мовний сигнал прослуховується і при цьому система зв'язку захищена скремблером, інформація зберігається в темпі мови, але паузи визначаються. При елементарних методах захисту, досвідчений фахівець має можливість розібрати від десяти до п'ятдесяти відсотків інформації, що передається.

2.1.2. Частотне перетворення

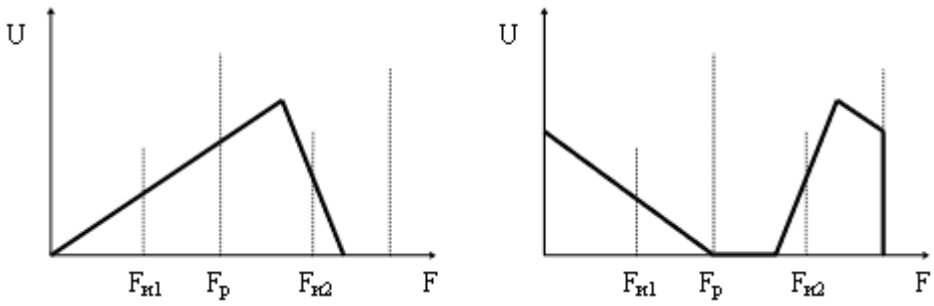
Принцип частотного перетворення або частотної інверсії полягає в тому, що частотна смуга сигналу обертається навколо деякого середнього значення частоти $F_н$. На рисунку 1.11 графічно показано це перетворення. На рисунку а) зображено вхідний спектр сигналу, а на рисунку б) показано спектр сигналу після його інверсії.



а) б)

Рис. 1.11. Принцип роботи частотного інвертора мовного сигналу.

Існує більш складний спосіб по відношенню до частотної інверсії, який полягає в перетворенні сигналу, який здійснює скремблер, який розбиває смуги мовного сигналу на під діапазони з частотною інверсією сигналу в кожному з цих під діапазонів, так званий смуго зсувний інвертор. На практиці здійснюється розбиття смуги на два під діапазони. Фізичний принцип такого двох під діапазонного частотного перетворення показано на рис.1.12. На рисунку а) показано вхідний спектр сигналу, а на рисунку б) показано спектр сигналу після перетворення. В даному випадку F_p - частота розбиття спектру сигналу, а F_{u1}, F_{u2} - частоти інверсії першого та другого під діапазонів відповідно.



а) б)

Рис. 1.12. Принцип роботи смугового зсувного інвертора мовного сигналу при розбитті спектру сигналу на два під діапазони.

В смугових скремблерах розбиття смуги мовного сигналу здійснюється на декілька під діапазонів з частотними перестановками цих під діапазонів. На

рисунку 1.13 показано принцип реалізації смугового скремблера з розбиттям спектру сигналу на чотири смуги.

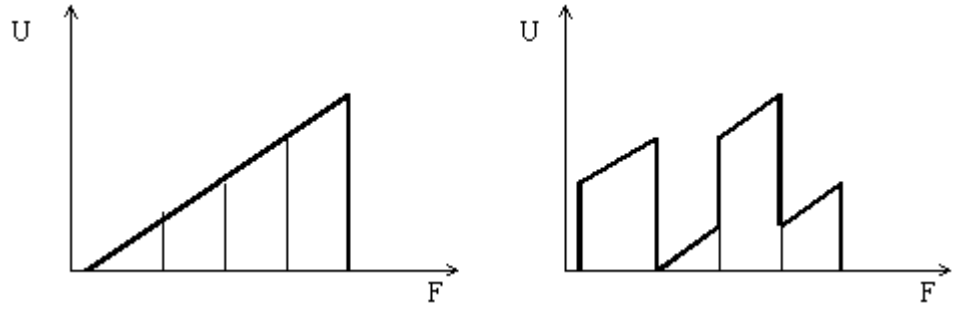


Рис. 1.13. Принцип реалізації чотирьох смугового скремблера.

Реалізація смугового спектру здійснюється за допомого швидкого перетворення Фур'є (ШПФ). Суть цього перетворення полягає в тому, що сигнал $x(n)$ розбивається на дві точкові послідовності рівної довжини, тобто складаються з відліків з парними та непарними номерами відповідно. Математично це записується наступним чином

$$C(k) = \frac{1}{M} \sum_{n}^{0.5M-1} x(n) w_M^{nk} + \frac{1}{M} \sum_{n}^{0.5M-1} x(n) w_M^{nk} . \qquad (1.1)$$

Замінюючи індекси сумування на $n = 2p$- при парному nі на $n = 2p+1$- при непарному n. В результаті отрмаємо

$$C(k) = \frac{1}{M} \sum_{p=0}^{0.5M-1} x(2p)\left(w_M^2\right)^{pk} + \frac{1}{M} w_M^k \sum_{p=0}^{0.5M-1} x(2p+1)\left(w_M^2\right)^{pk} . \qquad (1.2)$$

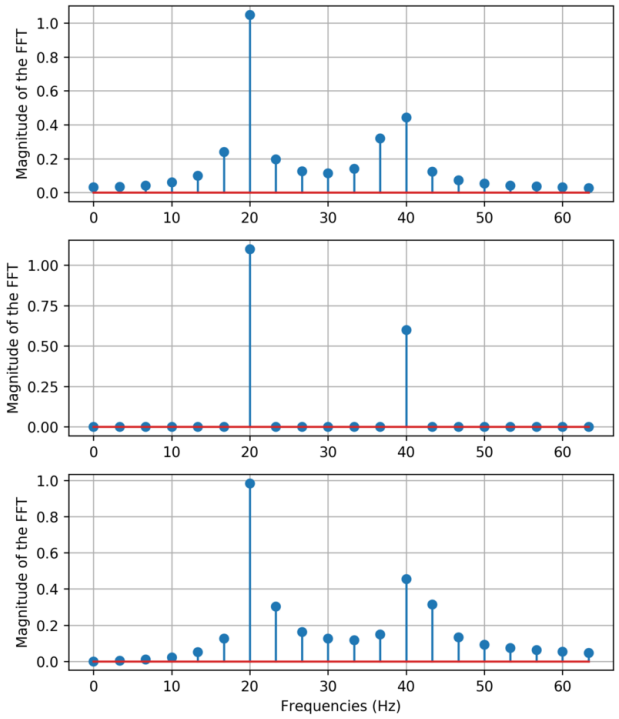


Рисунок 1.14. Розбиття сигналу на дві точкові послідовності

Нижче представлено обчислення модуля спектру дійсного масиву чисел на основі реалізації ШПФ на С++.

```
// MHbl - масив, дані якого аналізуються, MWl - довжина массиву повинна бути
кратна степені двійки.
// RPwl - масив отриманих значень, MFT - довжина масиву = MWl .

const double 2*Pi = 6.283185307179586;

void FFTAnalysis(double *MHb1, double *RPw1, int MW1, int MFT) {
  int i, j, n, m, Mmax, Istp;
  double Tmpr, Tmpi, Wtmp, Theta;
  double Wpr, Wpi, Wr, Wi;
  double *Tmvl;

  n = Nvl * 2; RPw1 = new double[n];

  for (i = 0; i < n; i+=2) {
   RPw1l[i] = 0;
   RPw1[i+1] = MW1[i/2];
  }

  i = 1; j = 1;
  while (i < n) {
    if (j > i) {
      Tmpr = Tmvl[i]; Tmvl[i] = Tmvl[j]; Tmvl[j] = Tmpr;
      Tmpr = Tmvl[i+1]; Tmvl[i+1] = Tmvl[j+1]; Tmvl[j+1] = Tmpr;
    }
    i = i + 2; m = Nvl;
    while ((m >= 2) && (j > m)) {
```

```
      j = j - m; m = m >> 1;
    }
    j = j + m;
  }

  Mmax = 2;
  while (n > Mmax) {
    Theta = -TwoPi / Mmax; Wpi = sin(Theta);
    Wtmp = sin(Theta / 2); Wpr = Wtmp * Wtmp * 2;
    Istp = Mmax * 2; Wr = 1; Wi = 0; m = 1;

    while (m < Mmax) {
      i = m; m = m + 2; Tmpr = Wr; Tmpi = Wi;
      Wr = Wr - Tmpr * Wpr - Tmpi * Wpi;
      Wi = Wi + Tmpr * Wpi - Tmpi * Wpr;

      while (i < n) {
        j = i + Mmax;
        Tmpr = Wr * Tmvl[j] - Wi * Tmvl[j-1];
        Tmpi = Wi * Tmvl[j] + Wr * Tmvl[j-1];

        Tmvl[j] = Tmvl[i] - Tmpr; Tmvl[j-1] = Tmvl[i-1] - Tmpi;
        Tmvl[i] = Tmvl[i] + Tmpr; Tmvl[i-1] = Tmvl[i-1] + Tmpi;
        i = i + Istp;
      }
    }

    Mmax = Istp;
  }

  for (i = 0; i < Nft; i++) {
    j = i * 2; FTvl[i] = 2*sqrt(pow(Tmvl[j],2) + pow(Tmvl[j+1],2))/Nvl;
  }

  delete []Tmvl;
}
```

На рисунку 1.15 представлено графічну реалізацію даного програмного алгоритму.

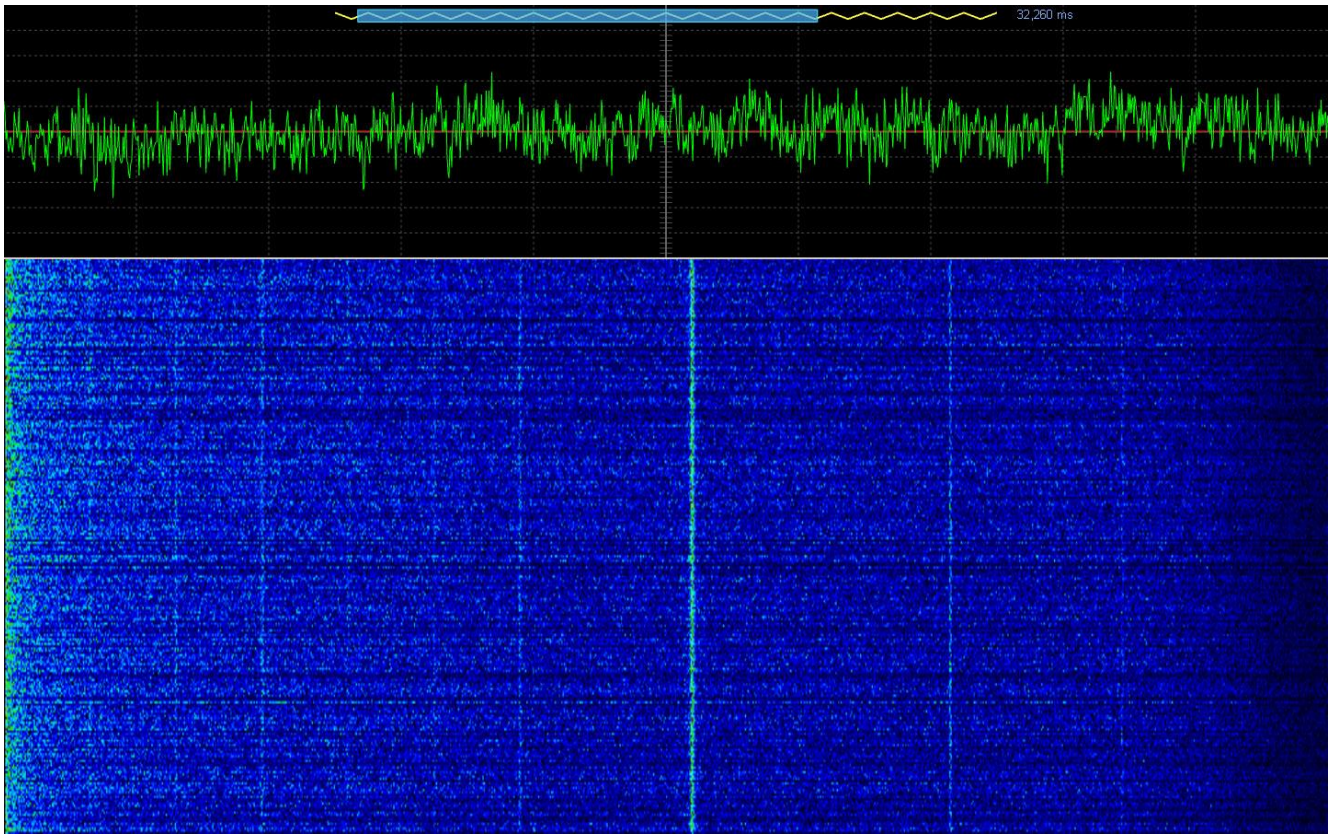


Рисунок 1.15. Графічна реалізація швидкого перетворення Фур'є

В такому скремблері на передавачу здійснюється пряме ШПФ, частотна перестановка смуг, а потім здійснюється обернене ШПФ. Сигнал поступає на приймач та здійснюється відповідне перетворення з оберненою частотною перестановкою смуг. В скремблерах, яких реалізовано ШПФ існує можливість досягти достатньо високого ступеня захисту інформації за рахунок збільшення кількості смуг, які перемішуються. Однак, на практиці цей принцип скремблювання в мобільній радіостанції використовується достатньо не часто. Це пов'язано зі складною технічною реалізацією. І ще одним недоліком скремблеру з ШПФ є те, що в каналі зв'язку виникає ефект запізнення.

На рисунку 1.15 показано схематичну реалізацію ШПФ

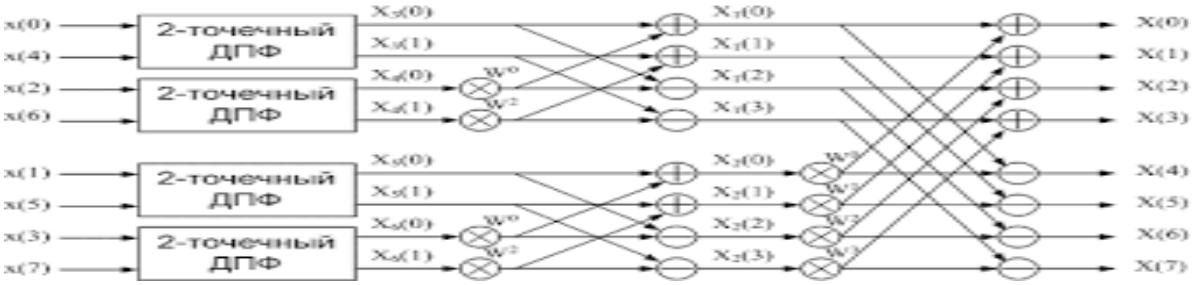


Рисунок 1.16. Схематична реалізація швидкого перетворення Фур'є.

2.1.3. Перетворення радіосигналів в часі

Найпростішим способом здійснення часового перетворення є інверсія часу. Суть даного перетворення полягає в тому, що початковий сигнал розділяється на послідовність часових кластерів та кожний з цих кластерів обернено передається в часі - від кінця до початку. Принцип роботи інвертора часу представлено на рисунку 1.17.

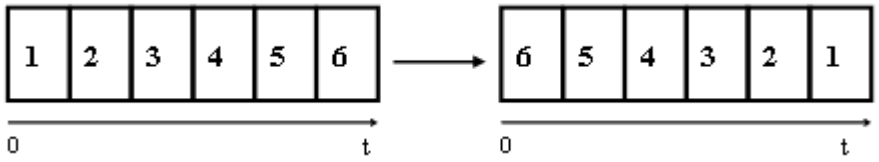


Рис. 1.17. Принцип роботи інвертора часу.

В скремблері з часовим перетворенням мовний сигнал ділиться на часові фрагменти. Кожному з цих фрагментів в свою чергу ставиться у відповідність свій кластер, а потім здійснюється перестановка кластерів мовного сигналу. Принцип роботи такого скремблера з фіксованим вікном та числом часових кластерів в фрагменті, що дорівнює шести, показано на рис.1.18.

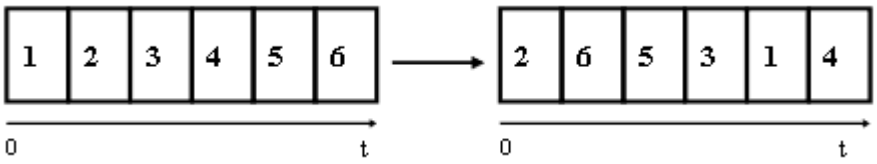


Рис. 1.18. Принцип роботи скремблера з часовими перестановками.

Перейдемо до математичного опису перетворення сигналів. Носієм інформації як правило є аналогові сигналл, які будемо позначати $x(t)$. В сучасних умовах з розвитком цифрової апаратури аналогові сигнали перетворюються в цифрові за допомогою аналогово-цифрових перетворювачів (АЦП). Фрагменти сигналів розбиваються на однакові часові інтервали T, та за допомогою ШПФ формується лінійний спектр кластерного сигналу при умові, що відповідний фрагмент повторюється нескінченне число разів з періодом T.

При захисті мовної інформації виявлення системи прослуховування, виникає необхідність здійснювати сильні завади сигналів, які проходять метрологічне

вимірювання у вигляді коливань в яких частота або монотонно зростає, або монотонно спадає. Ця частота є носієм мовного сигналу. В цьому випадку виникає необхідність змінювати масштаб часу не лінійно сигналу, який підлягає регістації. Флуктуації масштабу часу дають можливості визначати максимум енергії кластерного сигналу в деякій визначеній області частот.

Нехай задано масив E_{1i} складових кластерного сигналу з частотною модуляцією

$$E_{1i} = \cos\left((\omega_0 - kt_i)t_i\right), \tag{1.3}$$

де ω_0 - початкова частота, k - коефіцієнт модуляції. Вираз (1.3) перепишемо наступним чином

$$E_{1i} = \cos\left(\omega_0\left(t_i - \frac{kt_i^2}{\omega_0}\right)\right). \tag{1.4}$$

Права частина виразу (1.4) уявляє собою квадратну функцію від часу t. Ввівши заміну $tn_i = t_i - \frac{kt_i^2}{\omega_0}$. Тоді (1.4) можна записати інакше

$$E_{1i} = \cos(\omega_0 tn_i). \tag{1.5}$$

Представлене перетворення початкового сигналу $x(t)$ в масив $E_{1i}(t_i)$ і в масив $E_{1i}(n_i)$ дає можливість отримати не модульований за частотою радіоімпульс, спектр якого буде відрізнятися від спектру початкового сигналу (1.3). Щоб здійснити порівняння спектрів початкового сигналу (1.3) і и перетвореного в часі (1.5) сигналів обчислимо спектри дискретного сигналу для обох систем часу. Для часу t

$$S_1(\omega) = \int_0^T E_1(t)e^{-j\omega t}dt. \tag{1.6}$$

Для обчислення значень функції спектральної щільності в системі виміру часу tn_i, з урахування того, що $dtn_i = tn_{i+1} - tn_i$, визначимо інтегральну суму для обчислення спектральної щільності $S_2(\omega)$ в системі виміру tn_i з нелінійним диференціалом dtn

$$S_2(\omega) = \sum_{i=1}^{N} \left(E_{1i} e^{-j\omega tn_i} dtn_i \right). \qquad (1.7)$$

На рисунку 1.19 представлено графіки абсолютних величин щільність спектрів $S_1(\omega)$ і $S_2(\omega)$. Аналіз даних спектрів дає можливість зробити висновок про те, що запропоноване перетворення в часі суттєво збільшує енергію в зоні початкової частоти коливань ω_0.

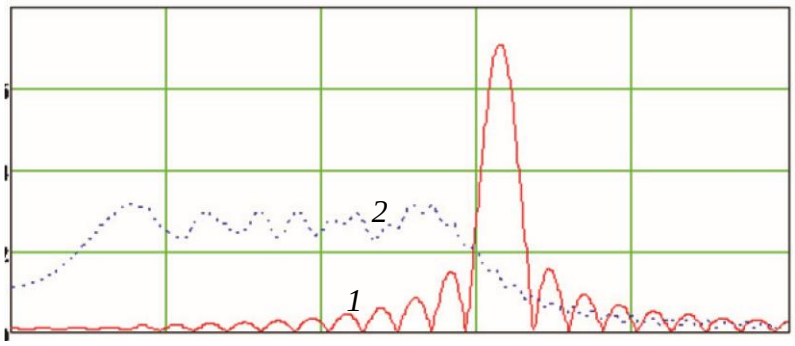


Рис. 1.19. Спектри частотної модуляції сигналів в системах часу t і tn_i: 1- $|S_1(\omega)|$, 2 - $|S_2(\omega)|$.

При наявності завад збільшення енергії в зоні початкової частоти відбувається збільшення можливості виявлення початкових коливань $E_{1i}(t)$ в частотній зоні, а також є можливість вимірювати спектральним методом значення ω_0. Представлення (1.7) має місце при $\omega_0 < \frac{\pi}{10}$.

Захист мовної інформації з використанням часового перетворення полягає в методиці обчислення спектру кластерного сигналу, при перетворенні масштабу часу фіксованого сигналу, де використовуються ті самі значення сигналу дискретних значень N сигналу $x(t)$, але при цьому результати цільової часової згортки зсуваються на моменти часу tn_i, але при цьому довжина дискретного інтервалу стає не рівномірним.

Задача визначення спектру фрагменту сигналу з використанням нерівномірності дискретного складається з трьох етапів:

– представляється апроксимація фрагменту сигналу у вигляді полінома в аналітичному вигляді з нерівномірним дискретним інтервалом та заданою похибкою;

– методом невизначених коефіцієнтів обчислюються параметри многочлена з спектрального перетворення;

– отримане представлення спектрального перетворення дає можливість отримати масив вибірки зі спектру апроксимуючого многочленом фрагменту сигналу.

Для того, щоб розкласти функцію в ряд Фур'є, яка представлена у вигляді одномірного масиву пари $(N;t)$ з використанням спектрального методу, на першому кроці будується многочлен, який апроксимує функцію $N(t)$, для якої виконується умова $N_0 = N(t_0),\ldots, N_i = N(t_i)$, $i = \overline{0,...n}$, і так як дискретні інтервали часу не рівномірні, то $t_1 - t_0 \neq t_2 - t_1 \neq ... \neq t_n - t_{n-1}$. Будемо використовувати інтерполяційну формулу Ньютона для аргументів, які один від одного відрізняються на різні значення.

$$x(t) = N_0 + \Delta_{11}(t - t_0) + \Delta_{21}(t - t_1)(t - t_0) + ... + \Delta_{n1}\prod_{i=0}^{n-1}(t - t_i), \text{ або}$$

$$x(t) = N_0 + \sum_{k=1}^{n}\left(\Delta_{k1}\prod_{i=0}^{k-1}(t - t_i)\right), \tag{1.8}$$

де Δ_{k1}, $k = 1,2,...,n$ - розділені різниці k-го порядку, які визначаються наступним чином

$$\Delta_{1i} = \frac{N(t_i) - N(t_{i-1})}{t_i - t_{i-1}}. \tag{1.9}$$

З використанням (1.9), обчислюються роздільні різниці Δ_{2i}, $i = 1,2,...,n-1$, які мають вид

$$\Delta_{2i} = \frac{\Delta_{1i+1} - \Delta_{1i}}{t_{i+1} - t_i}. \tag{1.10}$$

З використанням (1.10), обчислюємо роздільну різницю Δ_{3i}, $i = 1,2,...,n-1$, які мають наступний вид

$$\Delta_{3i} = \frac{\Delta_{2i+1} - \Delta_{2i}}{t_{i+1} - t_i}. \qquad (1.11)$$

Остання роздільна різниця n - го порядку буде мати вид

$$\Delta_{ni} = \frac{\Delta_{(n-1)2} - \Delta_{(n-1)1}}{t_n - t_0}. \qquad (1.12)$$

На рисунку 1.20 представлено блок-схему алгоритму обчислення двовимірного масиву Δ_{i1}.

Рисунок 1.20. Блок-схема обчислення двовимірного масиву.

2.2. Технічні засоби захисту мовної інформації в телефонних лініях

2.2.1. Автономні кодуючі пристрої

При використанні IP-телефонії слід розуміти, що в цьому випадку присутні дві операції:

Операція 1. Здійснюється перетворення аналогової мови, яка має два напрямки в цифровий вид в середині приладу, який виконує функції кодування та декодування.

Операція 2. Здійснюється пакування кластерів сигналів в дискретні групи для передачі через IP-мережу.

Дані функції в багатьох випадках виконують автономні шлюзи, які мають відмінність один від одного. Такими шлюзами можуть бути певні окремі засоби або маршрутизатори чи комутатори, в яких встановлено апаратне та програмне забезпечення шлюзу. Інші шлюзи об'єднані з устаткуванням віддаленого доступу та відповідним модемом.

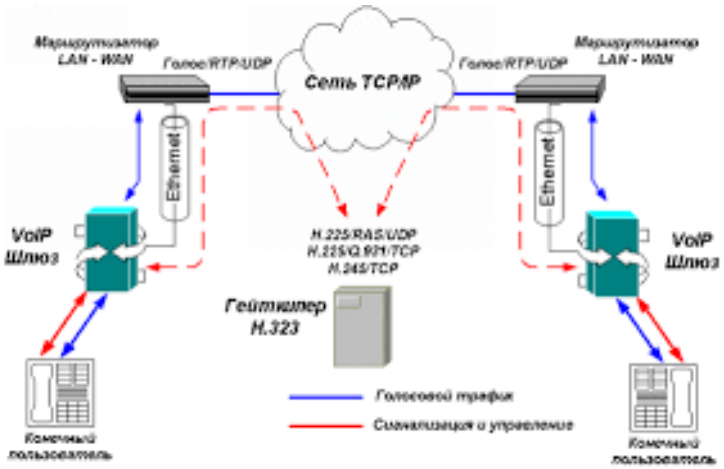


Рисунок 1.21. Технологія IP – телефонії.

Однак, не залежно від реалізації, ці шлюзи повинні мати наступні властивості:

Властивість 1. Шлюз повинен бути сумісний зі стандартом H.323. Згідно цьому стандарту базовим протоколом для роботи IP-устаткування було визначено протокол H.323v2, який створює стандарт мультимедійного зв'язку в мережах з комутацією пакетів. Ті користувачі персональних комп'ютерів, які мають

програмне забезпечення H.323 мають можливість підключатись до такої системи шлюзів. Виклики в цьому випадку мають можливість буди направлені на шлюзи інших користувачів, які підтримують стандарт H.323. В результаті даний комплекс має спроможність здійснювати інтеграцію мови, відео та даних в реальному масштабі часу.

Властивість 2. Шлюз повинен мати механізм резервування ресурсів. Підтримка довільної схеми протокол резервування RSVP або байт розділення послуг – DS byte для отримання спроможності вибору пріоритету між мовою, яка передається або тими даними, які характеризують шлюз. При цьому протокол RSVP дає можливість маршрутизаторам здійснювати резервування частини смуги пропуску для організації голосового трафіка.

Властивість 3. Шлюз повинен мати можливість підтримувати основні телефонні інтерфейси та відповідні типи сигналізації. Основним критерієм при оцінці характеристик шлюзів є спроможність більшості різноманітних телефонних інтерфейсів, які підтримуються IP-шлюзом (E1, PRI, BRI), а також аналогового, а також підтримка основних типів телефонної сигналізації: CAS, DTMF, PRI и ОКС № 7. Суттєвим є підтримка устаткування механізмів захисту інформації у відповідності H.235;

Властивість 4. Наявність в шлюзі планарності в архітектурі транспорту. Інтервал в архітектурі транспорту, по яким працюють теперішні шлюзи, мають достатньо широкий спектр: спеціальні лінії, які виділяються, ISDN, Frame Relay, ATM, Ethernet, тощо.

Властивість 5. Можливість здійснювати необхідні масштаби. Це дає можливість забезпечити модульне створення обладнання. На першому кроці розгортається мережа IP-телефонії з можливим використанням часткового ресурсу портів, що є в наявності з подальшим монотонним збільшенням кількості мовних портів, що використовуються. В цьому випадку кількість портів відповідає числу синхронних викликів, які може створити шлюз. Це пов'язано з тим, що кожний його порт

забезпечено власним дискретним сигнальним процесором для дискретизації мовних сигналів.

Властивість 6.Шлюз повинен бути забезпечено факсимільним зв'язком. Даний зв'язок відповідає двом стандартам. Стандарт Т.37 здійснює передачу факсимільного сигналу з спроможністю зберігання протягом деякого часового інтервалу. Це пов'язано з тим, що зображення факсимільного повідомлення передається у вигляді вкладень електронної пошти. Завдяки Т.37 факсимільні пристрої та факсимільні сервери спроможні взаємодіяти один з одним. Стандарт Т.38 визначає передачу факсимільного сигналу в реальному масштабі часу або завдяки імітації з'єднання з факсимільним апаратом, або за допомогою методу модуляції, який носить назву FaxRelay. Т.38 варто використовувати для реалізації функціональності, яка має ознаки.

Властивість 7. Спроможність керування шлюзом. Шлюзи відрізняються один від одного структурними принципами керування. Дані системи керування виконують функцію маршрутизації викликів між шлюзами та зміні кодів номерів телефонів в IP-адресі. Технічно ці системи керування бувають інтегровані зі шлюзом або уявляють собою відокремлений мультимедійний керівник конференцій або багатомовний керівник доступу. Таке рішення здійснюється завдяки використанню єдиного пакету, який включає в себе засоби біллінгу, маршрутизації викликів та мережевого адміністрування.

Властивість 8. Спроможність встановлювати різні алгоритми кодування мови. Це пов'язано з тим, що схема кодування впливає на показник якості мови, яка передається по IP-мережі. Ця схема використовується в шлюзі VoIP при стисканні мовної інформації. Найбільш популярною є схема, яка забезпечує найбільшу ступінь стискання інформації та відповідна специфікація G.723.1 до п'яти цілих трьох десятих кілобіт в секунду. Також використовуються і інші схеми так, як G.729a, G.711, G.726, G.728.

На теперішній час існують наступні види обладнання IP-телефонії для всіх можливих явищ:

1. Автономні шлюзи IP-телефонії, які приєднуються до АТС через цифрові та аналогові інтерфейси і при цьому здійснюють попередню обробку мовних сигналів, компресію, пакування в IP-пакети та передачу їх по мережі.

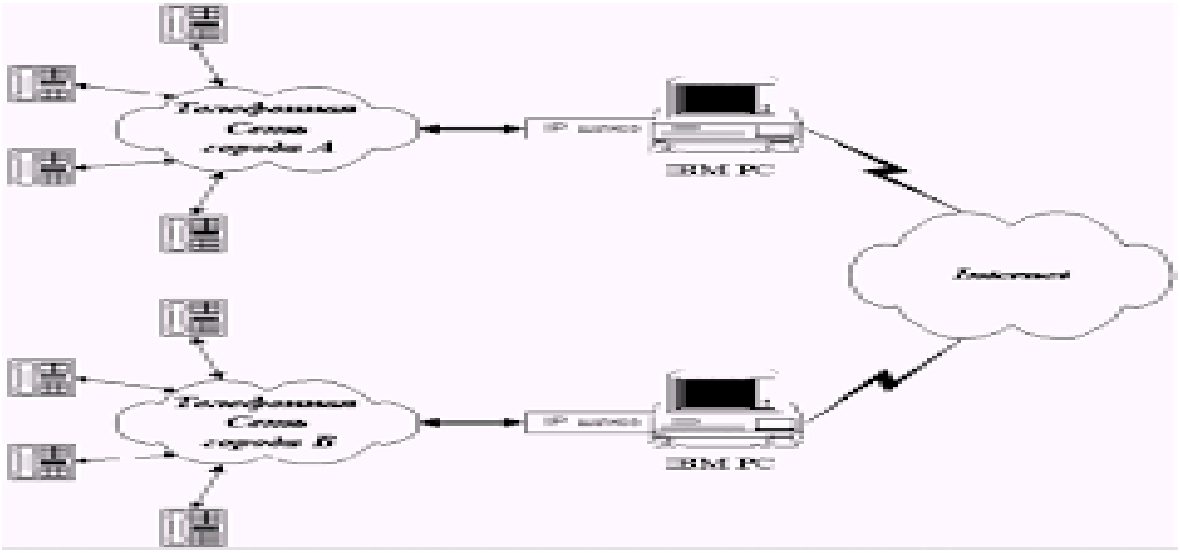


Рисунок 1.21. Структурна схема автономного шлюзу.

2. Магістральні мовні плати з інтерфейсом 10/100 BaseT для підключення до АТС існуючих моделей до корпоративної IP-мережі. Після встановлення в АТС такої плати, мовний трафік у вигляді IP-пакетів може бути направлено по локальній або глобальній пакетної мережі схоже на те, як він передається в поточний момент часу від АТС по телефонній системі зв'язку.

3. Телефонні апарати, які пакують мовну інформацію в IP-пакети та ті, що підключаються не до телефонної системи зв'язку, а до ЛВС Ethernet. Такі апарати потребують від мережевого адміністратора найменших налаштувань при використанні протоколу динамічної конфігурації DHCP.

4. Спеціалізовані комутатори мовних пакетів, які застосовуються для виконання функції істотної АТС на базі протоколу IP (IP-АТС).

Обладнання IP-телефонії виробники виробляють в сучасній або автономній конструкції. Сумісний сервер здійснює функцію шлюзу, та адміністратора, тобто здійснює маршрутизацію, збирає біллінгову інформацію, а саме IP-адресу, початковий момент часу та кінцевий момент часу розмови, вилучає луну сигналів, здійснює детектування пауз при проведенні перемовин, здійснює заповнення пауз

в момент прийому білим шумом , здійснює заповнення в буфер пам'яті пакетів, що приймаються для зменшення джитера, відновлює інтерполяцію загублених мовних пакетів, а також здійснює контроль стану мовного каналу, а саме визначає середній час затримки, джитер, відсоток втрат пакетів. Структура автономної конструкції така, що дані функції виконуються окремими блоками.

Модуль обробки телефонної сигналізації взаємодіє з телефонним обладнанням, який в свою чергу перетворює сигнали систем DSS1 та ОКС7 в атоми внутрішньої системи, які в свою чергу відображають стани процесу обслуговування викликів, тобто встановлюють з'єднання, виконують команду відбою та використовуються модулем логіки послуг шлюзу для встановлення з'єднання між Stop та IP-мережею. Модуль сигналізації H.323 оброблює сигнальну інформацію протоколів RAS, H.225.0 (Q.931) та H.245. Інформація про стани процесу обслуговування викликів в IP-мережі передаються в модуль логіки послуг шлюзу. Модуль логіки послуг шлюзу IP-телефонії відповідає за маршрутизацію викликів, які надходять від Stop в IP-мережу. При цьому виконуються операції контролю доступу та аналіз телефонного номеру, який викликає абонент з подальшим визначенням та наданню відповідної послуги. Модуль пакетування мови виконує функції підготовки мовного сигналу, який надходить з Stop з постійною швидкістю, для подальшої її передачі по мережі з маршрутизацією IP пакетів. Основними функціями модуля є перетворення мовного сигналу методом ІКМ, компенсація луни, кодування мовного сигналу, виявлення активних періодів та пауз в мові та адаптація відтворення. Крім того, модуль відповідає за детектування та генерацію сигналів DTMF та за обробку факсимільних та модемних сигналів.

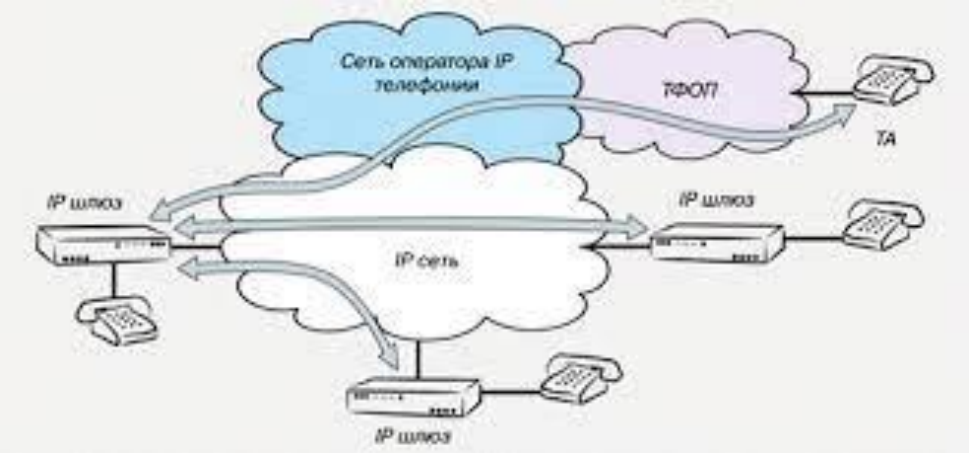


Рисунок 1.22. Структурна схема модуля обробки.

2.2.2. Апаратура закриття мовної інформації

Рисунок 1.23. Генератор імітації шуиму в мовному частотному діапазоні в режимі очікування виклику телефонного апарату в лініях аналогового телефонного зв'язку "РІАС-4ША".

Даний генератор дає можливість здійснювати мскування хибного сигналу при перетворенні акустичного сигналу в мовний частотний діапазон в режимі очікування виклику телефонного апарату [13].

Ефективне значення напруги сигналу шумової перешкоди - не перевищує 100 мВ в режимі очікування виклику і не більше 1 мВ в мовному режимі.

Ефективна смуга частот шумової перешкоди - від 0,3 до 10 кГц. Рівень загасання сигналу шумової перешкоди за межами заданої смуги частот - не менше 40 дБ. Коефіцієнт межспектральних кореляційних зв'язків - не більше 2,0. Коефіцієнт якості шуму - не менше 0,8. Постійний струм споживання від абонентської телефонної лінії - не більше 2 мА. Коефіцієнт загасання в смузі пропускання частот каналу тональної частоти - не більше 3 дБ. Нерівномірність амплітудно-частотної характеристики в смузі частот каналу тональної частоти - не більше 6 дБ. Коефіцієнт загасання в смузі частот придушення - не менше 30 дБ [13].

Рисунок 1.24. Мобільний акустичний шум PIAC-1M.

Даний прилад дає можливість захищати об'єкти від витоку конфіденційної інформації акустичними та вібро акустичними каналами за рахунок генерації шумового сигналу в діапазоні частот від 180 Гц до 5,6 кГц

Максимальна вихідна потужність акустичного та електромагнітного каналу - не перевищує 10 Вт.

Вихідна середня квадратична напруга акустичного та електромагнітного каналів при мінімальному опорі навантаження 4 Ом - не перевищує 5 В.

Максимальна вихідна потужність п'єзоелектричного каналу - не менше 10 Вт.

Вихідна среднеквадратическое напруга п'єзоелектричного каналу при максимальній ємності навантаження 0,5 мкФ - не менше 20 В.

Прилад забезпечуе добру глибину регулювання окремо низько - та високочастотних складових шумового сигналу в робочому діапазоні частот не менше 20 дБ [14].

Рисунок 1.25. Мобільний генератор акустичного шуму PIAC-2 ГМ

Прилад дає можливість захищати об'єкти від витоку конфіденційної інформації акустичними та вібро акустичними каналами шляхом генерації шумового сигналу в діапазоні частот від 180 Гц до 5,6 кГц. Максимальна вихідна потужність акустичного і електромеханічного каналу - не менше 10 Вт. Вихідна середньоквадратична напруга акустичного, п'єзоелектричного та електромагнітного каналів при мінімальному опорі навантаження 4 Ом - не менше 5 В. Вихідна середньоквадратична напруга п'єзоелектричного каналу при максимальній ємності навантаження 0,5 мкФ - не менше 20 в. Прилад забезпечує глибину регулювання окремо низько - і високочастотної складових шумового сигналу в робочому діапазоні частот не менше 20дБ.

Генератор призначений для захисту об'єктів від витоку конфіденційної інформації акустичними і віброакустичними каналами шляхом генерації маскує шумового сигналу.

Генератор забезпечує придушення сигналів в мовному частотному діапазоні в смузі частот від 180 Гц до 5,6 кГц.

Кількість каналів виходу на акустичні (електромагнітні) випромінювачі - 1 (2) шт.

Максимальна вихідна потужність акустичного (електромагнітного) каналу - не менше 10 Вт.

Вихідна середньоквадратична напруга акустичного (електромагнітного) каналу при навантаженні 4 Ом - не менше 5 в.

Кількість каналів виходу на п'єзоелектричні випромінювачі - 1 (2) шт.

Максимальна вихідна потужність п'єзоелектричного каналу - не менше 10 Вт. Вихідна середньоквадратична напруга п'єзоелектричного каналу при ємності навантаження 0,5 мкФ - не менше 20 в.

Ентропійний коефіцієнт якості сигналу шуму на виходах генератора в робочому діапазоні частот - не менше 0,8.

Глибина регулювання рівня шумового сигналу в робочому діапазоні частот не менше 20 дБ.
Регулювання рівня сигналу по верхніх і нижніх частотах на глибину не менше 20 дБ.

Регулювання рівня шумового сигналу здійснюється за допомогою потенціометрів ручками.

Усереднений максимальний рівень вихідного акустичного сигналу в діапазоні робочих частот з похибкою установки не більше 6 дБ на відстані 1 м від випромінювача щодо нульового значення 2х105 Па (для звукового тиску) - не менше 70 дБ.

Усереднений максимальний рівень вихідного віброакустичного сигналу в діапазоні робочих частот з похибкою установки не більше 6 дБ на віброізольоване приєднаної сталевій масі 10 кг циліндричної форми щодо нульового значення 3х10-4 м / с 2 (для віброприскорення) - не менше 70 дБ.

Час технічної готовності - не більше 1 сек.

Електроживлення від мережі змінного струму напругою 220 В плюс 22 в мінус 33 В, частотою 50 (±1) Гц, акумулятора або бортової мережі.

Габаритні розміри генератора - не більше 153х135х50 мм.

Маса генератора-не більше 2 кг.

Генератор зберігає працездатність в діапазоні температур: +10 ÷ + 40 ° С;

Генератор включений до переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначена законодавством України, формується адміністрацією Держспецзв'язку України.

Генератор комплектується експлуатаційною документацією відповідно до ГОСТ 2.601-95 [15].

2.2.3. Маскуватори

При забезпечені конспірації в телефонних перемовинах, бувають ситуації, коли достатньо, що не можна було впізнати мовний сигнал абонента. Для досягнення такої мети, існує спеціальний технічний засіб, який носить назву маскуватора мови. Даний прилад в усьому каналі зв`язку влаштовує відповідні особливі шум та завади, які не дають можливість зацікавленій особі, яка намагається втручатись не санкціоновано в перемовини, розбірливо отримати акустичну інформацію, яку абонент випромінює. Однак, на протилежній стороні зв`язку абонент достатньо якісно може розібрати інформацію, яка його стосується. Це пов`язано з тим, що відповідні фільтри вилучають шуми, які при цьому були

створенні. Первинно, дані технічні засоби були створені для стаціонарного зв`язку. Зі створенням сотових телефонів були створені нові засоби, які змінюють голос. Але такий вид захисту має свій недолік. Існують випадки, коли такий захист є одностороннім. Прикладом може бути використання стаціонарного телефону з маскуватором мови, а у протилежної сторони він відсутній і розмовляє завдяки сотовому телефону. В цьому випадку маскування мови здійснюється в односторонньому порядку. В цьому випадку зацікавлена сторона буде мати можливість отримувати пошкоджену мову через сотовий зв`язок, але зі стаціонарного телефону він буде чути явну річ. З одного боку виникає питання в тому, що це не зручно і такий засіб не є необхідним. Але з іншого боку спроможність змінювати голос призводить до можливості проводити наполовину скриті перемовини з власниками довільних телефонних апаратів так як їх розмови будуть вилучатися завадами, а дійсну мову завжди тим чи іншим чином можна замаскувати від зацікавлених осіб спеціальними кодуючими словами з урахуванням того, що саме ваша мова не є захищеною. На теперішній час на ринок багатий на різноманітні маскуватори мови. Діапазон цін від 100$ до 800$. На шумах, які мають стохастичну природу прцюють не дорогі маскуватори, але теоретично мову можна виявити. Це пов`язано з тим, що для цього необхідно спеціальне не дешеве устаткування та фахівець, який має достатньо великий досвід в шифруванні та дешифруванні. Є метрологічні прилади, які вимірюють мову, які не породжують шум, створює певні звуки, які нагадують мову. Це в свою чергу дає можливість забезпечити захист телефонної розмови з ймовірністю, ріною одиниці. Вартість таких маскуваторів вісімсот доларів США. Якщо вмонтувати такий маскуватор на один стаціонарний телефон, то в результаті будуть захищені всі телефонні промовини всіх абонентів, які будуть телефонувати на даний телефон. Однак, для дуже важливих конфіденційних перемовин все ж таки ризик існує. В даному випадку краще використовувати скремблер, який легко можна встановити в стаціонарний телефон а якщо виклик йде з мобільного телефону, то краще встановити криптофон. Цей прилад більш сучасний, дуже простий в

використанні та достатньо адаптивний до мобільного зв`язку, крім того має великий рівень надійності. Однак для підприємства, яке здійснює господарську діяльність, варто все ж таки використовувати маскиратор мови.

Рисунок 1.26. Радіосканер Alinco DR-135 CBA New

На рисунку 1.26 представлено радіостанцію Alinco DR135CBA New, яка працює в частотах 25,615-29,700 Мега герц, з подальшим можливим налаштуванням на частотний діапазон 29,700-30,105 Мега герц на ноутбук за допомогою програматора ERW-10, з необхідним спеціалізованим програмним забезпеченням.

Список використаної літератури

1. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

2. Безбогов, А.А. Методы и средства защиты компьютерной информации : учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.
3. Гайдур Г.І. Фізичні поля як носії інформації: [навчальний посібник] / Г.І. Гайдур, Я.А. Кремнецька, С.В. Морозова:. Київ. Державний університет телекомунікацій. 2019. —170 с.
4. Горбенко И.Д. Информационная безопасность и помехозащищённость телекоммуникационных систем в условиях различных внутренних и внешних воздействий / И.Д. Горбенко, А.А. Замула, В.Л. Морозов // Радиотехника, 2017, Вып. 189. С.- 5-14.
5. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
6. Квєтний Р. Особливості оцінювання параметрів процесу передавання даних із використанням турбо-кодів / Р. Квєтний, Ю. Іванов, С. Кривогубченко, О. Стукач // Метрологія та прилади, №3, 2017. С.- 25-32.
7. Коханович Г.Ф. Захист інформації в телекомунікаційних системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, В.М. Чуприн, О.О. Горбунов / Навчальний посібник.(лист МОНУ №1.4/18 – Г – 183 від 02.06.2009р.). –К.: НАУ,2009. – 380с.
8. Мамонтов О. Метод оптимального розміщення джерел шуму та ЕМП у виробничому приміщенні / О. Мамонтов, Ю. Колтун, О. Мамонтов // Метрологія та прилади, №3, 2017. С.- 67-72.
9. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України. / О.В. Рибальський, В.М. Смаглюк, В.Г. Хахановський – К.: Вид. Національної академії внутріш. справ, 2010. – 255 с.
10. Сулименко Э.А. Методы скремблирования речевого сигнала / Э.А Сулименко. – 2017. – 5с. 7. Сталенков С.Е., Шулика Е.В. НЕЛК – новая идеология комплексной безопасности. Способы и аппаратура защиты

телефонных линий. // Защита информации. Конфидент. – 1998. - №6(24). – 25-30с.

11. Скремблеры [Електронний ресурс]. – Режим доступу: //http://citforum.ru/internet/infsecure/ its2000_15.shtml.
12. Криптографические методы и средства защиты. [Електронний ресурс]. – Режим доступу: // http://pitbot.ru/37.shtml/.
13. PIAC-4ША [Електронний ресурс]. – Режим доступу: //http://glushilka.in.ua/ua/rias-4sha-detail
14. PIAC-2M [Електронний ресурс]. – Режим доступу: //http://glushilka.in.ua/ua/rias-2m-detail
15. PIAC-2M [Електронний ресурс]. – Режим доступу: //http://glushilka.in.ua/ua/rias-2gm-detail
16.