Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження методів захисту інформації в цифрових системах радіозв`язку»

Виконав: студент 2-го курсу,
групи ТКС-21мз
спеціальності 172 – Телекомунікації та радіотехніка
_____ Жук А.В.

Керівник: к.т.н., професор каф. ІКСТ
_____ Бортник Г.Г.
«____»_____ 2023 р.

Опонент: д.т.н., проф., зав. каф. ІРТС
_____ Осадчук О.В.
«____» _____ 2023 р.

Допущено до захисту
Завідувач кафедри ІКСТ
_____ д.т.н., проф. Кичак В.М.
«____» _____ 2023 р.

Вінниця ВНТУ – 2023 рік

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань - 17– Електроніка та телекомунікації
(шифр і назва)
Спеціальність - 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітньо-професійна програма - Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКСТ
д.т.н., професор В.М. Кичак
“___” _____2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Жуку Андрію Вікторовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Дослідження методів захисту інформації в цифрових системах радіозв`язку
керівник роботи Бортник Геннадій Григорович, канд. техн. наук, професор
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “20” 03 2023 року № 68

2. Строк подання студентом роботи 14 червня 2023 року

3. Вихідні дані до роботи: швидкість передачі інформації у каналах зв’язку 64 кбіт/с; ймовірність розкриття інформації не більше 10^{-5}; смуга вхідного сигналу – 300÷3400 Гц; динамічний діапазон – 40дБ; частота дискретизації телефонного сигналу – 8 кГц; розрядність аналого-цифрових перетворювачів – 12 розрядів; режим зв’язку – дуплексний; тип вхідних сигналів – первинні телефонні (мовні).

4. Зміст текстової частини: технічне обґрунтування; аналіз особливостей сучасних цифрових систем радіозв'язку; вибір та обґрунтування методів захисту інформації в цифрових засобах радіозв’язку; розробка пристроїв кодування розробка пристроїв кодування; моделювання процесу кодування мовних сигналів у цифрових системах радіозв'язку; аналіз економічної ефективності розробки; охорона праці та безпека в надзвичайних ситуаціях

5. Перелік ілюстративного матеріалу (з точним зазначенням обов’язкових креслень): структурна схема мовного скремблера; структурна схема захищеного каналу зв’язку; блок-схема алгоритму формування захищеного коду; структурна схема аналого-цифрового приймача закодованих телефонних сигналів; структурна схема аналого-цифрового передавача закодованих телефонних сигналів; результати моделювання кодера; результати моделювання скремблера.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня
Спеціальна частина	Бортник Г.Г., професор кафедри ІКСТ	30.01.23	26.05.23

7. Дата видачі завдання 30 січня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Прим
1.	Розробка технічного завдання (ТЗ)	10.02.2023р.	
2.	Технічне обґрунтування	20.02.2023р.	
3.	Аналіз методів захисту інформації в цифрових системах радіозв'язку	10.03.2023р.	
4.	Розробка пристроїв кодування мовних сигналів	03.04.2023р.	
5.	Моделювання процесу кодування мовних сигналів	05.05.2023р.	
6.	Аналіз економічної ефективності	19.05.2023р.	
7.	Охорона праці та безпека в надзвичайних ситуаціях	31.05.2023р.	
8.	Оформлення пояснювальної записки та графічної частини	13.06.2023р.	
9.	Нормоконтроль, попередній захист, опонування МКР	15.06.2023р.	
10.	Захист МКР ЕК	16.06.2023р.	

Студент _____ (підпис) Жук А.В.

Керівник роботи _____ (підпис) Бортник Г.Г.

АНОТАЦІЯ

УДК 621.396

Жук А.В. Дослідження методів захисту інформації в цифрових системах радіозв`язку. Магістерська кваліфікаційна робота зі спеціальності 172 – телекомунікації та радіотехніка, освітня програма – телекомунікаційні системи та мережі. Вінниця: ВНТУ, 2023. 125 с.

На укр. мові. Бібліогр.: 14 назв; рис.: 36; табл. 19.

У магістерській кваліфікаційній роботі проведено аналіз сучасних цифрових систем радіозв’язку.

У роботі розглянуто призначення, суть проблеми, що виникла та методи вирішення останньої, а також виконано аналіз методів дослідження поставленої задачі.

Виконано дослідження методів захисту інформації і обрано оптимальний цифровий метод для систем радіозв’язку. Здійснено вибір та обгрунтування методу кодування мовних сигналів на основі m-послідовностей.

Розроблено структурні схеми аналого-цифрових приймача та передавача закодованих телефонних сигналів та виконано оцінювання швидкодії цих пристроїв.

Виконано моделювання процесу кодування мовних сигналів у цифрових системах радіозв’язку та побудовано графік залежності числа помилок відновлення від кількості повторень кодової комбінації. Здійснено комп`ютерне моделювання скремблера.

Проведено розрахунки економічних витрат на проведення науково-дослідної роботи, а також доцільності капіталовкладень у цей пристрій.

Розглянуті питання безпеки життєдіяльності при дослідженні пристрою та проведено відповідний розрахунок.

Зроблено аналіз отриманих результатів.

ABSTRACT

Zhuk A. V. Research of information protection methods in digital radio communication systems. Master's thesis in the specialty 172 - telecommunications and radio engineering, educational program - telecommunications systems and networks. Vinnytsia: VNTU, 2023. 125 p.

In Ukrainian language. Bibliogr .: 14 titles; fig .: 36; table. 19.

In the master's qualification work, an analysis of modern digital radio communication systems was carried out.

The purpose, the essence of the problem that arose and the methods of solving the latter are considered in the work, as well as an analysis of research methods of the given task is performed.

The study of information protection methods was carried out and the optimal digital method was chosen for radio communication systems. The selection and justification of the method of encoding speech signals based on m-sequences was carried out.

The structural diagrams of the analog-digital receiver and transmitter of coded telephone signals were developed and the performance of these devices was evaluated.

Modeling of the process of coding speech signals in digital radio communication systems was performed and a graph of the dependence of the number of recovery errors on the number of repetitions of the code combination was made. A computer simulation of the scrambler was carried out.

Calculations of economic costs for conducting scientific research work, as well as the feasibility of capital investments in this device, were carried out.

The issues of life safety during the study of the device were considered and the corresponding calculation was carried out.

An analysis of the obtained results was made.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – абонентська станція
АЦП – аналого-цифровий перетворювач
АЧХ – амплітудно-частотна характеристика
БС – базова станція
ВДЖ – вторинне джерело живлення
ВСП – блок виділення спектральних параметрів
ГНН – години найбільшого навантаження
ДМС – джерело мовного сигналу
ДЗ – джерело збудження
ДЖ – джерело живлення
ДК – досліджуваний канал
ДКП – декодуючий пристрій
ЗЛ – з’єднувальні лінії
ЗО – зона обслуговування
ІП – імпульсний пристрій
КП – кодуючий пристрій
КУ – каналоутворююче устаткування
ПС – пристрій синхронізації
ФНЧ – фільтр нижніх частот
ЦАП – цифро-аналоговий перетворювач

ВСТУП

Актуальність теми. У сучасному світі інформація відіграє вирішальну роль. В таких умовах стає реальністю промисловий шпіонаж як сфера діяльності по добуванню, збору, аналізу, зберіганню та використанню конфіденційної інформації. Особливо актуальною ця проблема є у рухомих системах зв’язку [1].

В усьому світі для створення систем оперативного зв'язку, до яких висуваються високі вимоги по всьому комплексі параметрів, використовуються цифрові системи радіозв'язку, оскільки вони розроблялися спеціально для такого застосування. В них реалізовані такі принципи будівництва і функціональні можливості, що визначилися вимогами до них з боку систем зв'язку та тривалою практикою їхньої експлуатації.

Однією з основних тенденцій розвитку цифрових систем зв'язку є пошук найбільш ефективних шляхів використання частотного діапазону. Це позитивно позначиться як на зручності користування, так і на положенні справ з можливістю виділення частот.

Незважаючи на те, що сучасні цифрові системи можуть надавати користувачу широкі можливості при організації радіозв'язку, усі вони мають один загальний недолік - неефективне використання радіочастот. Цифрова система радіозв'язку - це система, у якій використовується принцип рівної доступності каналів для всіх абонентів чи груп абонентів. Цей принцип давно використовується в телефонних мережах, звідки у радіозв'язок і прийшло слово "trunk" [2, 3].

Аналіз останніх досліджень. Основною функцією устаткування цифрової системи радіозв'язку є автоматичне надання вільного радіоканалу за вимогою абонента радіостанції і переключення на цей канал абонента чи групи абонентів, що викликаються. Архітектура цифрових систем заснована на мережі з'єднаних один з одним базових станцій, кожна з який обслуговує визначену зону. Така архітектура дозволяє будувати мережі радіозв'язку будь-якого масштабу: від локальних однозонових мереж до великих регіональних

мереж із широким територіальним охопленням. Як будь-які мережі рухомого радіозв'язку, цифрові мережі містять наземну інфраструктуру (стаціонарне устаткування) та абонентські станції [4].

Абонентське устаткування цифрових систем включає досить широкий набір портативних і автомобільних радіостанцій, а також терміналів передачі даних. Існують абонентські цифрові радіостанції, що працюють як у режимі двочастотного симплекса (напівдуплекса), так і в дуплексному режимі. Більшість користувачів цифрових систем використовує напівдуплексні радіостанції при багатьох перевагах симплексного режиму (велика економічність, підвищена надійність підтримки каналу зв'язку, менша технічна складність і вартість, економія частотних ресурсів і т.і.).

Основним елементом наземної інфраструктури мережі цифрового радіозв'язку є базова станція, що містить кілька ретрансляторів з відповідним антенним устаткуванням і контролер, що керує роботою базової станції, комутує канали ретрансляторів, забезпечує вихід на телефонну мережу загального користування, чи іншу мережу фіксованого зв'язку.

Контролювати телефонні розмови можна на всьому продовженні телефонної лінії, а при використанні стільникового зв’язку у всій зоні. Основою будь-якої системи захисту інформації різного плану протидії є знання загроз і ступеня їх небезпеки.

Захист інформації цифрової мережі в сучасних умовах стає все більш складною проблемою, що зумовлено рядом обставин, основними з яких є: масове розповсюдження засобів електронної обчислювальної техніки; ускладнення шифрувальних технологій; необхідність захисту не тільки державної та військової інформації, але й промислової, комерційної та фінансової інформації; зростаючі можливості несанкціонованих дій над інформацією [5].

Окрім того, в наш час отримали широке розповсюдження засоби й методи несанкціонованого здобуття інформації. Вони знаходять все більше застосування не лише в діяльності державних правоохоронних органах, але і

в діяльності різного роду злочинних угруповань. Це ще раз доводить актуальність захисту інформації в цифровій мережі, оскільки цей вид радіозв'язку також використовується в правоохоронних органах.

Мета і завдання роботи. Метою даної магістерської кваліфікаційної роботи є підвищення ефективності пристроїв захисту інформації в цифрових засобах радіозв'язку за рахунок використання цифрового методу кодування мовних сигналів. Для досягнення заданої мети необхідно розв'язати такі задачі:

- виконати аналіз сучасних цифрових систем радіозв'язку;
- здійснити дослідження основних методів захисту інформації в цифрових засобах радіозв'язку;
- провести оптимізацію алгоритмів шифрування для засобів зв'язку з рухомими об'єктами;
- розробити засоби кодування мовних сигналів у цифровій мережі радіозв'язку;
- виконати моделювання процесу кодування мовних сигналів у цифрових засобах зв'язку.

Об'єктом дослідження є процес кодування мовних сигналів у цифрових засобах радіозв'язку.

Предметом дослідження є методи та засоби кодування мовних сигналів у цифрових засобах радіозв'язку.

Методи досліджень базуються на використанні: теорії кодування для синтезу ефективних кодів, теорії випадкових процесів для аналізу коду; еврістичного синтезу для розробки структур кодера мовних сигналів; комп'ютерне моделювання для аналізу та перевірки достовірності отриманих теоретичних положень.

Новизна одержаних результатів:

- вперше запропоновано вираз для оцінювання швидкодії передавача закодованих телефонних сигналів;
- вперше запропоновано для формування коду на базі m-послідовностей

використовувати 5-розрядний первинний ключ;

- вперше розроблено моделювальну схему скремблера мовних сигналів на базі балансного модулятора.

Апробація результатів магістерської кваліфікаційної роботи. Основні ідеї роботи доповідались і обговорювались на LII науково-технічній конференції підрозділів Вінницького національного технічного університету у 2023 році.

1 ТЕХНІЧНЕ ОБҐРУНТУВАННЯ

1.1 Аналіз технічної проблеми, що виникла

У наш час телефонні комунікації мають досить широке розповсюдження. Вірогідність використання телефонних ліній для несанкціонованого знімання інформації дуже велика. Число методів, якими можна скористатись для захисту інформації, досить великий, тим більше, що небезпека загрожує не тільки стаціонарним, але й стільниковим телефонним мережам. Захист від несанкціонованого знімання інформації може знадобитись як у справах державної важливості, так і для захисту комерційної або приватної інформації.

Цифрова мережа є досить використовуваним видом радіозв’язку. А також досить часто використовуються в спецслужбах та органах безпеки. Тому конфіденційність розмови є досить актуальною темою сьогодення. Існуючі системи радіозв'язку можна поділити за двома головними відмінностями:

- за способом організації доступу до системи зв'язку;
- за способом передачі мовних повідомлень.

Діапазони частот, що використовують для побудови цифрових систем радіозв'язку такі: 150, 300, 400 і 800 МГц. Чим нижча частота, тим більша дальність зв'язку. В Україні для цифрових систем у числі інших, виділений і традиційно використовується діапазон 300-330 МГц. Якщо будується система масштабу міста, найкраще використовувати цей діапазон. На ці частоти є вітчизняне устаткування. При орієнтації на імпортне устаткування краще використовувати 150 або 400 МГц. Якщо дуплексне рознесення менше 10%, то важко знайти носимі абонентські станції (АС). Радіоустаткування випускається на сітку частот 25 і 12,5 кГц [5].

Кількість радіоканалів визначається кількістю абонентів, завантаженням каналу абонентом, припустимою імовірністю відмов у з'єднанні через зайнятість усіх каналів. Ці величини зв'язуються формулою

Ерланга. При типових значеннях завантаження 0,025 Ерл (90 сек. заняття каналу в час найбільшого завантаження) і імовірності відмов 5%, при 4 каналах може працювати 60 абонентів, при 8 - 180, при 16 близько 400. Якщо поставити дві 4-риканальні БС і при цьому кожен абонент може працювати тільки на одній БС, то всього буде 120, а не 180 абонентів. Завантаження має максимальні значення ранком і ввечері, також воно чуттєве до тарифів [5].

Для згладжування перевантажень призначені тарифи, що залежать від години доби. Для стаціонарних АС завантаження вище 0,1 Ерл, а якщо АС розміщена в офісі і підключена до АТС закладу, то може доходити і до 0,8 Ерл. При малій кількості каналів може застосовуватися обмеження години розмови. БС звичайно випускаються на 4 або 8 каналів. У кожнім канали є передавач і приймач, іноді їх називають репитером. Склад інших блоків БС залежить від типові АФТ. Якщо є можливість поставити тільки одну антену, то необхідні додатково дуплексний фільтр, малошумлячий підсилювач (МШП), антенний розгалужувач, суматор потужності, циркулятори. При використанні суматора випромінювана потужність падає. Для звичайних суматорів у 4-х канальної БС потужність передавачів зменшується приблизно в 5 разів, наприклад з 50 до 10 Вт. Якщо є можливість установити АФТ з декількох антен, деякі вимоги до БС спрощуються. У якості БС можна використовувати репитери із двома антенами на кожен канал, розміщеними один від одного на кілька метрів. Задача вибору БС і АФТ повинна вирішуватися, виходячи з необхідної дальності зв`язку [6].

Захист інформації – найважливіший аспект побудови цифрової мережі, оскільки однією з основних груп користувачів є служби суспільної безпеки, для яких високий рівень захисту - обов'язкова вимога. Система захисту в мережі заснована на трьох принципах: структурність, відкритість і застосування добре перевірених методів. Для проробки питань безпеки системи в ETSI група спеціалістів підготувала специфікацію по захисту інформації в стандарті TETRA - ETSI TETRA Technical Requirements Specification ETR 086 - 3. Головною задачею групи було зробити цю частину

стандарту відкритою. Тому концепція безпеки в мережі повинна будуватися на основі підходів, уже використаних в інших цифрових стандартах - GSM і DECT [1]. GSM передбачає такі основні принципи безпеки, як аутентифікація термінала в мережі і захист інформації в процесі її передачі по мережі, а DECT використовує двосторонню аутентифікацію між терміналами та мережею і заснований на системі управління ключами.

При описі функцій захисту в мережі цифрового зв'язку важливо зрозуміти різницю між підсистемами захисту. Існують чотири підсистеми, що взаємодіють між собою:

1. Механізми захисту (МЗ) - незалежні функції, за допомогою яких можна вирішити проблему захисту інформації: наприклад, захищати інформацію, що циркулює в мережі, проводити аутентифікацію користувачів і т.і. Ця підсистема найбільш важлива в загальній схемі захисту і містить у собі такі механізми:

- обопільна аутентифікація по радіоінтерфейсу RAI. Даний механізм підтримує двосторонню аутентифікацію кінцевого устаткування і базових станцій. Це дозволяє системам контролювати доступ у мережу, а кінцевому устаткуванню - ідентифікувати свою мережу. Обопільна аутентифікація використовується в режимах передачі голосу, даних і оптимізованому режимі пакетної передачі інформації (PDO). У режимі прямого обміну (DMRAI) механізм аутентифікації недоступний. У цьому випадку для схованої двосторонньої аутентифікації використовуються ключі постійного шифру (КПШ);

- шифрування радіоінтерфейсу RAI. При роботі кінцевого устаткування з базовою станцією контрольна і керувальна інформація, а також індивідуальні (групові) зв'язки можуть бути зашифровані за допомогою великої кількості ключів. Даний механізм доступний у режимах передачі голосу, даних і режимі прямого обміну;

- шифрування радіоінтерфейсу DMRAI. При використанні цього алгоритму необхідна підтримка протоколом шифрування синхронізації і

режиму "пізнього входу". Цей механізм доступний у режимах передачі голосу, даних і режимі прямого обміну;

- забезпечення анонімності передбачає шифрування ідентифікаторів абонента або групи в радіоінтерфейсі.

2. Управління захистом (УЗ) - використовується для управління різноманітними МЗ такими способами, як:

- ключ аутентифікації. Цей ключ використовується для взаємного впізнання мобільного термінала і базової станції. Існує три способи генерації ключа аутентифікації [5]:

1) із довгого (128 біт) ключа аутентифікації споживача (КАС), що зберігається в кінцевому устаткуванні або в смарт-карті;

2) з аутентифікаційного коду (PIN), вручну введеного абонентом;

3) комбінацією КАС і PIN;

- ключі шифрування. Існує декілька видів таких ключів:

1) отриманий ключ шифрування (ОКІП) виробляється в процесі процедури аутентифікації - у такий спосіб забезпечується схована аутентифікація протягом сеансу зв'язку. ОКІП може також використовуватися для шифрування переданої інформації;

2) загальний ключ шифрування (ЗКІП) шифрується за допомогою ОКІП і передається на кінцеве устаткування. ЗКШ використовується для шифрування повідомлень;

3) груповий ключ шифрування (ГКШ) використовується спеціально виділеною групою абонентів. Він створюється станцією генерації ключів і розсилається на кінцеві пристрої (подібно ЗКШ, на смарт-картах або за допомогою OTAR - Over the air rekeying - методу заміни ключів);

4) статичний ключ шифрування (СКЛІ) застосовується без попередньої аутентифікації і не змінюється в процесі аутентифікаційного обміну. У мережі може використовуватися до 32 СКШ. Вони можуть поширюватися аналогічно ГКШ і діяти в режимі прямого обміну. Також за допомогою даного ключа може провадитися шифрування усередині закритої

користувальної групи і шифрування в ситуаціях, коли аутентифікація не працює;

- метод заміни ключів (ОТАК). Існує можливість поширення/відновлення ЗКШ, ГКШ, СКШ за допомогою механізму ОТАК. Цей механізм дозволяє завантажувати ключі зі станції генерації ключів по радіоінтерфейсу RAI прямо в кінцеве устаткування і доступний доти, поки змінюваний ключ доступний для кінцевої станції;

- передача аутентифікаційної інформації між мережами. Якщо кінцеве устаткування однієї мережі звернеться до іншої мережі як до свого, то остання повинна одержати з мережі абонента інформацію про нього для виконання двосторонньої аутентифікації або доставки ключів. Можливі три способи рішення цієї задачі:

• передача необхідного ключа в іншу мережу;

• передача інформації, необхідної для процедури аутентифікації;

• передача одного сеансового ключа аутентифікації, що може бути використаний для повторної аутентифікації без пересилки ключа.

3. Стандартні криптографічні алгоритми - це стандартизовані математичні функції, що працюють із ключами і забезпечують визначений рівень захисту при використанні в окремих МЗ. Стандартні криптографічні алгоритми входять у систему TETRA як опції і забезпечують взаємодію різноманітних мереж.

4. Механізм законного прослуховування (МЗП) - функція, яка використовується усередині мережі для законного доступу до інформації. У багатьох країнах світу існують законні шляхи доступу до інформації, обумовлені національним законодавством. Для виконання зазначеного механізму оператор цифрової мережі повинен надавати можливість доступу до інформації з запиту державних структур.

Викладений підхід до побудови системи захисту дозволив забезпечити високу безпеку без збитку масштабності і чудових характеристик мережі. Шифрування даних у радіоканалі, наскрізне кодування навіть при взаємодії

різних мереж, анонімність, контроль підключення / відключення мобільних терміналів - усе це робить систему TETRA привабливою не тільки для спецслужб, яким вона призначалася, але і для цивільних організацій.

Метою даної роботи є дослідження сучасних методів захисту інформації та вибір найбільш оптимального методу для закриття інформації в цифровій мережі радіозв'язку.

Існують такі методи закриття мовного сигналу: скремблювння, криптографічний захист телефонних повідомлень, кодування, шифрування та дешифрування інформації.

Під скремлюванням розуміється зміна характеристик мовного сигналу таким чином, щоб отриманий модульований сигнал, маючи властивості розбірливості і невпізнання, займав ту ж смугу частот, що й початковий сигнал. Перевагою даного методу є відносно невелика складність реалізації, а недоліком – низька якість відновленого сигналу.

Криптографічний захист мовних сигналів базується на шифруванні повідомлення з наступним розшифруванням з метою відновлення відкритого повідомлення. Недоліком такого захисту є висока вартість реалізації, яка компенсується важливими перевагами, і достатньо високий рівень відновленого каналу та ефективного захисту інформації.

1.2 Розробка технічного завдання

У даній магістерській кваліфікаційній роботі виконується дослідження методів захисту інформації в цифрових засобах радіозв'язку та виконується аналіз і синтез структурної схеми пристрою захисту інформації.

Цифровий метод кодування є доволі надійним і економічно вигідним методом захисту інформації в цифрових радіотелефонах. Основна задача кодування – завадостійке кодування сигналу мови. Завадостійке кодування здійснюється за рахунок введення до складу сигналу, що передається, доволі

великого об’єму надлишкової (контрольної) інформації. Відомі два напрямки кодування мови:

- кодування форми сигналу (Waveform codin);

- кодування джерела сигналу (Source cafing).

Перший метод заснований на використанні статистичних характеристик сигналу та практично не залежить від механізму формування сигналу. Кодери цього типу забезпечують високу якість передачі мови, але відрізняються меншою, порівняно з другим методом, економічністю.

Другий метод – кодування джерела сигналу. У радіозв’язку застосовується саме вокодерні методи на основі лінійного передбачення, в яких оцінка параметрів, що передаються в лініях зв’язку, відбувається на основі статистичних характеристик сигналу за визначеним алгоритмом, як при кодування форми сигналу. Тому фактично межа між двома класичними методами кодування – кодування форми сигналу та кодування джерела сигналу, до деякої міри стирається.

Запропонована система кодування в магістерській роботі може створювати конкуренцію відносно інших систем. Тому, що дана система розроблена для побутових радіотелефонів, є простою реалізацією, не потребує значних матеріальних витрат, але забезпечує не гіршу якість у порівнянні зі складними системами, що орієнтовані не тільки на передачу мови. Розроблена система може бути використана і тоді, коли необхідно зашифрувати інформацію, щоб запобігти прослуховуванню. Дана система успішно може застосовуватись у роботі правоохоронних органів, на відміну від дорогих систем, що вони використовують.

Сьогодні постають проблеми, що пов’язані зі швидкістю та якістю передачі мовних сигналів, завадостійкістю та досконалістю систем кодування. З’явилась необхідність швидкого та надійного кодування, при цьому дуже важливо зберегти зміст, точність повідомлення та забезпечити високу якість сигналу на приймальному кінці. Система, що призначена для передачі та кодування мовних сигналів, повинна мати найкращі технічні

показники, забезпечувати високу якість сигналу як на приймальному, так і передавальному кінцях, і відповідно бути економічно вигідною.

При розробці будь-якої нової технології дослідники повинні домагатися технічної досконалості, з одного боку, і низької вартості реалізації, з іншого. Стосовно методів кодування мови поняття досконалості має на увазі високу якість сигналу і малу часову затримку. Вартість реалізації визначають такі чинники, як загальна складність системи і швидкість бітового потоку, що необхідні для досягнення визначеної якості сигналу.

Отже, суть технічної проблеми, що виникла на сучасному етапі розвитку науки та техніки, полягає в тому, що потрібно розробити таку систему кодування мовних сигналів, яка буде найкращою як за технічними, так і економічними показниками. Існуючі методи кодування мовних сигналів не дають змогу вирішити всі поставлені проблеми, в той час, як цифрові дозволяють це зробити.

Істотною перевагою цифрових систем радіозв’язку є можливість досягнення дуже високого ступеня захисту від несанкціонованого доступу і закриття кодованої інформації, а також є такі переваги як простота кодування і знаходження помилок, висока завадостійкість тощо. Але є один недолік – це висока тактова частота лінійного сигналу. Цифрові системи кодування інформації значно підвищили якість послуг телефонного зв’язку.

Технічна доцільність розробки такої системи полягає в тому, що за технічними показниками, такими як точність, надійність, потужність, безвідмовність у роботі тощо, дана система кодування перевершує інші системи.

Вже певний час дослідники, які конкурують з нами, посилено займаються створенням комплексних систем захисту інформації у радіозв’язку, які базуються на доповненні і комбінуванні методу цифрового кодування шифруванням. Ці дослідження спрямовані на застосування таких систем у стільниковому зв’язку.

Принцип цифрового кодування полягає в наступному: аналоговий

сигнал від мікрофона подається на аналого-цифровий перетворювач (АЦП), на виході якого маємо n-розрядний код. Потім цей код шифрується за допомогою певних алгоритмів, переноситься в діапазон радіочастот, модулюється і передається в ефір. До вимог можна віднести такі поняття:

- якість перетворення повідомлень;
- економне використання ресурсів каналу зв'язку;
- швидкість і якість передачі мовних сигналів;
- завадостійкість та досконалість систем кодування;
- простота реалізації системи;
- висока якість сигналу на приймальному кінці.

Технічні параметри засобів захисту інформації такі:

- швидкість передачі інформації у каналах зв'язку 64 кбіт/с;
- вид вхідних сигналів – первинні телефонні;
- ймовірність розкриття інформації не більше 10^{-5};
- смуга вхідного сигналу – 300÷3400 Гц;
- динамічний діапазон – 40дБ;
- частота дискретизації телефонного сигналу – 8 кГц;
- розрядність аналого-цифрових перетворювачів – 12 розрядів;
- режим зв'язку – дуплекс.

Головною метою даної роботи є підвищення ступеня закриття інформації при збереженні високої якості радіозв'язку. Тому результати даного дослідження можуть бути дуже корисні при розробці новітніх сучасних засобів цифрового рухомого зв'язку, і можуть бути безпосередньо використанні як на виробництві подібних пристроїв, так і як основа для подальших дослідів в даному напрямку.

Серед підприємств, що займаються розробкою та виготовленням засобів телекомунікацій, а також побудовою та обслуговуванням телекомунікаційних систем, можливе запровадження результатів досліджень даної магістерської роботи. Серед цих підприємств можуть бути: Київстар, Водофон, Лайф, Укртелеком, Дата Груп, Huawei, СМАРТ, Еверест.

Результати досліджень даної магістерської кваліфікаційної роботи можуть також бути використанні як теоретичне підґрунтя для подальших досліджень в галузі телекомунікацій, науково дослідними інститутами, або на відповідних кафедрах технічних університетів.

У Додатку А наведено технічне завдання до даної магістерської кваліфікаційної роботи.

2 АНАЛІЗ ОСОБЛИВОСТЕЙ СУЧАСНИХ ЦИФРОВИХ СИСТЕМ РАДІОЗВ'ЯЗКУ

2.1 Аналіз основних стандартів сучасних цифрових систем радіозв`язку

Цифровими радіосистемами називаються радіально-зонові системи наземного рухомого радіозв'язку, що здійснюють автоматичний розподіл каналів зв'язку ретрансляторів між абонентами. Це досить загальне визначення, але воно відображає сукупність ознак, що об'єднують усі радіосистеми від простих SmarTrunk до сучасних TETRA.

Автоматичне керування радіочастотним ресурсом у цифровій системі радіозв`язку дозволяє підвищити її пропускну спроможність у порівнянні з традиційною (conventional) радіомережею з такою ж кількістю каналів. Чим більше каналів включено до складу цифрової системи, тим вище буде її ефективність. Якщо припустити, що число абонентів на один радіоканал у радіомережах двочастотного симплекса в середньому не повинно перевищувати 35...50, то в цифрових мережах число абонентів на канал може сягати 80... 100 [4].

Ефективність використання наявних частот у цифрових системах у 7 разів перевищує аналогічний показник звичайних систем рухомого зв'язку. Цифрові системи зв'язку динамічно розподіляють канали між всіма абонентами системи, що дозволяє рівномірно і більш щільно завантажувати канали. Використання технології транкінгу дозволяє на обмеженому частотному ресурсі надати послуги істотно більшій кількості абонентів у порівнянні з диспетчерськими системами при заданій можливості відмови.

Звичайно, транкінг не відміняє звичайних систем зв'язку. Адже за його ефективність доводиться сплачувати набагато дорожче, ніж при створенні звичайних радіомереж. Вибір типу радіомережі визначається наявним частотним ресурсом, кількістю користувачів і специфікою їх роботи. У традиційних диспетчерських системах радіозв'язку за кожною групою закріплюється виділений частотний канал. Такий засіб організації

радіозв'язку достатньо ефективний у тих випадках, коли загальна кількість абонентів системи незначна, а необхідна зона радіопокриття обмежена. Основною перевагою подібних систем радіозв'язку є простота і невисока вартість. До недоліків можна віднести неефективне використання частотного спектра і незначний набір сервісних функцій. Диспетчерські радіомережі частіше всього використовуються для організації технологічного або службового радіозв'язку.

Серед основних переваг цифрових систем зв'язку, що виявляється в сфері професійного зв'язку слід вказати:

• гнучку систему викликів - індивідуальних, групових, вітальних, пріоритетних, аварійних та ін.;

• гнучку систему нумерації - від коротких і двозначних до повноцінних міських номерів;

• незначний час встановлення з'єднання (звичайно менше 1 с);

• економічність (за вартістю устаткування і за експлуатаційними витратами ТСР: у декілька разів дешевше стільникових систем).

Загальною тенденцією розвитку професійних систем рухомого радіозв'язку є перехід від аналогових корпоративних або національних стандартів до цифровим міжнародних із забезпеченням конфіденційності зв'язку і роумінгу абонентів.

Переваги від переходу до цифрової системи для багатьох споживачів перевищують все ще дуже значну вартість як інфраструктури, так і абонентського устаткування. Особливо це стосується вимог, що подають силові структури, значні корпорації й адміністративні органи. Перед вітчизняними виробниками й операторами постає завдання вибору цифрового протоколу: TETRA, APCO 25 або Tetrapol PAS.

Широкі можливості та гнучкість побудови сучасних цифрових систем радіозв'язку з урахуванням глибокого аналізу потреб різноманітних корпоративних користувачів дозволяють сьогодні створювати ефективні міжвідомчі системи рухомого радіозв'язку, які максимально використовують

існуючу в споживачів інфраструктуру, ощадливо використовують частотний ресурс і дозволяють надавати більш якісні і надійні послуги зв'язку.

В Україні склалися економічні, правові і технічні передумови кількісного і якісного розвитку цифрових систем нового покоління, а досвід закордонних країн, де цифрові мережі успішно співіснують із стільниковими, зайвий раз підтверджує необхідність і життєздатність цього напрямку ринку послуг рухомому зв'язку.

Можливість обслуговування різнорідних за функціональним призначенням пристроїв у єдиній системі - це ще один шлях до мінімізації витрат.

Цифрові системи радіозв'язку дозволяють на базі своїх каналів організовувати незалежні виділені мережі зв'язку (або, як прийнято говорити останнім часом, приватні віртуальні мережі). Це означає, що декілька організацій можуть спільними зусиллями розгорнути єдину систему замість установки окремих систем. При цьому досягається суттєва економія радіочастотного ресурсу, а також зниження вартості інфраструктури.

Все вище вказане свідчить про тривкість позицій цифрових систем радіозв'язку у корпоративному секторі ринку систем і засобів рухомого зв'язку.

2.2 Служби цифрових систем радіозв'язку

Цифрова система радіозв'язку характеризується широким розмаїттям служб, що забезпечують роботу різноманітного устаткування, а також підтримання мереж зв'язку всередині цих систем.

Найбільше важливою і часто використовуваною службою цифрових систем є служба внутрішніх викликів. Цифрові мережі надають абонентам можливість робити різноманітні типи викликів усередині системи: індивідуальний (персональний) і груповий (диспетчерський). У першому

випадку виклик направляється тільки одному абоненту, у другому - декільком.

Основним типом викликів у цифрових систем радіозв'язку є груповий виклик у межах однієї групи. Груповий виклик принципово може бути зроблений тільки в напівдуплексному режимі. Доки абонент, що викликає, говорить, і його радіостанція знаходиться в режимі передача, всі інші члени групи приймають повідомлення абонента, що викликає. У ході наступного радіообміну, репліка кожного члена групи автоматично стає чутна всім учасникам групи. Груповий виклик може проводитися із самої простої (а отже, недорогої) напівдуплексної радіостанції - для цього користувачеві достатньо лише натиснути кнопку "Передача". Входження в зв'язок із "своєю" групою абонентів відбувається автоматично. Якщо треба зв'язатися з абонентами інших груп, слід спочатку набрати на клавіатурі радіостанції номер потрібної групи. Груповий виклик забезпечують усі відомі транкінгові системи.

У більшості існуючих цифрових систем передбачена можливість одночасного виклику абонентів декількох груп або відразу всіх абонентів мережі (All Call). У деяких системах використовується ієрархічне вкладення груп і передбачаються відповідні типи викликів: багаторівневий, багатогруповий і т.і. Як правило, право робити настільки складні виклики надається тільки диспетчеру.

Деякі системи забезпечують можливість з'єднання з довільно обраною групою не тільки для абонентів цифрових систем радіозв'язку, але і для абонентів ТФЗК.

Персональний внутрішній виклик є більш привілейованим типом виклику. Для його посилання користувач повинен використовувати радіостанцію з цифровою клавіатурою. Персональний внутрішній виклик може бути зроблений не тільки в напівдуплексному, але й у дуплексному режимі (зрозуміло, якщо обидві абонентські радіостанції є дуплексними).

Існує ще один специфічний різновид внутрішніх викликів - статусні

повідомлення. Вони належать, скоріше, до галузі передачі даних і служать заміною тривіальним реплікам, таким як "вас зрозумів", "повторіть" і т.п. Замість мовної відповіді абонент може натиснути відповідну функціональну кнопку, що викликає передачу короткого цифрового повідомлення. Застосування статусних повідомлень дозволяє істотно зменшити завантаження системи, тому що в умовах диспетчерського зв'язку і групової роботи такі репліки вживаються дуже часто.

Пріоритетність. Багато цифрових систем радіозв'язку передбачають опрацювання викликів із декількома рівнями пріоритету. Так, у системі DigiStar передбачено 10 рівнів пріоритету, у системі EDACS - 8. Розмежування пріоритетів може використовуватися в різноманітних цілях: надання привілеїв для окремих абонентів або груп, а також для оптимізації опрацювання трафіка. У будь-якому випадку, вплив пріоритетного опрацювання викликів починає позначатися тільки при значному завантаженні системи.

Оптимізація опрацювання трафіка полягає в тому, що викликам абонентів, які вже розпочали і продовжують розмову, присвоюється більш високий пріоритет, ніж викликам абонентів, що тільки встановлюють з'єднання. Таким чином, ціною деякого збільшення часу на перше встановлення з'єднання мінімізується тривалість пауз у розмові абонентів, що в кінцевому рахунку веде забезпечує поліпшення комфортності радіопереговорів.

Деякі системи передбачають наділення ряду абонентів правом виклику з надвисоким пріоритетом, або, так званого, виклику, що витискує. При надходженні такого виклику в ситуації, коли всі ретрансляційні ресурси зайняті (тобто в ситуації блокування), одне з поточних з'єднань переривається, а ресурс, що звільнився, приділяється для обслуговування виклику, що надійшов, із надвисоким пріоритетом.

Існує ще один тип пріоритетного опрацювання викликів - надання, так званого, відкритого каналу, що полягає в тимчасовому переключенні одного з

каналів у монопольне володіння однієї групи абонентів. Це дозволяє групі одержати гарантований і швидкий доступ до ретранслятора. Надання відкритого каналу є засобом, що використовується лише у виняткових ситуаціях і доступним для вкрай обмеженого кола користувачів. Вмикання режиму відкритого каналу створює помітні незручності іншим абонентам системи, тому що за рахунок зменшення числа каналів, що розподіляються, погіршується якість обслуговування, особливо в ситуації високого навантаження. Як правило, доступ до телефонних мереж загального користування (ТФЗК) повинні мати лише деякі абоненти цифрових систем радіозв'язку.

Виклики абонентів ТФЗК в основному проводяться з радіостанцій, що мають цифрову клавіатуру. Проте, і деякі безклавіатурні радіостанції дозволяють робити виклик обмеженого кола абонентів ТФЗК, номера яких були заздалегідь занесені в "записну книжку" радіостанції при її програмуванні.

Абонент ТФЗК може викликати не тільки окремого абонента цифрових систем радіозв'язку, але і групу абонентів. Процедура виклику для абонентів ТФЗК може бути двохступінчатою в тому випадку, якщо інтерфейс ТФЗК залучений до телефонної мережі за допомогою дводротової комутуємої лінії, або одноступінчатої - при підключенні інтерфейсу ТФЗК за методом Direct Inward Dialing (DID).

При двоступінчатій процедурі абонент ТФЗК повинен спочатку набрати номер телефону, до якого залучений інтерфейс ТФЗК, а потім - номер абонента усередині системи. Як правило, набір додаткового номера повинен проводитися в тональному режимі, що створює значні незручності для абонентів ТФЗК. До того ж, у цьому випадку набір додаткового номера абонента системи відбувається в умовах уже встановленого з'єднання через ТФЗК, що часто супроводжується імпульсними й іншими перешкодами. Тому можливість помилкового з'єднання або обривання зв'язку відносно висока.

Щоб підвищити надійність встановлення з'єднань, розроблювані

системи і стандарти цифрових систем радіозв'язку передбачають використання методу DID, що дозволяє організувати доступ із ТФЗК із використанням єдиної системи нумерації абонентів. Абоненту ТФЗК для виклику абонента цифрових систем радіозв'язку, оснащеною апаратурою DID, достатньо набрати звичайний міський телефонний номер, так само як і в стільниковій мережі.

У багатозонових цифрових систем радіозв'язку здійснюється відслідковування поточного місцезнаходження абонентів. При переміщенні абонентів з однієї зони в іншу, забезпечується реєстрація і підключення нових каналів доступу. У системах із розподіленою комутацією кожна базова станція самостійно здійснює комутацію викликів, що надходять. У системах із централізованою комутацією роумінг більш надійний, а швидкість опрацювання міжзональних викликів вища. Що ж стосується забезпечення безперервності розмови при переміщенні абонентів цифрових систем радіозв'язку з однієї зони обслуговування в іншу (м'яка або естафетна передача), то в сучасних аналогових системах таке завдання не постає. Насамперед, це пов'язано з тим, що зони обслуговування транкінгових систем, як правило, мають значні розміри і, у випадку наявності декількох зон, на межах достатньо сильно перекриваються. Можливість того, що абонент мережі вийде за межі своєї зони обслуговування саме в момент розмови, настільки мала, що немає необхідності витрачати зусилля на розробку механізму естафетної передачі.

Для аналогових цифрових систем радіозв'язку перемикання при переміщенні абонента з однієї зони обслуговування в іншу відбувається з перериванням поточного сеансу зв'язку (Hard Hand-Over), що практично не впливає на якість обслуговування в таких системах. У той час у новітніх цифрових системах стандарту TETRA, де зони обслуговування в силу ряду причин будуть набагато меншими, передбачається естафетна передача при переключенні зон.

Особливий аспект роумінгу в цифрових систем радіозв'язку -

обслуговування багатозональних групових викликів. Відслідковуючи переміщення абонентів, система при надходженні групового виклику забезпечує його доведення до всіх членів групи, у якій би зоні вони не знаходилися.

У цифрових системах радіозв'язку передача даних є додатковою послугою, тому до останнього часу вона не одержувала розвинених засобів підтримання. Швидкість передачі даних у всіх аналогових системах знаходиться у межах 0,6 - 4,8 кбіт/с. Як правило, аналогові системи лише надають канали для передачі даних, не забезпечуючи мережну маршрутизацію. У той час, для цифрових систем передача даних є більш близькою службою.

2.3 Класифікація цифрових систем радіозв'язку

Про різноманіття створених цифрових систем радіозв'язку свідчить рис. 2.1. На ньому показаний розподіл систем за окремими класифікаційними ознаками. Слід зазначити, що на рисунку наведені далеко не всі системи, стандарти і протоколи тому, що існує багато схожих систем із різноманітними назвами, які базуються на протоколах Smar Trunk і SmarTrunk II. Водночас, системи стандарту МРТ (початкові букви найменувань різноманітних стандартів і рекомендацій Міністерства пошти і телекомунікацій Великобританії (Ministry of Post and Telecommunication), схожі на наше скорочення "ДЕРЖСТАНДАРТ", від різних фірм-виробників мають суттєві структурні і функціональні відмінності. Це ж стосується і систем стандарту TETRA (Trans European Trunked Radio - Загальноєвропейська система транкінгового зв'язку).

Усі протоколи транкових систем розподіляються між двома класами:

1. Відкриті протоколи.

2. Спеціалізовані (що ліцензуються) протоколи.

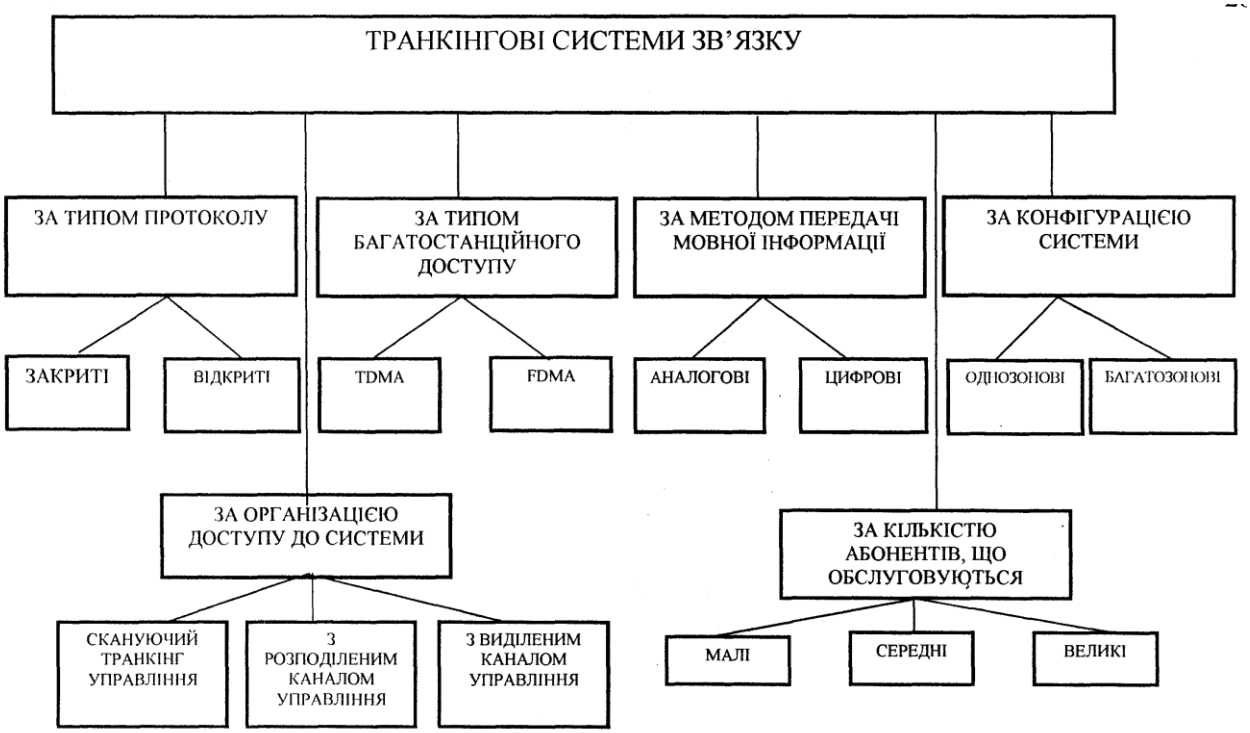


Рисунок 2.1 – Класифікація цифрових систем радіозв'язку

Формати відкритих протоколів не запатентовані і доступні для будь-якого виробника. Ці протоколи рекомендовані для використання в багатьох країнах. Допускається внесення змін, пов'язаних із національними особливостями. Системи з такими протоколами впроваджуються багатьма фірмами. Устаткування з урахуванням масовості виробництва, як правило, дешевше, ніж у спеціалізованих системах.

У Європі для широкого використання рекомендований відкритий радіопротокол аналогових систем MPT 1327 [8]. Надалі цей стандарт був уточнений протоколами MPT 1343, MPT 1347, MPT 1352, MPT 1318 і протоколом для передачі даних MAP 27. Перспективним цифровим стандартом є стандарт TETRA [9]. Переваги цього протоколу дають підстави очікувати, що системи з TETRA прийдуть на зміну системам MPT. При цьому будуть забезпечені сумісність і спадкоємність систем MPT і TETRA.

Водночас знаходять своє застосування і закриті системи, тобто системи фірма-виробник яких не публікує протоколи їх роботи і сама розробляє все абонентське і базове устаткування для таких систем. При цьому споживач

знаходиться в повній залежності від фірми-виробника.

Для українських операторів найкращим варіантом стало б приєднання до відкритих міжнародних стандартів. Як би не були ефективними системи з закритими протоколами зв'язку, було б неправильним ставити себе в абсолютну залежність від фірм-розроблювачів. Крім того, при розробці вітчизняних систем радіозв'язку доцільно дотримуватися меж міжнародних стандартів - це дасть можливість користуватися міжнародною корпорацією в галузі елементної бази, програмного забезпечення тощо.

За кількістю абонентів, що обслуговуються, системи можна класифікувати на:

- малі системи, в яких кількість абонентів не перевищує 300;
- середні системи, в яких кількість абонентів складає 300 – 3000;
- великі системи, в яких кількість абонентів більша 3000.

За організацією доступу до системи ТСР можна класифікувати на:

- системи без каналу керування;
- системи з розподіленим керуючим каналом;
- системи з виділеним каналом керування.

Найбільш популярними в класі систем без каналу керування стали системи на базі протоколу SmarTrunk II американської компанії SniarTnmk Systems Inc (колишня Selectone). Ця система не має каналу керування, тому функції пошуку вільного каналу перекладені на абонентські станції. При запиті з'єднання радіостанція послідовно сканує всі ретранслятори системи. При виявленні вільного, вона захоплює його, після чого ретранслятор передає в ефір сигнал виклику кореспондента. Якщо станція, що викликається, окликається, ретранслятор організує сеанс зв'язку. Середній час з'єднання складає декілька секунд. Системи без каналу керування ідеальні для оперативного і мобільного радіозв'язку з виходом у телефонну лінію в одній зоні радіусом 38-50 км. Кількість абонентів в межах від 2 до 4000, а вартість базового й абонентського комплекту значно менша, ніж у стільникових мережах [6, 7].

Головними перевагами систем Smar Trunk II є простота, надійність, невисока вартість, різноманітний асортимент апаратури, відсутність недоліків звичайних радіостанцій, невибагливість у виборі робочих частот.

Проте, таким ТСР притаманний ряд принципових вад. Із зростанням кількості каналів швидко зростає тривалість установлення з'єднання в такій системі, тому що вона не може бути меншою тривалості повного циклу сканування. Реально до цього додається ще і тривалість пошуку вільного каналу радіостанцією, що викликає. Крім того, в скануючих ТСР складна реалізація багатьох сучасних вимог, у числі яких багатозоновість, гнучкість і надійна система пріоритетів, захист від несанкціонованого доступу, встановлення в чергу при зайнятості системи або абонента, що викликається.

У такий спосіб скануюча ТСР ідеально підходить у якості незначної (1-8 каналів, до 200 абонентів) однозонової системи зв'язку, до якої висуваються мінімальні вимоги.

2.4 Цифрові системи радіозв'язку з розподіленим керуванням

Цей клас наданий протоколом LTR (Logic Trunked Radio) фірми E.F. Jonhson [10]. У цих ТСР керуюча інформація передається безупинно по всіх каналах, у тому числі і по зайнятим. Це досягається використанням для її передачі частот нижче 300 Гц. Кожен канал є керуючим для радіостанцій, закріплених за ним. У черговому режимі радіостанція прослуховує свій керуючий канал. У цьому каналі БС безупинно передає номер вільного каналу, який радіостанція може використовувати для передачі. Якщо ж на якомусь каналі починається передача, адресована одній з радіостанцій, то інформація про це передається на її керуючому каналі, у результаті чого ця радіостанція перемикається на канал, де відбувається виклик.

Такі ТСР характеризуються всіма перевагами, які властиві ТСР із керуючим каналом, не вимагаючи в той же час виділення частот для нього. У

системі LTR встановлення з'єднання відбувається настільки швидко, що воно здійснюється щораз при вмиканні передавача станції, тобто в паузах розмови канал не зайнятий.

Проте, при виході з ладу якогось каналу, в системі LTR відбувається відмова всіх радіостанцій, для яких він є керуючим. Крім того, у таких ТСР швидкість передачі керуючої інформації вкрай обмежена. Це утрудняє реалізацію багатьох розгортання стільникових систем не планується, а також для повсякденної роботи підприємств, рядовий і керуючий персонал яких постійно потребує якісного оперативного зв'язку.

Цифрові системи надають сервіс не тільки канального, але і мережного рівня, а в ряді випадків і транспортного. Можливе підтримання накладених мереж, наприклад IP-мереж. Стандарт TETRA передбачає швидкість до 28,8 кбіт/с. При проектуванні власних мереж передачі даних на базі цифрових систем радіозв'язку користувачеві надається, як правило, можливість вибору параметрів протоколу канального і транспортного рівня, а також можливість використання датаграм.

Устаткування базових станцій або центрального комутатора цифрових систем радіозв'язку здійснює також функції шлюзу з зовнішніми мережами передачі даних, тобто мережами з комутацією пакетів. До функцій шлюзу належать: конвертування протоколів, включаючи взаємне перетворення адрес внутрішньої і зовнішньої мереж, а також підтримання накладеної мережі.

Найважливіша галузь застосування служб передачі даних - організація в межах цифрових систем мереж дистанційного моніторингу та контролю місця розташування рухомих об'єктів.

У деяких цифрових системах радіозв'язку передбачена можливість безпосереднього зв'язку абонентів без участі ретранслятора. Цей режим, що називається також Talk Around або Direct Mode Operation, використовується в тому випадку, якщо один або декілька абонентів вийшли з зони дії всіх ретрансляторів системи , або при аварії контролерів і обриві ліній зв'язку в зоні обслуговування базової станції.

Устаткування цифрових систем радіозв'язку дозволяє вести облік і тарифікацію з'єднань з одержанням докладної інформації з кожного з'єднання. До даних обліку і тарифікації можуть належати такі параметри: ідентифікація абонента, який викликає і абонентів, які викликаються, дата і час початку встановлення з'єднання, тривалість з'єднання, тип виклику, категорія пріоритету. Дані тарифікації можуть використовуватися для документування зв'язку і надання рахунків абонентам, а також для виявлення спроб несанкціонованого доступу.

Ряд цифрових систем радіозв'язку надає оператору можливість оперативної зміни параметрів доступу абонентських радіостанцій. Так, у системі EDACS можна дистанційно перепрограмувати мережний ідентифікатор (Ш), частоти каналів, а також переконфігурувати групи абонентів.

2.5 Аналіз особливостей організації односайтових та багатосайтових систем

Кожній станції (радіомережі) на час розмови виділяється один дуплексний чи симплексний радіоканал. Сукупність рівнодоступних каналів, що виділяються декільком РГ (радіомережам), складає канальну базу (trunk) системи. Для забезпечення зв'язку великій кількості M мобільних радіоабонентів, розподілених по розмовних групах, виділяється обмежена кількість N радіоканалів (робочих частот). Використання умови M > N засновано на статистичній нерівномірності потоку заявок на виклики навіть у години найбільшого навантаження (ГНН) системи.

Цифрові системи зв'язку залежно від площі зон обслуговування можуть бути односайтовими і багатосайтовими. В односайтових системах зона обслуговування (ЗО) формується у вигляді одного телекомунікаційного осередку СТО), що обслуговується комплектом базового устаткування.

Структура односайтової цифрової системи зв'язку показана на рис. 2.2. З рисунка видно, що на одній несучій частоті може працювати 4 абонента.

Системний комплект базового устаткування сайту включає: базове устаткування (базовий багатоканальний ретранслятор, комбайнерка система, антенно-фідерний пристрій, базовий контролер з телефонним інтерконнектом).

До складу базового устаткування може входити також базовий комп'ютер сайту.

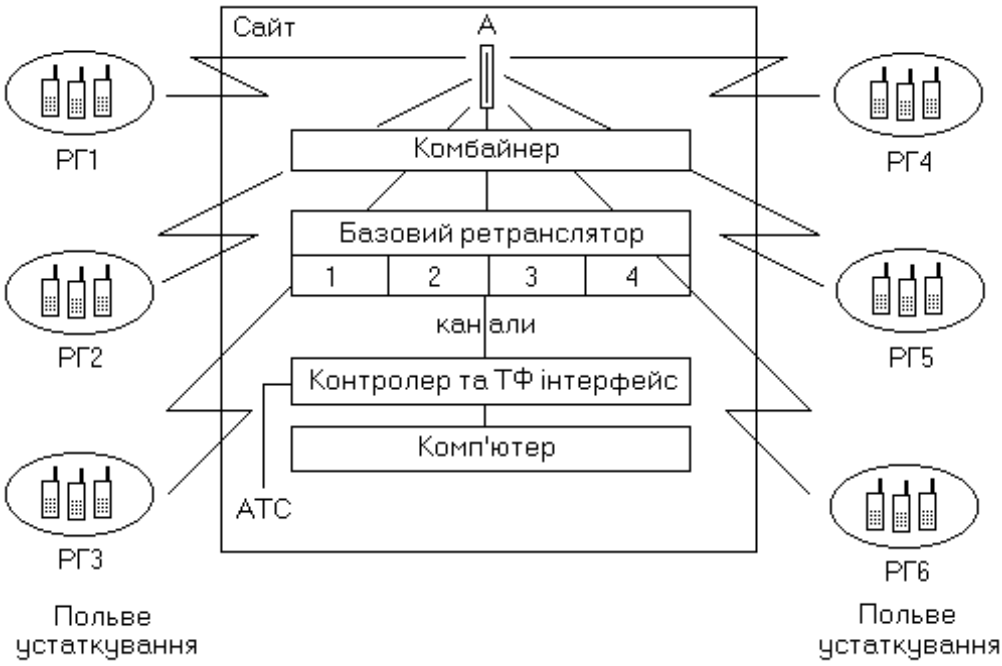


Рисунок 2.2 – Структура односайтової цифрової системи зв'язку

Базовий багатоканальний ретранслятор включає кілька незалежних трактів передачі й прийому, об'єднаних у блоці каналів у канальні пари. Кількість канальних пар ретранслятора визначає канальну базу (trunk) сайта. Антенно-фідерний пристрій (АФП) базового устаткування включає загальну прийомопередаючу антену (А), фідерну лінію і комбайнерку систему. Комбайнерка система забезпечує розв'язку трактів передачі блоку каналів при їх роботі на один АФП. Базовий контролер є центральним процесором сайта, що забезпечує автоматизацію процесів каналоутворення та контролю.

Телефонний інтерконнект дозволяє підключати базовий контролер сайта до фіксованої телефонної мережі загального користування, а також до каналоутворюючого устаткування (КУ) при побудові багатосайтової системи. Базовий комп'ютер сайту виконує задачі системного менеджера. Він забезпечує керування конфігурацією системи та користувальницьких функцій абонентів.

Формування розмовних груп здійснюється шляхом виділення кожної з них кодових послідовностей (адрес) за допомогою системного менеджера (базового комп'ютера). Системний менеджер забезпечує також програмування елементів польового устаткування і привласнює адреси привілейованим MS. Він дозволяє змінювати конфігурацію системи, змінювати склад і кількість РГ за заявкою замовника. Розмовні групи (РГ) у системі можуть поєднуватися в макрогрупи.

У багатосайтовій системі (рис. 2.3) створюється декількома сайтами, що з'єднуються між собою високошвидкісними каналами зв'язку через зоновий комутатор передачі даних.

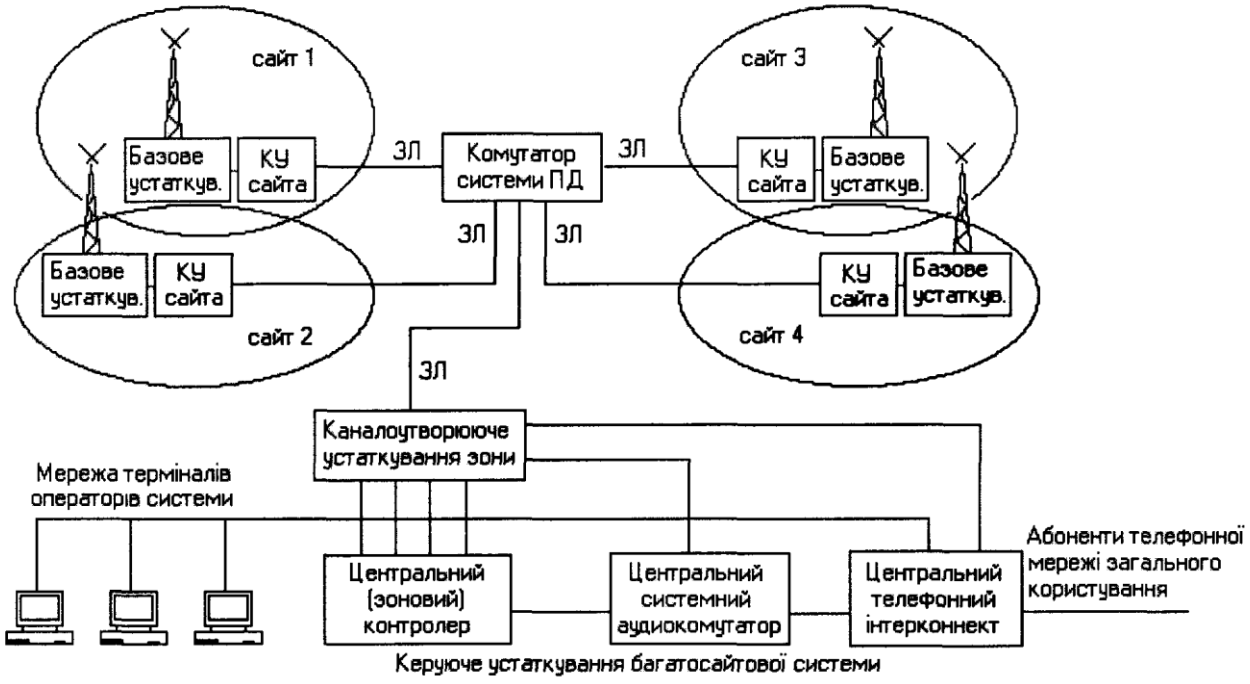


Рисунок 2.3 - Структура багатосайтової цифрової системи зв'язку МРТ 1327

До складу базового устаткування кожного сайта входить каналоутворююче устаткування, що забезпечує формування цифрових потоків з іншими сайтами. Для організації міжсайтового зв'язку використовують виділені багатоканальні сполучні лінії. З'єднувальні лінії (ЗЛ) можуть будуватися за допомогою апаратури радіорелейного зв'язку, волоконно-оптичних ліній і кабельних ліній зв'язку.

Для передачі інформаційних потоків в інші ЗО використовується зонове устаткування, що включає: зонове каналоутворююче устаткування (ЗКУ); зоновий контролер (ЗК); зоновий телефонний інтерконнект (ЗТІ); зоновий аудіокомутатор (ЗАК). Таким чином, міжзонова система телекомунікацій дозволяє маршрутизувати основні інформаційні потоки минаючи міжміську мережу загального користування.

2.6 Оцінювання площі покриття цифрової системи радіозв'язку з рухомими об'єктами

Відомо велику кількість методик розрахунку забезпеченості абонентів радіозв'язком в цифрових мережах [1-3].

Більшість методик опираються на результати теоретичних та практичних досліджень РРВ в реальних умовах. Процес оцінки зони обслуговування складається з декількох етапів:

1. Визначають потужність сигналу, який випромінюється в ефір.

2. Визначають середню потужність сигналу на приймальній антені, при якій забезпечується потрібна чутливість приймача.

3. По результатам розрахунків 1-го та 2-го етапів визначають допустимий рівень втрат на трасі РРВ.

4. Вибирають модель розрахунку втрат на трасі РРВ і на її основі будують графік залежності втрат від відстані. По даному графіку визначають середню дальність радіозв'язку з урахуванням запасу на забезпечення

зв'язком по місцю та часу.

Розглянемо дані етапи більш докладно.

Випромінююча потужність сигналу визначається виразом:

$$P_{випр} = P_{прд} + G_A + B_{фс}, \text{ (дБ)}, \quad (2.1)$$

де $P_{прд}$ - потужність передавача дБ Вт;

G_a - коефіцієнт підсилення передавальної антени;

$B_{пфс}$ - коефіцієнт передачі фідера та інших ланцюгів між передавачем та приймальною антеною.

Таблиця 2.1 – Дані для розрахунку основних параметрів мережі

Параметри	БС 1	БС 2	БС 3	БС 4	БС 5	БС 6	БС 7	БС 8	БС 9	БС 10	БС 11	БС 12	БС 13	БС 14
Площа обсл., тис.	1,3	2,5	1,3	1,8	2,8	2,5	1,8	2,3	2,5	2,0	1,98	2,54	3,9	1,5
Кількість населення, тис.	67,6	96,5	42,7	55,1	70,3	60,7	56,6	64,7	86,1	68,9	71,1	72,2	113	45,1
Втрати в зоні, %	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Середнє число викликів від 1 абон.	3,4	3,9	3,0	3,2	3,5	3,2	3,0	3,4	3,6	3,4	3,4	3,5	4,0	2,9
Радіус зони, км.	20	28	20	24	30	28	24	27	28	28	28	28	30	20
Кількість абон.	180	350	100	100	190	140	100	150	300	200	230	250	400	100
Число викликів від 1 абон. в ЧНН	2,7	3,6	2,2	2,8	3,0	2,9	2,7	2,6	3,4	2,8	3,1	3,0	4,0	2,5
Середній час розмови	10	15	12	10	15	18	20	10	15	18	20	10	15	20
Коефіцієнт тяжіння абонентів до АТС	0,05	0,05	0,03	0,03	0,05	0,03	0,05	0,05	0,1	0,1	0,1	0,1	0,15	0,03

Необхідна потужність сигналу на приймальній антені визначається виразом:

$$P_A = P_{прм} - G_{па} - B_{пфс} + \Delta_c, \text{ (дБ)}, \quad (2.2)$$

де $P_{прм}$ - чутливість приймача дБ Вт;

$G_{па}$ - коефіцієнт підсилення приймальної антени, дБ;

$B_{пфс}$ - коефіцієнт передачі фідера та інших кіл між антеною та приймачем;

Δ_c - коефіцієнт забезпечення зв'язком по місцю та часу, дБ.

Подвійний коефіцієнт вносить поправку для забезпечення з заданою імовірністю перевищення потужності сингала на вході антени відносно середнього значення. Значення цього коефіцієнта визначається багатьма факторами, в тому числі характером РРВ, щільністю забудованості місцевості, потрібним забезпеченням зв'язком. Так у відповідності з (2.2) при Δ_c=0 дБ потужність сигналу на вході приймача буде перевищувати заданий рівень в 50% випадках, а при Δ_c = 10 дБ - в 90%.

Допустимий рівень втрат на трасі РРВ визначається у відповідності з виразом [1]

$$L_g = P_{випр} - P_A = P_{прд} + G_A + B_{фс} - P_{прм} + G_{па} - B_{пфс} - \Delta_c, \text{ (дБ)} \qquad (2.3)$$

Для оцінки L_g системи TETRA використовується модель розрахунку втрат на трасі РРВ, яка заснована на моделі Харта. Вона дозволяє прогнозувати усереднені втрати при РРВ у відкритому просторі, в сільській місцевості та в місті.

Вихідними даними для оцінки втрат являються:

h_b - висота установки антени базової станції, м;

h_m - висота установки антени мобільної станції, м;

f_c - несуча частота сигналу, МГц.

Коефіцієнт втрат у вільному просторі визначається виразом

$$L_{OA} = 27{,}81 + 27{,}72\,Lg(f_c) - 13{,}82\,Lg(h_g) - [11Lg(f_c) - 0{,}7]h_m + \\ + [44{,}9 - 6{,}55Lg(h_b)] \cdot LgR - 4{,}78[Lg(f_c)]^2, \text{ дБ}, \qquad (2.4)$$

де R - відстань в км від передавача до точки прийому.

У відповідності з моделлю Харта коефіцієнт втрат при РРВ в сільській місцевості на відкритому просторі визначається виразом [1]

$$L_{RA} = L_{OA} + 10\ дБ. \qquad (2.5)$$

При РРВ в місті:

$$L_{OA} = 63{,}35 + 27{,}72\,Lg(f_c) - 13{,}82\,Lg(h_g) - [11Lg(f_c) - 0{,}7]h_m + \\ + [44{,}9 - 6{,}55Lg(h_b)] \cdot LgR - 2[Lg(f_c/28)]^2, \text{ дБ}. \qquad (2.6)$$

У відповідності з виразами (2.5) та (2.6) при значенні висоти антени мобільної станції h_m = 15 та трьох значень висот базової станції h_b = 30; 50; 100 та f_c = 400 МГц для отриманих раніше значень радіусу зон обслуговування R розрахуємо значення коефіцієнта втрат на трасі РРВ для сільської місцевості та міста для кожної БС мережі. Результати розрахунків представимо у вигляді таблиці.

Для забезпечення заданої якості зв'язку розраховані втрати повинні бути на (6-7) дБ менше втрат, які визначені у відповідності з виразом (2.3) тобто:

$$Lg \geq L_{RA} + (6\text{-}7)\ дБ,$$

$$Lg \geq L_{OA} + (6\text{-}7)\ \text{дБ}. \qquad (2.7)$$

Використовуючи нерівності (2.7) та вираз (2.3) визначимо необхідну потужність передавача БС1.

Приклад розрахунку втрат для БС1 при висоті антени 30 метрів

а) для сільської місцевості (відкритий район):

$$L_{RA} = 27{,}81 + 27{,}72lg(400) - 13{,}82lg(30) - [11lg(400) - 0{,}7] \cdot 1{,}5 +$$
$$+ [44{,}9 - 6{,}55lg(30)] \cdot lg(20) - 4{,}78[lg(400)]^2 + 10 = 61{,}1\ дБ;$$

б) для міста:

$$L_{OA} = 63{,}35 + 27{,}72lg(400) - 13{,}82lg(30) - [11lg(400) - 0{,}7] \cdot 1{,}5 +$$
$$+ [44{,}9 - 6{,}55lg(30)] \cdot lg(20) - 4{,}78[lg(400/28)]^2 = 116{,}342\ дБ.$$

Для висот 50 м.,100 м., та решти БС проводимо аналогічний розрахунок і результати зводимо до таблиці 2.2.

Далі після розрахунку втрат розраховуємо значення $P_{прд}$ для двох значень Δ_c (Δ_c =0; Δ_c = 10) та трьох значень h_b = 30 м; h_b = 50 м; h_b =100 м, та двох видів мобільних станцій (носима, возима).

$B_{фсбс}$ = -6дБ; $B_{фпс\ мс}$ = -2 дБ; $B_{пфс\ нос.ст}$ = 0 дБ;

$G_{АБС}$ = 8 дБ; $G_{ПАМС}$ = 2 дБ; $G_{ПАпост}$ = -4дБ.

Таблиця 2.2 – Результати розрахунків втрат базових станцій

	БСІ	БС2	БС3	БС4	БС5	БС6	БС7	БС8	БС9	БС10	БС11	БС12	БС13	БС14
LRA 30м LOA	61Д	66	61Д	67,5	67	66	67	65,6	66	66	66	66	67	61
	116	121	116	122	122	121	122	120	121	121	121	121	122	116
LRA 50м LOA	56,1	63	56,2	58,8	62	63	58,8	60.5	63	63	63	63	62	56
	111	116	111,4	114	117	116	114	115	116	116	116	116	117	111
LRA 100м LOA	49,4	54	49,4	51,9	55	54	51,9	53	54	54	54	54	55	49
	104	109	105	107	110	109	107	108	109	109	109	109	110	104

Для динамічних умов $P_{ПРМмс} = P_{ПРМнос.мс} = -103$ дБм.

Розраховуємо для МС1:

$$\Delta_c = 0\ дБ;\ \ h = 30\ м.$$

Для сільської місцевості:

$$P_{ПРД} \geq L_{RA} + 6 - G_A - B_{фс} + P_{ПРМ} - G_{па} - B_{пфс} + \Delta_c. \qquad (2.8)$$

Для міста:

$$P_{ПРД} \geq L_{OA} + 6 - G_A - B_{фс} + P_{ПРМ} - G_{па} - B_{пфс} + \Delta_c, \qquad (2.9)$$

$$P_{ПРДRA} \geq 61{,}1 + 6 - 8 + 6 - 103 - 2 + 2 + 0 = -37\ дБ;$$

$$P_{ПРДOA} \geq 116 + 6 - 8 + 6 - 103 - 2 + 2 + 0 = 17\ дБ.$$

Далі розраховуємо для решти мобільних станцій. Для носимих мобільних станцій розрахунок аналогічний.

В результаті розрахунку здійснено оцінку потужності передавачів мобільних і носимих мобільних станцій, а також визначено оптимальні потужності, які підходять для забезпечення необхідної якості зв'язку по всій зоні покриття Базових станцій. Розрахунки виконано для різних висот антен і різних коефіцієнтів забезпечення зв'язком по місцю і в часі.

3 ВИБІР ТА ОБГРУНТУВАННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ЦИФРОВИХ ЗАСОБАХ РАДІОЗВ'ЯЗКУ

3.1 Метод скремблювання

3.1.1 Аналогове скремблювання

У мовних системах зв'язку відомі два основних методи закриття мовних сигналів, що розрізняються за способом передачі по каналах зв'язку: аналогове скремлювання і дискретизація мови з подальшим шифруванням. Під скремблюванням розуміється зміна характеристик мовного сигналу таким чином, що отриманий модульований сигнал, володіючи властивостями нерозбірливості і невпізнання, займає ту ж смугу частот, що і початковий сигнал.

Кожен з цих методів має свої переваги та недоліки. Так, для аналогових скремблерів характерна присутність при передачі в каналі зв'язку фрагментів початкового відкритого мовного повідомлення, перетворення в частотній і часовій області. Це означає, що зловмисники можуть спробувати перехопити і проаналізувати інформацію, що передається, на рівні звукових сигналів. Тому раніше вважалося, що, не дивлячись на високу якість і розбірливість відновлюваної мови, аналогові скремблери можуть забезпечувати лише низький або середній в порівнянні з цифровими системами ступінь закриття, проте новітні алгоритми аналогового скремблювання, здатні забезпечити високий рівень закриття.

Аналогові скремблери поділяються на:

- мовні скремблери найпростіших типів на базі часових і(або) частотних перестановок мовного сигналу (рис. 3.1);

- комбіновані мовні скремблери на основі частотно-часових перестановок відрізків мови, представлених дискретними відліками, зі застосуванням цифрової обробки сигналів (рис. 3.2).

Аналогові скремблери перетворюють початковий мовний сигналі за допомогою зміни його амплітудних, частотних і часових параметрів в різних

комбінаціях. Скрембльований сигнал потім може бути переданий по каналу зв'язку в тій же смузі частот, що й відкритий.

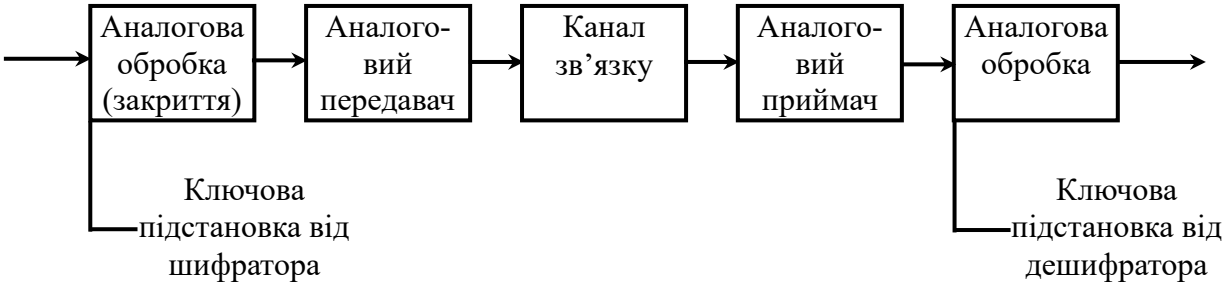


Рисунок 3.1 – Структура найпростішого мовного скремблера

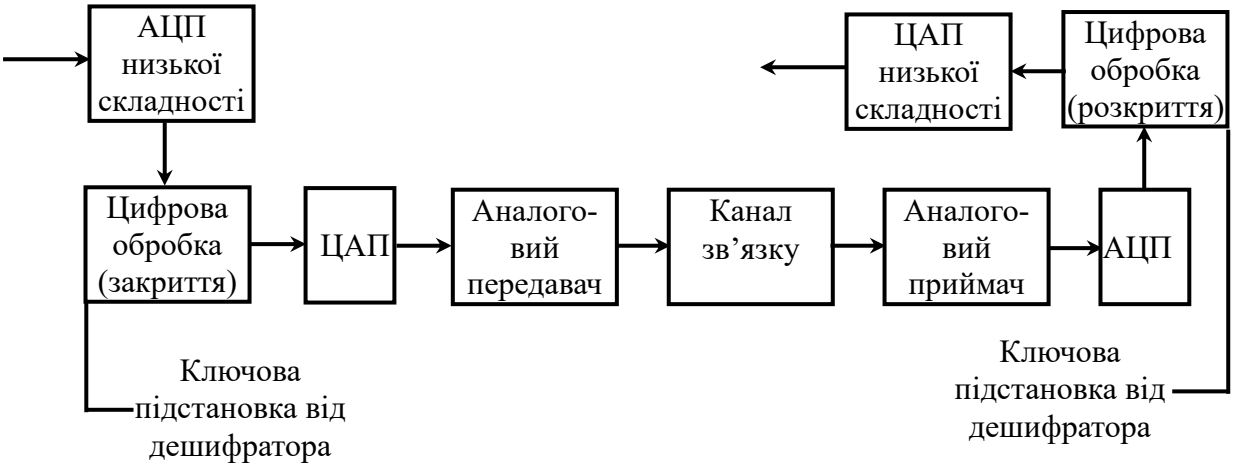


Рисунок 3.2 – Структура комбінованого мовного скремблера

В апаратах мовного типу використовується наступні принципи аналогового скремблювання:

1) скремблювання в частотній області: частотна інверсія (перетворення спектру сигналу за допомогою гетеродина і фільтра), частотна інверсія і зсув (частотна інверсія зі змінним стрибкоподібним зміщенням несучої частоти), розділення смуги частот мовного сигналу на ряд піддіапазонів з подальшою їх перестановкою і інверсією;

2) скремблювання в часовій області – розбиття фрагментів на сегменти

з перемішуванням їх прямим і(або) інверсним прочитуванням;

3) комбінація часового і частотного скремблювання.

Існує два основні види частотних скремблерів – інверсні та смугові. Обидва засновані на перетвореннях спектру початкового мовного сигналу для закриття інформації, яка передається, і відновлення отриманого повідомлення шляхом зворотних перетворень.

3.1.2 Цифрове скремблювання

При цифровому скремблюванні мовний сигнал перетворюється шляхом дискретизації у часі в цифровий сигнал, який піддається будь-якому з криптографічних алгоритмів. Забезпечує значно вищий захист. У процесі цифрового скремблювання може застосовуватися збереження форми вхідного сигналу, тобто збереження всіх властивостей надлишковості аналогового сигналу. Таке цифрове скремблювання називають широкосмуговим. Використовують для цього різні види ІКМ та при цьому швидкість цифрових сигналів у каналах зв’язку достатньо висока.

Для вузькосмугових систем цифрового скремблювання перед шифруванням інформації здійснюють процедуру зменшення надлишковості, яка виконується у вокодерних пристроях, при цьому можна досягти швидкості передачі інформації 1200-1400 біт/с.

Вокодери ділять на дві групи: смугові та з лінійним передбаченням. В смугових вокодерах принцип стиснення інформації полягає в тому, що мовний сигнал ділиться на відрізки приблизно в 20 мс і кожен з таких сегментів надходить на групу фільтрів, яких нараховується в межах 16-20. Після проходження фільтрами визначаються амплітуди вихідних сигналів і ці параметри передаються каналом зв’язку.

На приймальній частині здійснюється процедура синтезу мовного сигналу, яка відбувається шляхом встановлення відповідних коефіцієнтів передачі таких же фільтрів відповідно до переданих параметрів. На виході фільтрів синтезується вхідний сигнал.

У вокодерах з лінійним передбаченням, що знайшли значно ширше застосування, зменшення швидкості передачі інформації забезпечується завдяки принципу кусочно-лінійної апроксимації, який полягає в тому, що здійснюється кодування кожного поточного відліку амплітуди з урахуванням певної кількості попередніх відліків. В такому вокодері існують алгоритми мінімізації відхилень значень параметрів від реальних. Після вокодерних пристроїв у системах мовної передачі інформації встановлюються шифратори, які працюють по одному з криптографічних алгоритмів без перетворення в аналоговий сигнал, а шляхом узгодження отриманих цифрових потоків з каналом зв'язку сигнал передається до приймальної частини.

В стандарті GSM процедура шифрування мовного сигналу здійснюється в кодері каналу перед процедурою завадостійкого кодування. Процес закриття мовної інформації полягає в тому, що до двійкової послідовності сигналів після вокодерного пристрою додаються біти псевдовипадкової послідовності по модулю 2, для цього за певним алгоритмом генерується псевдовипадкова послідовність S1. Вона працює в прямому каналі при передачі сигналу від базової станції до рухомої. В зворотному каналі типу ПВП-S2, яка також працює по модулю 2. В стандарті GSM для кожного сеансу відбувається генерування своєї псевдовипадкової послідовності. В системах мобільного зв'язку при кожному встановленні зв'язку виконуються процедури аутентифікації та ідентифікації.

3.2 Криптографічні методи захисту інформації

Криптографія представляє собою сукупність методів перетворення даних, спрямованих на те, щоб знайти ці дані непотрібними для противника. Такі перетворення дозволяють розв'язати дві головні проблеми захисту даних: проблему конфіденційності та цілісності.

Вирішення проблеми конфіденційності означає позбавлення

противника можливості скористатися інформацією з каналу зв'язку. Проблема цілісності означає позбавлення противника можливості модифікації повідомлення (рис. 3.3).

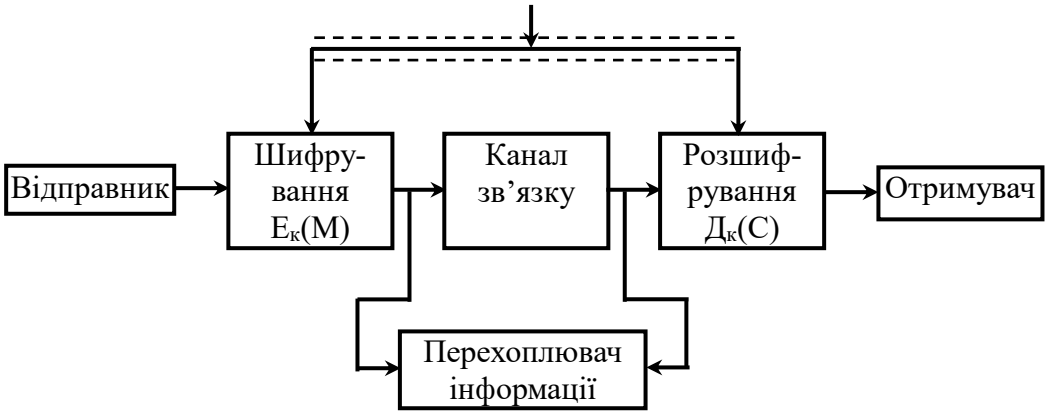


Рисунок 3.3 – Схема проходження сигналу

Відправник генерує відкритий текст повідомлення "М", яке повинно бути передане законному отримувану незахищеним каналом зв'язку. За каналом слідкує перехоплювач з метою перехопити і розкрити передане повідомлення. Для того, щоб перехоплювач не зміг впізнати зміст повідомлення "М" відправник шифрує його за допомогою оберненого перетворення $E_к$ і отримає шифр-текст або криптограму "С", яка є результатом перетворення $C = E_к(M)$.

Отримувач, прийнявши шифр-текст "С" розшифровує його за допомогою зворотного перетворення. Повідомлення "М", яке отримує отримувач $M = Д_к(C) = E_к^{-1}(E_к(M))$. Перетворення $E_к$ вибирається з сімейства криптографічних перетворень, що називаються криптоалгоритмами. Параметр, за допомогою якого вибирається окреме перетворення, називається криптографічним ключем К. На наведеній схемі (рис. 3.3) схемі "К" надходить відправнику і отримувачу по захищеному каналу. Криптосистема має різні варіанти реалізації, набір інструкцій, апаратні засоби, комплекс програм комп'ютера, які дозволяють зашифрувати відкритий текст з використанням ключа К. Перехоплення інформації в криптографічній системі може бути пасивним і активним. Якщо перехоплювач обмежується лише

функцією підслуховування, то має місце лише пасивне перехоплення. Якщо перехоплювач знімає з каналу зв'язку інформацію, змінює чи модифікує її і спрямовує знову в канал в бік отримувача, то має місце електронно-активне перехоплення. Активний перехоплювач не тільки зчитує всі тексти, які передаються по каналу, але й може змінити їх на свій розсуд. Перетворення шифрування може бути симетричним або асиметричним відносно перетворення шифрування. Ця властивість функції перетворення визначає два класи криптосистеми: симетричні (одноключові) криптосистеми, асиметричні (двоключові). Наведена схема (рис. 3.4) є схемою криптосистеми з одним секретним ключем.

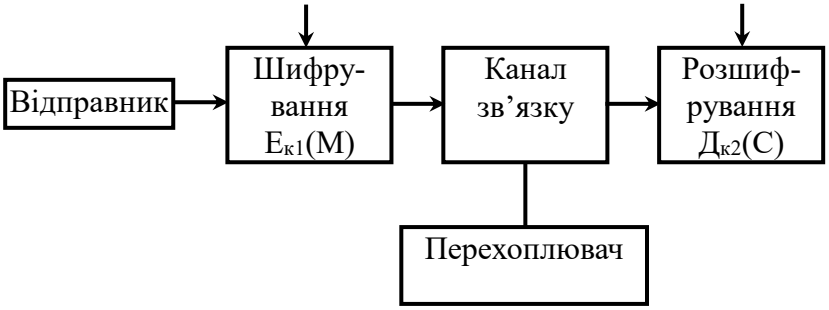


Рисунок 3.4 – Схема перехоплення сигналу

Ключ передається відправнику і отримувачу по захищеному каналу, це не завжди зручно і не завжди забезпечує. В асиметричній криптосистемі передають по незахищеному каналу тільки відкритий клич, а секретний зберігають на місці його генерації. Будь-яка спроба з боку перехоплювача розшифрувати шифр-текст "С" для отримання відкритого тексту "М" або зашифрувати свій власний "М" для отримання правдоподібного "С", не маючи дійсного ключа, називається криптоаналітичною атакою. Якщо спроби криптоаналітичних атак не досягають поставленої мети і криптоаналітик не може (не маючи ключа) вивести повідомлення М з криптосистеми, то вважають, що така система є криптостійкою.

3.2.1 Криптосистема шифрування даних RSA

Алгоритм RSA запропонували у 1978 році такі автори: Р. Райвест, А.

Шамір і А. Адлеман. Алгоритм одержав свою назву по перших буквах прізвищ його авторів. Алгоритм RSA став першим повноцінним алгоритмом з відкритим ключем, що може працювати як у режимі шифрування даних, так і в режимі електронного цифрового підпису [7].

Надійність алгоритму ґрунтується на труднощах факторизації великих чисел і труднощів обчислення дискретних логарифмів.

У криптосистемі RSA відкритий ключ $К_в$, секретний ключ $k_в$, повідомлення M і криптограма C належать безлічі цілих чисел

$$Z_N = \{0, 1, 2, ..., N-1\}, \quad (3.1)$$

де N - модуль:

$$N = P \cdot Q. \quad (3.2)$$

Тут P і Q – випадкові великі прості числа. Для забезпечення максимальної безпеки вибирають P і Q рівної довжини і зберігають у секреті.

Множина Z_N з операціями додавання і множення по модулю N утворює арифметику по модулю N.

Відкритий ключ $К_в$ вибирають випадковим чином так, щоб виконувалися умови:

$$1 < К_в \le \varphi(N), \qquad НОД(К_в, \varphi(N)) = 1, \quad (3.3)$$

$$\varphi(N) = (P - 1)(Q - 1), \quad (3.4)$$

де φ(N) - функція Эйлера.

Функція Эйлера φ(N) вказує на кількість позитивних цілих чисел в інтервалі від 1 до N, що взаємно прості з N.

Друга із зазначених вище умов означає, що відкритий ключ $К_в$ та функція Эйлера φ(N) повинні бути взаємно простими.

Далі, використовуючи розширений алгоритм Евкліда, обчислюють секретний ключ $k_в$, такий що

$$k_в \cdot К_в \equiv 1 (mod \varphi(N)) \quad (3.5)$$

$$k_в = К_в^{-1} (mod\ (P-1)(Q-1)).$$

Це можна здійснити, тому що одержувач B знає пару простих чисел (P,

Q) і може легко знайти φ(N). Помітимо, що $k_в$ і N повинні бути взаємно простими.

Відкритий ключ $К_в$ використовують для шифрування даних, а секретний ключ $k_в$ – для розшифрування.

Перетворення шифрування визначає криптограму С через пару (відкритий ключ $К_в$, повідомлення М) відповідно до наступної формули:

$$C = E_{Кв}(M) = К_в\ (M) = M^{Кв}(mod\ N). \quad (3.6)$$

Як алгоритм швидкого обчислення значення С використовують ряд послідовних зведень у квадрат цілого М і множень на М з приведенням по модулю N.

Обернення функції $C = M^{Кв}(mod)$, тобто визначення значення М за відомим значенням С, $К_в$ та N, практично не здійсненно при $N \approx 2^{512}$.

Однак зворотну задачу, тобто задачу розшифрування криптограми С, можна вирішити, використовуючи пари (секретний ключ ke, криптограма З) за наступною формулою:

$$M = D_{кв}(C) = D_в(C) = C^{кв}\ (mod\ N). \quad (3.7)$$

Процес розшифрування можна записати так:

$$D_в(E_в(M)) = M. \quad (3.8)$$

Підставляючи в (3.8) значення (3.7) і (3.6), одержуємо:

$$(M^{Кв})^{кв} = M\ (mod\ N)\ \text{або}$$

$$M^{Квкв} = M(mod). \quad (3.9)$$

Величина φ(N) відіграє важливу роль у теоремі Ейлера, що стверджує, що якщо НОД (x, N) = 1, то

$$x^{\varphi(N)} \equiv 1(mod\ N),$$

або в більш загальній формі

$$x^{n\cdot\varphi(N)\div 1} \equiv x(mod\ N). \quad (3.10)$$

Співставляючи вирази (3.9) і (3.10), одержуємо

$$K_в \cdot k_в = n \cdot \varphi(N) + 1$$

або, що те ж саме,

$$K_в \cdot k_в = 1(mod\varphi(N)).$$

Для обчислення ключа $k_в$ використовують співвідношення (3.5).

Таким чином, якщо криптограму C = $M^{K_в}$(mod 1(mod N) піднести до степеня $k_в$, то в результаті відновлюється вихідний відкритий текст M, оскільки

$$(M^{K_в})^{k_в} = M^{K_в k_в} = M^{n \cdot \varphi(N)+1} = M \ (mod\ N).$$

Таким чином, одержувач B, що створює криптосистему, захищає два параметри: 1) секретний ключ $k_в$ і 2) пари чисел (P, Q), добуток яких дає значення модуля N. З іншого боку, одержувач B відкриває значення модуля N і відкритий ключ $K_в$.

Сторонньому абоненту відомі лише значення $K_в$ і N. Якби він зміг розкласти число N на множники P і Q, то він довідався б про "потайной хід" - трійку чисел {P, Q, $K_в$}, обчисливши значення функції Ейлера

$$\varphi(N) = (P-1)(Q-1)$$

і визначивши значення секретного ключа $k_в$.

Однак, як вже відмічалося раніше, розташування дуже великого N на множники обчислювально не здійсненне (за умови, що довжини вибраних P і Q складають не менше 100 десяткових знаків).

Щоб гарантувати необхідний захист інформації до систем з відкритим ключем, висуваються наступні вимоги:

1. Перетворення початкового тексту повинно виключати його відновлення на основі відкритого ключа.

2. Визначення закритого ключа на основі відкритого повинне бути обчислюване отримувачем. При цьому бажана точна нижня оцінка складності (кількості операцій) розкриття шифру.

Алгоритми шифрування з відкритим ключем отримали широке розповсюдження в сучасних інформаційних системах.

3.2.2 Американський стандарт шифрування даних DES

Стандарт шифрування даних DES (Data Encryption Standard) опублікований у 1977 році Національним бюро стандартів США. Стандарт DES призначений для захисту від несанкціонованого доступу до важливої, але несекретної інформації в державних і комерційних організаціях США.

До цього часу DES є найбільш розповсюдженим алгоритмом, що використовується у системах захисту комерційної інформації. Більш того, реалізація алгоритму DES у таких системах стає ознакою гарного тону.

Основні достоїнства алгоритму DES:

• використовується тільки один ключ довжиною 56 біт;

• зашифрувавши повідомлення за допомогою одного пакета програм, для розшифровки можна використовувати будь-який інший пакет програм, що відповідає стандарту DES;

• відносна простота алгоритму забезпечує високу швидкість обробки;

• досить висока стійкість алгоритму.

Спочатку метод, що лежить в основі стандарту DES, був розроблений фірмою IBM для своїх цілей і реалізований у виді системи "Люцифер". Система "Люцифер" заснована на комбінуванні методів підстановки і перестановки і складається з послідовності блоків перестановки і підстановки, що чергуються. В ній використовувався ключ довжиною 128 біт, що керував станами блоків перестановки і підстановки. Система "Люцифер" виявилася досить складною для практичної реалізації через відносно малу швидкість шифрування (2190 байт/с – програмна реалізація, 96970 байт/с – апаратна реалізація).

Алгоритм DES також використовує комбінацію підстановок і перестановок. DES здійснює шифрування 64-бітових блоків даних за допомогою 64-бітового ключа, у якому значущими є 56 біт (інші 8 біт - перевірні біти для контролю на парність). Дешифрування в DES є операцією, зворотною шифруванню, і виконується шляхом повторення операцій шифрування в зворотній послідовності.

Процес шифрування полягає в початковій перестановці бітів 64-бітового блоку, шістнадцяти циклах шифрування і, нарешті, у кінцевій перестановці бітів. Слід відразу зазначити, що всі таблиці, що приводяться, є стандартними і повинні включатися в реалізацію алгоритму DES у незмінному виді.

Усі перестановки і коди в таблицях підібрані розроблювачами таким чином, щоб максимально утруднити процес розшифровки шляхом підбору ключа. При описі алгоритму DES застосовані наступні позначення:

L і R - послідовності бітів (ліва (left) і права (right));

LR-конкатенація послідовностей L і R, тобто така послідовність бітів, довжина якої дорівнює сумі довжин L і R; у послідовності LR біти послідовності R слідують за бітами послідовності L;

⊕ - операція побітового додавання по модулю 2.

При багаторазовому чергуванні простих перестановок і підстановок, керованих досить довгим секретним ключем, можна одержати дуже стійкий шифр із гарним розсіюванням і перемішуванням. Розглянуті нижче криптографічні алгоритми DES, IDEA і вітчизняний стандарт шифрування даних побудовані в повній відповідності із зазначеною методологією.

Нехай з файлу вихідного тексту лічений черговий 64-бітовий (8-байтовий) блок T. Цей блок T перетворюється за допомогою матриці початкової перестановки IP.

Біти вхідного блоку T (64 біта) переставляються відповідно до матриці IP: біт 58 вхідного блоку T стає бітом 1, біт 50-бітом 2 і т.д. Цю перестановку можна описати вираженням $T_0 = 1P(T)$. Отримана послідовність бітів T0 розділяється на дві послідовності: LQ - ліві або старші біти, R_0 - праві або молодші біти, кожна з яких містить 32 біта.

Потім виконується ітеративний процес шифрування, що складається з 16 кроків (циклів). Нехай T_i - результат *i*-ї ітерації:

$$T_i = L_i R_i,$$

де $L_i = t_1 t_2 \ldots t_{32}$ (перші 32 біти); $R_i = t_{33} t_{34} \ldots t_{64}$ (останні 32 біта).

Тоді результат *i*-ї ітерації описується наступними формулами:

$$L_i = R_{i-1}, \quad i = 1, 2, ..., 16;$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \quad i = 1, 2, ..., 16.$$

Функція f називається функцією шифрування. Її аргументами є послідовність R_{i-1}, одержувана на попередньому кроці ітерації, і 48-бітовий ключ K_i, який є результатом перетворення 64-бітового ключа шифру К.

На останньому кроці ітерації одержують послідовності R_{16} і L_{16} (без перестановки місцями), що трансформуються в 64-бітову послідовність $R_{16}L_{16}$.

По закінченні шифрування здійснюється відновлення позицій бітів за допомогою матриці зворотної перестановки IP^{-1}.

Процес розшифрування даних є інверсним стосовно процесу шифрування. Усі дії повинні бути виконані в зворотному порядку. Це означає, що розшифровувані дані спочатку переставляються відповідно до матриці IP^{-1}, а потім над послідовністю бітів $R_{16}L_{16}$ виконуються ті ж дії, що й в процесі шифрування, але в зворотному порядку. Ітеративний процес розшифрування може бути описаний наступними формулами:

$$R_{i-1} = L_i, \quad i = 1, 2, ..., 16;$$

$$L_{i-1} = R_i \oplus f(L_i, K_i), \quad i = 1, 2, ..., 16.$$

Таким чином, для процесу розшифрування з переставленим вхідним блоком $R_{16}L_{16}$ на першій ітерації використовується ключ K_{16}, на другий - K_{15} і т.д. На 16-й ітерації використовується ключ K_1. На останньому кроці ітерації будуть отримані послідовності L_0 і R_0, що трансформуються в 64-бітову послідовність L_0R_0. Потім у цій послідовності 64 біта переставляються відповідно до матриці IP. Результат такого перетворення - вихідна послідовність бітів (розшифроване 64-бітове значення).

3.2.3 Оптимізація алгоритмів шифрування для засобів зв'язку з рухомими об'єктами

Безпека алгоритму RSA базується на складності рішення задачі факторизації великих чисел, що є добутком двох великих простих чисел. Криптостійкість алгоритму RSA визначається тим, що після формування секретного ключа $k_в$ і відкритого ключа $К_в$ "стираються" значення простих чисел P і Q, і тоді виключно важко визначити секретний ключ $k_в$ по відкритому ключу $К_в$, оскільки для цього необхідно вирішити задачу знаходження дільників P і Q модуля N.

Розкладання величини N на прості множники P і Q дозволяє обчислити функцію $\varphi(N) = (P - 1)\cdot(Q - 1)$ і потім визначити секретне значення $k_в$, використовуючи рівняння

$$K_в \cdot k_в = 1 \ (mod \ \varphi(N)). \qquad (3.11)$$

Іншим можливим засобом криптографічного аналізу алгоритму RSA є безпосереднє обчислення або підбір значення функції $\varphi(N) = (P - 1)\cdot(Q - 1)$. Якщо встановлено значення $\varphi(N)$, то співмножники P і Q обчислюються достатньо просто. Насправді, нехай:

$$X = P + Q = N + 1 - \varphi(N), \qquad (3.12)$$

$$Y = (P - Q)^2 = (P+Q)^2 - 4N. \qquad (3.13)$$

Знаючи $\varphi(N)$, можна визначити X, а потім Y; знаючи X і Y, можна визначити числа P і Q з наступних співвідношень

$$P = \frac{1}{2}(X + \sqrt{Y}); \qquad Q = \frac{1}{2}(X - \sqrt{Y}). \qquad (3.14)$$

Проте, цей вираз не простіше за задачу факторизації модуля N. Криптосистеми RSA реалізуються як апаратним, так і програмним шляхом. Для апаратної реалізації операції шифрування і розшифрування RSA розроблені спеціальні процесори, які дозволяють виконувати операції RSA, пов'язані зі зведенням великих чисел у ступінь по модулю N, за відносно короткий час. Апаратна реалізація RSA приблизно в 1000 разів повільніша апаратної реалізації симетричного криптоалгоритму DES.

Одна із самих швидких апаратних реалізацій RSA з модулем 512 біт на надвеликій інтегральній схемі має швидкодію 64 кбіт/с. Програмна реалізація RSA приблизно в 100 разів повільніше програмної реалізації DES. Із розвитком технології ці оцінки можуть дещо змінитись, але асиметрична криптосистема RSA ніколи не досягне швидкодії симетричних криптосистем.

Слід зазначити, що мала швидкодія криптосистеми RSA обмежує область її застосування, але не знижує її цінності.

3.3 Методи та засоби руйнування інформації

До методів руйнування відносять завади, силову дію по колах живлення, комп'ютерні віруси, програмні закладки. Організовані завади ділять на маскуючі та інвертуючі. Маскуючі створюють шумовий фон, на якому важко виділити корисний сигнал. Імітуючі є підробкою корисних сигналів по одному або декілька параметрів.

Введення завад ЛЗ лише виконувались за симетричною або несиметричною схемою, а також створювались завади від нееквіпотенціальності точок заземлення. Симетрична схема передбачає подачу завади до 2-х провідників ЛЗ між провідниками. Несиметрична схема – це створення напруги завади між одним провідником ЛЗ і корпусом. Створення завади (рис. 3.5) через нееквіпотенціальність точок заземлення може мати місце, якщо зворотний зв'язок (лінія зворотного зв'язку) не має роз'єднання з корпусами приладів на обох кінцях ЛЗ.

Під навмисною силовою дією розуміють спеціальні стрибки напруги в мережі живлення з амплітудою тривалістю і енергією, які здатні спричинити збої в роботі обладнання або вивести його з ладу. Комп'ютер чи інше електричне обладнання системи має два значимих для проникнення енергії НСФ канали. Кондуктивний шлях від джерела енергії до системи через джерело вторинного електроживлення. Наведення відбуваються через

паразитні ємності та індуктивні зв’язки між спільно прокладеними силовими кабелями та інформацією.

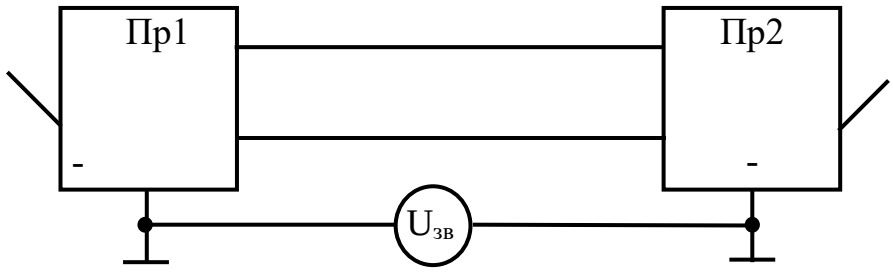


Рисунок 3.5 – Несиметрична схема створення завад

Пристрій навмисної силової дії під’єднується до силової мережі перед Пзах (рис. 3.6). Цифрові схеми, які працюють в комп’ютері, можуть вийти з ладу або почати працювати зі збоями, якщо імпульси від ТЗ НСД сягають значень 5 - 15 В. Якщо інформаційна лінія знаходиться на відстані до 100 мм силового кабелю і має спільну ділянку в декілька метрів, то через паразитну ємність Ск в інформаційній лінії створюється імпульс амплітудою, близькою до напруги в силовій мережі. Такий імпульс пошкоджує ізоляцію ПГР і фактично роз’єднує інформаційний ЛЗ.

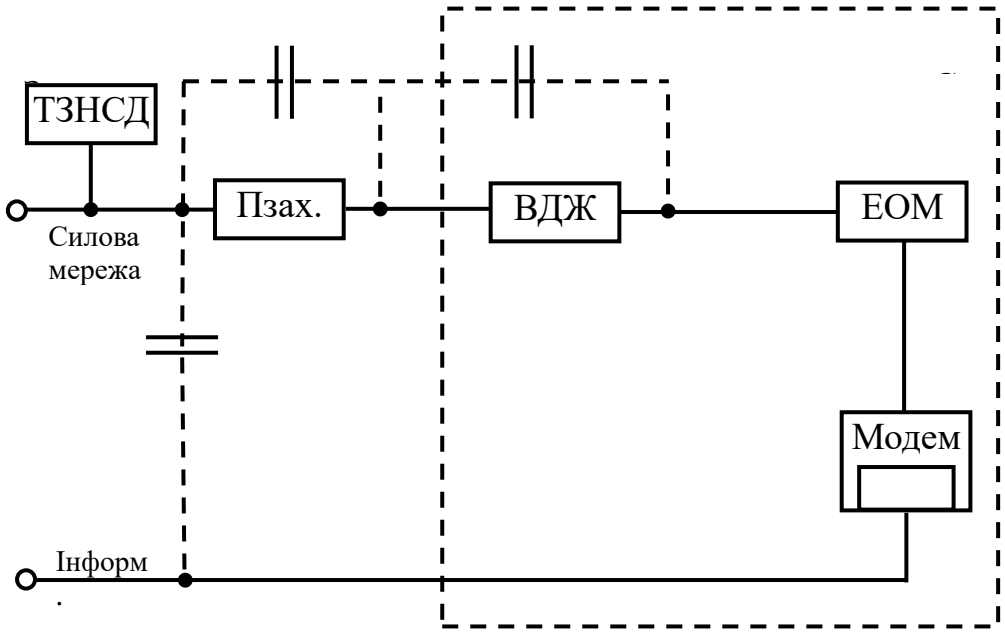


Рисунок 3.6 – Схема пристрою навмисної силової дії

На рис. 3.6 наведено такі умовні позначення: ТЗНСД – технічний засіб навмисної силової дії; Пзах. – пристрій захисту (стабілізатор змінної напруги, UPS); ВДЖ – вторинне джерело живлення; ПГР – пристрій гальванічного розділення (трансформатор, оптопара); Спз, Свдм – власні ємності монтажу пристрою захисту; Ск – міжкабельна ємність (паразитна) забезпечує ємнісний паразитний зв'язок з інформаційним каналом.

Визначальним фактором, який впливає на ТЗ НСД, є спосіб під'єднання до мережі живлення. Використовується послідовний або паралельний спосіб під'єднання. Послідовний або трансформаторний потребує втручання в мережу живлення для під'єднання обмотки трансформатора в розрив кола. Через вторинну обмотку трансформатора проходить повний струм споживача, тому ТЗ НСД має великі розміри і масу. Ефективність такого способу полягає в тому, що навмисна силова дія спрямовується до одного споживача. Паралельний спосіб під'єднання не потребує втручання в мережу живлення. Такі технічні засоби компактні і не мають демаскуючого кабелю великого перетину, але у цьому випадку складніше організувати сеанс зв'язку

За принципом дії ТЗ НСД поділяють на:

1) перемикаючі ТЗ, побудовані на принципі подачі замість фазної напруги лінійної, яка більша фазної в $\sqrt{3}=1{,}73$ рази. Очевидно, побудова такого пристрою є складною в зв'язку з необхідністю перекомутації і встановлюватись на етапі монтажу силових ліній приміщення чи будівлі;

2) технічний засіб НСД з використовуванням при послідовному під'єднанні технічного засобу. Такі ТЗ дозволяють короткочасно підняти напругу на об'єкті атаки відповідною трансформацією мережної напруги або трансформувати в мережу електроживлення імпульс напруги необхідної форми і амплітуди від ємнісного накопичувача;

3) ТЗ з паралельним під'єднанням і ємнісними накопичувачами.

3.4 Засоби комбінованого захисту мовної інформації

У комбінованих засобах відбувається процедура частотно-часових перестановок при збереженні ширини спектру початкового сигналу. Мовний сигнал ділиться за допомогою АЦП перетворюється у цифровий код. Потім отриманий цифровий сигнал розділяється на частотно-часові компоненти, які піддаються перестановкам під дією алгоритму шифрування. Після чого здійснюється зворотна процедура, тобто цифро-аналогове перетворення за допомогою ЦАП і отриманий сигнал надходять в канал зв'язку.

Структура скремблера, що працює на базі частотно-часових перестановок представлена на рис. 3.7.

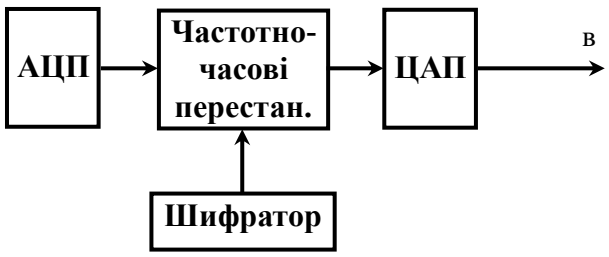


Рисунок 3.7 – Структура скремблера

Скремблери вносять певні спотворення в сигнал, при цьому з'являються складові сигналу, які впливають на нелінійні спотворення. Вони знаходять застосування у відомчих каналах зв'язку для захисту конфіденційної інформації.

4 РОЗРОБКА ПРИСТРОЇВ КОДУВАННЯ МОВНИХ СИГНАЛІВ У ЦИФРОВИХ СИСТЕМАХ РАДІОЗВ`ЯЗКУ

4.1 Кодування мовних сигналів на основі m-послідовностей

У ході виконання магістерської роботи була поставлена задача знайти найбільш оптимальний метод кодування мовних сигналів для цифрової системи радіозв'язку. Критерій, за яким було здійснено оцінювання різних методів для того, щоб вибрати оптимальний варіант – це якість передачі системи.

Цей критерій включає в себе: завадостійкість, кількість помилок, швидкість передачі, розбірливість. Безумовно, до найкращого методу кодування можна віднести цифровий метод кодування. Оскільки система радіозв'язку доволі інтенсивно переходить на цифрове обладнання, даний метод буде актуальним.

Цей метод при використанні робить систему кодування надійною, стійкою та економічно вигідною. Він забезпечує високу розбірливість та завадостійкість.

Слабке місце багатьох систем кодування – це статистична слабкість коду, тобто, аналізуючи статистику за деякий період, можна скласти думку про те, що це за система, і тоді діяти більш спрямовано. Тобто різко скорочується час пошуку ключа. Дана система оперує шумоподібними сигналами, що за своїми статистичними властивостями практично ідентичні білому гаусівському шуму.

На рис. 4.1 представлено енергетичні спектри білого гаусівського шуму і сигналу.

За визначенням складності закону генерації ряду чисел, якщо складність послідовності {gi} = m, то будь-які m+1 послідовності її значення залежні. Якщо ця залежність є лінійною, то виходить рекуррентне співвідношення такого виду:

$$C_0 g_i + C_1 g_{i-1} + \ldots + C_m g_{i-m} = 0 \qquad (4.1)$$

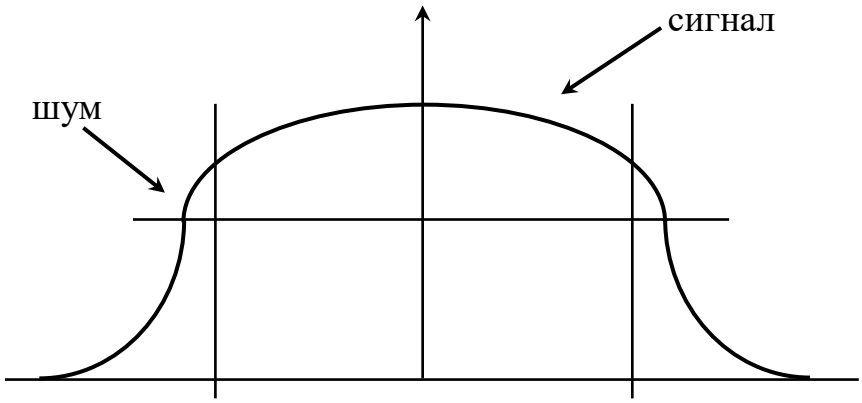


Рисунок 4.1 – Енергетичні спектри білого гаусовського шуму і сигналу

При цьому C_0g_0 повинні бути ненульовими. Кожен наступний член послідовності визначається з m попередніх. Виходить простий вид реалізації, коли всі складові приймають лише значення 0 і 1, що робить їх дуже зручними для передачі на ЕОМ.

Арифметичні операції у GF(2) будуть наступними:

+	01		*	01
0	01		0	00
1	10		1	01

Поля біт можна представити як вектори, кожен компонент яких приймає значення з GF(2). Такі вектори зручно розглядати як багаточлен:

$$(10010101) = x^7 + x^4 + x^2 + 1.$$

Нерозкладність багаточлена: над полем комплексних чисел у будь-який багаточлен розкладемо лінійні множники, або по-іншому він має стільки коренів, яким буде його ступінь. Однак це не так для інших полів – у полях дійсних чи раціональних чисел багаточлен $x^2 + x + 1$ коренів не має. Аналогічно, у полі GF(2) багаточлен $x^2 + x + 1$ теж не має коренів.

Розглянемо схему розподілу даних у поле з *n* біт на поліном (рис. 4.2).

$$F(x) = C_0 + C_1x + ... + C_nx^n. \qquad (4.2)$$

Одержана послідовність буде виражена за допомогою формули:

$$S(x) = a(x) / g(x), \quad (4.3)$$

де a(x) – вихідні дані;

g(x) – відповідні коефіцієнти багаточлена.

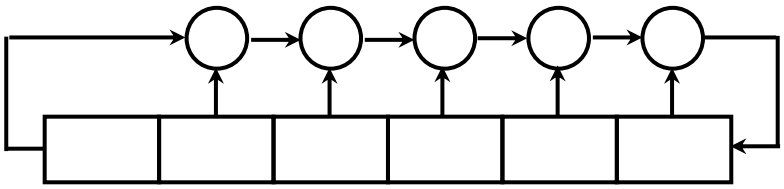


Рисунок 4.2 – Схема розподілу даних

Природно, що бажано одержати якомога більш довгий період послідовності від багаточлена заданого ступеня, а максимально можлива її довжина – $2^N - 1 y GF(2^N)$.

Послідовності максимальної довжини формуються за правилом: якщо багаточлен g(x) ступеня N поділяє багаточлен $X^N - 1$ лише при $K > 2^N - 1$, то період його будь-якої ненульової послідовності буде дорівнювати $2^N - 1$. Існують таблиці коефіцієнтів m-послідовностей.

Розглянемо властивості m-послідовностей:

1. В кожному періоді послідовності числа 1 і 0 відрізняються не в більше ніж на 1.

2. Серед груп з послідовністю 1 і 0 в кожному періоді половина має тривалість в 1 символ, четверта частина має тривалість у два символи, 8 частина має тривалість у 4 символи і т. д.

Кореляційна функція послідовності має єдиний значний мінімум амплітуди 1 і при всіх зсувах дорівнює 1/m (m – довжина послідовності).

Кореляція між векторами обчислюється за формулою:

$$P(\chi) = (A-B)/(A+B), \quad (4.4)$$

де A – число позицій, в яких символи послідовностей *x* і *y* збігаються;

B – число позицій, в яких символи *x* і *y* різні.

4.2 Розробка структури формування коду

Для формування коду використовується 5-розрядний первинний ключ, одержаний з генератора псевдовипадкових чисел. На рис. 4.3 наведено блок-схему формування коду.

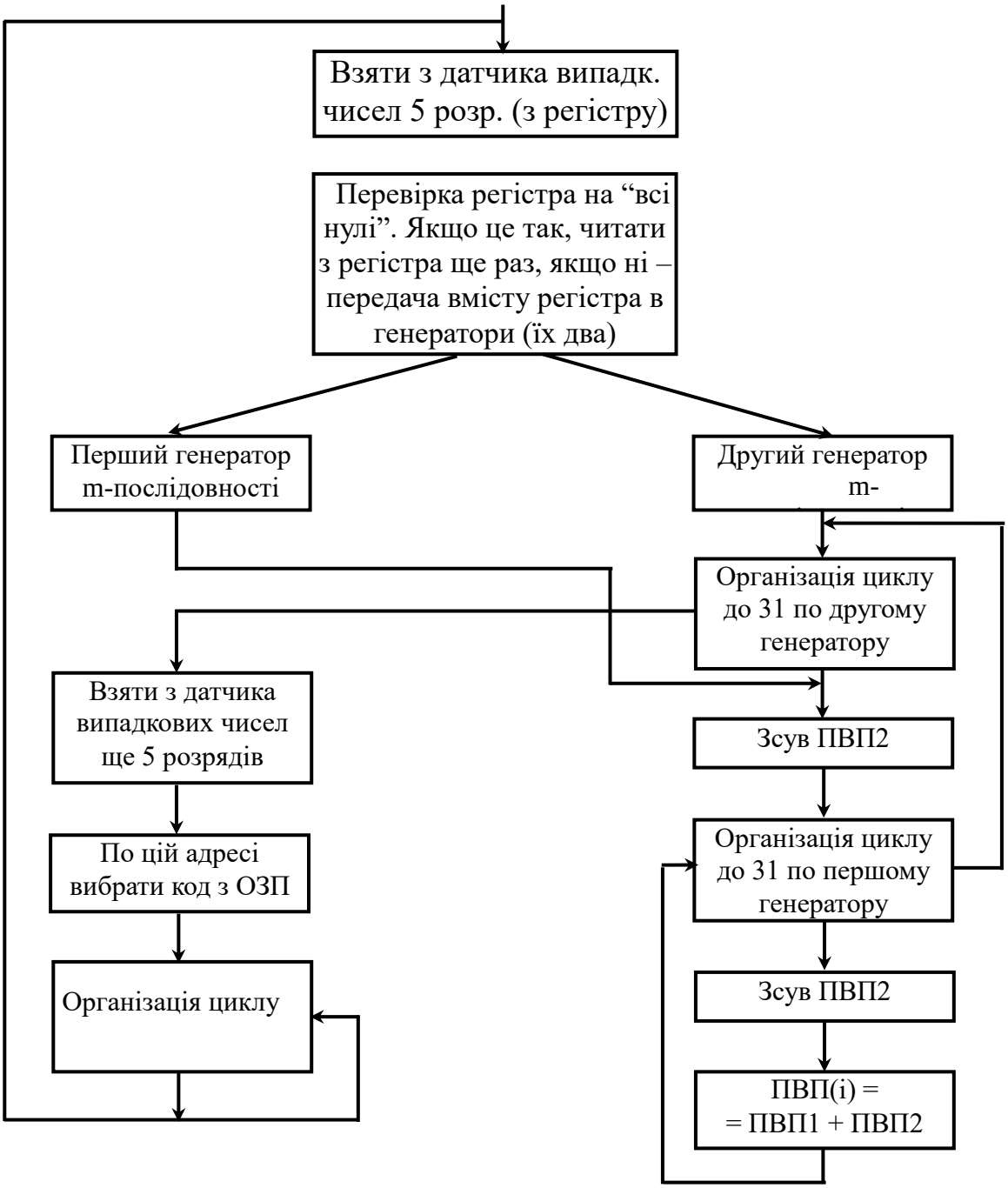


Рисунок 4.3 – Блок-схема формування коду

В даному випадку можна скористатися відносно простим методом генерації псевдовипадкової послідовності, а саме: аналізом теплових шумів стабілітрона, що працює в режимі пробою. Шуми моделюються і подаються на тригер Шмідта, а потім передають отримані біти в регістр зсуву. Оскільки теплові шуми мають досить випадковий характер, то і послідовність буде випадковою. Таким чином, на початковому етапі формування ключа маємо кількість комбінацій $2^5 – 2 = 30$ (оскільки 0000 є неприпустимою).

На наступному етапі первинний ключ подається на два генератори, що формують по цьому ключеві 31-розрядні m-послідовності. Ці послідовності переміщуються по модулю 2, циклічно зсуваючись, утворюючи два вкладених цикли, видають 31^2 варіантів ключа.

Так, загальне число принципових комбінацій складає $30 – 31^2$. Ці 31^2 варіантів зберігаються в ОЗП базового апарату. Вибір одного ключа здійснюється шляхом повторного звертання до генератора псевдовипадкових чисел.

Разом одержуємо оптимальну для даних умов криптографічного захисту цифру $30 – 31^3 = 900000$ комбінацій. При цьому статистичні властивості даної послідовності практично не відрізняються від m-послідовності.

В таблиця 4.1 представлено усі етапи і команди формуваня коду з 5-розрядним первинним ключем.

Таблиця 4.1 – Формуваня коду

Команда ASM	Примітка
MOV ECX, ADDR1	Завантаження регістрів S1 розрядними значеннями ПСП
MOV EBX, ADDR2	
MOV ADDR3, 1Fh	Організація лічильників
MOV ADDR4, 1Fh	
MOV AL, ADDR3	Завантаження значення лічильника № 1
M1: J2 M3	Якщо це “0” – вихід
PCL ECX, 1	Зрушення значення ПСП1
DEC AL	Декремент лічильника № 1
MOV ADDR3, AL	Значення лічильника – у пам’ять
M2: MOV AL, ADDR4	Завантаження значення лічильника № 2
JZ M1	Якщо “0” – перехід на зовнішній цикл
MOV EDX, ECX	Множення по модулю 2 однієї ПСП на іншу
XOR EDX, EBX	
RCL EBX	Декремент лічильника № 2
MOV [AL]; EDX	Заносимо чергове значення в пам’ять
JMP M2	Замикання внутрішнього циклу
M3: EWD	

4.3 Генератор m-послідовностей

Формування ПВП відбувається апаратно, хоча можна здійснити це програмним способом, використовуючи МП з 32-розрядними регістрами.

Час виконання і частота, на якій працюють елементи, некритичні, оскільки формування ПВП і самого ключа відбувається в той час, коли трубка лежить на базовому апараті. Генератор m-послідовностей зображений на рис. 4.2.

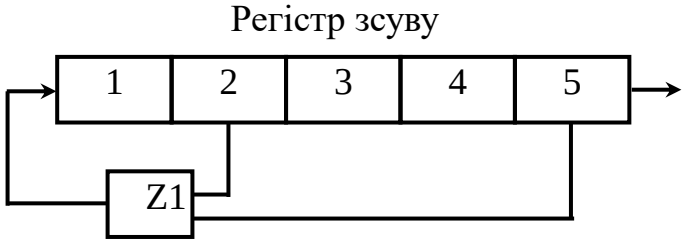


Рисунок 4.2 – Генератор ПВП

4.4 Структури приймача та передавача сигналів

На рис. 4.3 і 4.4 зображені структурні схеми аналого-цифрових приймача та передавача закодованих телефонних сигналів.

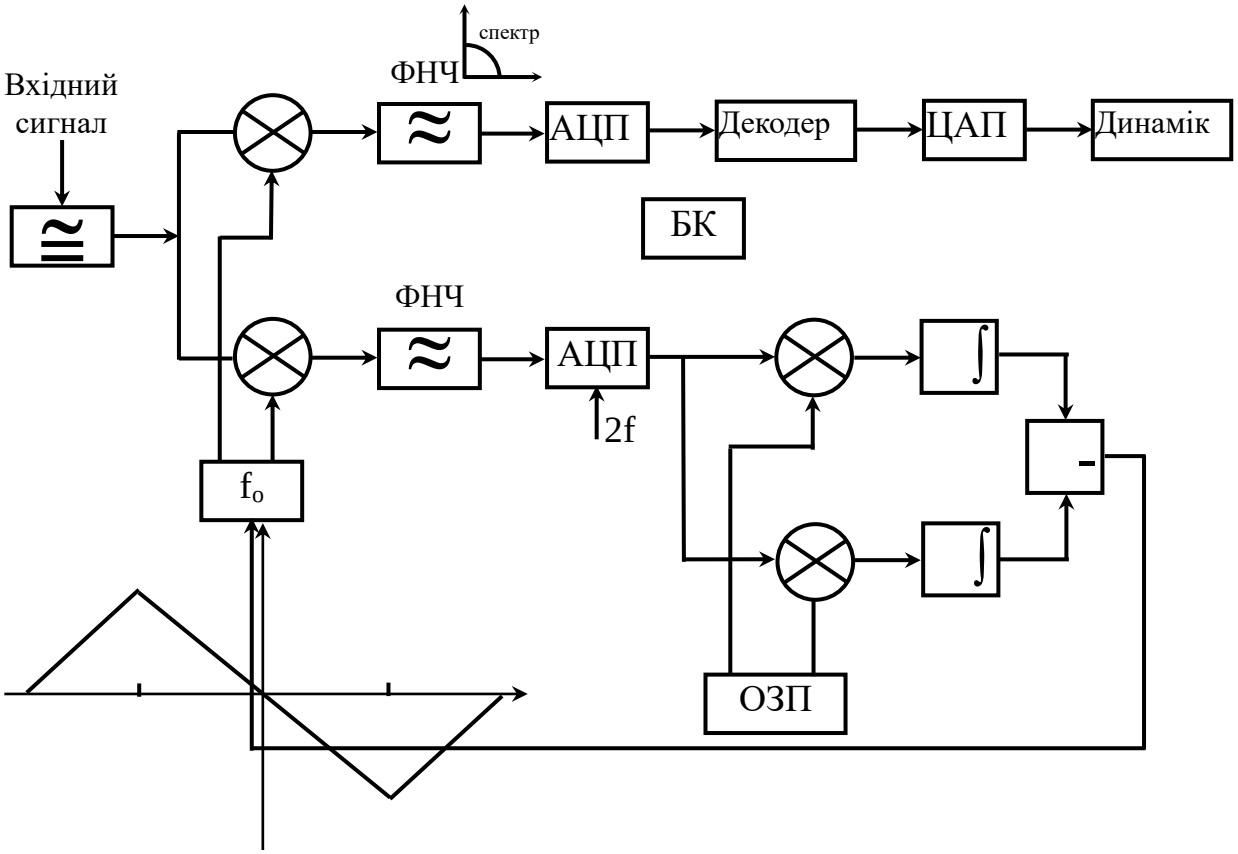


Рисунок 4.3 - Структурна схема приймання сигналу

Схема передавача більш проста в порівнянні із схемою приймача. Це пояснюється повною визначеністю переданого сигналу, тоді як сигнал на вході приймача неможливо передбачити.

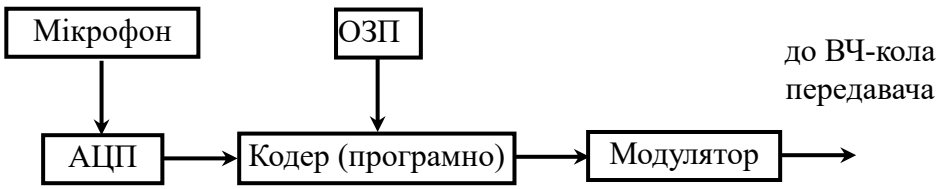


Рисунок 4.4 – Структурна схема передавання сигналу

Базовими складовими цих пристроїв є АЦП і ЦАП, параметри і

характеристики яких безпосередньо впливають на якість функціонування приймально-передавальних пристроїв.

4.5 Оцінювання швидкодії програмно-апаратної реалізації кодера

Якщо виходити з припущення, що частота, з якою дискретизується мовний сигнал, дорівнює 8 кГц, а АЦП 12-розрядний, то одержимо наступні дані. Частота надходження сигналу на кодер (декодер) визначається за формулою:

$$f_{код/декод} = f_д \cdot N_{розАЦП}, \tag{4.5}$$

де $f_д$ – частота дискретизації;

$N_{розАЦП}$ – кількість розрядів АЦП.

$$T_{формПСП} \cdot f_{код/декод} = 8 \cdot 10^3 \cdot 12 = 96\ кГц.$$

Період надходження сигналу визначається

$$T_{формПСП} = 1/f_{код/декод}, \tag{4.6}$$

де $f_{код/декод}$ – частота надходження сигналу на кодер (декодер).

$$T_{формПСП} = 1/f_{МП} = 30{,}3\ нс.$$

Допустима кількість тактів для виконання програми кодування або декодування:

$$N_{такт.доп} = T_{формПСП} / T_{тактМП} = 10{,}4 \cdot 10^{-6} / 30{,}3 \cdot 10^{-9} = 343 \text{ такти}.$$

Цього більше, ніж досить для оброблення мовної інформації. Отже, система має резерв для подальших розширень і поліпшень.

Таким чином, було доведено, що запропонована в магістерській роботі система кодування мовних сигналів є оптимальною, вона задовольняє основним вимогам, дешева у виконанні, проста і має достатню надійність, ефективність та стійкість до завад.

5 МОДЕЛЮВАННЯ ПРОЦЕСУ КОДУВАННЯ МОВНИХ СИГНАЛІВ У ЦИФРОВИХ СИСТЕМАХ РАДІОЗВ'ЯЗКУ

5.1 Моделі цифрового кодування інформації у рухомих засобах зв'язку

У цьому підрозділі виконаємо моделювання процесу кодування мовних сигналів для спрощеного варіанту у вигляді п'яти умовних символів. Для передачі повідомлення через такий канал з перешкодами використовується алгоритм кодування за методом Шеннона-Фано з кодуванням (n , 1) кодом.

Кодування та передавання закодованої мовної інформації у каналі зв'язку здійснюється відповідно до схеми каналу на рис. 5.1.

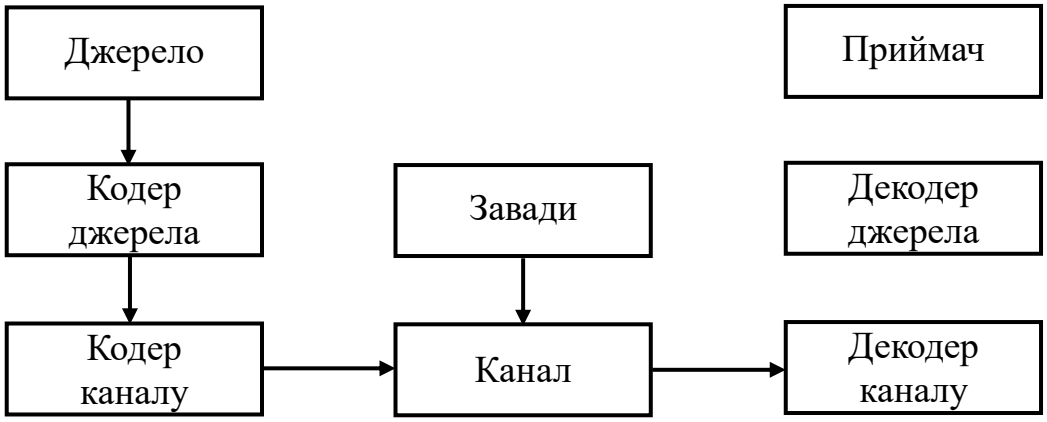


Рисунок 5.1 – Структурна схема передачі інформації.

Джерело генерує послідовність повідомлень з ансамблю

$$\{V, P(V)\},$$

де V – символ повідомлення;

$P(V)$ – ймовірність символу повідомлення, що розраховується за формулою:

$$P(V_i) = \frac{1 + (i - r)^2}{m + \sum_{j=1}^{m} (j - r)^2}, \qquad (5.1)$$

де $i = 1, ..., m_i$;

m, r – задані величини.

Кодер джерела кодує повідомлення V_i в Z_i за алгоритмом Шеннона-

Фано. Ентропія повідомлення H(z), біт/символ, обчислюється за формулою:

$$H(z) = -\sum_{i=1}^{m} P(Z_i) \cdot \log_2 P(Z_i). \quad (5.2)$$

Формула для розрахунку середньої довжини коду $L_{с.р.}$, біт, має вигляд:

$$L_{c.p.} = \sum_{i=1}^{m} L(Z_i) \cdot P(Z_i), \quad (5.3)$$

де $L(Z_i)$ – довжина коду, біт;

$P(Z_i)$ – ймовірність коду.

Максимальна ентропія $H(z)_{max}$, біт/символ, нерівномірного двійкового коду Z_i визначається за формулою:

$$H(z)max = log2(m). \quad (5.4)$$

Знаючи середню довжину коду, можна визначити коефіцієнт ефективності $K_{еф}$ коду Z_i за формулою:

$$K_{еф} = \frac{H(z)}{L_{c.p.}}. \quad (5.5)$$

Для розрахунку коефіцієнта надлишковості $K_{надл.}$ використовується формула:

$$K_{надл} = \frac{H(z)_{\max} - H(z)}{H(z)_{\max}}. \quad (5.6)$$

Кодер каналу здійснює просте кодування повторюванням n = 3 разів кожного двійкового сигналу повідомлення Z_i. Таким чином, маємо всього два коди

$$X_1 = (0\ 0\ 0) \qquad X_2 = (1\ \ 1\ \ 1).$$

Ймовірність кожного з них визначається за формулою:

$$P(X_k) = \sum_{i=1}^{m} \frac{n \cdot Z_i^k}{L(Z_i)} P(Z_i), \quad (5.7)$$

де $k = 0,1$;

$n \cdot Z_i^k$ - кількість елементів <<k>> у події Z_i.

При передачі X_k по каналу зв’язку можливі помилки з ймовірностями,

обумовленими в такий спосіб:

$$P10 = 0,2 + 0,02A; \tag{5.8}$$

$$P01 = 0,2 + 0,02B, \tag{5.9}$$

де $P10$ – ймовірність прийняття нуля при передачі одиниці;

$P01$ – ймовірність прийняття одиниці при передачі нуля;

A, B – задані величини.

Надалі для зручності будуть використовуватись наступні прийняті позначення: X – переданий код; Y – прийнятий код.

При побудові канальної матриці P(Y/X) скористаємося тим, що при передачі може відбутися помилка лише в одному розряді X_1 або X_2. Тоді в 1 рядку матриці елементи визначаються в такий спосіб:

$$P(X_i; Y_i) = \begin{cases} 1 - P01, i = 1; \\ P01/3, i = 2,3,4; \\ 0, i = 5,6,7,8. \end{cases} \tag{5.10}$$

Елементи канальної матриці спільної ймовірності P(X,Y) визначаються за формулою:

$$P(Xi, Yi) = P(Xi)P(Yi/Xi). \tag{5.11}$$

Знаючи матрицю спільної ймовірності P(X,Y), можна обчислити елементи матриці ймовірностей P(Y). Вони знаходяться за формулою:

$$P(Yi) = P(X1, Yi) + P(X2, Yi). \tag{5.12}$$

В свою чергу, формула для розрахунку елементів матриці умовної ймовірності $P(Y/X)$ має вигляд:

$$P(Xi/Yi) = P(Yi/Xi)/P(Yi). \tag{5.13}$$

Ентропія переданого сигналу $H(x)$, біт/символ, і прийнятий сигнал $H(y)$, біт/символ, визначаються відповідно до формули:

$$H(x) = -\sum_{i=1}^{2} P(X_i) \cdot \log_2 P(X_i), \tag{5.14}$$

$$H(y) = -\sum_{j=1}^{8} P(Y_i) \cdot \log_2 P(Y_i). \tag{5.15}$$

Умовні ентропії H(x/y), біт/символ, і H(y/x), біт/символ, розраховуються відповідно до формул:

$$H(x/y) = -\sum_{i=1}^{2}\sum_{j=1}^{8} P(X_i/Y_i)\cdot \log_2 P(X_i/Y_i)\cdot P(Y_i), \quad (5.16)$$

$$H(y/x) = -\sum_{i=1}^{2}\sum_{j=1}^{8} P(Y_i/X_i)\cdot \log_2 P(Y_i/X_i)\cdot P(X_i). \quad (5.17)$$

Спільна ентропія *H(x/y),* біт/символ, знаходиться за формулою:

$$H(x/y) = -\sum_{i=1}^{2}\sum_{j=1}^{8} P(X_i/Y_i)\cdot \log_2 P(X_i/Y_i) \quad (5.18)$$

Взаємна ентропія *I(x/y),* біт/символ, визначається за формулою:

$$I(x/y) = H(x) - H(x/y). \quad (5.19)$$

Передача інформації з каналу зв'язку здійснюється зі швидкістю v, що розраховується по формулі:

$$v = 1000(A + 1). \quad (5.20)$$

Постійну швидкість передачі двійкових символів по каналу зв'язку R, можна розрахувати за формулою:

$$R = v \cdot I(x,y)/3. \quad (5.21)$$

Продуктивність джерела $\tilde{I}$, біт/с, визначається за формулою:

$$\tilde{I} = H(x) \cdot v. \quad (5.22)$$

5.2 Аналіз результатів, отриманих в процесі моделювання цифрового кодування

Визначені наступні постійні: m = 15; r = 10. Визначимо потрібні характеристики. Ймовірності символів V_i (це ймовірності коду Z_i), що генеруються джерелом, розраховуємо за формулою (5.1). Отримані значення ймовірностей зводимо в табл. 5.1.

Таблиця 5.1 – Ймовірності і коди символів

V_i	$P(V_i)$	Z_i	$L(Z_i)$
1	0,231	11	2
2	0,183	10	2
3	0,1408	011	3
4	0,1042	0101	4
5	0,0732	01001	5
6	0,0732	01000	5
7	0,0479	00111	5
8	0,0479	00110	5
9	0,0282	00101	5
10	0,0282	00100	5
11	0,0141	00011	5
12	0,0141	00010	5
13	0,0056	000011	6
14	0,0056	000010	6
15	0,0028	000000	6

Спочатку ймовірності складаються по спаданню. Після цього всі ймовірності поділяються на дві групи так, щоб в межах кожної групи їх значення були приблизно однаковими. В старший розряд кодів, що відповідають першій групі ймовірностей, записується 1, для другої групи кодів – 0. Потім кожна з отриманих підгруп, в свою чергу, поділяється аналогічним чином. При проходженні циклу розподілу по одному розряду відбувається перехід на розряд вправо. Розподіл продовжується до тих пір, поки в кожній групі не виявиться по одному коду.

Обчислимо ентропію повідомлення H(z) за формулою (5.2):

$$H(z) = 3{,}218 \text{ (біт/символ)}.$$

Середню довжину нерівномірного коду $L_{с.р.}$ визначимо за (5.3):

$$L_{c.p.} = 3{,}5652 \text{ (біт)}.$$

Максимальну ентропію нерівномірного двійкового коду Z_i визначаємо за формулою (5.4):

$$H(z)_{max} = 3{,}218 \text{ (біт)}.$$

За формулою (5.5) обчислимо коефіцієнт ефективності $К_{еф}$ нерівномірного двійкового коду Z_i:

$$К_{еф} = 0,903.$$

Для розрахунку коефіцієнта надлишковості $К_{надл.}$ скористаємося формулою (5.6):

$$К_{надл.} = 0,176.$$

При простому кодуванні повторенням n = 3 разів кожного двійкового сигналу повідомлення Z_i має два коди: X_1 і X_2, ймовірності яких $P(X_1)$ і $P(X_2)$ знаходяться за формулою (5.7):

$$P(X_1) = 0,4113; \qquad P(X_2) = 0,5885.$$

Ймовірності можливих помилок при проходженні коду по каналу визначаються за формулами (5.8) і (5.9) відповідно:

$$P10 = 0,3; \qquad P01 = 0,2.$$

Канальна матриця P(Y/X) з боку приймача для коду X_0 і X_1, розрахована за формулою (5.10), приведена в таблиці 5.2. Для перевірки розрахунку в останньому стовпці таблиці 5.2 наведена сума по поточному рядку. Значення ймовірностей в таблиці 5.2 приводяться в десятичних частках одиниці.

Таблиця 5.2 – Канальна матриця P(Y/X)

X	Y								Сума
	000	001	010	100	011	101	110	111	
000	8000	0667	0667	0667	0000	0000	0000	0000	10000
111	0000	0000	0000	0000	1000	1000	1000	1000	10000

В таблиці 5.3 приведені значення елементів канальної матриці спільної ймовірності P(Y,X), визначені формулою (5.11). Значення ймовірностей в таблиці 5.3 приводяться в десяткових частках одиниці.

Таблиця 5.3 – Матриця спільних ймовірностей P(Y,X)

X	Y							
	000	001	010	100	011	101	110	111
000	3292	0274	0274	0274	0000	0000	0000	0000
111	0000	0000	0000	0000	0588	0588	0588	4119

Елементи матриці ймовірностей P(Y) знаходяться за формулою (5.12). Отримані дані приведені в таблиці 5.4 у десяткових частках одиниці. В останньому стовпці для перевірки приведені сума по рядку.

Таблиця 5.4 – Матриця P(Y)

Y								Сума
000	001	010	100	011	101	110	111	
3292	0274	0274	0274	0588	0588	0588	4119	1000

Розрахувавши матриці P(X,Y) і P(Y), можна обчислити елементи матриці умовної ймовірності P(X/Y) за формулою (5.13). Матриця P(X/Y) наведена в табл. 5.5.

Таблиця 5.5 – Матриця P(X/Y)

X	Y		Сума
000	1	0	1,0000
001	1	0	1,0000
010	1	0	1,0000
100	1	0	1,0000
011	0	1	1,0000
101	0	1	1,0000
110	0	1	1,0000
111	0	1	1,0000

Розрахуємо ентропію переданого сигналу H(x) і ентропію прийнятого сигналу H(y) за формулами (5.14) і (5.15) відповідно:

H(x) = 0,9777 (біт/символ);

$$H(y) = 2{,}2025 \text{ (біт/символ)}.$$

Умовні ентропії H(x/y) і H(y/x) розраховуємо, скориставшись формулами (5.16) і (5.17) відповідно:

$$H(x/y) = 0{,}0000 \text{ (біт/символ)};$$

$$H(y/x) = 1{,}2244 \text{ (біт/символ)}.$$

За формулою (5.18) знаходимо спільну ентропію H(x/y).

$$H(x/y) = 2{,}2014 \text{ (біт/символ)}.$$

Зробимо перевірку отриманих значень ентропії:

$$H(y/x) + H(x) = 2{,}2025 \text{ (біт/символ)};$$

$$H(x/y) + H(y) = 2{,}2025 \text{ (біт/символ)}.$$

Збіжність отриманих значень свідчить про правильність знайдених значень ентропії. Визначимо значення взаємної ентропії I (x,y), використовуючи формулу (5.19):

$$I(x,y) = 0{,}9771 \text{ (біт/символ)}.$$

Для знаходження наступних характеристик каналу обчислимо швидкість передачі двійкових символів по каналу зв’язку за допомогою формули (5.20):

$$V = 6000 \text{ (символів/с)}.$$

Інформація передається по каналу зв’язку з постійною швидкістю R, що обчислюється за допомогою формули (5.21):

$$R = 1956{,}1.$$

Продуктивність джерела інформації (5.22) дорівнює:

$$\tilde{I} = 5868{,}3 \text{ (біт/с)}.$$

Результатом роботи програми є графіки числа помилок відновлення інформації від параметра *n* (n, 1)–коду та від P01 і P10 (рис. 5.2).

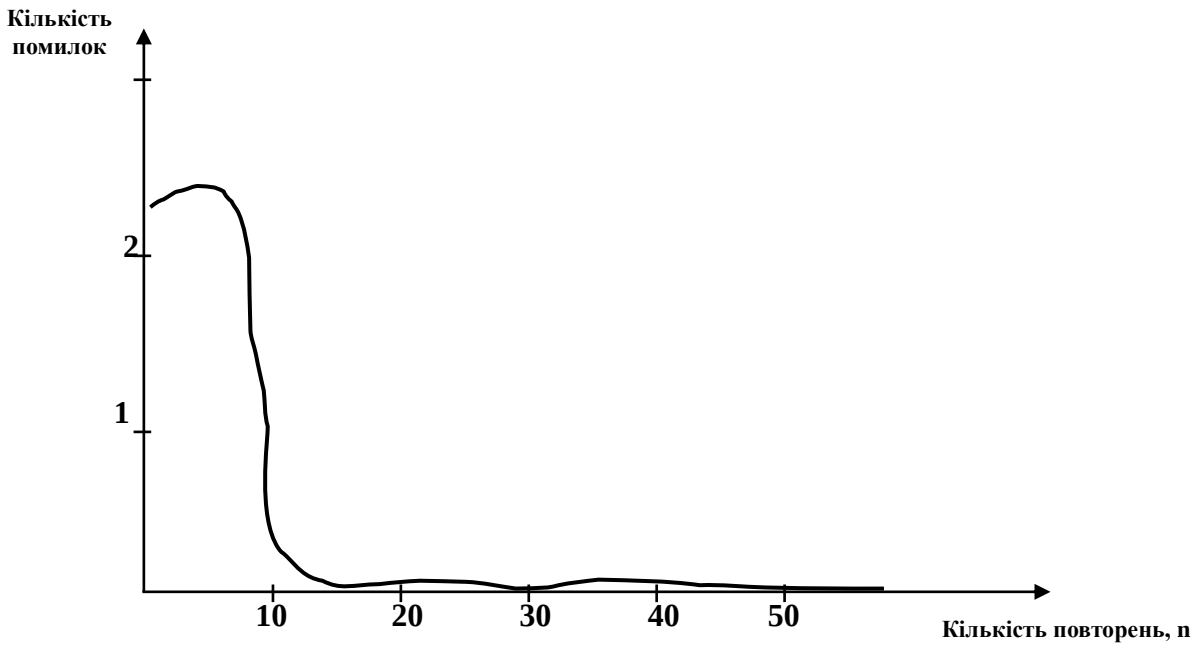


Рисунок 5.2 – Залежність числа помилок відновлення
від кількості повторень

При теоретичному розрахунку ми припустили, що в каналі немає помилок. Дійсно, отримане нульове значення ентропії H(x/y) також про це свідчить.

Однак, отриманий графік говорить про те, що це припущення відповідає дійсності, тільки починаючи зі значень *n*, що дорівнюють 20...25.

5.3 Аналіз моделювальної програми цифрового кодування

У процесі моделювання була розроблена програмна модель каналу з графіком залежності числа помилок від числа n.

Програма написана мовою Borland Pascal 7.0.

Для програмної реалізації каналу програма запитує довжину переданого масиву повідомлень, число n і виконує підрахунок числа помилок при його передачі. Потім йде розрахунок масиву даних для побудови графіка залежності числа помилок від n для n, що змінюється в інтервалі 1…100 з кроком 3. Після цього відбувається виведення на екран потрібного графіка.

У програмі використовуються наступні процедури і функції.

Функція slog може приймати булівське значення в залежності від вхідної ймовірності. Вона служить для здійснення в програмі випадкової події з наперед задано. Ймовірністю.

Процедура ver розраховує ансамбль ймовірностей вихідного повідомлення в залежності від A, B і C, також впорядковує його по спаданню.

Процедура set_codes заповнює масив кодів по алгоритму Шеннона-Фено і ініціалізує маски для декодування нерівномірного коду.

Функція без параметрів source при кожному зверненні до неї приймає значення повідомлення з ансамблю відповідно до його ймовірності. Вона використовує той самий принцип, що й функція slog.

Процедура deranges вносить у код, що відповідає повідомленню source, перешкоди відповідно до моделі (n, 1) – коду. В ній використовуються функції побітного зсуву shr і shl, а також функція slog.

Процедура decoder виконує розкодування нерівномірного коду, після дії на нього перешкод у каналі. Оскільки найбільша довжина коду не перевищує 8 біт, то для їх збереження, передачі і декодування використовується тип даних – байт, причому розташовуються вони у старших бітах.

Процедура raphic служить для відображення на екрані графіка залежності числа помилок відновлення інформації від значень параметра n (n, 1) – коду. Все зображення прив’язане до початку координат (X_0, Y_0). Для зручності по осі Y відкладаються значення Y у відсотках. Графік відображується відрізками прямих для згладжування різких стрибків значень.

Висновок: кодування інформації за Шенноном-Фано в поєднанні з кодуванням (n, 1) кодом, показало оптимальні результати при програмному моделюванні. Так, при передачі порядку 1000 символів при n = 20…25 практично не спостерігається помилок при P10 і P01.

5.4 Комп`ютерне моделювання скремблера

Для моделювання роботи схеми скремблера обираємо програму MicroCap 9, яка є простою у використанні, багатофункціональною та має велику базу як іноземних, так і вітчизняних елементів.

Проведено моделювання окремих вузлів схеми для більш детального аналізу роботи. Вхідні кола забезпечують фільтрацію та підсилення мовного сигналу. Смуга пропускання становить 300 – 7700 Гц.

Моделювальна схема генератора скремблера показана на рис. 5.3.

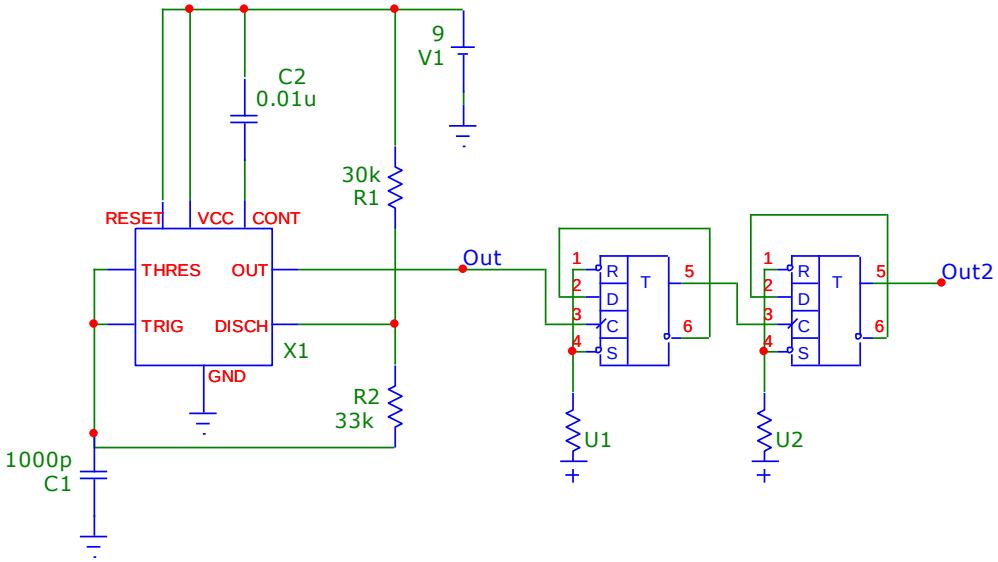


Рисунок 5.3 – Схема генератора скремблера

Елементи C1, R1, R2 забезпечують частоту на виході Out 14 кГц. На двох D-тригерах реалізований подільник частоти на 4. Тому на виході Out2 значення частоти вихідного сигналу складає 3500 Гц. Дане значення обрано саме таким, щоб забезпечити в подальшому необхідну частотну інверсію вхідного сигналу в модуляторі.

Схема для моделювання ключового балансного модулятора та НЧ-фільтра скремблера показана на рис. 5.4. Замість комутатора К561КТ3 використовуємо MAX4601.

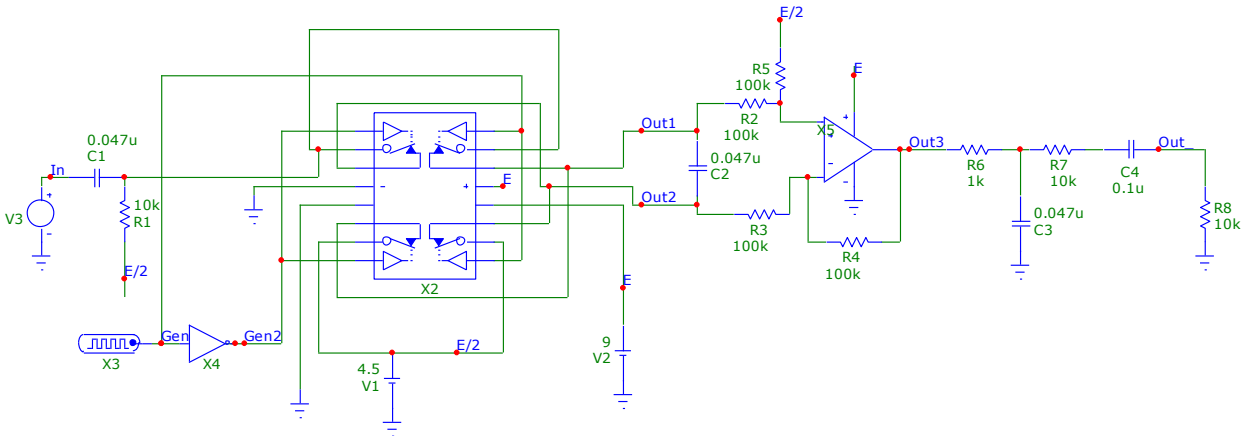


Рисунок 5.4 – Схема ключового балансного модулятора та НЧ-фільтра скремблера

При подачі на вхід сигналу частотою 300 Гц на виході модулятора маємо одержати сигнал частотою 3500-300=3200 Гц. Часова діаграма сигналу на вході та виході схеми показана на рис. 5.5.

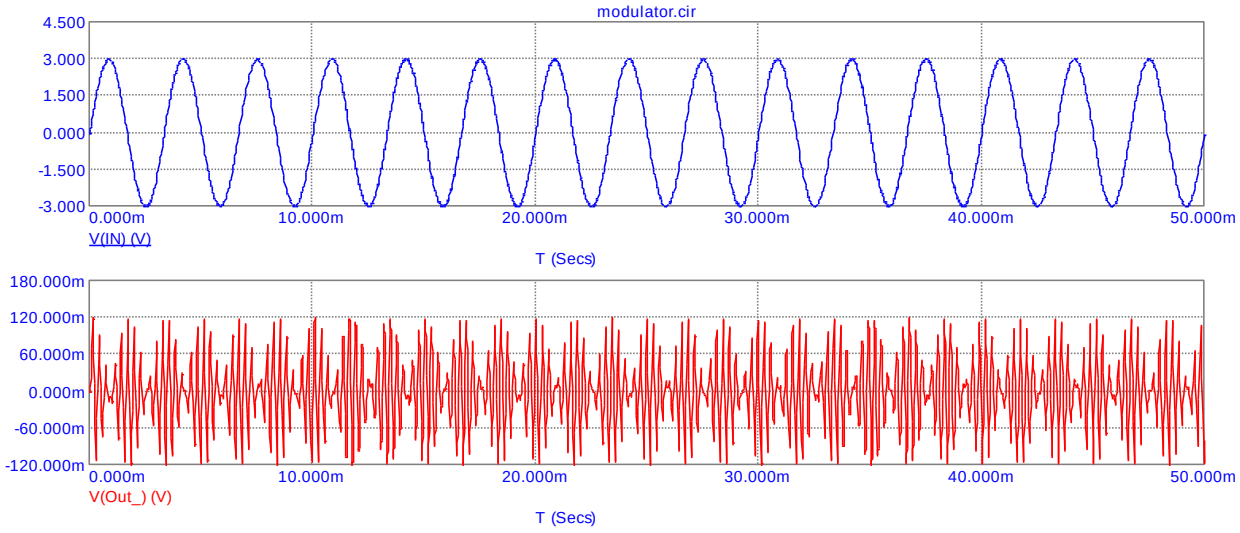


Рисунок 5.5 – Часові діаграми сигналу на вході та виході балансного модулятора скремблера

На рис. 5.6 наведений спектр вихідного сигналу. В ідеальному випадку спектр мав би містити лише одну частоту: 3200 Гц. З рисунка видно, що у вихідному спектрі окрім гармоніки 3200 Гц присутня і дзеркальна частота 3800 Гц внаслідок слабкого придушення вихідним фільтром верхньої бокової

смуги. Для кращого придушення необхідно використовувати фільтри більшого порядку, що буде ускладнювати схему. З рисунка також видно, що сигнал несучої частоти 3500 Гц відсутній у вихідному спектрі, що і є перевагою використання балансного модулятора.

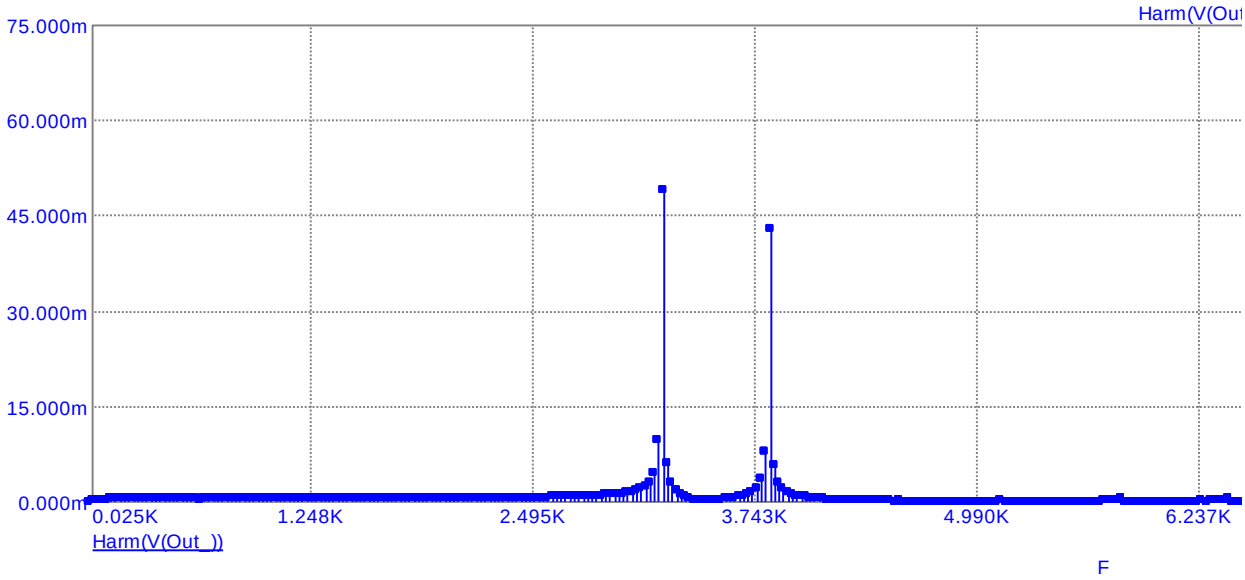


Рисунок 5.6 – Спектр вихідного сигналу скремблера при подачі на вхід сигналу частотою 300 Гц

При подачі на вхід сигналу частотою 3200 Гц на виході в ідеальному випадку маємо одержати сигнал частотою 3500 – 3200 = 300 Гц.

Часова діаграма на вході та виході схеми скремблера для даного випадку показана на рис. 5.7.

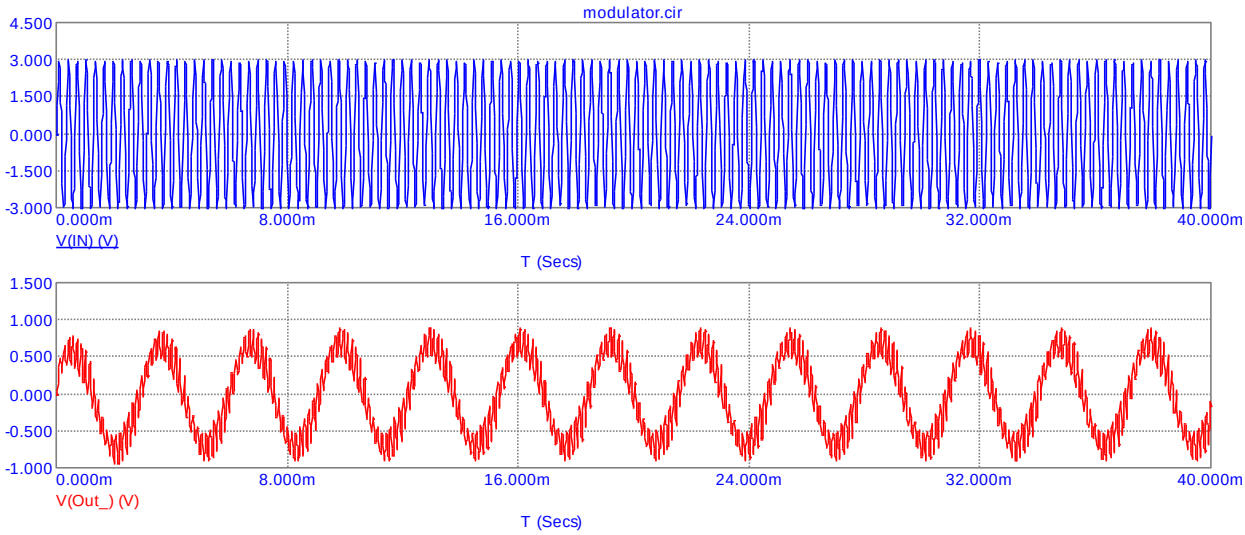


Рисунок 5.7 – Часові діаграми сигналу на вході та виході скремблера

Спектр вихідного сигналу показаний на рис. 5.8.

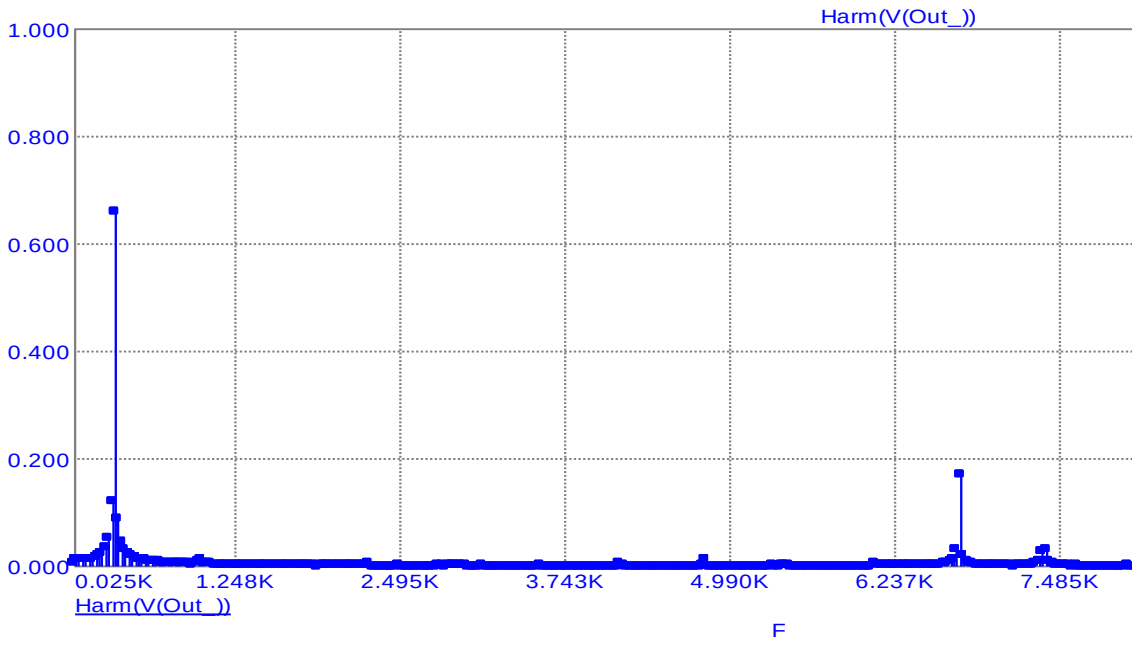


Рисунок 5.8 – Спектр вихідного сигналу скремблера при подачі на вхід сигналу частотою 3200 Гц

З графіку видно, що в спектрі вихідного сигналу: відсутня частота гетеродину; окрім частоти 300 Гц нижньої бокової смуги присятня і дзеркальна частота 6700 Гц з верхньої бокової смуги, внаслідок недосконалості вихідного фільтру.

Проведене моделювання роботи схеми скремблера підтвердило її працездатність. Довело, що використання частотної інверсії в запропонованій схемі дозволяє забезпечити закриття мовного сигналу. Проте моделювання виявило також досить низьку якість вихідного сигналу, що на практиці буде призводити до поганої розбірливості мови, що складатиме біля 65%.

Покращення якості мовного сигналу можливо за рахунок використання вхідного та вихідного фільтрів більших порядків, що дозволить уникнути накладання спектрів бічних смуг частот.

Використання фільтрів більшого порядку також дозволить забезпечити розбиття сигналу на певні смуги частот з подальшою їх перестановкою та інверсією. Це значно підвищить ступінь закриття мовного сигналу.

Проте даний шлях призведе до значного ускладнення схеми скремблера, збільшення масо-габаритних характеристик та вартості пристрою.

Тому найбільш доцільним є цифровий метод скремблювання шляхом перетворення вхідного сигналу в цифрову форму з подальшою цифровою обробкою сигналів на базі використання алгоритмів швидкого перетворення Фур'є. З урахуванням малої вартості сучасних сигнальних процесорів даний шлях буде більш ефективним та економнішим. Після цифрової обробки сигнал можна перетворити у аналогову форму з метою подальшої передачі аналоговими каналами зв'язку.

Використання цифрової обробки дозволить збільшити як якість відтворення мовного сигналу, так і ступінь закриття мовного сигналу.

6 АНАЛІЗ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ РОЗРОБКИ

Виконання науково-дослідної роботи завжди передбачає отримання певних результатів і вимагає відповідних витрат. Результати виконаної роботи завжди дають нам нові знання, які в подальшому можуть бути використані для удосконалення та/або розробки (побудови) нових, більш продуктивних зразків техніки, процесів та програмного забезпечення.

Дослідження на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» може бути віднесено до фундаментальних і пошукових наукових досліджень і спрямоване на вирішення наукових проблем, пов’язаних з практичним застосуванням. Основою таких досліджень є науковий ефект, який виражається в отриманні наукових результатів, які збільшують обсяг знань про природу, техніку та суспільство, які розвивають теоретичну базу в тому чи іншому науковому напрямку, що дозволяє виявити нові закономірності, які можуть використовуватися на практиці.

Для цього випадку виконаємо такі етапи робіт:

1) здійснимо проведення наукового аудиту досліджень, тобто встановлення їх наукового рівня та значимості;

2) проведемо планування витрат на проведення наукових досліджень;

3) здійснимо розрахунок рівня важливості наукового дослідження та перспективності, визначимо ефективність наукових досліджень.

6.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР на тему «Дослідження методів захисту інформації в цифрових системах

радіозв'язку» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 6.1 та 6.2.

Таблиця 6.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	0	0	0
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	55	52	57
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	0	0	0
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	0	0	0
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	0	0	0
Середнє значення балів експертів		54,7		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як нова, тобто отримана нова інформація, яка суттєво зменшує невизначеність наявних знань (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту) та проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів.

Таблиця 6.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерти (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	0	0	0
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	62	0	63
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	0	60	0
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	0	0	0
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	0	0	0
Середнє значення балів експертів	61,7		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою [14]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \qquad (6.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 54,7, k_{теор} = 61,7$ балів;

0,6 та *0,4* – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 54,7 + 0,4 \cdot 61,67 = 57,47 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 6.3.

Таблиця 6.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку», даний рівень становить 57,47 балів і відповідає статусу - середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

6.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

6.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій,

секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [14]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (6.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 15450{,}00 \cdot 21 / 21 = 15450{,}00 \; грн.$$

Проведені розрахунки зведемо до таблиці.

Таблиця 6.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	15450,00	735,71	21	15450,00
Старший науковий співробітник	13500,00	642,86	14	9000,00
Інженер розробник телекомунікаційних систем	10250,00	488,10	7	3416,67
Технік	7300,00	347,62	7	2433,33
Консультант (забезпечення безпеки інформаційних систем)	15000,00	714,29	3	2142,86
Всього				32442,86

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i \,, \tag{6.3}$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} \,, \tag{6.4}$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо *Мм*=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [14];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}35 \,/\, (21 \cdot 8) = 59{,}22$ *грн.*
$З_{р1} = 59{,}22 \cdot 6{,}00 = 355{,}34$ *грн.*

Таблиця 6.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
встановлення обладнання	6,00	2	1,10	59,22	355,34
налагодження обладнання	3,00	5	1,70	91,53	274,58
формування цифрових систем радіозв'язку	10,00	4	1,50	80,76	807,59
відлагодження	4,50	5	1,70	91,53	411,87
формування бази даних	11,00	3	1,35	72,68	799,51
підбір компонентів дослідження	4,00	4	1,50	80,76	323,04
Всього					2971,93

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (6.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (32442,86 + 2971,93) · 11 / 100% = 3895,63 грн.

6.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (6.6)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (32442,86 + 2971,93 + 3895,63) · 22 / 100% = 8648,29 грн.

6.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Дослідження методів захисту інформації в цифрових системах радіозв'язку».

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення експериментальних математичних моделей або програмного забезпечення, тому дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

Витрати на матеріали (M), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj} , \qquad (6.7)$$

де H_j – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

K_j – коефіцієнт транспортних витрат, (K_j = *1,1 … 1,15*);

B_j – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

$M_1 = 3{,}0 \cdot 215{,}00 \cdot 1{,}1 - 0 \cdot 0 = 709{,}50$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 6.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір офісний А4 MONDI Smart-line (500)	215,00	3,0	0	0	709,50
Папір для записів А5 Navigator 500	120,00	3,0	0	0	396,00
Органайзер офісний SKIPER 2500	185,00	4,0	0	0	814,00
Канцелярське приладдя SoBB Eco 2	210,00	4,0	0	0	924,00
Картридж для принтера HP Laser jet 1020	1950,00	2,0	0	0	4290,00
Диск оптичний CD-R Optic	14,50	4,0	0	0	63,80
Flesh-пам'ять 64 GB	190,00	1,0	0	0	209,00
Всього					7406,30

6.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (6.8)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j = 1,1 \ldots 1,15$).

$К_в = 4 \cdot 1650,00 \cdot 1,1 = 7260,00$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 6.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Стекові інтерфейси JP100-AUX	4	1650,00	7260,00
Всього			7260,00

6.2.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (6.9)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, (K_i = *1,10…1,12);*

k – кількість найменувань устаткування.

$B_{спец}$ = *2200,00 · 1 · 1,1 = 2420,00 грн.*

Отримані результати зведемо до таблиці:

Таблиця 6.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Модем для цифрових систем передачі	1	2200,00	2420,00
Всього			2420,00

6.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (6.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 9420,00 \cdot 1 \cdot 1,1 = 10362,00$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 6.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Математичне середовище MatLab 12	1	9420,00	10362,00
Прикладне ПЗ Mathematica	1	7150,00	7865,00
Модель імітатора передавача	1	2560,00	2816,00
Модель імітатора приймача	1	3640,00	4004,00
Всього			25047,00

6.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12} \ , \qquad (6.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (5100,00 \cdot 1) / (2 \cdot 12) = 212,50$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 6.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
ОС Windows	5100,00	2	1	212,50
Комп'ютерне обладнання для вирішення проблем моделювання мереж	62400,00	3	1	1733,33
Прикладне програмне забезпечення проектування та аналізу комунікаційних систем	7100,00	2	1	295,83
Модем для стільникових систем зв'язку	6820,00	3	1	189,44
Модем для пакетних радіомереж	7360,00	3	1	204,44
Модем для локальних радіомереж	6900,00	3	1	191,67
Оргтехніка	8430,00	5	1	140,50
Приміщення лабораторії досліджень	289000,00	25	2	1926,67
Робоче місце інженера-розробника телекомунікаційних систем	6300,00	5	2	210,00
Робоче місце старшого наукового співробітника	6800,00	5	2	226,67
Всього				5331,06

6.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \qquad (6.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_е$ = 6,25 грн;

$К_{вп і}$ – коефіцієнт, що враховує використання потужності, $К_{вп і} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_е = 0,35 \cdot 160,0 \cdot 6,25 \cdot 0,95 / 0,97 = 350,00$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 6.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Комп'ютерне обладнання для вирішення проблем моделювання мереж	0,35	160,0	350,00
Модем для стільникових систем зв'язку	0,03	50,0	9,38
Модем для пакетних радіомереж	0,04	50,0	12,50
Модем для локальних радіомереж	0,03	50,0	9,38
Робоче місце старшого наукового співробітника	0,10	80,0	50,00
Робоче місце інженера-розробника телекомунікаційних систем	0,10	80,0	50,00
Оргтехніка	0,52	2,0	6,50
Всього			487,75

6.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (6.13)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$В_{св}$ = (32442,86 + 2971,93) · 20 / 100% = 7082,96 грн.

6.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (6.14)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$В_{сп}$ = (32442,86 + 2971,93) · 30 / 100% = 10624,44 грн.

6.2.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (6.15)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 60%.

$I_в$ = *(32442,86 + 2971,93) · 60 / 100% = 21248,87 грн.*

6.2.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (6.16)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 105%.

$B_{нзв}$ *= (32442,86 + 2971,93) · 105 / 100% = 37185,53 грн.*

Витрати на проведення науково-дослідної роботи на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + B_{спец} + B_{прг} + A_{обл} + B_е + B_{св} + B_{сп} + I_в + B_{нзв}. \quad (6.17)$$

$B_{заг}$*= 32442,86 +2971,93 +3895,63 +8648,29 +7406,30 +7260,00 +2420,00 + 25047,00 + 5331,06 +487,75 +7082,96 +10624,44 +21248,87 +37185,53 = 172052,60 грн.*

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (6.18)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,95.

ЗВ = 172052,60 / 0,95 = 181108,00 грн.

6.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \qquad (6.19)$$

де I – коефіцієнт важливості роботи. Приймемо $I = 4$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо n=2;

T_C – коефіцієнт складності роботи. Приймемо $T_C = 3$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 4$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо B =181108,00 грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників I, n, T_C, R, B, t здійснюється експертним шляхом або на основі нормативів [14].

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 4^2 \cdot 3 \cdot 4 \,/\, 181{,}1 \cdot 0{,}08 = 12{,}72.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

6.4 Висновок до розділу 4

Витрати на проведення науково-дослідної роботи на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» складають 181108,00 грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково-дослідної роботи на тему «Дослідження методів захисту інформації в цифрових системах радіозв'язку» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1. Оцінка радіаційного захисту в приміщенні першого поверху будівлі

Коефіцієнт протирадіаційного захисту приміщення, в якому перебуватимуть люди розраховуватимемо за формулою

$$K_з = \frac{0{,}65 \times K_1 \times K_{СТ}}{(1 - K_Ш)(K_0 \times K_{СТ} + 1)K_М} \quad (7.1)$$

Основні характеристики:

1. Стіни цегляні (380 мм), маса 1м^2 – 532 кг.
2. Внутрішні стіни цегляні (120 мм), маса 1м^2 – 168 кг.
3. Перегородки піноблочні (100 мм), маса 1м^2 – 40 кг.
4. Площа віконних прорізів: В-1 – 3 м^2.
5. Площа дверних прорізів: Д-1 – 1,9 м^2; Д-2 – 2,73 м^2.
6. Висота підвіконників – 0,55 м;
7. Площа підлоги для розрахунку приміщення – 51,6 м^2;
8. Висота приміщення – 3 м;
9. Ширина зараженої дільниці, що примикає до приміщення – 6 м;
10. Маса 1 м^2 перекриття – 400 кг/м^2;
11. Плоскі кути приміщення:

Кут α_1 =110°. Проти кута розташовані:

- стіни цегляна (380 мм) площею 25,8 м^2;
- 2 стіни цегляні (380 мм) площею 25,8 м^2 з прорізом площею 3,8 м^2.

Кут α_2 =70°. Проти кута розташовані:

- стіна цегляна (380 мм) площею 18 м^2 з прорізом площею 6 м^2.

Кут α_3 =110°. Проти кута розташована:

- стіна цегляна (380 мм) площею 25,8 м^2 з прорізом площею 4,63 м^2;
- стіни цегляна (380 мм) площею 25,8 м^2;.

Кут α_4 =70°. Проти кута розташована:

- стіна цегляна (380 мм) площею 18 м^2 з прорізом площею 6 м^2.

Визначаємо сумарні маси 1 м^2 стін і перегородок, розташованих проти плоских кутів.

Кут α_1 =110°.

Маса 1 м^2 стіни цегляної (380 мм) площею 25,8 м^2

$$G_{зв} = 532\,(\text{кг}).$$

Маса 1 м^2 стіни цегляної (380 мм) площею 25,8 м^2 з прорізом площею 3,8м^2

$$\alpha_{\text{ст}} = \frac{3,8}{25,8} = 0,15,\ G_{зв} = 532\left(1-0,15\right) = 452,2\,(\text{кг}).$$

Сумарна маса 1 м^2 стін і перегородок плоского кута α_1

$$G_{\Sigma}^{1} = 532 + 452,2 = 984,2\,(\text{кг}).$$

Кут α_2 =70°.

Маса 1 м^2 стіни цегляної (380 мм) площею 18 м^2 з прорізом площею 6 м^2

$$\alpha_{\text{ст}} = \frac{6}{18} = 0,33,\ G_{зв} = 532\left(1-0,33\right) = 356,4\,(\text{кг}).$$

Сумарна маса 1 м^2 стін і перегородок плоского кута α_2

$$G_{\Sigma}^{2} = 356,4\,(\text{кг}).$$

Кут α_3 =110°.

Маса 1 м^2 стіни цегляної (380 мм) площею 25,8 м^2 з прорізом площею 4,63м^2

$$\alpha_{\text{ст}} = \frac{4,63}{25,8} = 0,18,\ G_{зв} = 532\left(1-0,18\right) = 436,5\,(\text{кг}).$$

Маса 1 м^2 стіни цегляної (380 мм) площею 25,8 м^2

$$G_{зв} = 532\,(\text{кг}).$$

Сумарна маса 1 м^2 стін плоского кута α_3

$$G_{\Sigma}^{3} = 436,5 + 532 = 968,5\,(\text{кг}).$$

Кут α_4 =70°.

Маса 1 м^2 стіни цегляної (380 мм) площею 18 м^2 з прорізом площею 6 м^2

$$\alpha_{\text{ст}} = \frac{6}{18} = 0,33,\ G_{зв} = 532\left(1 - 0,33\right) = 356,4\,(\text{кг}).$$

Сумарна маса 1 м^2 стін плоского кута α_4

$$G_{\Sigma}^{4} = 356,4\,(\text{кг}).$$

Сумарні маси стін і перегородок проти плоских кутів приміщення

$$G_{\Sigma}^{1} = 984,2\,(\text{кг});\ G_{\Sigma}^{2} = 356,4\,(\text{кг});$$

$$G_{\Sigma}^{3} = 968,5\,(\text{кг});\ G_{\Sigma}^{4} = 356,4\,(\text{кг}).$$

Сумарна маса стін і перегородок проти всіх кутів менша за 1000 кг/м^2, тому при визначенні коефіцієнта K_1, що враховує долю радіації після послаблення зовнішніми і внутрішніми стінами, враховуватимемо всі кути

$$K_1 = \frac{360}{36 + \sum \alpha_i} = \frac{360}{36 + 360} = 0,91$$

За мінімальною сумарною масою стін $G_{\Sigma}^{4} = 356,4\,(\text{кг})$ визначаємо [1] коефіцієнт $K_{\text{ст}}$ = 12.

За шириною будівлі визначаємо коефіцієнт, який враховує долю розсіювання випромінювання $K_{ш}$=0,47 (висота приміщення складає 3 м).

Коефіцієнт K_0, що враховує зниження поглинальної здатності зовнішніх стін за рахунок наявності в них віконних і дверних прорізів та проникнення в приміщення вторинного випромінювання, з врахуванням висоти від підлоги до вікон 3 м розрахуємо

$$K_0 = 0,8\frac{S_0}{S_{П}} = 0,8\frac{12}{51,6} = 0,19,$$

де S_0 = 12 м^2 – загальна площа віконних і дверних прорізів приміщення, що виходять на вулицю; $S_п$ = 51,6 м^2 – площа підлоги приміщення.

Коефіцієнт, що враховує зниження дози радіації в приміщенні, розташованому в багатоповерховій будівлі, від екранувальної дії сусідніх споруд $К_м$=0,55 [1,2].

Тоді

$$К_з = \frac{0,65 \times К_1 \times К_{СТ}}{(1 - К_{Ш})(К_0 \times К_{СТ} + 1) К_М} =$$

$$= \frac{0,65 \times 12 \times 0,91}{(1 - 0,47)(0,19 \cdot 12 + 1) 0,55} = 7,4$$

Проведені для приміщення першого поверху будівлі розрахунки показали, що коефіцієнт протирадіаційного захисту цього приміщення складає 7,4, тому дане приміщення не може бути використане для перебування людей в умовах радіаційного забруднення.

ВИСНОВКИ

У магістерській кваліфікаційній роботі було проведено дослідження методів захисту інформації і обрано оптимальний цифровий метод для цифрових систем радіозв’язку.

У перших розділах наведено результати аналізу сучасних цифрових систем радіозв’язку, розглянуто основні стандарти та класифікацію. Потім було розглянуто основні методи захисту інформації в системах радіозв’язку.

Виконано оцінювання площі покриття цифрової системи радіозв'язку з рухомими об'єктами. В результаті розрахунку здійснено оцінку потужності передавачів базових і носимих мобільних станцій, а також визначено оптимальні потужності, які підходять для забезпечення необхідної якості зв'язку по всій зоні покриття базових станцій. Розрахунки виконано для різних висот антен і різних коефіцієнтів забезпечення зв'язком по місцю і в часі.

Здійснено вибір та обгрунтування методу кодування мовних сигналів на основі m-послідовностей. Запропоновано для формування коду використовувати 5-розрядний первинний ключ, одержаний з генератора псевдовипадкових чисел. Розроблено блок-схему формування коду.

Розроблено структурні схеми аналого-цифрових приймача та передавача закодованих телефонних сигналів та виконано оцінювання швидкодії цих пристроїв.

Виконано моделювання процесу кодування мовних сигналів у цифрових системах радіозв’язку та побудовано графік залежності числа помилок відновлення від кількості повторень кодової комбінації. Здійснено комп`ютерне моделювання скремблера, в результаті якого розроблено моделювальну схему пристрою та виконано спектральний аналіз вихідного сигналу скремблера. Результати моделювання підтвердили високу ефективність цифрових методів і засобів захисту інформації в цифрових системах радіозв`язку.

В останніх розділах був проведено аналіз економічної ефективності розробки та досліджено питання щодо охорони праці та безпеки в надзвичайних ситуаціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ільченко М.Ю., Кравчук С.О. Сучасні телекомунікаційні системи. – К.: НВП “Видавництво “Наукова думка” НАН України”. 2008. – 328 с.

2. Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні телекомунікації. – К.: Азимут-Україна, 2013. – 608 с.

2. Жураковський Ю.П. Теорія інформації та кодування: Підручник. – К.: Вища школа, 2001. – 255 с.

3. Методи та засоби цифрового оброблення високочастотних сигналів для систем безпеки та моніторингу: монографія / Г. Г. Бортник, М. В. Васильківський, В. М. Кичак. – Вінниця: ВНТУ, 2020. – 126 с.

4. Методи та засоби первинного цифрового оброблення радіосигналів: монографія / Г. Г. Бортник, М. В. Васильківський, В. М. Кичак. Вінниця: ВНТУ, 2016. 168 с.

5. Методи та пристрої оцінювання бітових помилок у телекомунікаційних системах: монографія / В. М. Кичак, Г. Г. Бортник, В. Д. Тромсюк. Вінниця: ВНТУ, 2017. 212 с.

6. Бортник Г. Г., Кичак В. М., Яблонський В. Ф. Методи та засоби оцінювання параметрів абонентських ліній зв’язку. Вінниця: УНІВЕРСУМ-Вінниця, 2006. 139 с.

7. Телекомунікаційні системи передачі: підручник / В.М. Кичак, О.М. Шинкарук, Г.Г. Бортник, І.І. Чесановський. – Хмельницький: Видавництво НАДПСУ, 2016. – 424 с.

8. Бортник Г.Г., Васильківський М.В., Кичак В.М. Транспортні телекомунікаційні технології: навч. посібник.– Вінниця: ВНТУ, 2017. – 172 с.

9. Бортник Г.Г., Кичак В.М. Цифрова обробка сигналів в телекомунікаційних системах: підручник. – Вінниця : ВНТУ, 2014. – 232 с.

10. Волощук Ю.І. Сигнали та процеси у радіотехніці: підручник, Т.1. – Харків: СМІТ, 2003. – 580 с.

11. Костюк О. А., Лазарєв О. О. Передача та захист інформації на ТКМ: навчальний посібник. В.: ВНТУ, 2006. 132 с.

12. Бондарчук А.П., Срочинська Г.С., Твердохліб М.Г. Основи інфокомунікаційних технологій: навчальний посібник. К.: АНВА Прінт, 2015. 76 с.

13. Кривуца В. Г., Беркман Л. Н., Лапінський В. В., Основи інфокомунікацій: навчальний посібник. К.: ДУІКТ, 2011. 276 с.

14. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

ДОДАТКИ

Додаток А
(обов'язковий)

ПОГОДЖЕНО
ВНТУ

ЗАТВЕРДЖУЮ
Зав.кафедри ІКСТ ВНТУ,
докт. техн. наук, професор
В.М. Кичак
"__" _____ 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на виконання магістерської кваліфікаційної роботи
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ЦИФРОВИХ СИСТЕМАХ РАДІОЗВ`ЯЗКУ
08-34.МКР.001.00.000 ТЗ

Керівник роботи
к.т.н., проф. кафедри ІКСТ ВНТУ
Бортник Г.Г.

Виконавець: ст. гр. ТКС-21мз
Жук А.В.

Вінниця-2023

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “20” 03 2023 року № 68 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 30.01.2023 р.

Дата закінчення: 15.06.2023 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою даної роботи є роботи є підвищення ефективності пристроїв захисту інформації в рухомих засобах зв’язку за рахунок використання цифрового методу кодування.

Об’єкт дослідження є процеси цифрового кодування інформації у рухомих засобах зв’язку.

Предмет дослідження є ефективні методи та засоби захисту інформації в цифрових пристроях радіозв’язку.

Основними завданнями роботи є:

- технічне обґрунтування доцільності даної розробки;
- розробка технічного завдання;
- виконати аналіз сучасних цифрових цифрових систем радіозв’язку;
- здійснити дослідження основних методів захисту інформації в цифрових засобах зв’язку;
- провести оптимізацію алгоритмів шифрування для засобів зв’язку з рухомими об’єктами;
- розробити систему кодування мовних сигналів у цифровій мережі зв’язку;
- виконати моделювання процесу кодування мовних сигналів у рухомих засобах зв’язку.

Розроблені в ході виконання магістерської роботи пристрої захисту інформації дозволить розв’язати протиріччя між ймовірністю розкриття мовних повідомлень та якістю зв’язку.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Робота базується на результатах переддипломної практики, яка виконувалась з 30.01.2023 р. по 10.03.2023р. Під час підготовки магістерської кваліфікаційної роботи будуть використані матеріали цієї практики.

Список використаних джерел розробки:

3.1 Жураковський Ю.П. Теорія інформації та кодування: Підручник. – К.: Вища школа, 2001. – 255 с.

3.2 Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти у Вінницькому національному технічному університеті / Уклад. А. О. Семенов, Л. П. Громова, Т.В. Макарова, Сердюк О.В. – Вінниця: ВНТУ, 2021. – 60 с.

3.3 Бортник Г.Г., Васильківський М.В. Методичні вказівки до підготовки магістерських кваліфікаційних робіт для студентів спеціальності «Телекомунікації та радіотехніка» усіх форм навчання. – Вінниця:ВНТУ, 2018. – 50 с.

3.4 Стеклов В.К. Сучасні системи управління в телекомунікаціях: монографія/ В.К. Стеклов, Б.Я. Костік, Л.Н. Беркман. – К. : Техніка, 2005.– 396 с.

3.5 ДСТУ 3008-2015. Інформація та документація, звіти у сфері науки і техніки.- К.: ДП «УкрНДНЦ», 2016.

3.6. Методи та засоби цифрового оброблення високочастотних сигналів для систем безпеки та моніторингу: монографія / Г. Г. Бортник, М. В. Васильківський, В. М. Кичак. – Вінниця: ВНТУ, 2020. – 126 с.

3.7. Методи та засоби первинного цифрового оброблення радіосигналів: монографія / Г. Г. Бортник, М. В. Васильківський, В. М. Кичак. Вінниця: ВНТУ, 2016. – 168 с.

3.8. Костюк О. А., Лазарєв О. О. Передача та захист інформації на ТКМ: навчальний посібник. В.: ВНТУ, 2006. – 132 с.

3.9. Бондарчук А.П., Срочинська Г.С., Твердохліб М.Г. Основи інфокомунікаційних технологій : навчальний посібник. К. : АНВА Прінт, 2015. – 76 с.

3.10 Телекомунікаційні системи передачі: підручник / В.М. Кичак, О.М. Шинкарук, Г.Г. Бортник, І.І. Чесановський, О.В. Стальченко. – Хмельницький: Видавництво НАДПСУ, 2016. – 424 с.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра інфокомунікаційних систем і технологій, студент групи ТКС-21мз Жук А.В.

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати дослідження методів і пристроїв захисту інформації у цифрових засобах рухомого зв’язку.

5.1 Технічні вимоги, яким повинна відповідати розробка, наступні:

- швидкість передачі інформації у каналах зв’язку 64 кбіт/с;
- ймовірність розкриття інформації не більше 10^{-5};
- смуга вхідного сигналу – 300÷3400 Гц;
- динамічний діапазон – 40дБ;
- частота дискретизації телефонного сигналу – 8 кГц;
- розрядність аналого-цифрових перетворювачів – 12 розрядів.

5.2 Режим функціонування пристрою захисту інформації у цифрових засобах рухомого зв’язку – реальний масштаб часу.

5.3 Тип вхідних сигналів – первинні телефонні.

5.4 Тип базових елементів – інтегральні мікросхеми.

5.5 Режим зв’язку – дуплекс.

5.6 При розробці пристрою захисту інформації у цифрових засобах рухомого зв’язку слід використовувати стандартні та уніфіковані деталі.

6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№	Назва та зміст етапу	Термін виконання		Очікувані результати	Звітна документ-тація
		початок	закінчення		
1.	Розробка технічного завдання (ТЗ)	30.01.2023р.	10.02.2023р.	Розроблене ТЗ	Додаток А
2.	Технічне обґрунтування (ТО)	13.02.2023р.	20.02.2023р.	Розроблене ТО	Вступ. Розділ 1.
3.	Аналіз методів захисту інформації в системах зв'язку	21.02.2023р.	10.03.2023р.	Проведений аналіз	Розділи 2, 3
4.	Розробка пристроїв кодування мовних сигналів	13.03.2023р	03.04.2023р.	Розроблені пристрої	Розділ 4
5.	Моделювання процесу кодування мовних сигналів	06.04.2023р.	05.05.2023р.	Характеристики і параметри	Розділ 5
6.	Аналіз економічної ефективності	08.05.2023р.	19.05.2023р.	Економічна частина МКР	Розділ 6
7.	Охорона праці та безпека в надзвичайних ситуаціях	22.05.2023р.	31.05.2023р.	Частина ОТ та БНС	Розділ 7
8.	Оформлення пояснювальної записки (ПЗ) та графічної частини	01.06.2023р.	13.06.2023р.	Оформлена документація	ПЗ та графічна частина
9.	Нормоконтроль, попередній захист, опонування МКР	14.06. 2023р.	15.06.2023р.	Позитивні відзиви	Відгуки
10.	Захист МКР ЕК		16.06.2023р.	Позитивний захист	Протокол ЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- алгоритм кодування мовних сигналів;
- структурні електричні схеми засобів;
- моделювальні програми;
- економічна частина МКР;

- розділ безпеки життєдіяльності
- рекомендації щодо подальшого використання розробленого пристроїв.

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій:

- Вінницька філія ЗАТ «Київстар» шляхом впровадження алгоритму захисту інформації;
- ПАТ “Укртелеком” шляхом впровадження нових структур пристроїв захисту інформації.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується підвищення ступеня захисту мовної інформації.

8. МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ ТА ПІД ЧАС ЕТАПІВ

За результатами виконання МКР до ЕК подаються пояснювальна записка, графічна частина МКР, відзив і рецензія.

9. ПОРЯДОК ПРИЙМАННЯ МКР ТА ЇЇ ЕТАПІВ

Поетапно результати виконання МКР розглядаються керівником роботи та обговорюються на засіданні кафедри. Захист МКР відбувається на відкритому засіданні ЕК.

10. ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

Документація, що розробляється в процесі виконання досліджень повинна містити:

- технічне обґрунтування розробки;
- нові структури засобів;
- структурні електричні схеми пристроїв;
- економічну частину та розділ БЖД;
- рекомендації щодо подальшого використання пристроїв.

11. ВИМОГИ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У зв’язку з тим, що інформація не є конфіденційною, заходи з її технічного захисту не передбачаються.

Додаток Б
(обов’язковий)

Протокол
перевірки кваліфікаційної роботи
на наявність текстових запозичень

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Дослідження методів захисту інформації в цифрових системах радіозв`язку

Тип роботи: Магістерська кваліфікаційна робота

Підрозділ кафедра Інфокомунікаційних систем і технологій, факультет Інформаційних електронних систем

(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 95,55 % Схожість 4,45 %

Аналіз звіту подібності (відмітити потрібне):

■ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа відповідальна за перевірку _____ Васильківський М.В.
(підпис) (прізвище, ініціали)

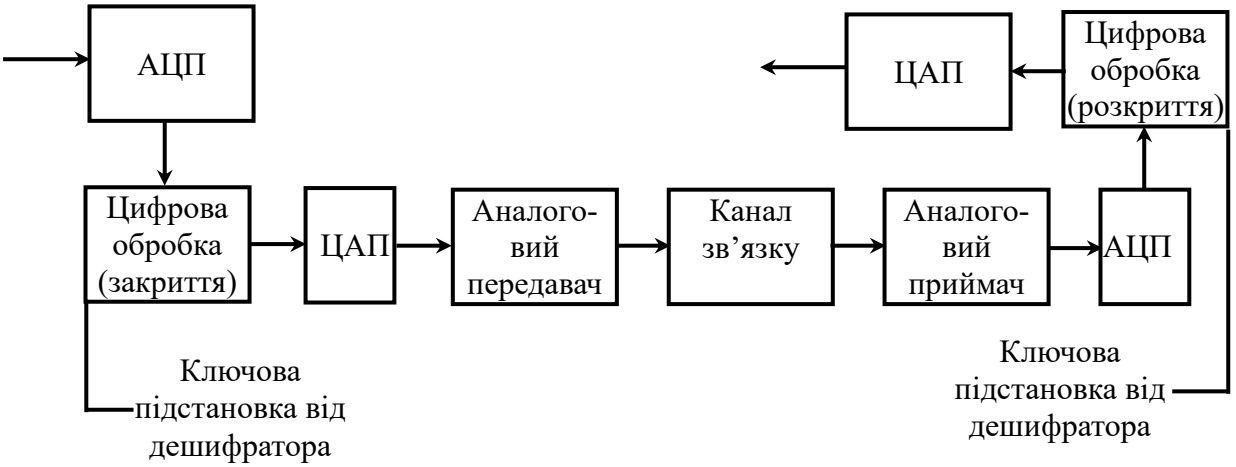
Ознайомлені з повним звітом, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Жук А.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Бортник Г.Г.
(підпис)

Додаток В
(обов’язковий)

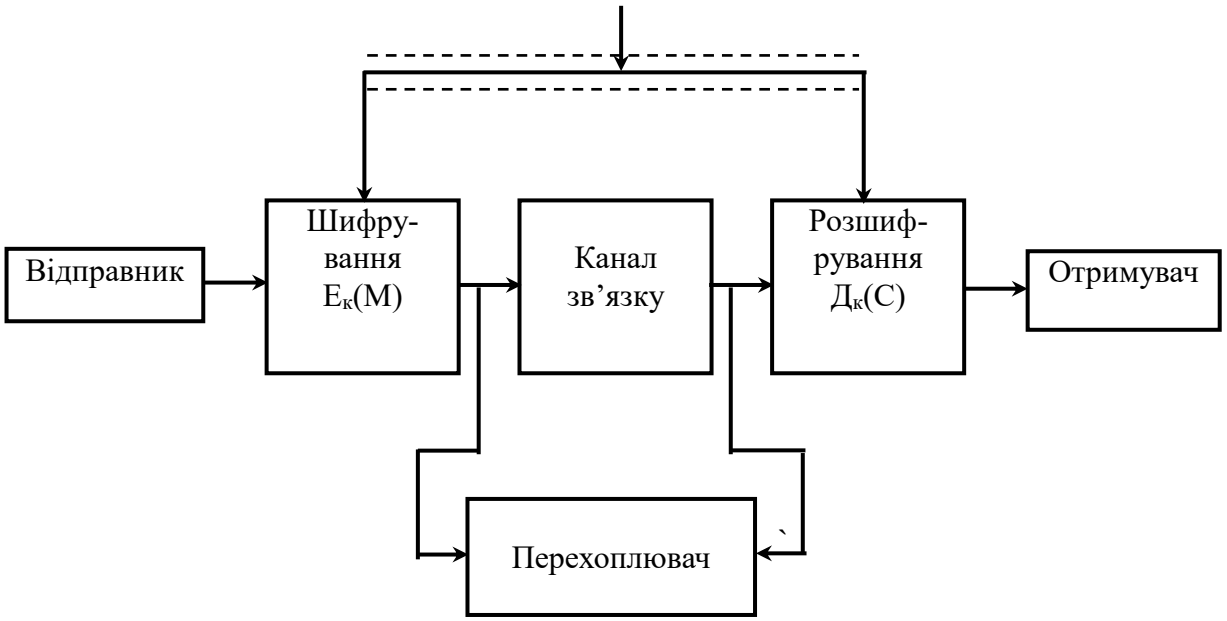
Структурна схема мовного скремблера



					08-32.МКР.001.00.000 Е1	
					Структурна схема мовного скремблера	Літ. / Маса / Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата		
Розроб.		Жук А.В.				Арк. 1 / Аркушів 1
Перевір.		Бортник Г.Г.				
Т. Контр.						ВНТУ, ТКС-21мз
Реценз.						
Н. Контр.		Бортник Г.Г.				
Затверд.		Кичак В.М.				

Додаток Г
(обов’язковий)

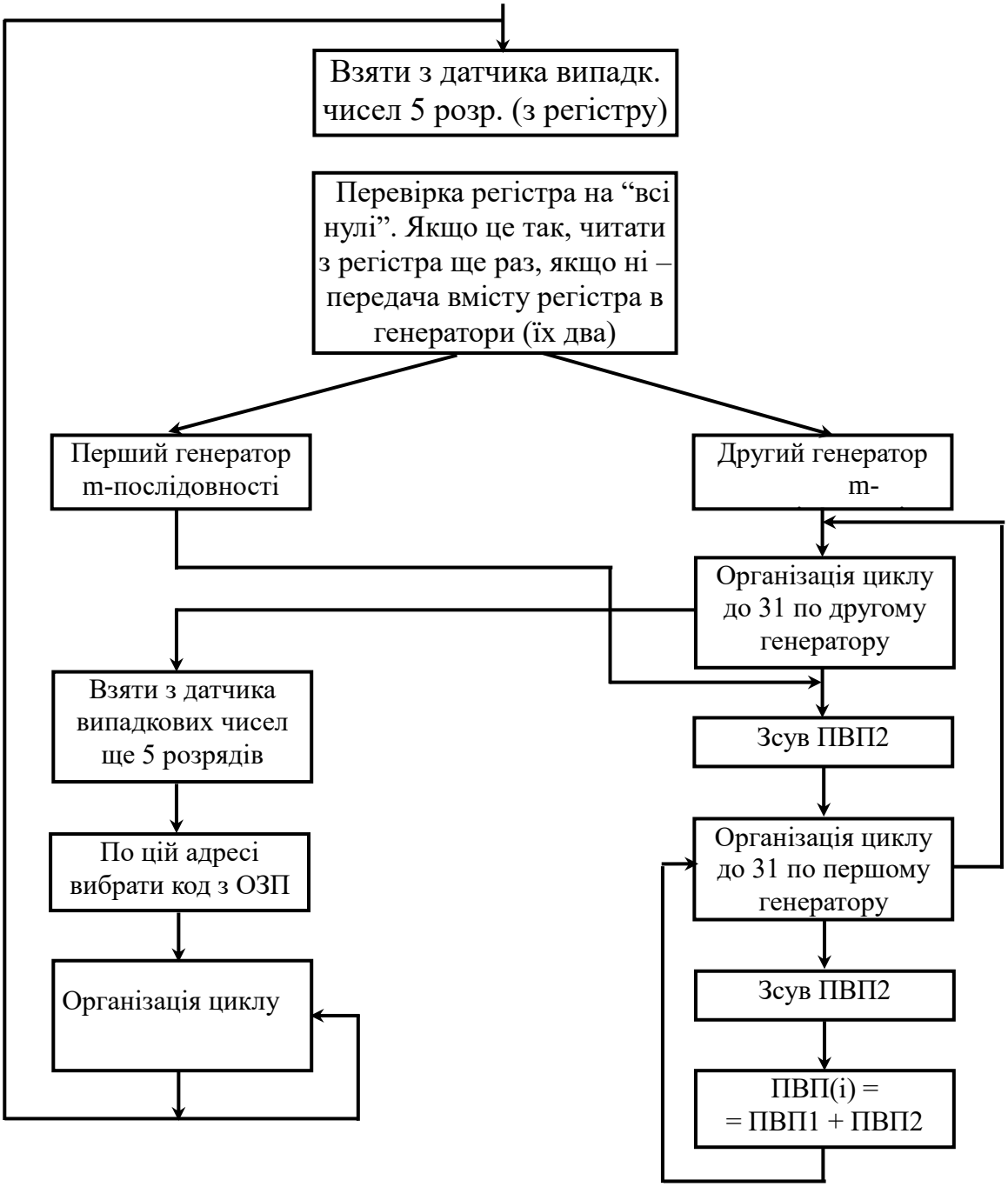
Структурна схема захищеного каналу зв’язку



					08-32.МКР.001.00.000 Е1		
					Структурна схема захищеного каналу зв'язку	Літ.	Маса	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Жук А.В.				Арк. 1	Аркушів 1	
Перевір.		Бортник Г.Г.						
Т. Контр.								
Реценз.								
Н. Контр.		Бортник Г.Г.				ВНТУ, ТКС-21мз		
Затверд.		Кичак В.М.						

Додаток Д
(обов’язковий)

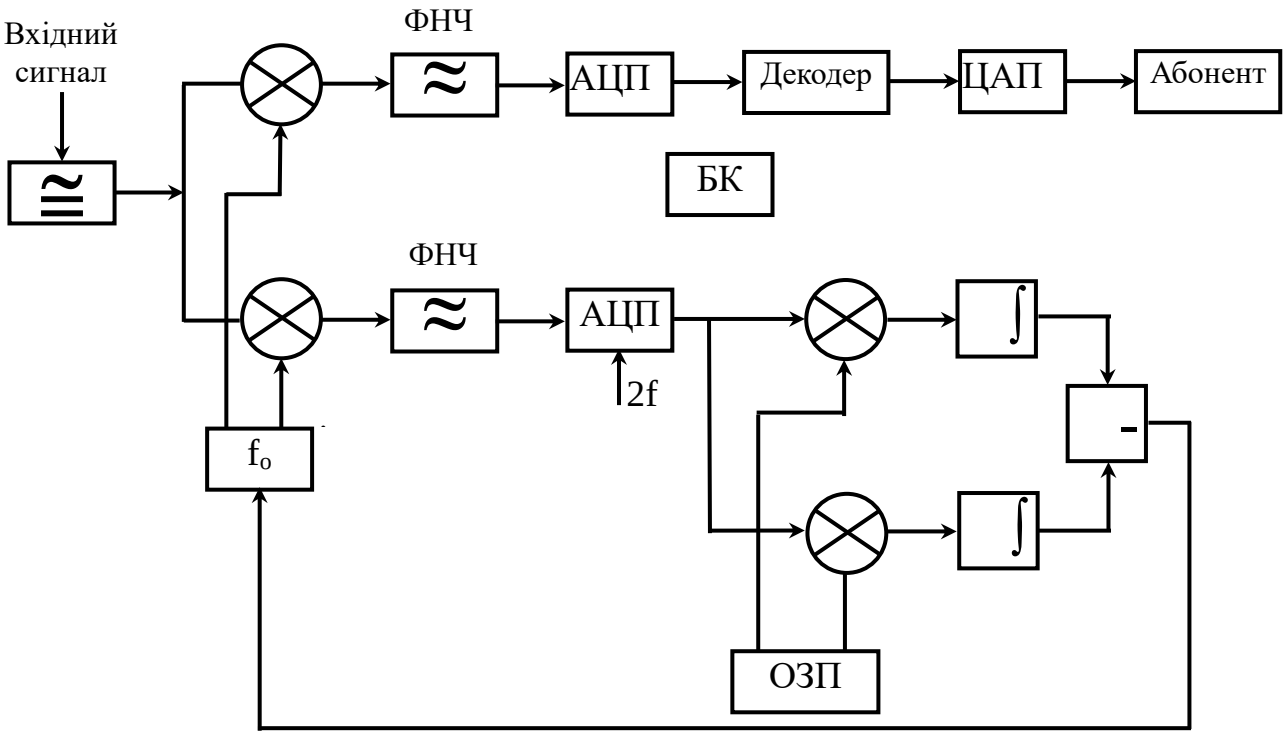
Блок-схема алгоритму формування захищеного коду



					08-32.МКР.001.00.000 Е8	
Змн.	Арк.	№ докум.	Підпис	Дата	Блок-схема алгоритму формування захищеного коду	Літ. / Маса / Масштаб
Розроб.		Жук А.В.				
Перевір.		Бортник Г.Г.				Арк. 1 / Аркушів 1
Т. Контр.						
Реценз.						
Н. Контр.		Бортник Г.Г.				ВНТУ, ТКС-21мз
Затверд.		Кичак В.М.				

Додаток Е
(обов’язковий)

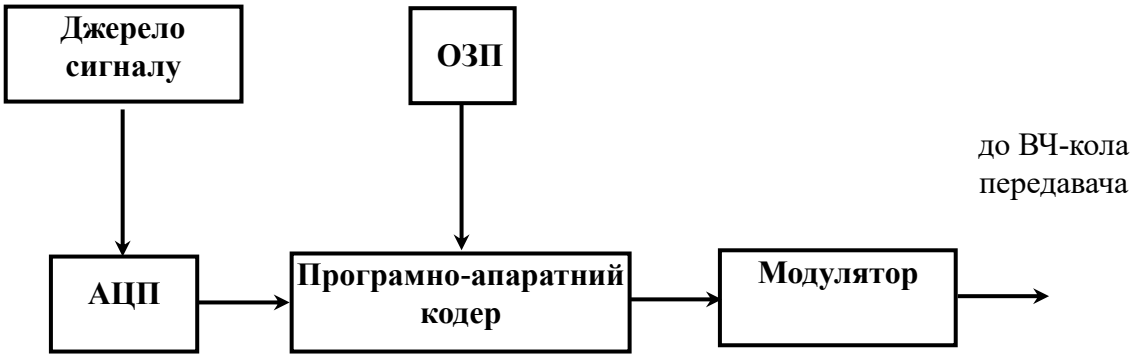
Структурна схема аналого-цифрового приймача
закодованих телефонних сигналів



					08-32.МКР.001.00.000 Е1		
					Структурна схема аналого-цифрового приймача закодованих телефонних сигналів	Літ.	Маса	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Жук А.В.				Арк. 1	Аркушів 1
Перевір.		Бортник Г.Г.					
Т. Контр.							
Реценз.							
Н. Контр.		Бортник Г.Г.				ВНТУ, ТКС-21мз	
Затверд.		Кичак В.М.					

Додаток Ж
(обов’язковий)

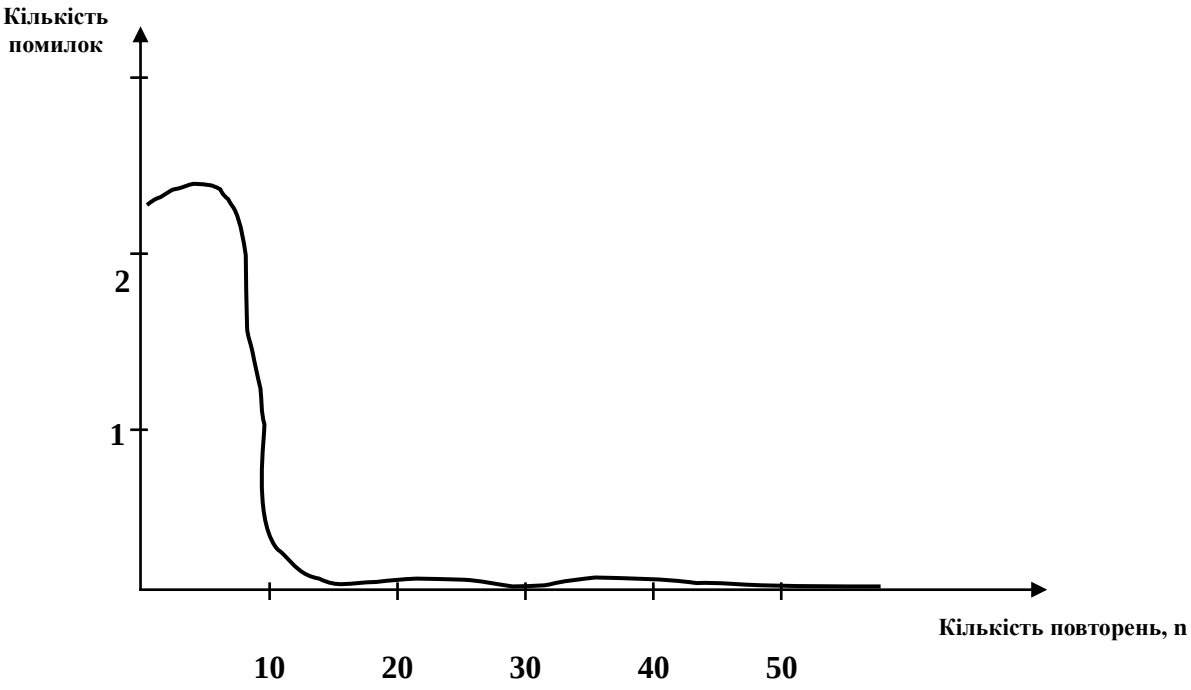
Структурна схема аналого-цифрового передавача
закодованих телефонних сигналів



					08-32.МКР.001.00.000 Е1		
					Структурна схема аналого-цифрового передавача закодованих телефонних сигналів	Літ.	Маса	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Жук А.В.				Арк. 1	Аркушів 1
Перевір.		Бортник Г.Г.					
Т. Контр.							
Реценз.							
Н. Контр.		Бортник Г.Г.				ВНТУ, ТКС-21мз	
Затверд.		Кичак В.М.					

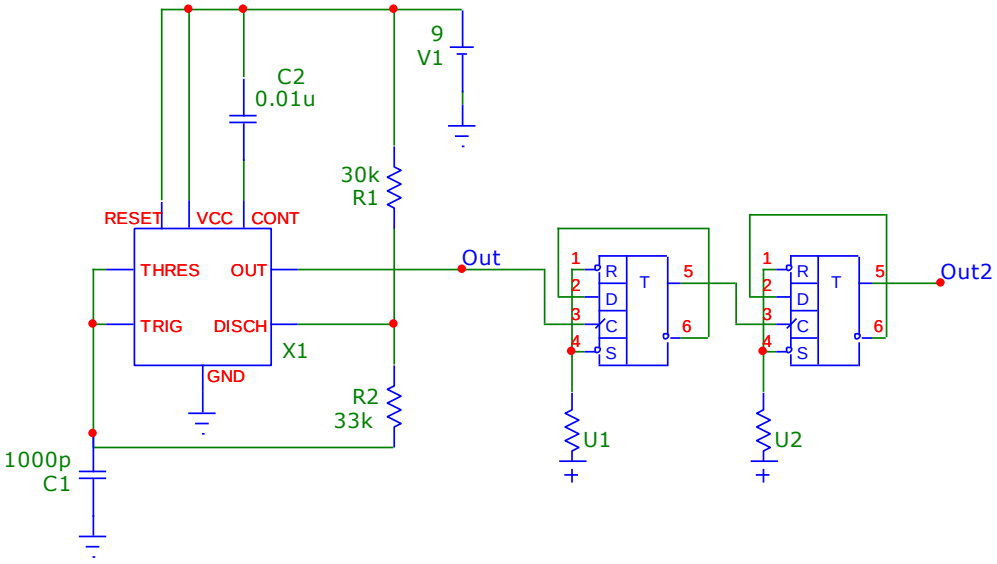
Додаток З
(обов’язковий)

Результати моделювання кодера

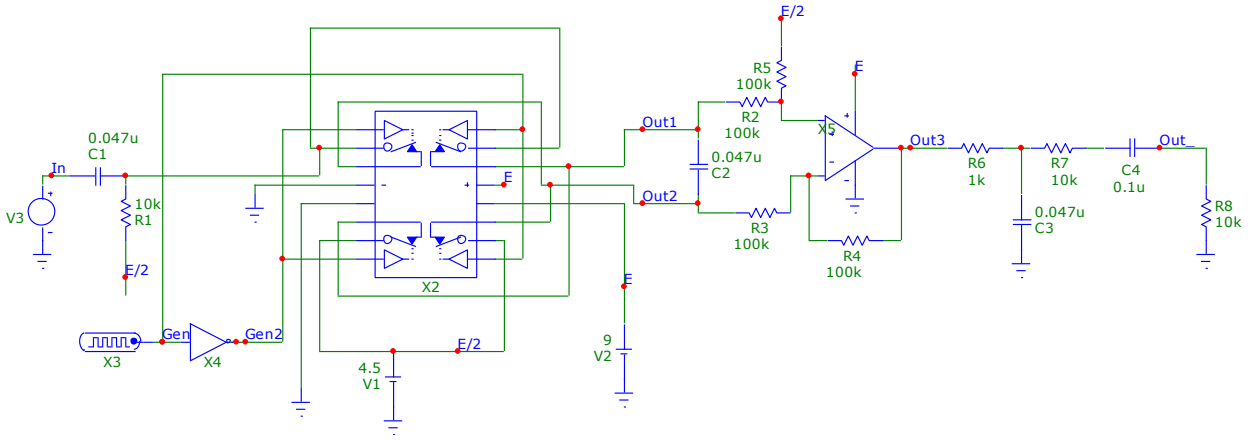

Кількість помилок
2
1
Кількість повторень, n
10
20
30
40
50

Додаток К
(обов’язковий)

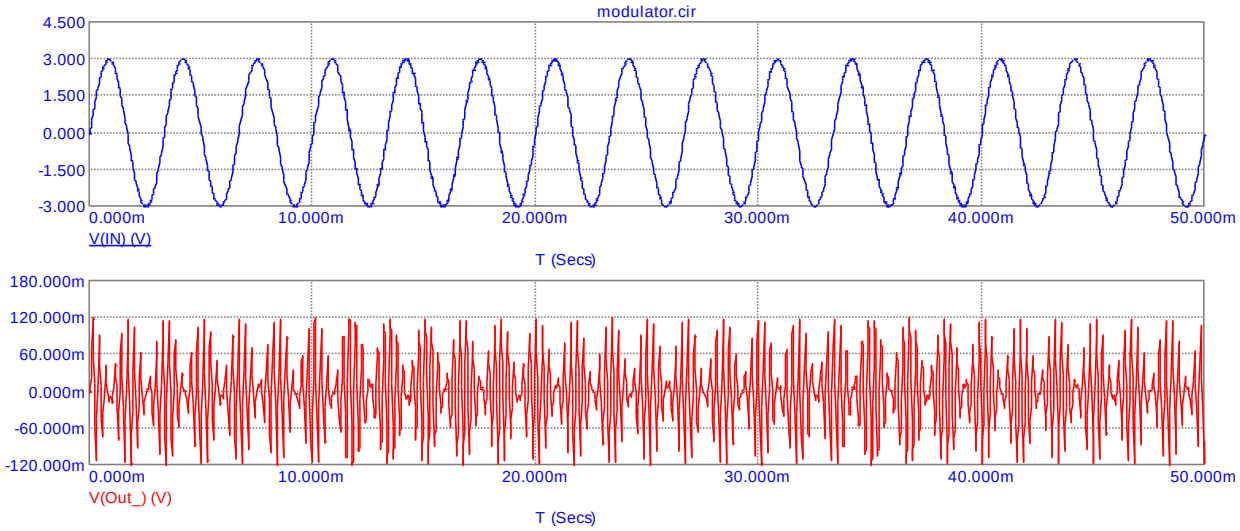
Результати моделювання скремблера



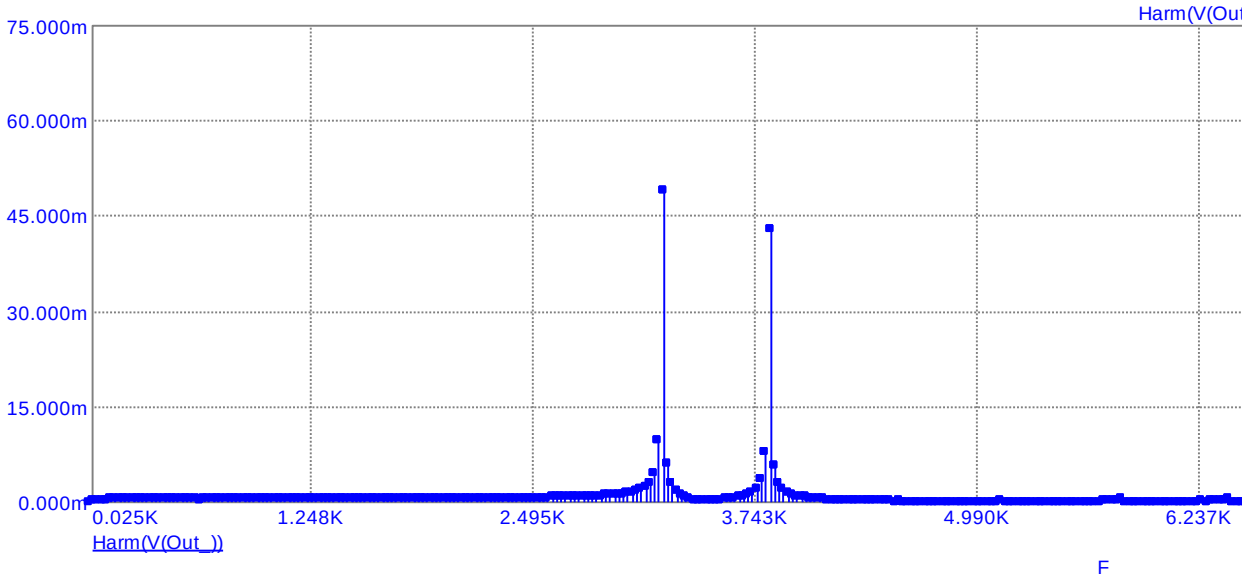
Моделювальна схема генератора скремблера



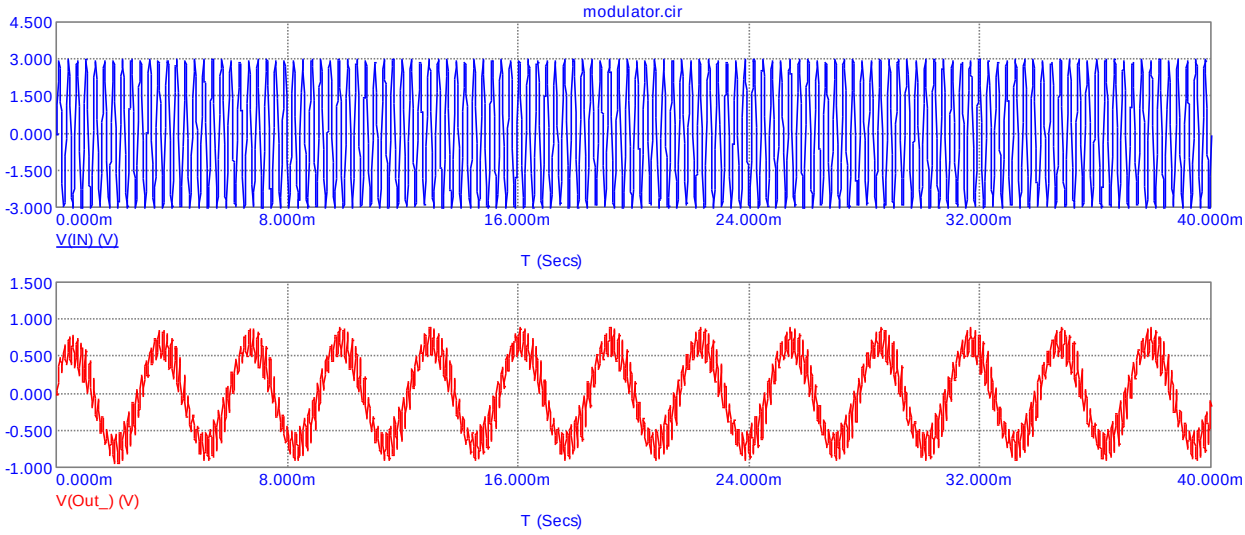
Моделювальна схема ключового балансного модулятора та НЧ-фільтра скремблера



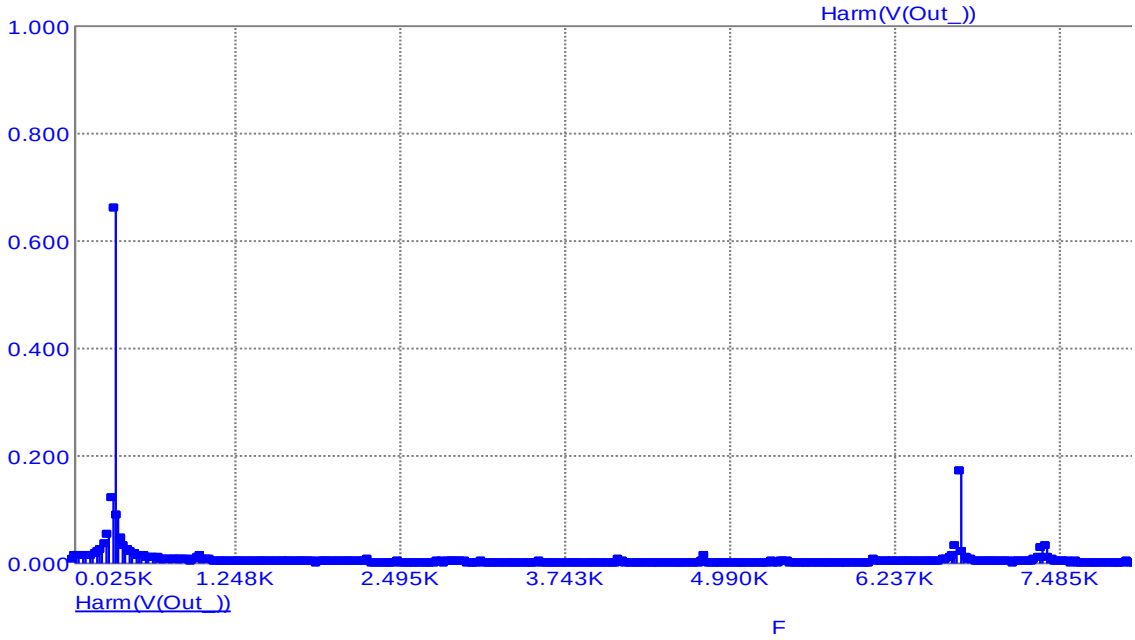
Часові діаграми сигналу на вході та виході балансного модулятора скремблера



Спектр вихідного сигналу скремблера при подачі на вхід сигналу частотою 300 Гц



Часові діаграми сигналу на вході та виході скремблера



Спектр вихідного сигналу скремблера при подачі на вхід сигналу частотою 3200 Гц