Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу»

Виконав: студент 2-го курсу,
групи ТКС-20м
спеціальності 172 – Телекомунікації та радіотехніка _____.
_____ Мирончак В.М.

Керівник: к.т.н., доцент каф. ТКСТБ
_____ Стальченко О.В.
«____» _____ 2021 р.

Опонент: д.т.н., професор каф. РТ
_____ Семенов А.О.
«____» _____ 2021 р.

Допущено до захисту
Завідувач кафедри ТКСТБ
_____ д.т.н., проф. Кичак В.М.
«____» _____ 2021 р.

Вінниця ВНТУ - 2021 рік

Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення
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 ТКСТБ
д.т.н., професор В.М. Кичак
“___”_____2021 року

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

Мирончаку Вадиму Михайловичу .
(прізвище, ім’я, по батькові)

1. Тема роботи Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу

керівник роботи Стальченко Олександр Володимирович, канд. техн. наук,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “24” 09 2021 року № 277

2. Строк подання студентом роботи 01 грудня 2021 року

3. Вихідні дані до роботи: робоча частота – 1800 МГц; довжина хвилі – 0,167 м; довжина хвилі – 0,167 м; висота рефлектора – 0,13м; ширина стінки рефлектора – 0,25м; сектор сканування антени – 120°.

4. Зміст текстової частини: вступ; аналіз принципів побудови САРД; безпека і захищеність безпровідних систем передачі інформації; розрахунок антени і антенної гратки для базової станції; економічна частина; охорона праці та безпека в надзвичайних ситуаціях; висновок; література.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов’язкових креслень)
Типова структура і склад мереж абонентського доступу; Архітектура САРД; Методи доступу і розширення спектру; Залежності ВБП для видів модуляції САРД; Структурна схема відвідного каналу в режимі перехоплення; Система MIMO з двома передавальними і двома приймаючими антенами; Моделювання параметрів антени.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Стальченко О.В., доцент кафедри ТКСТБ		

7. Дата видачі завдання 01 вересня 2021 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	10.09.2021р.	
2.	Техніко-економічне обґрунтування розробки	17.09.2021р.	
3.	Аналіз принципів побудови САРД	01.10.2021р.	
4.	Аналіз безпеки і захищеності безпровідних систем передачі інформації	29.10.2021р.	
5.	Розрахунок антени і антенної гратки для базової станції	19.11.2021р.	
6.	Аналіз економічної ефективності розробки	30.11.2021р.	
7.	• Охорона праці та безпека життєдіяльності	06.12.2021р.	
8.	Оформлення пояснювальної записки та графічної частини	13.12.2021р.	
9.	Нормоконтроль МКР	14.12.2021р.	
10.	Попередній захист МКР, опонування МКР	17.12.2021р.	
11.	Захист МКР ЕК	20.12.2021р.	

Студент _____ Мирончак В.М.
(підпис)

Керівник роботи _____ Стальченко О.В.
(підпис)

АНОТАЦІЯ

УДК 621.396

Мирончак В.М. Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу. Магістерська кваліфікаційна робота зі спеціальності 172 – телекомунікації та радіотехніка, освітня програма - телекомунікаційні системи та мережі. Вінниця: ВНТУ, 2021. 129 с.

На укр. мові. Бібліогр.: 36 назв; рис.: 32; табл. 27.

Магістерська кваліфікаційна робота присвячена актуальним питанням систем абонентського радіодоступу, побудованих на основі різних стандартів, у тому числі LTE, IEEE802.11xx. Предмет дослідження - інформаційна безпека з урахуванням особливостей систем радіозв'язку, забезпечення захисту і високої швидкості передачі даних, а також поодинока куткова антена і антенні грати на її основі.

Графічна частина складається з 6 плакатів із результатами моделювання.

У розділі охорони праці опрацьовано такі питання, як причини виникнення, дія на організм людини та нормування шкідливих та небезпечних виробничих факторів у виробничому приміщенні; карта умов праці (обґрунтування вибору нормованих значень шкідливих та небезпечних виробничих факторів, оцінка факторів виробничого і трудового процесів, гігієнічна оцінка умов праці, оцінка технічного і організаційного рівня, атестація робочого місця); рекомендації щодо поліпшення умов праці, а також розглянуто норми пожежної безпеки.

Ключові слова: система абонентського радіодоступу, інформаційна безпека, антенні гратки, MIMO.

SUMMARY

UDC 621.396

Mironchak VM Improving the information security of the local subscriber radio access network. Master's thesis in specialty 172 - telecommunications and radio engineering, educational program - telecommunications systems and networks. Vinnytsia: VNTU, 2021. 129 p.

In Ukrainian language. Bibliogr .: 36 titles; fig .: 32; table 27.

The master's qualification work is devoted to topical issues of subscriber radio access systems, built on the basis of various standards, including LTE, IEEE802.11xx. The subject of the research is information security taking into account the peculiarities of radio communication systems, protection and high speed data transmission, as well as a single corner antenna and antenna lattice based on it.

The graphic part consists of 6 posters with simulation results.

The section of labor protection deals with such issues as the causes, effects on the human body and the rationing of harmful and dangerous production factors in the production premises; map of working conditions (substantiation of the choice of normalized values of harmful and dangerous production factors, assessment of factors of production and labor processes, hygienic assessment of working conditions, assessment of technical and organizational level, certification of the workplace); recommendations for improving working conditions, as well as fire safety standards.

Key words: subscriber radio access system, information security, antenna gratings, MIMO.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ

BER - bit error rate

DSSS - direct sequence spread spectrum

FDD - Frequency Division Duplex

FHSS - frequency hopping spectrum spreading

IEEE - Institute of Electrical and Electronics Engineers

ISM - industrial, scientific and medical

LTE - Long Term Evolution

MIMO - Multiple Input Multiple Output

MIMO - multiple input multiple output

OFDMA - Orthogonal Frequency Division Multiplexing Access

SNR - signal - to - noise ratio

TDD - Time Division Duplex

TDMA - time division multiple access

UMTS - Universal Mobile Telecommunications System

WEP - wired equivalent privacy

WPA - Wi - Fi protected access

АГ - антенні грати

АС - абонентська станція

АТ - абонентський термінал

БС - базова станція

ВБП - вірогідність бітової помилки

ДПФ - дискретне перетворення Фур' є

ЕМС - електромагнітна сумістність

МС - мобільна станція

САРД - система абонентського радіодоступу

ВСТУП

Мережеві технології є однією з найбурхливіше прогресуючих галузей науки і техніки. Швидкий ріст кількості мереж передачі даних різного типу супроводжується використанням в них досконаліших методів передачі (протоколів, методів кодування і так далі), зміною архітектури мереж і, зрештою, вищим рівнем обслуговування абонентів. Особливо великі можливості відкриваються у разі застосування безпровідних мереж, які активно розвиваються. На їх стороні економічність і простота установки.

Актуальність роботи. Сучасне людство будує глобальне інформаційне співтовариство, матеріальним носієм якого є інформаційно-комунікаційні технології і системи, включаючи безпровідні системи зв'язки, що дозволяють значно збільшити об'єм передаваної інформації. У зв'язку з цим, питання безпеки каналів зв'язку в цих системах є актуальними і виходять на перший план при подальшому розвитку безпровідних технологій. Для безпровідних цифрових систем передачі інформації, основними проблемами безпеки є: порушення цілісності і конфіденційності передаваної інформації, моніторинг і перехоплення трафіку, атаки типу «відмова в обслуговуванні», підключення до мережі неавторизованих клієнтів. Важко обмежити фізичний доступ зловмисників до системи через те, що неможливо ефективно екранувати усі приміщення, в яких встановлені точки доступу, тому частково мережі діють і зовні. Усе це - негативні сторони безпечного використання безпровідних технологій. Вони ставлять під загрозу безпеку безпровідних мереж.

Безпровідні мережі володіють, в порівнянні з традиційними дротяними мережами, чималими перевагами, головним з яких, звичайно ж, являється простота розгортання і гнучкість архітектури мережі.

Останніми роками різко зросла кількість систем, що використовують безпровідний зв'язок всередині приміщень. При цьому виникає ряд проблем, пов'язаних з багатопроменевим поширенням сигналів усередині приміщень.

При обмеженнях ширини спектру і рівня випромінюваної потужності традиційні побудови безпровідних систем мають обмеження. Можливим проривом є заміна одиничних антен в приймальних (передавальних) вузлах на багатоелементні антенні грати і використання багатопроменевого підходу. Це так звані MIMO системи (Multiple Input Multiple Output, багато входів - багато виходів).

Використання технології MIMO є одним з найбільш важливих шляхів розвитку широкосмугових безпровідних систем. При цьому висока пропускна здатність, яку повинні забезпечувати ці системи, залежить від ефективності використання каналів зв'язку. Найбільшою завадою при цьому є множинні канали із завмираннями, особливо у разі відсутності прямої видимості.

Середовищем передачі для систем передачі інформації є в основному радіолінії за відсутності прямої видимості, де електромагнітні хвилі приходять в точку прийому в результаті багатопроменевого поширення, що викликає флуктуації амплітуди, фази, часової затримки, кута прибуття сигналу, що приймається, і як наслідок - його завмирання. Сигнал, що приймається, є сумою окремих каналів, що отримуються в результаті великого числа віддзеркалень від досить великого числа відбивачів і розсіювачів, розташованих випадковим чином навколо мобільного терміналу. Нестаціонарна поведінка просторових багатопроменевих каналів внаслідок завмирань є головною проблемою безпровідних телекомунікацій для забезпечення необхідних високих характеристик, таких як пропускна здатність і вірогідність бітової помилки.

Мета роботи - забезпечення захищеності інформації в мережах локального рівня на основі систем абонентського радіодоступу (САРД) сімейства стандартів IEEE 802.11xx та LTE, виконання конструктивних розрахунків кутової антени та решітки для базової станції, розрахунок її основних параметрів. Для досягнення цієї мети в роботі вирішуються такі завдання:

1) аналізу сучасного стану безпровідних систем;

2) класифікації САРД;

3) порівняльного аналізу різних САРД;

4) безпеці і захищеності безпровідних систем передачі інформації;

5) аналізу завадостійкої різних видів модуляції, використовуваних в САРД;

6) проектування антени і лінійних антенних грат на її основі.

Об'єктом дослідження є система абонентського радіодоступу, побудована на основі різних стандартів, у тому числі стандарту IEEE 802.11n с технологією MIMO.

Предметом дослідження є захищені системи абонентського радіодоступу, побудовані на основі теорії скритності і завадозахищеності систем передачі інформації і теорії електродинаміки антен. Кількісні оцінки параметрів САРД проводилися за допомогою розрахунків і моделювання в середовищі Mathcad.

Метод дослідження - обчислювально-аналітичний за допомогою комп'ютера (система символічної математики MathCAD).

Основні результати. У магістерській роботі досліджені актуальні питання побудови сучасних САРД, проведене огляд особливостей таких систем, виконано порівняльний аналіз систем радіодоступу. Представлена розробка моделі загроз для мережі на основі обладнання сімейства стандартів IEEE 802.11xx. Розглянуто питання безпеки та захищеності САРД, критерії оцінки скритності та завадозахищенності систем, побудованих на основі цих стандартів. Виконано конструктивний розрахунок кутової антени та антенної решітки, розрахунок їх параметрів.

Новизна. Виконано аналіз особливостей сучасних САРД, розглянуто актуальні питання безпеки та захищеності безпроводових систем передачі інформації, проведене розрахунки та отримано нові результати щодо антени та антенної решітки для базових станцій таких систем.

Апробація результатів - сучасні системи абонентського радіодоступу та їх захищеність. З причини практичної цінності отриманих результатів вони впроваджені у використання в навчальному процесі.

1. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ САРД

1.1. Користувацький (абонентський) для користувача доступ

Одна з проблемних і динамічно розвинених частин сучасних мереж зв'язку є доступ користувачів і абонентів до вузлів зв'язку транспортних мереж для надання телекомунікаційних послуг. Для цього широко використовується технологія радіодоступу RLL (Radio Local Loop) для фіксованого і мобільного, вузькосмугового і широкосмугового доступу з розподілом радіочастотних ресурсів по спектру частот, за часом, кодовим розподілом, пакетною передачею (приклад останнього - технологія WiMAX.

У зв'язку з якісними змінами, що відбуваються в розвитку сучасних телекомунікаційних мереж (ТКС), і зокрема із створенням мультисервісних мереж, здійснюється впровадження сучасних технологій і на абонентських мережах доступу. У міжнародних стандартах і рекомендаціях прийнятий термін "Access Network" - "мережа доступу". У вітчизняних концепціях ТКС частіше використовується словосполучення "мережа абонентського доступу" (МАД), що дає чіткіше уявлення про відповідний фрагмент телекомунікаційної системи. На рис.1.1 даний фрагмент телекомунікаційної мережі з виділеними типовими елементами МАД [1-4].

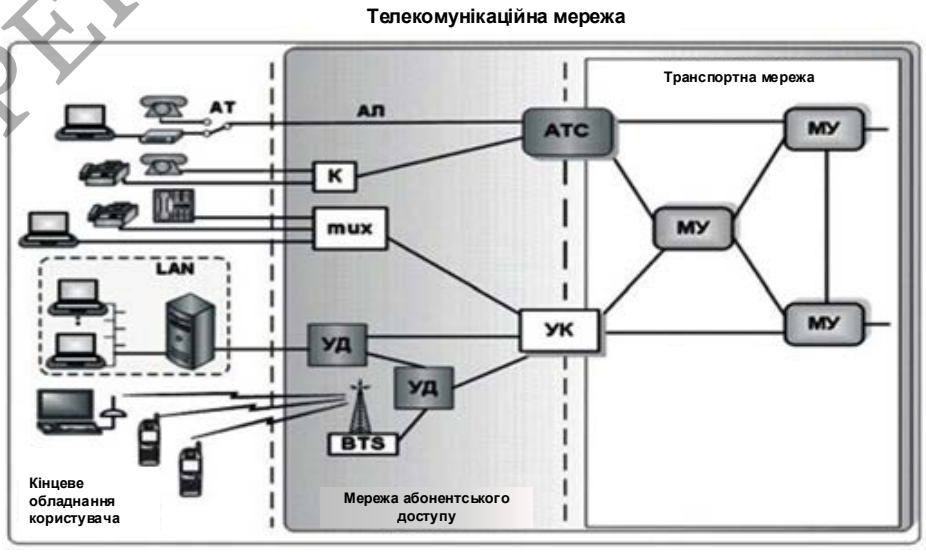


Рисунок 1.1 - Типова структура і склад мереж абонентського доступу

Абонентська мережа в простому випадку складається з наступних елементів:

– абонентського (призначеного для користувача) терміналу (АТ);

– абонентської (призначеної для користувача) лінії (АЛ);

– вузла комутації (ВК).

У загальному випадку під мережами абонентського доступу розуміється сукупність ліній, кінцевих і проміжних вузлів, що включаються в комутаційне устаткування транспортної мережі безпосередньо або через виносний модуль (концентратор, мультиплексор)[1-4].

Структурно МАД розташовується між устаткуванням, що поміщається безпосередньо в місці розташування абонентів (користувачів), і транспортною мережею. Межею між МАД і термінальним устаткуванням може бути розподільна коробка або розетка, до якої підключається АТ. Межа між МАД і транспортною мережею проходить в місці установки ВК, в абонентські комплекти якого входять АЛ [1-4].

На рис. 1.2 представлена модель МАД, заснована на нових підходах до її побудови. Відповідно до цієї моделі, МАД складається з двох вузлових елементів. Перший є сукупністю підмереж АЛ, що утворюють мережу АЛ, а другий - безпосередньо підмережа доступу (іменована ще базовою мережею, розподільною мережею або мережею перенесення). Кожна підмережа АЛ забезпечує підключення абонентів (користувачів) до вузла доступу (ВД) або ВК безпосередньо або через мультиплексор [1-4].

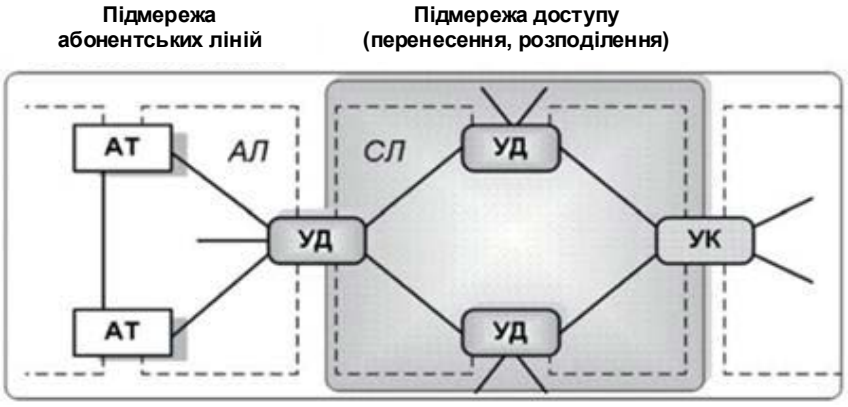


Рисунок 1.2 - Модель мережі абонентського доступу

Коли прокладення кабельних ліній зв'язку недоцільне, а також для мобільного розгортання мережі доступу, ефективним може виявитися безпровідне підключення абонентів (Wireless Local Loop). Останнім часом значно зріс інтерес до технологій безпровідного абонентського доступу WLL-технологій (Wireless Local Loop). Поширеніші технології радіодоступу (на відміну від технологій оптичного безпровідного доступу) скорочено називають RLL (Radio Local Loop)[1-4].

Технології безпровідного абонентського доступу мають безперечну перевагу перед дротяними рішеннями [20]:

- застосування в місцях відсутності кабельної інфраструктури, а також у важкодоступних і малонаселених районах;

- швидке розгортання і введення в експлуатацію

- організація доступу у будь-якому місці (в межах зон покриття)

- підтримка зв'язку при русі абонентів.

Головні недоліки WLL - обмежена пропускна здатність і відносно висока вартість з розрахунку на одного абонента, а також традиційні для радіозв'язку проблеми «відкритості» до зовнішніх дій.

Типова архітектура системи абонентського радіодоступу (САРД) представлена на рис.1.3. Вона включає в себе наступні основні компоненти: контролер базових станцій, базові станції (БС), абонентські термінали і термінал технічного обслуговування і експлуатації - комп'ютер зі спеціальним керуючим застосуванням. БС пов'язані з контролером дротяними або безпровідними мікрохвильовими лініями зв'язку. Розглянемо функції кожного компонента САРД.

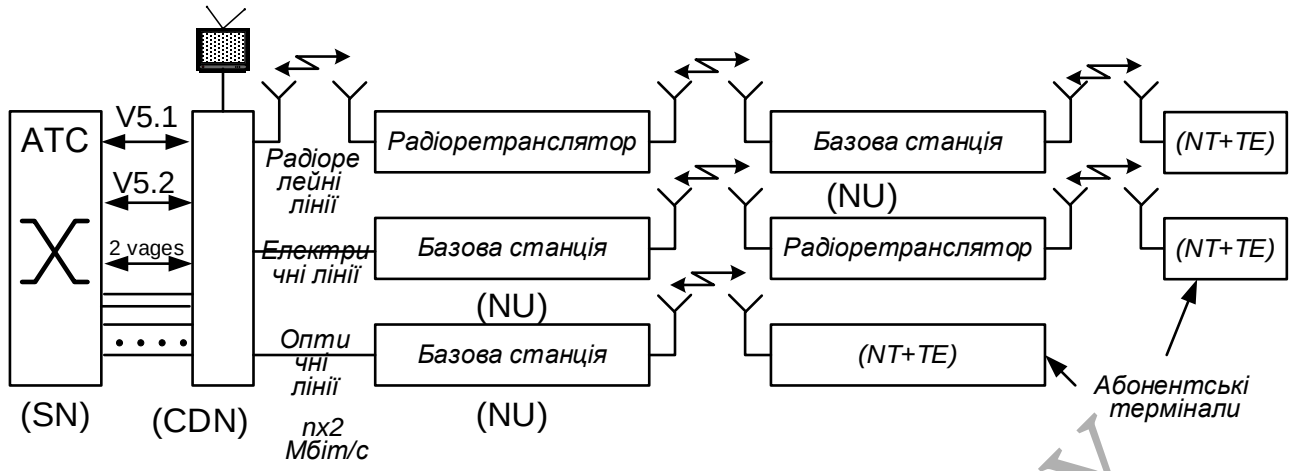


Рисунок 1.3 - Архітектура САРД

Сучасні технічні розробки дозволяють вирішувати широкий спектр питань, пов'язаних із створенням мереж абонентського радіодоступу, забезпеченням високоякісними послугами зв'язку абонентів різних категорій.

При виборі САРД зазвичай виходять з декількох типових завдань, які вирішуються за допомогою таких систем :

– надання послуг зв'язку або доступу в Інтернет;

– побудова територіально-розподілених корпоративних безпровідних мереж;

– організація магістральних каналів для передачі даних і телефонії.

На споживчому рівні сучасні системи абонентського радіодоступу повинні характеризуватися наступними особливостями:

– надання послуг з якістю, порівнянною з дротяним підключенням, включаючи можливість використання модему і факсу;

– можливість надання послуг в районах, що не мають лінійно-кабельної мережі, а також в регіонах, де виконання земляних робіт ускладнене і економічно не виправдане;

– можливість швидкого розгортання і нарощування системи;

– можливість підключення абонента по цифровому інтерфейсу;

– можливість централізованого управління системою.

1.2. Класифікація САРД

Системи САРД класифікують за різними ознаками.

По методу обробки сигналу - аналогові і цифрові WLL системи.

По топології мережі WLL системи розділяють на:

− системи, створені по топології "точка - точка"; зазвичай використовуються для прямого підключення великих (комерційних) абонентів до комутованої мережі і призначені для розподілу N-потоків 2 Мбіт/с і зазвичай застосовуються в міських або приміських районах;

− системи, створені по топології "точка - багато точок"; призначені для забезпечення телефонним зв'язком великих малонаселених територій (приміські райони і сільська місцевість); мають малу системну ємність і конфігуровані для забезпечення великого числа багатолінійних відгалужень, переважно для індивідуальних абонентських будівель.

Відповідно до займаної ширини смуги частот розрізняють вузькосмугові і широкосмугові системи WLL.

По використовуваних технологіях і стандартах WLL системи можна розділити на три категорії:

− системи, реалізовані відповідно до стандартів мікростільникових систем безпровідної телефонії(DECT, CT2, PHS та ін.);

− системи, реалізовані на базі стандартів стільникових систем;

− спеціалізовані системи, використовуючі свої стандарти.

По робочому частотному діапазону. Діапазони радіочастот для безпровідного доступу визначені таким чином.

Діапазон 300 МГц. Для радіодоступу визначені частоти: 307,5 - 308 і 343,5 - 344 МГц. Діапазон 1427 - 1525 МГц. Цей діапазон в основному призначений для зв'язку «Земля - Космос», проте в ньому виділені ділянки спектру для радіодоступу (Multi Gain Wireless, IRT 2000 - Франція, A 9800 Alcatel).

Діапазон 1880-1900 МГц. Визначений для розгортання систем абонентського доступу технології DECT (Digital Enhanced Cordless Telecommunication).

Діапазон 2,1 - 2,7 ГГц. Відведений для радіолокації, космічних досліджень і має категорію урядового призначення. Проте нині ділянка спектру частот 2,1 - 2,3 ГГц використовується для радіо доступу (Alcatel A 9800). Діапазон 2,3065 - 2,4815 ГГц відведений для систем радіодоступу.

Діапазон 3,4 - 3,8 ГГц. може бути використаний за індивідуальним погодженням.

Діапазон 10 - 10,7 ГГц. Має ділянки, які в перспективі визначені для високошвидкісного радіодоступу (10,15 - 10,3 і 10,5 - 10,65 ГГц).

Діапазон 24,5 - 25,25 ГГц. Має ділянки спектру (24,549 - 25,053 і 25,557 - 26,061 ГГц) рекомендовані до розгортання мереж доступу з високою швидкістю передачі даних. Ділянка спектру радіочастот 27,5 - 29,5 ГГц виділений цільовим чином для стільникового телебачення.

Діапазон 40,5 - 42,5 ГГц вільний. Для його використання рекомендовано розгорнути системи телемовлення (стільникове телебачення високої чіткості).

Є багато різних САРД, які принципово відрізняються один від одного архітектурою, технічними параметрами і типами вирішуваних завдань. Загальноприйнятої класифікації систем АРД не існує. Проте, деяка систематизація за основними характеристиками можлива (таблиця.1.1).

Таблиця 1.1 - Класифікація САРД

	Ознака	Параметри, типи, характеристики
1	Спосіб передання сигналу	Аналоговий, цифровий
2	Призначений для користувача тип	Фіксований доступ, мобільні системи
3	Спосіб реалізації	Гібридний (частково дротяний), безпровідний
4	Технологія	Стільникові, транкінгові і безшнурові технології, на базі РР систем, "точка - багато точок"
5	Архітектура	Мікростільникові, зонові, точка - багато точок, стільникові
6	Метод множинного доступу	Множинний доступ з частотним (FDMA), часовим (TDMA) і кодовим (CDMA) розподілом
7	Топологія	Радіальні, типу "дерево"
8	Послуги, що надаються	Передача телефонії, даних, ТБ-мовлення, мультисервісні

1.3. Переваги САРД

Застосування САРД для обслуговування стаціонарних абонентів, не підключених до телефонної мережі загального користування (PSTN), дозволяє операторам розширити їх потенційні можливості і поліпшити якість послуг мереж доступу і способів їх надання. До безперечних переваг цих систем відносяться:

– короткі терміни розгортання - установка і введення в експлуатацію здійснюються за декілька днів;

– рентабельність - вартість каналу зв'язку з розрахунку на одного абонента значно нижче за вартість каналу дротяних систем;

– малий об'єм інвестицій на початковому етапі будівництва мережі, що зводить до мінімуму фінансовий ризик оператора і дозволяє проводити поетапне інвестування відповідно до потреб і отриманих прибутків;

– можливість повторної установки і переустановлення, які обумовлені гнучкою модульною конфігурацією системи. Якщо реальні потреби міняються або стають нижче за прогнозованих, систему можна демонтувати і встановити у іншому місці, уникнувши при цьому грошових втрат (терміни окупності систем WLL коротші по порівнянню с дротяними системами);

– ефективне використання комутаційних і інших ресурсів мережі завдяки застосуванню багатократного доступу, що концентрує навантаження на стику радіопортів і абонентських терміналів;

– зниження експлуатаційних витрат, обумовлене високою надійністю і відмовостійкістю системи.

Сучасні системи абонентського радіодоступу забезпечують реалізацію різних пакетів послуг : від послуг традиційної телефонії до повного набору послуг мультисервісних мереж зв'язку по одній лінії зв'язку

1.4. Принципи побудови мережі і особливості устаткування

САРД призначені для організації безпровідних мереж з архітектурою «точка-многоточка» і забезпечення інтегрованого сервісу: телефонії і високошвидкісного доступу в Інтернет. У загальному випадку архітектура систем фіксованого радіодоступу відповідає організації стільникових мереж з територіально-розподіленим покриттям. Елементом, що утворює, стільники являється базова станція (БС) з круговою діаграмою покриття. Кругова діаграма може бути розбита по азимуту на сектори. Як правило, кожен сектор обслуговується пристроєм БС і спрямованою антеною з секторною діаграмою. Таким чином, подібні системи мають таку важливу якість, як легка розширюваність і масштабованість.

При виборі системи абонентського радіодоступу зазвичай виходять з декількох типових завдань, які вирішуються за допомогою таких систем:

– надання послуг зв'язку або доступу в Інтернет;

– побудова територіально-розподілених корпоративних безпровідних мереж;

– організація магістральних каналів для передачі даних і телефонії.

Оскільки в основу більшості систем покладені загальні принципи модуляції і передачі радіосигналів, для класифікації таких систем доцільніше використовувати характеристики мережевого устаткування і послуг що надаються користувачам, чим технології радіодоступу.

З'єднання між БС різних сотів виконуються за допомогою технологій дротяного (найчастіше оптичні лінії зв'язку) або безпровідного доступу (радіорелейні або радіомодемні лінії зв'язку).

Система абонентського радіодоступу складається з базової станції, контроллера базових станцій і абонентських терміналів (рис.1.4).

Базові станції пов'язані з контроллером дротяними або безпровідними мікрохвильовими лініями зв'язку з пропускною здатністю nx2 Мбіт/с.

Контроллер базових станцій призначений для концентрації трафіку WLL,

обробки викликів і забезпечення зв'язку з АТС, здійснюваною по цифрових каналах з високою пропускною здатністю (інтерфейси V5.1, V5.2). Крім того, він підтримує функції управління системою.

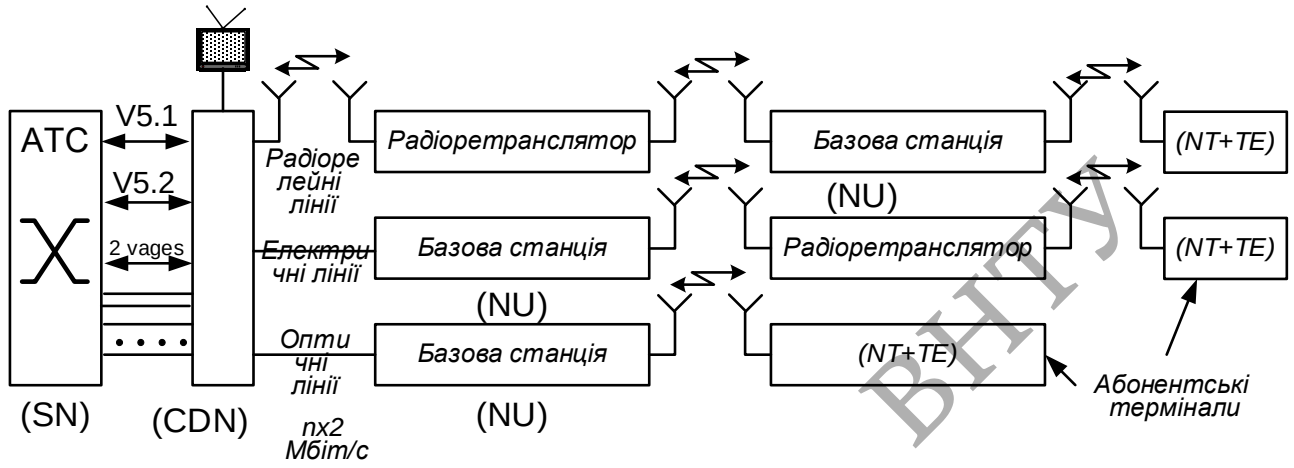


Рисунок 1.4 - Архітектура системи абонентського радіодоступу

Базові станції здійснюють радіозв'язок із стаціонарними або мобільними абонентами в межах своїх зон обслуговування, величина яких залежить від використовуваної в системі радіотехнології (FDMA, TDMA, CDMA), і забезпечують передачу викликів контроллеру базової станції. Базова станція складається з тракту антенного фідера, приймально-передавальної апаратури, системи управління, інтерфейсів і підсистеми живлення

Абонентські термінали є портативними безпровідними телефонними трубками, що забезпечують обмежену рухливість зв'язку.

Термінал технічного обслуговування і експлуатації є комп'ютером із спеціальним керуючим застосуванням, для забезпечення конфігурації і моніторингу роботи компонентів системи WLL, здійснення контролю абонентських терміналів, проведення операцій діагностики і технічного обслуговування.

При використанні декількох БС, працюючих в пересічних зонах обслуговування, потрібно частотно-просторове планування системи.

Можливості просторового планування визначаються використовуваними

антенами. Можливі варіанти частотно-просторового планування системи представлені на рис.1.5, де f1 - f6 - значення носійних частот в кожному секторі.

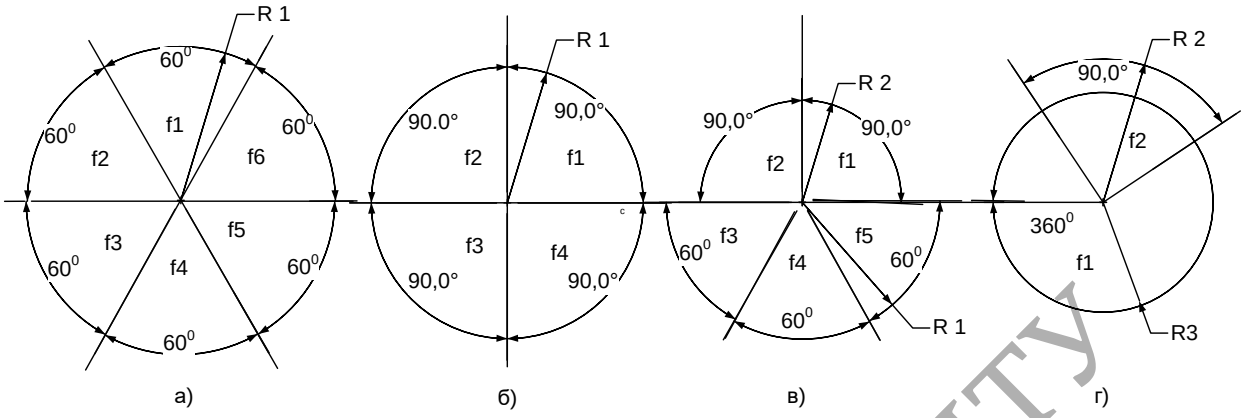


Рисунок 1.5 - Варіанти частотно-просторового планування

Значення носійних частот в сусідніх просторових секторах мають бути різними, оскільки на межах секторів відбувається перекриття зон діаграм спрямованості антен.

Так, наприклад, для випадку а) можна вибрати наступні співвідношення частот : $f1 = f3 = f5$, $f2 = f4 = f6$, $f1 \neq f2$.

Абонентські станції (АС) призначені для обслуговування окремих груп абонентів. Пристрої АС мають зовнішню спрямовану антену, яка може бути прикріплена до стіни будинку або встановлена на даху. Як правило, АС мають різні призначені для користувача інтерфейси.

На споживчому рівні сучасні системи абонентського радіодоступу повинні характеризуватися наступними перевагами:

– надання послуг з якістю, порівнянною з дротяним підключенням, включаючи можливість використання модему і факсу;

– можливість надання послуг в районах, що не мають лінійно-кабельної мережі, а також в регіонах, де виробництво земляних робіт ускладнене і економічно не виправдано;

– можливість швидкого розгортання і нарощування системи;

– можливість підключення абонента по цифровому інтерфейсу;

– можливість централізованого управління системою.

1.5. Порівняння радіоінтерфейсів САРД

Існує багато технологічних і експлуатаційних особливостей того або іншого стандарту WLL, але відмінності між ними полягають в ефективності експлуатації мереж, отримуваному прибутку, а також в мірі задоволеності споживачів від якості послуг зв'язку.

Особливе значення мають такі характеристики, як ємність системи і зона покриття мережі, оскільки саме вони в першу чергу визначають об'єми капітальних витрат і експлуатаційні витрати. Міра задоволеності користувача залежить від якості передачі мови і даних і процентного співвідношення успішних викликів.

Статистичні дослідження довели, що ємність мережі, що визначає кількість користувачів, здатних працювати в зоні дії однієї базової станції, найбільша для CDMA-мереж і найменша для FDMA-мереж.

Зразкове співвідношення таке: технологія CDMA дає можливість отримати ємність в 3-4 рази більше, ніж TDMA, яка, у свою чергу, в стільки ж разів перевершує по цьому показнику FDMA. До того ж, CDMA - єдина технологія, що не вимагає частотного планування.

Досягнення максимально можливої ємності мережі тісно пов'язане з таким чинником, як максимальна величина зони покриття. І по цьому показнику CDMA в 3-4 рази перевершує свого найближчого конкурента - TDMA. Менше число осередків мережі означає швидше розгортання мережі, менші початкові капіталовкладення і наступні експлуатаційні витрати.

Ємність мережі і зона покриття є важливими критеріями для оператора. Проте абонентів мережі в першу чергу хвилює якість зв'язку і її стійкість. Перевага CDMA в тому, що це цифровий зв'язок, що використовує широкосмугову модуляцію сигналу. Крім того, вона майже повністю забезпечує надійний зв'язок, практично без вузькосмугових завад, і не допускає несанкціонований доступ до інформації.

1.6. Аналіз технологій організації множинного доступу до мережі

У системах радіодоступу широко використовуються самі різні технології організації множинного доступу, зокрема [4]:

− FDMA (Frequency Division Multiple Access) - множинний доступ з частотним розподілом, при цьому виділений для певної системи спектр ділиться на смуги частот, в яких здійснюється передача канальної інформації від різних абонентів;

− TDMA (Time Division Multiple Access) - множинний доступ з тимчасовим розподілом, при цьому виділена смуга частот надається для передачі канальної інформації на певний короткий проміжок часу, в наступний проміжок часу здійснюється передача інформації від іншого абонента на цій же частоті;

− CDMA (Code Division Multiple Access) - множинний доступ з кодовим розподілом, повідомлення від абонентів шифруються і передаються одночасно, цей спосіб має певні достоїнства (наприклад, скритність інформації), але при цьому для передачі потрібно досить широку смугу частот, що може бути недоліком при обмеженості частотного ресурсу, зате в цій смузі можна надати зв'язок набагато більшому числу абонентів і легше будувати мережі.

Системи, що використовують технологію CDMA, мають ряд переваг:

– висока завадостійка до вузькосмугових завад;

– ефективна робота приймальних пристроїв в умовах багатопроменевого поширення сигналу;

– процедура м'якого перемикання каналів під час переходу абонента з одного стільника в інший;

– ефективне використання частотного ресурсу;

– архітектура дозволяє гнучко і ефективно управляти радіоресурсами;

– досить висока конфіденційність і захищеність від несанкціонованого доступу.

Декілька недоліків:

– складність устаткування;

– вузький круг виробників апаратури;

– при зростанні числа активних абонентів виникають взаємні завади, погіршуючі умови прийому;

– необхідність виділення операторам широких ділянок спектру.

У багатьох сучасних системах WLL системах мають місце комбіновані методи доступу, що є поєднанням CDMA з різними методами розширення спектру сигналу або з іншими методами множинного доступу до мережі (рис.1.6).

Найбільш широке поширення отримали CDMA-системb з розширенням спектру, яке полягає в розподілі інформаційних сигналів по широкій смузі частот.

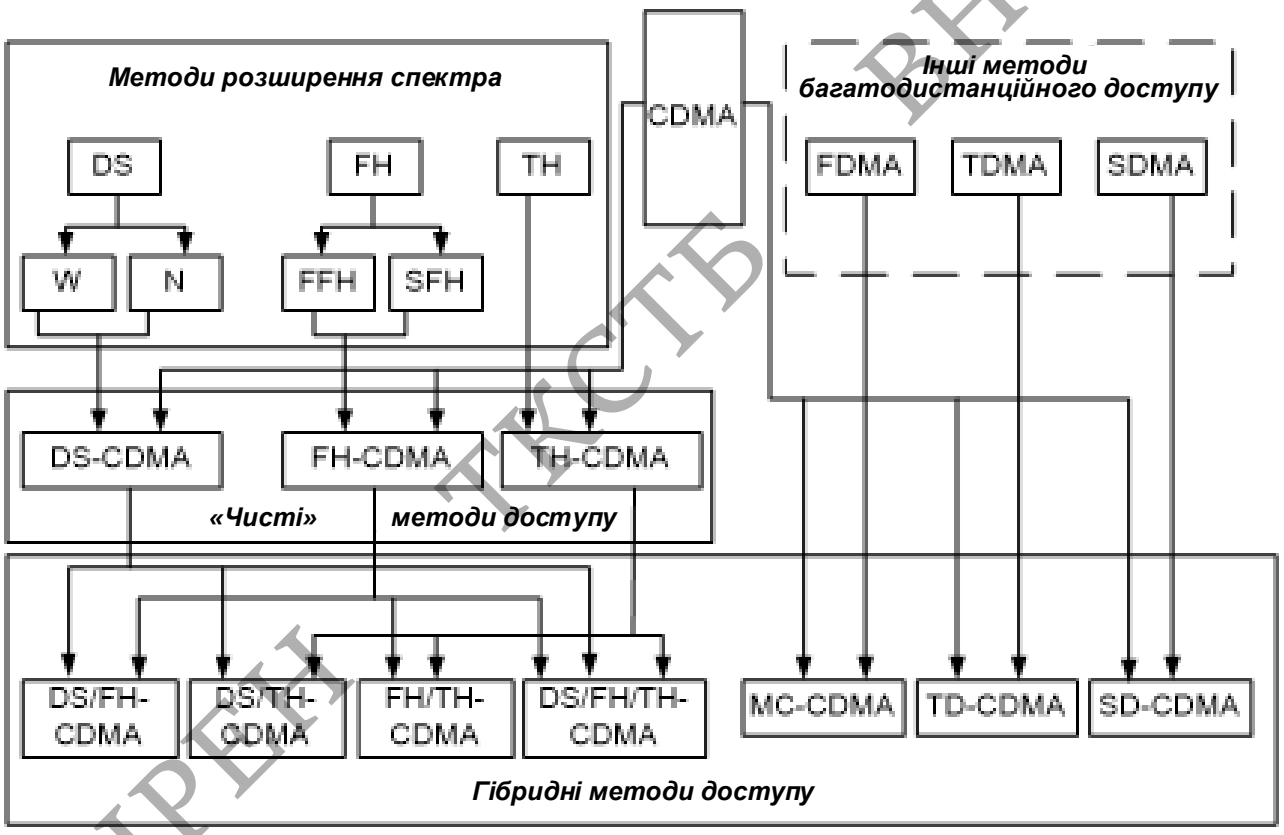


Рисунок 1.6 - Методи доступу і розширення спектру

1.7. Порівняльний аналіз САРД

Наразі відомі три ключові методи розширення спектру: DS (Direct Sequence) - пряма послідовність, FH (Frequenc Hopping) - стрибкоподібна перебудова частоти і TH (Time Hopping) - псевдовипадкова перебудова в часі в часі. Відповідно, існує три способи передання сигналу з розширенням спектру : DSSS, FHSS і THSS.

Системи абонентського радіодоступу DS-CDMA, будучи принципово однаковими з точки зору використовуваної в них технології шумоподобного сигналу, проте, мають ряд відмінностей з точки зору універсальності їх тактико-технічних характеристик (ТТХ), можливостей сервісу і застосування, а також гнучкості.

Одне з важливих понять, що визначають завадостійкість і ефективність системи CDMA - «база сигналу» (термін processing gain) - це показник, який характеризує виграш у відношенні «сигнал/шум» при обробці сигналів з розширеним спектром. Для систем DS-CDMA, в яких передача інформації здійснюється з використанням псевдовипадкових кодових послідовностей з чіповою швидкістю Rc, база сигналу обчислюється у вигляді B = Rc/R, де R - швидкість передачі інформації. Частіше величина бази сигналу (B) обчислюється як добуток ширини спектру (F) на тривалість елементарного символу T. Для широкосмугових сигналів база значно перевищує 1 (B >> 1). Очевидно, що чим ширша смуга частот в ефірі і нижче швидкість вхідного сигналу, тим більша база сигналу і вище завадостійкість. Схема роботи методу DS-CDMA і якісні зміни сигналу і завад на передавачі і приймачі показані відповідно на рис.1.7 і 1.8.

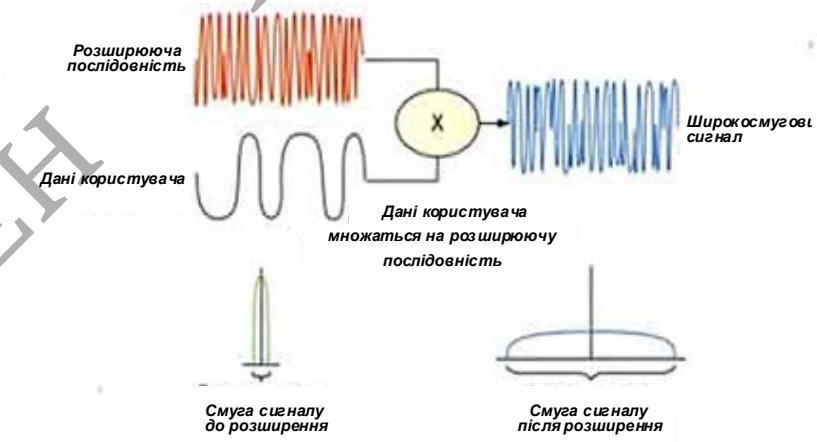


Рисунок 1.7 - Спрощена блок-схема CDMA -передавача

У системі CDMA для кожної станції виділяється своя унікальна псевдовипадкова кодова послідовність, що відрізняє її від інших і використовувана для підвищення завадостійкості і забезпечення безпеки. У передавачі вузькосмуговий інформаційний сигнал множиться на цю N-символьну

послідовність. База сигналу дорівнює числу символів псевдовипадкової послідовності (B = N).

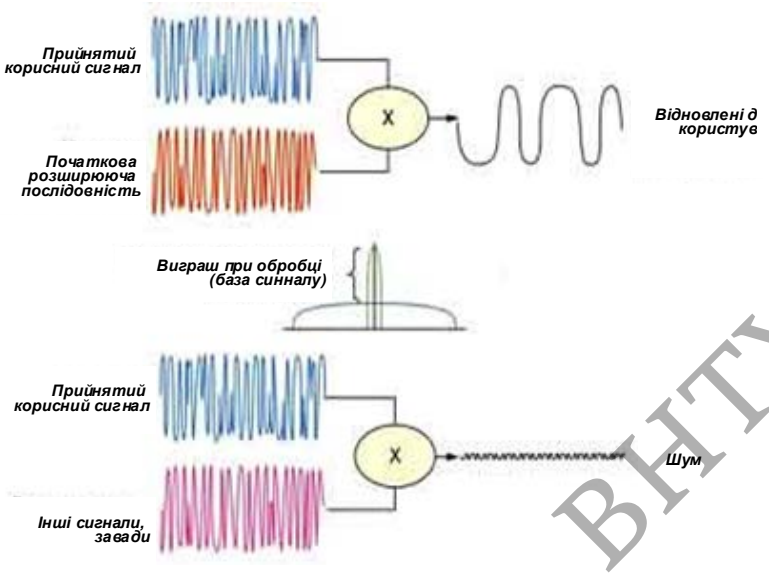


Рисунок 1.8 - Спрощена блок-схема CDMA-приймача

У приймачі початковий сигнал відновлюється за допомогою такої ж псевдовипадкової послідовності (зворотна операція). Будь-які інші сигнали, відмінні від початкового, поступають на цей приймач, сприймаються як шум. Окремо слід зазначити, що безпровідні системи зв'язки, побудовані за технологією CDMA, здатні ефективно працювати в умовах багатопроменевого поширення радіохвиль [3].

Для боротьби з впливом багатопроменевості в системах CDMA застосовується пристрій для прийому рознесених сигналів - так званий Rake-приймач. Принцип дії Rake-приймача заснований на роздільній обробці усіх багатопроменевих компонентів і обчисленні їх середньозваженої суми. У наземних радіоканалах характеристики цих компонентів можуть трохи розрізнятися (на величину, порівнянну з тривалістю одного символу шумоподібного сигналу-чіпа).

1.8. Принципи побудови мереж LTE

Мережі LTE є подальшим розвитком мереж 2-го і 3-го поколінь. При розробці архітектури мереж LTE взяті до уваги наступні загальні принципи [2]:

– логічно розділені транспортні мережі передачі призначених для користувача даних і службової інформації;

– мережа радіодоступу і базова пакетна мережа повністю звільнені від транспортних функцій. Схеми адресації, використовувані в цих мережах, не мають бути пов'язані з схемами адресації, використовуваними при реалізації транспортних функцій;

– управління мобільністю абонентів і призначених для користувача терміналів повністю покладено на мережу радіодоступу;

– функціональний розподіл інтерфейсів мережі радіодоступу повинен мати декілька можливих опцій;

– інтерфейси повинні базуватися на логічній моделі блоку, керованого цим інтерфейсом;

– один фізичний елемент мережі може при реалізації містити в собі декілька логічних блоків.

У LTE мережах відмовилися від технології радіоінтерфейсу W-CDMA (Wideband Code Division Multiple Access - широкосмуговий множинний доступ з кодовим розподілом) і перейшли до прогресивнішої технології OFDMA (Orthogonal Frequency - Division Multiple Access) - широкосмуговий доступ з ортогональним частотним розподілом каналів. Основні вимоги до системи:

– значне підвищення спектральної ефективності (доведення її до 5 біт/с/Гц);

– збільшення пропускної здатності в лінії «вниз» до 100 Мбіт/с при ширині смуги одного частотного каналу 20 МГц (з можливістю його масштабирования:1, 4; 3; 5; 10; 15 МГц) і до 50 Мбіт/с в лінії «вгору»;

– скорочення часу затримки пакетів даних до 10 мс в порівнянні із затримкою в 80 мс при технології HSDPA (High - Speed Downlink Packet Access)

високошвидкісна пакетна передача даних від базової станції до мобільного телефону) і спрощення архітектури мережі.

Нове покоління безпровідних локальних мереж загального призначення відповідає стандарту 802.11ac. У його основу покладені ідеї, які уперше застосували при створенні його попередника, - широко поширеного сьогодні стандарту 802.11n, який підтримують практично усі доступні на масовому ринку мобільні і мережеві пристрої.

Нова версія стандарту безпровідного зв'язку 802.11 пропонує ще ефективніше використовувати радіодіапазон. Якщо попередня версія (802.11n) підтримувала до чотирьох паралельних каналів, яким відводився 40 МГц діапазон частот, то в 802.11ac число паралельних каналів збільшено до восьми, а мінімальне значення діапазону смуги пропускання складе 80 МГц. Оптимальне значення ж виявиться в два рази вище, тобто 160 МГц: тут спостерігається чотирикратний приріст).

Версія стандарту LTE-A (LTE - Advanced) запозичила безліч ідей і рішень з інших перспективних стандартів безпровідного зв'язку: зокрема, із стандарту 802.11ac вона переймає принципи паралелізування, на що вказує підтримка восьмиканального інтерфейсу MIMO, поліпшені методи кодування сигналу, а також автоматичне налаштування і управління частотами і діапазонами смуги пропускання [5].

LTE A - це черговий крок в еволюції мереж LTE. Це нова технологія, яка, допоможе впоратися з активним ростом трафіку безпровідних даних, а також допоможе підвищити середні швидкості у безпровідних стільникових мережах. Це означає також краще покриття, велику стабільність і швидкість мереж. Тобто мова не лише про те, що скачування даних стане швидше.

У таблиці.1.2 приведені дані росту швидкості безпровідної передачі даних для різних стандартів.

Таблиця 1.2 - Ріст швидкості безпровідної передачі даних для стандартів

	3G	WiMax	HSPA+	LTE	LTE-A
Пікова швидкість	3 Мбіт/с	128 Мбіт/с	168 Мбіт/с	300 Мбіт/с	1 Гбіт/с
Швидкість завантаження	0,5-1,5 Мбіт/с	2-6 Мбіт/с	1-10 Мбіт/с	10-100 Мбіт/с	100-300 Мбіт/с
Швидкість видачі	0,2-0,5 Мбіт/с	1-2 Мбіт/с	0,5-4,5 Мбіт/с	5-50 Мбіт/с	10-70 Мбіт/с

LTE - Advanced може працювати з різною шириною спектру, в т.ч. із смугою частот більше 20 МГц, за рахунок чого досягається вища продуктивність і цільова швидкість передачі даних.

LTE-A забезпечить для операторів можливість наростити ємність їх мереж, поліпшити якість призначеного для користувача досвіду, поліпшити можливості розподілу мережевих ресурсів. Для цього використовується цілий набір різних технологій, ряд яких не є новим, але раніше не використовувалися в єдиній системі зв'язку.

Основні принципові нововведення, які відрізняють LTE-A від LTE - це агрегація частот (CA - Carrier Aggregation), поліпшене використання багатоантенних технологій (MIMO), а також підтримка релейного режиму включення базових станцій (RN - Relay Nodes).

1.9. Аналіз стандарту IEEE 802.11a

Стандарт IEEE 802.11a орієнтований на виділений Федеральною комісією із зв'язку США 5 ГГц діапазон, який складається з двох частотних смуг загальною шириною 300 МГц, - це смуги 5,15-5,35 ГГц і 5.725-5.825 ГГц відповідно шириною

200 і 100 МГц. Механізм кодування даних заснований на частотному мультиплексуванні за допомогою ортогональних носійних (OFDM). Стандарт IEEE 802.11a визначає характеристики устаткування, вживаного в офісних або міських умовах, коли поширення сигналу відбувається по багатопроменевих каналах із-за безлічі віддзеркалень.

При переході від діапазону 2,4 ГГц до діапазону 5 ГГц зі збереженням рівня випромінюваної потужності і способу кодування сигналу, дальність дії системи зменшується. Для компенсації зменшення дальності в технології 802.11a передбачений підвищений рівень ефективної ізотропної випромінюваної потужності. Проте збільшення потужності недостатньо для забезпечення такої ж дальності дії пристроїв стандарту 802.11a, яку мають пристрої стандарту 802.11b. Розроблений метод модуляції носійної - ортогональне частотне мультиплексування (Orthogonal Frequency Division Multiplexing) - OFDM, що відрізняється від DSSS.

У IEEE 802.11a кожен кадр передається за допомогою 52 ортогональних носійних, кожна з шириною смуги близько 300 кГц (20 МГц/64). Ширина одного каналу - 20 МГц. Носійні модулюють за допомогою BPSK, QPSK, а також 16 - і 64-позиційної квадратурної амплітудної модуляції (QAM). У таблиці.1.3 показано, як необхідна швидкість передачі даних перетвориться у відповідні параметри вузлів передавача OFDM.

Мінімальну пропускну здатність канал має при використанні двійкової фазової маніпуляції (BPSK). При цьому забезпечується швидкість передачі даних по кожному підканалу, рівна 125 кбіт/с, що в цілому складає 6 Мбіт/с.

У разі застосування квадратурної фазової маніпуляції (QPSK) швидкість передачі даних в кожному підканалі збільшується вдвічі - до 250 кбіт/с, а пропускна здатність усього каналу стає рівною 12 Мбіт/с. При використанні 16-рівневої квадратурної амплітудної модуляції (16QAM), що кодує 4 біт на один герц носійної пропускна здатність каналу складе 24 Мбіт/с.

Таблиця 1.3 - Параметри передавача стандарту IEEE 802.11a

Швидкість передачі даних (Мбіт/с)	Модуляція	Швидкість згорткового кодування	Число канальних біт на підносійну	Число канальних біт на символ	Число біт даних на символ OFDM
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

1.10. Аналіз стандарту IEEE 802.11g

Стандарт 802.11g поєднаємо із стандартами 802.11b. Пристрій, що підтримує стандарт 802.11g, працюватиме і в мережах стандарту 802.11b і навпаки. Сумісність стандартів g і b обумовлена використанням одного і того ж частотного діапазону.

У протоколі 802.11g передбачена передача на швидкостях 1, 2, 5,5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48 і 54 Мбіт/с. Деякі з цих швидкостей є обов'язковими, а деякі - по вибору. Обов'язковими є швидкості передачі 1; 2; 5,5; 6; 11; 12 і 24 Мбіт/с. Співвідношення між різними швидкостями передачі і методами кодування приведене в таблицю.1.4.

Таблиця 1.4 - Швидкість передачі і кодування в стандарті IEEE 802.11g

Швидкість передачі, Мбіт/с		Метод кодування	Модуляція
1	(обов'язково)	Код Баркера	DBPSK
2	(обов'язково)	Код Баркера	DQPSK
5,5	(обов'язково)	CCK	DQPSK
	(по вибору)	PBCC	DBPSK
6	(обов'язково)	OFDM	BPSK
	(по вибору)	CCK - OFDM	BPSK
11	(обов'язково)	CCK	DQPSK
	(по вибору)	PBCC	DQPSK
12	(обов'язково)	OFDM	QPSK
	(по вибору)	CCK - OFDM	QPSK
24	(обов'язково)	OFDM	16-QAM
	(по вибору)	CCK - OFDM	

У протоколі 802.11b використовується або двійкова (DBPSK), або квадратурна (DQPSK) відносна фазова модуляція. Для передачі на низьких швидкостях 6 і 9 Мбіт/с використовується BPSK, а на швидкостях 12 і 18 біт/з використовується модуляція QPSK. Для передачі на вищих швидкостях використовується квадратурна амплітудна модуляція 16QAM і 64QAM.

Основні технічні характеристики стандарту 802.11g дані в таблиці.1.5. Як показує аналіз ринку, продаж засобів телекомунікацій, САРД знаходять все більшу популярність серед споживачів завдяки своїм перевагам. Ведеться робота над створенням нових специфікацій зв'язку у безпровідних мережах, у тому числі над удосконаленням технології, заснованої на концепції багатьох входів - виходів (Multiple Input - Multiple Output, MIMO).

Таблиця 1.5 - Технічні характеристики IEEE 802.11g

Сумісність	802.11b
Частотний діапазон	2,4 ГГц
Частоти	2,400–2,4835 ГГц
Максимальна швидкість	54 Мбіт/с
Швидкість	6, 12, 24 Мбіт/с; 1, 2, 5,5, 11 Мбіт/с (по 802.11b)
Максимальне число каналів	3
Дальність роботи	Приміщення: 100 м, пряма видимість: 300 м
Тільки пряма видимість	Ні
«Точка-точка»	Так
«Точка-зірка»	Так
Чутливість приймача при різних швидкостях передачі	
Швидкість передачі	Чутливість приймача
48 Мбіт/с	-71 dBm
24 Мбіт/с	-80 dBm
18 Мбіт/с	-83 dBm
12 Мбіт/с	-85 dBm
Потужність передавача при різних швидкостях передачі	
Швидкість передачі	Потужність передавача
54Мбіт/с, 108Мбіт/с	від 14 до 15 dBm
48Мбіт/с	від 14 до 16 dBm
36; 24; 18; 12 Мбіт/с	від 16 до 18 dBm

Нові стандарту дозволять використовувати безпровідні мережі там, де це було неможливо із-за обмеженої швидкості.

1.11. Перспективні САРД на базі технології DS - CDMA

Сучасні технічні розробки дозволяють вирішувати широкий спектр питань, пов'язаних із створенням САРД, забезпеченням високоякісними послугами зв'язку абонентів різних категорій. При виборі САРД зазвичай виходять з декількох типових завдань:

- надання послуг зв'язку або доступу в Інтернет;
- побудова територіально-розподілених корпоративних мереж;
- організація магістральних каналів для передачі даних.

На споживчому рівні сучасні САРД повинні характеризуватися наступними перевагами і особливостями :

- надання якості послуг, порівнянним з дротяним підключенням;
- можливість надання послуг в районах, де застосування земляних робіт ускладнене і не виправдано;
- можливість швидкого розгортання системи;
- можливість підключення абонента по цифровому інтерфейсу.

Принцип технології множинного доступу з кодовим розподілом каналів (CDMA)[1] полягає в розширенні спектру початкового інформаційного сигналу. При цьому забезпечується висока міра захисту від активних і пасивних завад.

У DS-CDMA-системі кожній абонентській станції виділяється своя унікальна псевдовипадкова кодова послідовність, що відрізняє її від інших і одночасно використовувана для підвищення завадостійкості і забезпечення безпеки. У передавачі вузькосмуговий інформаційний сигнал множиться на цю псевдовипадкову N-символьну послідовність. У ефірі такий сигнал займає смугу частот, що значно перевищує по ширині смугу частот початкового вузькосмугового сигналу. Вузькосмуговий сигнал «розмазується» в широкій смузі і стає менше рівня шуму.

У приймачі початковий сигнал відновлюється за допомогою такої ж псевдовипадкової послідовності (зворотна операція). Будь-які інші сигнали,

відмінні від початкового сигналу, що також поступають на цей приймач, сприймаються як шум.

Технологія DS-CDMA знайшла застосування в засобах зв'язку завдяки таким характеристикам, як завадозахищеність, несхильність до інтерференційних вплоиів, низькі рівні радіовипромінювань, можливість роботи в режимі багатопроменевого поширення, практичні труднощі з виявленням, що задовольняє вимогам скритності і захисту від несанкціонованого доступу до передаваної інформації.

Принципи побудови мережі і особливості устаткування. САРД призначена для організації безпровідних мереж з архітектурою «точка-багатоточка» і забезпечення інтегрованого сервісу: телефонії і високошвидкісного доступу в Інтернет. Елементом, що утворює, стільники являється базова станція (БС) з круговою діаграмою покриття. Кругова діаграма може бути розбита по азимуту на сектори. Кожен сектор обслуговується пристроєм БС і спрямованою антеною з секторною діаграмою

При використанні декількох БС, працюючих в зонах, що перекриваються, зонах обслуговування, стає необхідне частотно-просторове планування системи. При такому плануванні системи додатково необхідно враховувати рельєф місцевості, оскільки можлива поява перевідбитих променів, які визначаються характеристиками відзеркалювальних поверхонь.

Абонентські станції (АС) призначені для обслуговування окремих груп абонентів. АС мають зовнішню спрямовану антену, різні призначені для користувача інтерфейси, наприклад, для передачі даних - Ethernet, Frame Relay з синхронним інтерфейсом, ISDN.

У більшості цифрових систем абонентського радіодоступу для кодування мови використовується або імпульсно-кодова модуляція мови (ІКМ) із швидкістю передачі 64 кбіт/с (стандарт ITU - T G. 711), або адаптивна диференціальна імпульсно-кодова модуляція (АДІКМ) зі швидкостями передачі 40, 32, 24 і 16 кбит/с (стандарт ITU - T G. 726).

Системи DS-CDMA: порівняльний аналіз. САРД CDMA, будучи принципово однаковими з точки зору використовуваної в них технології шумоподобного сигналу, мають ряд відмінностей з точки зору універсальності їх характеристик. При порівнянні різних САРД DS-CDMA доцільно розглянути САРД на базі:

– AsterPlex компанії «Кедах Електронікс Інжиніринг» [2];
– AirLoop компанії Alcatel - Lucent [3];
– AirSpan AS4020 компанії AirSpan Networks [4].

Для наочного аналізу проведемо порівняння за споживчими і експлуатаційними характеристиками цих систем абонентського радіодоступу на базі технології DS-CDMA (таблиця.1.8).

Розглянуті САРД дозволяють будувати мережі зв'язки, обслуговуючі до декількох тисяч абонентів в радіусі до 30 км. Це можуть бути чисто телефонні низькошвидкісні канали, а також і виділені канали передачі даних швидкістю до 128 кбіт/с.

Оскільки це канали, які виділяються абонентові, реальна швидкість передачі даних в каналі не поступається багатьом широкосмуговим системам з піковою швидкістю, що декларує, більше 1 Мбіт/с. Конфігурація абонентських станцій за швидкістю передачі даних здійснюється програмним способом, що дозволяє надати ще більшу гнучкість розгортання системі по сервісу, що надається.

Як правило, основними параметрами при порівнянні систем радіозв'язку є пропускна здатність і радіус дії. Як видно з таблиці 1.8, система AirLoop поступається системам AsterPlex і AirSpan 4020 як по радіусу дії, так і по максимальній пропускній здатності базової станції. Максимальна пропускна здатність базової станції AirSpan 4020 істотно вища, ніж у аналогів, проте вона досяжна лише при мінімальному радіусі дії і зменшується при збільшенні відстані до абонентської станції. Система AsterPlex, у свою чергу, має максимальний радіус дії.

Ці дані необхідно враховувати при розгортанні САРД в конкретних умовах. На сьогодні діапазони 2,4 і 3,5 ГГц досить завантажені, і отримання дозволів може представляти утруднення, особливо в мегаполісах і передмістях. Найбільш

перспективними з точки зору розвитку САРД є діапазони в районі 5,1-5,8 ГГц.

Таблиця 1.8 - Порівняння систем AsterPlex, AirLoop і AirSpan 4020

Параметр	AsterPlex	AirLoop	AirSpan 4020
Діапазон частот, ГГц	3,4 – 3,6; 5,1 – 5,9	3,6 –4,0	1,8–4,0 (у дозволених діапазонах)
Дальність зв'язку, км	30	2,5 – місто 4,0 – передмістя 5,0 – село	2–5 – місто 5–10 – передмістя 15–25 –сільська місцевість
Пропускна здатність, Мбіт/с	4,096	2,048	1–17 (залежно від завантаженості мережі)
Смуга сигналу, МГц	5	10	1,25 – 6,0
Кодування мови	PCM ADPCM: 16, 32, 64 кбіт/з	PCM ADPCM: 16, 32, 64 кбіт/з	PCM, ADPCM: 16, 32, 64 кбіт/з
Дуплекс	FDD	FDD	FDD
Число просторових секторів	1 – 6	1 – 4	1 – 4
Вихідна потужність, Вт	0,3	3,0 для БС 0,25 для АС	2,0 для БС і АС
Чутливість приймача, дБм	– 96 для БС – 112 для АС	немає даних	– 112 для БС – 116 для АС
Температурний режим, град.С	+5… +40 для внутрішнього модуля – 40…+60 для зовнішнього модуля	немає даних	+5… +45 для внутрішнього модуля – 40…+60 для зовнішнього модуля

1.12. Проблеми безпеки систем безпровідного доступу

Основне питання при побудові систем безпровідного доступу - питання забезпечення необхідного рівня безпеки інформації в мережі. На відміну від

звичайних дротяних мереж здійснити перехоплення інформації в радіоканалі набагато простіше - досить мати комплект устаткування, аналогічний комплекту устаткування абонента безпровідної мережі.

Забезпечення безпеки мережі безпровідного доступу зводиться до рішення трьох основних проблем :

– захист від підключення до мережі нелегальних користувачів;

– запобігання несанкціонованому доступу до ресурсів мережі;

– гарантування підтримки цілісності і конфіденційності даних, що передаються по радіоканалу.

Для вирішення перших двох завдань застосовуються процедури аутентифікації (Authentication), авторизації (Authorization) і обліку (Accounting). Сукупність цих трьох дій, що розглядаються як єдиний елемент забезпечення безпеки мережі, скорочено називають абревіатурою ААА. Розрізняють два типи систем ААА: централізовану, засновану на використанні сервера доступу; децентралізовану, яка базується на робочих станціях.

Досвід показує, що для мереж безпровідного доступу єдино прийнятним рішенням є централізований варіант.

Висновки

У розділі розглянуті принципи і особливості побудови САРД, сформульовані їх переваги і недоліки, проведені класифікація, аналіз їх складу і основних характеристик. Відзначається, що в системах радіодоступу широко використовуються різні технології організації множинного доступу, зокрема, FDMA, TDMA, CDMA.

2 БЕЗПЕКА І ЗАХИЩЕНІСТЬ БЕЗПРОВІДНИХ СИСТЕМ ПЕРЕДАЧІ ІНФОРМАЦІЇ

2.1 Модель загроз і забезпечення безпеки САРД

2.1.1 Загрози інформаційної безпеки САРД

Звернемося до визначення інформаційної безпеки (ІБ). ІБ - означає захист інформації і інформаційних систем від неавторизованого доступу, використання, виявлення, спотворення, знищення, модифікації. ІБ забезпечує доступність, цілісність і конфіденційність інформації.

Під загрозою безпеки інформації розуміється сукупність умов і чинників, що створюють потенційну небезпеку, пов'язану з просочуванням інформації і несанкціонованими і неумисними діями на неї [7, 8].

Загрози можна класифікувати таким чином [7 - 9]:

а) загрози порушення конфіденційності :

– порушення конфіденційності інформації шляхом перехоплення безпровідного трафіку;

– несанкціонований доступ до інформації і сервісів сегментів дротяних мереж, з якими працює користувач, використовуючи безпровідною доступ;

– розкриття параметрів безпровідної мережі або сегментів дротяних мереж, з якими працює користувач, використовуючи безпровідною доступ, за межами КЗ.

б) загрози порушення цілісності :

– спотворення циркулюючої в мережі інформації;

– знищення інформації користувача або інформації, що зберігається в сегментах дротяних мереж, з якими працює користувач, використовуючи безпровідний доступ;

– розсилка пакетів інформації не за адресою, втрата пакетів, невірна зборка пакетів, їх підміна.

в) загрози порушення доступності :

– втручання в процес обміну повідомленнями по мережі;

– блокування повідомлень, що приймаються, або передаваних, на рівні користувачів або точок доступу;

– виведення із ладу точки доступу разом з усіма приєднаними користувачами.

г) специфічні загрози:

– протиправні анонімні дії від імені користувача безпровідної мережі;

– розкрадання клієнтських пристроїв або точок доступу з метою отримання інформації про налаштування системи захисту безпровідної мережі;

– установка несанкціонованих точок доступу і клієнтських мережевих карт;

– несанкціонована зміна налаштувань засобів захисту безпровідної мережі;

– відмови роботи безпровідного устаткування.

Розглянемо способи отримання загроз, характерні для САРД [8 -11].

Підслуховування. Найбільш поширена проблема у безпровідних мережах - це можливість анонімних атак. Анонімні абоненти можуть перехоплювати радіосигнал і розшифровувати передавані дані. Устаткування, використовуване для підслуховування в мережі, може бути не складніше того, яке використовується для звичайного доступу до цієї мережі. Щоб перехопити передачу, зловмисник повинен знаходитися поблизу від передавача. Перехоплення такого типу практично неможливо зареєструвати і ще важче завадити ім. Використання антен і підсилювачів дає зловмисникові можливість знаходитися на значній відстані від мети в процесі перехоплення.

Підслуховування дозволяє зібрати інформацію в мережі, яку згодом передбачається атакувати. Первинна мета зловмисника - зрозуміти, хто використовує мережу, які дані в ній доступні, які можливості мережевого устаткування, в які моменти його експлуатують найбільш і найменш інтенсивно і яка територія розгортання мережі. Усе це згодиться для того, щоб організувати атаку на мережу. Багато загальнодоступних мережевих протоколів передають таку важливу інформацію, як ім'я користувача і пароль, відкритим текстом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ

до мережевих ресурсів. Навіть якщо передавана інформація зашифрована, в руках зловмисника опиняється текст, який можна запам'ятати, а потім вже розкодувати.

Інший спосіб підслуховування - підключення до безпровідної мережі. Активне підслуховування в локальній безпровідній мережі зазвичай засноване на неправильному використанні протоколу Address Resolution Protocol (ARP). Це атака типу Man In The Middle («людина посередині») на рівні зв'язку даних. Вони можуть приймати різні форми і використовуються для руйнування конфіденційності і цілісності сеансу зв'язку. Атаки MITM складніші, ніж більшість інших атак: для їх проведення потрібно детальну інформацію про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Коли жертва атаки ініціює з'єднання, шахрай перехоплює його і потім завершує з'єднання з необхідним ресурсом, а потім пропускає усі з'єднання з цим ресурсом через свою станцію. При цьому зловмисник може посилати і змінювати інформацію або підслуховувати усі переговори і потім розшифровувати їх. Той, що атакує посилає ARP-відповіді, на які не було запиту, до цільової станції локальної мережі, яка відправляє йому увесь трафік, що проходить через неї. Потім зловмисник посилатиме пакети вказаним адресатам. Таким чином, безпровідна станція може перехоплювати трафік іншого безпровідного клієнта [10 - 12].

Відмова в обслуговуванні (Denial of Service - DOS). Повну паралізацію мережі може викликати атака типу DOS. У усій мережі, включаючи базові станції і клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися одна з одною. Ця атака вимикає усі комунікації в певному районі. Якщо вона проводиться в досить широкій області, то може потребувати значних потужностей. Атаці DOS на безпровідні мережі важко запобігти або зупинити. Більшість безпровідних мережевих технологій використовують неліцензовані частоти - отже, допустима інтерференція від цілого ряду електронних пристроїв.

Глушення клієнтської і базової станції. Глушення в мережах відбувається тоді, коли умисна або неумисна інтерференція перевищує можливості відправника або одержувача в каналі зв'язку, і канал виходить з ладу. Зловмисник може використовувати різні способи глушення.

Глушення клієнтської станції дає шахраєві можливість підставити себе на місце заглушеного клієнта. Також глушення може використовуватися для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Витонченіші атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника.

Глушення БС надає можливість підмінити її атакуючою станцією. Таке глушення позбавляє користувачів доступу до послуг.

Загрози криптозахисту. У безпровідних мережах стандарту IEEE 802.11n застосовуються такі криптографічні засоби як WEP, WPA і WPA2 для забезпечення цілісності і конфіденційності інформації. Проте помилки призводять до порушення комунікацій і використання інформації зловмисниками.

WEP - це криптографічний механізм, створений для забезпечення безпеки мереж стандарту 802.11. Цей механізм розроблений з єдиним статичним ключем, який застосовується усіма користувачами. Доступ до ключів, часта їх зміна і виявлення порушень, практично неможливі. Дослідження WEP-шифрування виявило вразливі місця, із-за яких той, що атакує може повністю відновити ключ після захоплення мінімального мережевого трафіку. У Internet є засоби, які дозволяють зловмисникові відновити ключ впродовж декількох годин. Тому WEP не може вважатися як на засіб аутентифікації і конфіденційності у безпровідній мережі. Використовувати описані криптографічні механізми краще, ніж не використовувати ніяких, але, з урахуванням відомих вразливостей, потрібні інші методи захисту від атак. Усі безпровідні комунікаційні мережі схильні до атак прослуховування в період контакту (установки з'єднання, сесії зв'язку і припинення з'єднання). Сама природа безпровідного з'єднання не дозволяє його контролювати, і тому воно вимагає захисту. Управління ключем, як правило, викликає додаткові проблеми, коли застосовується при роумінгу і у разі загального користування відкритим середовищем [14-17].

Вторгнення і модифікація даних. Вторгнення відбувається, коли зловмисник додає інформацію до існуючого потоку даних, щоб перехопити з'єднання або пересилати дані або команди у своїх цілях. Зловмисник може маніпулювати

командами, що управляють, і потоками інформації, посилаючи пакети або команди на базову станцію, і навпаки. Подаючи команди, що управляють, в потрібний канал управління, можна добитися від'єднання користувачів від мережі.

Вторгнення може використовуватися для відмови в обслуговуванні. Той, що атакує переповнює точку доступу в мережі командами з'єднання, «обдуривши» її перевищенням максимуму можливих звернень, - таким чином, іншим користувачам буде відмовлено в доступі.

Помилкова точка доступу. Зловмисник може організувати помилкову точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї помилкової точки доступу і повідомляють їй свої важливі реквізити, наприклад аутентифікаційну інформацію. Цей тип атак іноді застосовують у поєднанні з прямим глушенням, щоб «заглушити» істинну точку доступу в мережу. Користувачі, що мають доступ до дротяної мережі, можуть також сприяти встановленню помилкових точок доступу, ненавмисно відкриваючи мережу для нападів.

Загрози, як можливі небезпеки здійснення якої-небудь дії, спрямованої проти об'єкту захисту, проявляються не самі по собі, а через вразливості (чинники), що призводять до порушення безпеки інформації на конкретному об'єкті інформатизації.

Вразливості, властиві безпровідним мережам стандарту IEEE 802.11, невід'ємні від них і обумовлюються недоліками процесу функціонування, властивостями архітектури мережі, протоколами обміну і інтерфейсами, вживаними програмним забезпеченням і апаратною платформою, умовами експлуатації і розташування [18].

Кожній загрозі можуть бути зіставлені різні вразливості.

Усунення або істотне послаблення вразливостей впливає на можливість реалізації загроз безпеки інформації.

Для безпровідних мереж стандарту IEEE 802.11n характерні наступні вразливості [9, 10]:

1) обумовлені середовищем передачі і діапазоном робочих частот стандарту IEEE 802.11;

2) системи аутентифікації;

3) криптографічних протоколів;

4) використовуваного програмного забезпечення;

5) обумовлені людськими чинниками.

Розглянемо детальніше вразливості, обумовлені середовищем передачі і діапазоном робочих частот стандарту IEEE 802.11 [8, 9].

Діапазон робочих частот стандарту IEEE 802.11 є таким, що не ліцензується. У діапазоні робочих частот 2,4 ГГц працюють деякі моделі радіотелефонів, побутові пристрої, протокол Bluetooth, які створюють завади. Усі стандарти IEEE 802.11 схильні до впливу наступних явищ, пов'язаних з середовищем передачі:

– завади від інших джерел, зокрема від передавачів, працюючих на тій же частоті, шум від силових пристроїв;

– багатопроменеві ефекти при проходженні листя дерев, що знаходяться в сильній залежності від вітру;

– вплив інших завад.

Окрім проблем пов'язаних з поширенням радіохвиль, середовище передачі визначає наступну проблему. Інформація, циркулююча у безпровідних мережах схильна до перехоплення. Це пояснюється тим, що переносником інформації є радіохвилі.

Таким чином, для перехоплення інформації зловмисникові досить мати недорогий набір пристроїв, аналогічний комплекту устаткування користувача безпровідної мережі [17-19].

2.1.2 Методи захисту інформації в САРД

Розглянемо безпровідні мережі стандарту IEEE 802.11n як об'єкт загроз інформаційної безпеки і проведемо їх класифікацію за конфігурацією використовуваних засобів захисту.

Для безпровідних мереж стандарту 802.11n усіх засобів і методи захисту можна розділити на наступні типи [8-10]:

а) засоби і методи аутентифікації;

б) засоби криптографічного захисту передаваних даних;

в) засоби технічного захисту;

г) додаткові кошти захисту.

До засобів і методів аутентифікації відносяться:

– базова аутентифікація (відкрита аутентифікація, аутентифікація із спільно використовуваним ключем, аутентифікація по MAC-адресі);

– аутентифікація з використанням загальних ключів (Pre-Shared Key);

– аутентифікація по протоколу EAP (Extensible Authentication Protocol) з використанням RADIUS-сервера (служба дистанційної аутентифікації користувачів).

До засобів і методів криптографічного захисту відносяться:

– шифрування з використанням програмних методів захисту WEP, WPA, WPA2;

– шифрування з використанням протоколу цілісності тимчасового ключа (Temporal Key Integrity Protocol);

– застосування поліпшеного алгоритму шифрування AES (Advanced Encryption Standard).

До технічних засобів можна віднести використання генератора штучного шуму того, що пригнічує приймач-виявник. Штучний шум впливатиме лише на вхід приймача-виявника. При цьому умови виявлення легітимного каналу істотно погіршуються. Ще одним технічним методом захисту інформації є екранування виділених приміщень або об'єктів інформаційної діяльності. Це значно утруднить перехоплення інформації по безпровідному з'єднанню за рахунок обмеження зони доступності сигналу [11, 12].

До додаткових засобів захисту, не передбачених виробниками устаткування, можна віднести [13, 14]:

– міжмережеві екрани - застосовуються для блокування атак із зовнішнього середовища. Вони управляють проходженням мережевого трафіку відповідно до правил безпеки. Міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) і зовнішні (загального доступу) мережі;

– системи виявлення вторгнень (Intrusion Detection System) - для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі. Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно понизити час простою в результаті атаки і витрати на підтримку працездатності мережі;

– засоби створення віртуальних приватних мереж (Virtual Private Network) - для організації захисту каналів передачі даних. Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

– засоби аналізу захищеності - для аналізу захищеності безпровідної мережі і виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє запобігти можливим атакам на мережу, оптимізувати витрати на захист інформації і контролювати поточний стан захищеності мережі.

2.2 Захищеність безпровідних систем зв'язку

Захищеність каналу зв'язку САРД характеризується двома основними параметрами: завадозахищеністю і скритністю. Дамо визначення цих понять згідно [13].

Завадозахищеність - це здатність системи зв'язку функціонувати із заданою якістю в умовах завад, за рахунок застосування додаткових засобів захисту від завад, що не відносяться до принципу дії або побудови технічного засобу [13].

Скритність - це здатність системи зв'язку зберігати в таємниці інформацію, циркулюючу в системі, а також зміну структури і характеру функціонування [13].

Ці характеристики дозволяють вирішувати завдання забезпечення зв'язку не лише за наявності завад, але і при цілеспрямованих діях порушника.

Критерієм захищеності цифрової системи передачі інформації є вірогідність виконання завдання передачі інформації із заданими показниками якості за наявності завад [13].

Для оцінки завадозахищеності САРД в умовах дії різних видів завад необхідно мати відповідні показники. При вибраних моделях сигналу, власного шуму приймального пристрою і адитивних завад в системах передачі інформації переважним показником кількісної міри завадостійкої є середня вірогідність помилки на біт інформації BER (Bit Error Rate).

Враховуючи випадковий характер, як характеристик каналу зв'язку, так і можливостей порушника по протидії роботи легітимного каналу, критерій захищеності каналу зв'язку можна представити у формі вірогідності складної події Рз, що є сумою двох елементарних подій : вірогідність потайної роботи Рскр і завадозахищеності каналу Рпз [14].

2.2.1 Аналіз завадостійкої видів модуляції для стандарту IEEE 802.11n

У САРД стандарту IEEE 802.11n використовуються наступні види модуляції: двійкова і квадратурна фазова маніпуляції (BPSK, QPSK), 16- і 64-позиційна квадратурна амплітудна маніпуляції (QAM)[5, 6].

Однією з найважливіших характеристик якості в системах цифрового зв'язку є вірогідності бітової помилки (ВБП) появи помилкового біта як функція відношення енергії сигналу, що доводиться, на 1 біт повідомлення (E_b), що приймається, до енергетичної спектральної густини шуму (N_0) - E_b/N_0.

Отже, необхідне відношення E_b/N_0 можна розглядати, як характеристику, що дозволяє порівнювати якість систем зв'язку : ніж менше необхідне відношення E_b/N_0, тим ефективніше процес визначення при цій вірогідності помилки [5].

З літератури [5,6] відомі формули для розрахунку ВБП для різних модуляцій. BER для бінарної і квадратурною PSK визначається як

$$P_b = Q(\sqrt{2\gamma_0}). \tag{2.1}$$

де γ_0 - відношення енергії біта до спектральної щільності шуму;

$Q(z)$ – інтеграл помилок Гауса, що використовується при описі вірогідності з щільністю гауса розподілу.

Визначається ця функція як

$$Q(z) = \frac{1}{\sqrt{2\pi}} \int_z^{\infty} \exp(-\frac{u^2}{2}) du. \tag{2.2}$$

При використанні m-арної QAM з довільним числом позицій (m - QAM) ВБП рівна

$$P_b = \frac{4(\sqrt{m}-1)}{\sqrt{m}\log_2 m} Q(\sqrt{\frac{3\gamma \log_2 m}{m-1}}). \tag{2.3}$$

Залежності ВБП P_b від відношення сигнал/шум даних видів модуляції САРД, побудовані згідно (2.2-2.4) приведені на рис.2.1.

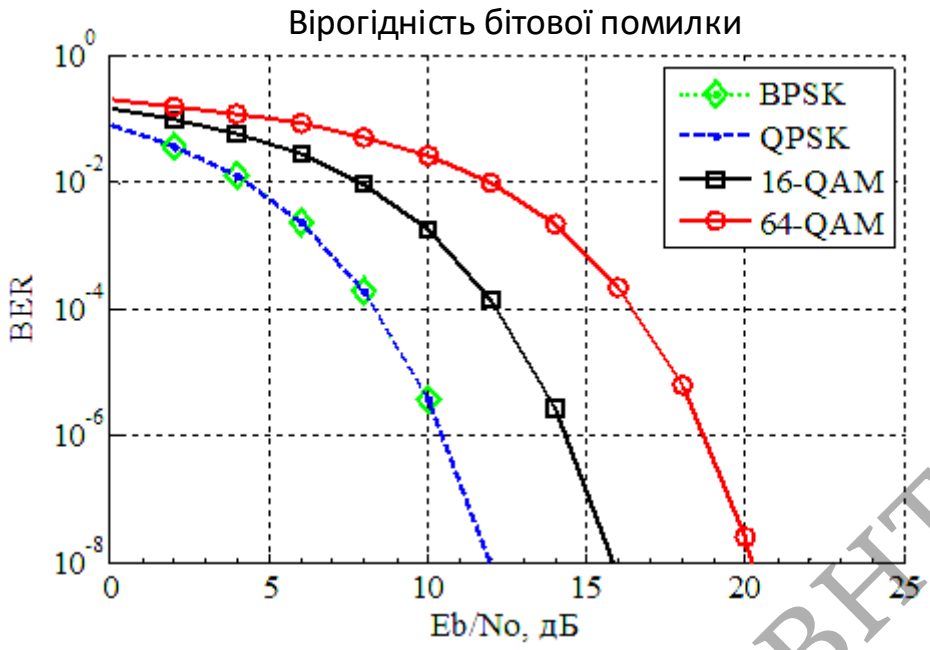


Рисунок 2.1 - Залежності ВБП для видів модуляції САРД IEEE 802.11n

З аналізу цих кривих виходить, що зі збільшенням позиційності модуляції вірогідність бітової помилки збільшується, тобто для підтримки заданого рівня бітової помилки необхідно збільшувати відношення сигнал/шум на вході приймача. Найбільшу завадостійкість (чи найменші енергетичні втрати) при заданій вірогідності помилки мають сигнали BPSK і QPSK. Проте для підвищення спектральної ефективності доцільно застосовувати методи модуляції з великим m, особливо QAM16 і QAM64, проте при цьому вимагається забезпечити високе відношення сигнал/шум в каналі передачі.

2.2.2 Оцінка скритності системи зв'язку

Радіотехнічна розвідка припускає послідовне виконання трьох основних завдань: виявлення факту роботи радіосистеми (виявлення сигналу), визначення структури виявленого сигналу і розкриття інформації, що міститься (передається) в сигналі.

Перерахованим завданням розвідки каналу зв'язку порушником можуть бути протиставлені три види скритності сигналів: енергетична; структурна; інформаційна (рис.2.2).

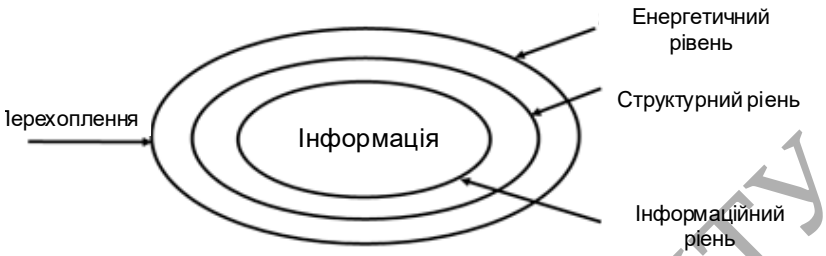


Рисунок 2.2 - Трирівнева система захисту інформації від перехоплення

Енергетична скритність спрямована на виключення або істотне утруднення виявлення сигналів. Енергетична скритність може бути оцінена різними показниками, наприклад: вірогідністю виявлення сигналів при заданій вірогідності помилкової тривоги, дальністю виявлення (розвідки) сигналів при заданому відношенні сигнал-шум.

Структурна скритність спрямована на виключення або істотне утруднення розкриття структури (виду) сигналів. Структура сигналу визначається характером його кодування і модуляції. Показником структурної скритності може служити вірогідність розкриття структури сигналу за умови, що цей сигнал виявлений.

Інформаційна скритність визначається здатністю протистояти заходам радіотехнічної розвідки, спрямованим на розкриття сенсу передаваного за допомогою системи безпровідного зв'язку інформації. В якості міри інформаційної скритності можна прийняти вірогідність розкриття змісту передаваного повідомлення за умови, що сигнал виявлений і виділений.

Якщо захист інформації забезпечений тільки на інформаційному рівні, то завжди існує загроза підміни інформації (тобто дезинформація). Забезпечуючи інформаційний і структурний рівні системи можна захистити інформацію від перехоплення, але шляхом постановки завад можна розірвати сеанс зв'язку.

У загальному випадку скритність роботи каналу зв'язку можна оцінити вірогідністю потайної роботи [14]:

$$P_{скр} = 1 - P_р = 1 - P_{об} \times P_{стр} \times P_{инф}, \quad (2.4)$$

де $P_{об}$ - вірогідність виявлення сигналу або факту роботи каналу зв'язку;

$P_{стр}$ - вірогідність розкриття структури сигналу;

$P_{інф}$ - вірогідність розкриття сенсу передаваної інформації.

Основними критеріями оцінки енергетичної скритності каналу зв'язку окрім вірогідності виявлення сигналу при заданій вірогідності помилкової тривоги є відношення сигнал/шум на вході приймача виявника SNR2, що забезпечує задану вірогідність виявлення, і радіус виявлення сигналу $R_{об}$ при заданому відношенні сигнал/шум на вході приймача виявника SNR2 зад.

Радіус виявлення Rоб знаходить застосування при рішенні цілого ряду практичних завдань, пов'язаних з розробкою організаційно-технічних заходів і визначенням розмірів контрольованих зон [14].

Якщо припустити, що в приймачі-виявнику реалізовані оптимальні або квазіоптимальні алгоритми виявлення сигналів, то радіус виявлення можна приблизно визначити з виразу:

$$R_{об} = \frac{\lambda}{4\pi}\left[\frac{P_{пер} G_{пер} G_{пр\,о}}{P_{пр\,о} PL_о SNR_2}\right]^{1/2} \quad (2.5)$$

де λ- довжина хвилі передавача системи зв'язку;

$P_{пер}$– потужність передавача;

$G_{пер}$ – коефіцієнт спрямованої дії антени передавача;

$G_{пр\,о}$ – коефіцієнт спрямованої дії антени передавача-виявника;

$P_{пр\,о}$ – чутливість приймача-виявника;

PL_o – величина втрат на радіотрасі між передавачем і приймачем-виявником, пов'язаних з умовами поширення сигналу;

SNR2 - відношення сигнал/шум на вході приемника-виявника при заданих параметрах якості виявлення сигналу САРД [14].

Приведемо структурну схему відвідного каналу в режимі перехоплення.

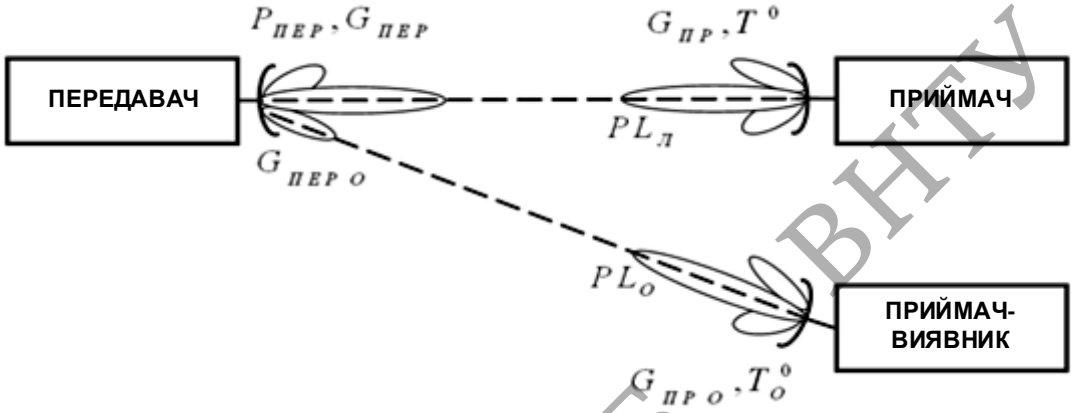


Рисунок 2.3 - Структурна схема відвідного каналу в режимі перехоплення

Умова перехоплення сигналу може бути виражена нерівністю, яку можна представити у вигляді декількох співмножників, що характеризують основні параметри каналу зв'язку:

$$\left(\frac{G_{пр}}{T^0}\right)\left(\frac{G_{пер}}{G_{пер\,o}}\right)\left(\frac{PL_л}{PL_o}\right)\left(\frac{1}{k_З}\right)\left[\frac{1}{\left(\frac{2E_B}{N_0}\right)\frac{1}{T}\left(\frac{T_u}{F}\right)}\right] \le \left(\frac{G_{пр\,o}}{T_o{}^0 z_o}\right), \qquad (2.7)$$

де $G_{пр}$ – коефіцієнт спрямованої дії антени приймача;

T_0 - шумова температура приймача;

$\left(PL_л / PL_o\right)$ – втрати в лінії зв'язку для легітимного каналу і каналу порушника ;

$\left(1/k_З\right)$ – коефіцієнт запасу по потужності kз;

$\left[1/\left(\frac{2E_B}{N_0}\right)\frac{1}{T}\left(\frac{T_u}{F}\right)\right]$ – коефіцієнт, що визначає параметри модуляції і широкосмугової сигналу :

E_B - енергія сигналу на біт інформації;

N_0 - спектральна щільність шуму;

$F * T = B_c$ - база сигналу;

T_u- час інтеграції сигналу в приймачі-виявнику;

$\left(G_{пр\,o} / T_o{}^0 z_o\right)$ – параметри приймача-виявника, що характеризують його технічну досконалість і небезпеку перехоплення :

T_0^0 - шумова температура приймача-виявника;

z_0 – поріг виявлення [25].

З виразу можна зробити наступні висновки:

– для збільшення енергетичної скритності легітимного каналу зв'язку, тобто зменшення відношення сигнал/шум на виході лінійної частини приймача виявника необхідно використовувати передачу з мінімально можливим показником якості;

– використовувати в каналі спрямовані антени з мінімально можливим рівнем бічних пелюсток;

– використовувати приймач з малим рівнем власних шумів; втрати на поширення електромагнітної енергії сигналу на трасі легітимного каналу мають бути значно менше, ніж втрати на трасі порушника;

– використовувати як сигнал - переносника складні сигнали з найбільшим значенням бази (Вс>>1)[14].

2.2.3 Критерії оцінки завадозахищеності системи зв'язку

Критерії завадозахищеності САРД показують здатність безпровідної системи зв'язку протистояти впливу завад як природного, так і штучного походження.

Оскільки завадозахищеність також залежить від ряду випадкових чинників, то її кількісною мірою може бути також імовірнісний критерій, що має наступний вигляд [14]:

$$P_{пз} \geq P_{пз\,зд}, \tag{2.7}$$

де $P_{пз}$ - вірогідність функціонування системи зв'язку із заданим рівнем завадозахищеності.

Виходячи з виразу (2.7) вірогідність залежить від вірогідності придушення завадами каналу зв'язку, який можна визначити як вірогідність того, що фактичне значення відношення сигнал/шум на вході приймача САРД, стане менше деякого критичного значення SNRкр, при якому порушується функціонування системи зв'язку.

Для оцінки вірогідності пригнічення каналу необхідно знати щільність вірогідності qпр на вході вирішального пристрою приймача, яка залежить від щільності вірогідності діючих завад, а також від характеристик використовуваного сигналу [14-16].

Якщо в якості приймача складного сигналу САРД використовувати приймач з рівномірним підсиленням в смузі частот F, то завадозахищеність радіоканалу буде забезпечена при дотриманні наступної нерівності :

$$\left(P_{пер}G_{пер}\right)\left(\frac{G_{пр}}{G_{пр\,о}}\right)\left(\frac{PL_{о}}{PL_{л}}\right)\left(\frac{1}{k_{З}}\right)\left[\frac{r^{2}BR}{F}\frac{E_{B}}{N_{n}}\right]^{-1} \geq \left[P_{пер\,п}G_{пер\,п}\right] \tag{2.8}$$

де E_B - енергія сигналу на біт інформації;

N_n - спектральна щільність завади;

r_2 - середнє значення коефіцієнта взаємної кореляції сигналу і завади.

Із спільного порівняння нерівностей (2.7) і (2.8) виходить, що одночасне підвищення скритності і завадозахищеності САРД досягається збільшенням бази сигналу ВС, спрямованістю антен передавача і приймача і ефективним

використанням радіоканалу за рахунок точнішої оцінки каналу поширення на радіотрасі.

Розглянуто три види скритності сигналу: енергетичний, структурний, інформаційний. Скритність оцінюється вірогідністю потайної роботи.

При цьому радіус виявлення сигналу (визначення розмірів контрольованих зон) пропорційний довжині хвилі передавача системи зв'язку, коефіцієнтам посилення антен і потужності передавача. Це накладає свої вимоги на підсилювальні параметри антени базової станції.

Можливість зміни спрямованості (діаграми спрямованості) антени показана на прикладі куткової антени. Такі зміни можливі за рахунок варіювання конструктивними параметрами антени і антенних грат.

3 РОЗРАХУНОК АНТЕНИ І АНТЕНОЇ ГРАТКИ ДЛЯ БАЗОВОЇ СТАНЦІЇ

3.1 Підтримка багатоантенних систем MIMO

Подальше підвищення пропускної здатності і якості послуг в мережах LTE пов'язане з технологією MIMO. MIMO - Multiple Input Multiple Output - є технологією передачі даних за допомогою N-антен і прийому інформації M-антенами. При цьому приймаючі і передавальні сигнал антени рознесені між собою на таку відстань, щоб отримати слабку міру кореляції між сусідніми антенами.

Технологію MIMO можна ще вважати не технологією, а методом формування каналу зв'язку з декількома антенами. Позначення MIMO дозволяє використовувати цілий ряд технологій :

– використання «інтелектуальних» антен, що дозволяють формувати вузьку спрямованість передачі даних, усувати дію завад, що заважає, за рахунок їх компенсації в приймальному пристрої, що дає можливість підвищити завадостійкість каналу зв'язку і збільшити ефективність використання спектру за рахунок передачі даних в паралельних променях;

– використання просторово-часового кодування (Space - Time Coding - STC);

– використання поляризаційного розподілу каналів, поляризаційної обробки сигналів.

Усі різновиди технології MIMO спрямовані на збільшення пікової швидкості передачі даних за рахунок покращення завадостійкості. Фізичний сенс збільшення швидкості передачі даних пояснюється за допомогою формули Шенона [15].

Для однопроменевого каналу SISO (Single Input Single Output) справедливий вираз

$$C_{SISO} = f_g \cdot log_2(1 + S/N), \quad (3.1)$$

де f_g - ширина спектру сигналу;

S/N – відношення сигнал/шум;

C_{SISO} – пікова швидкість передачі даних.

Подальше збільшення швидкості передачі даних можливо за рахунок збільшення ширини спектру сигналу, збільшення відношення сигнал/шум, а також використання багатопозиційних сигналів.

При використанні технології MIMO пікова швидкість передачі даних визначається виразом

$$C_{MIMO} = M \cdot f_g \cdot log_2(1 + S/N), \qquad (3.2)$$

Тут параметр залежить від конфігурації MIMO :

$M = min\{M_{\text{прд}}, M_{\text{пр}}\}$,

де $M_{\text{прд}}$- число передавальних антен;

$M_{\text{пр}}$ – число приймальних антен.

Наприклад, система зв'язку з антенними системами, у якої (конфігурація 2x3) або (конфігурація 2x4), еквівалентна системі зв'язку з двома просторовими потоками сигналів. Таким чином, швидкість передачі даних в системі MIMO лінійно збільшується зі збільшенням числа антен.

Для несиметричних антенних конфігурацій MIMO (наприклад, 1x2, або 2x1) швидкість передачі даних має логарифмічну залежність

$$C_{M\text{прд/пр}} = M \cdot f_g \cdot log_2(1 + S/N), \qquad (3.3)$$

Технологія MIMO дозволяє зменшити число помилок при радіообміні даними без зниження швидкості передачі в умовах множинних перевідбивань сигналів. Багатоелементні антенні системи забезпечують:

– розширення зони покриття радіосигналами і згладжування в ній «мертвих» зон;

– використання декількох шляхів поширення сигналу. Це підвищує вірогідність роботи по трасах, зменшує проблеми із завмираннями і перевідбиваннями;

– збільшення пропускної здатності каналів зв'язку за рахунок формування систем обробки сигналів, заснованих на фізично різних принципах (просторове рознесення сигналів, кодове рознесення за допомогою ортогональних кодів, частот, поляризаційне рознесення).

У системах LTE передбачені різні режими роботи з декількома передавальними і приймаючими антенами. Робота таких систем може бути організована по двох принципах: а) за принципом просторового ущільнення і б) за принципом просторово-часового кодування.

Суть першого принципу полягає в тому, що різні передавальні антени передаватимуть різні частини блоку інформаційних символів або різні інформаційні блоки. Передача даних ведеться паралельно з двох або з чотирьох антен. На приймальній стороні робиться прийом і розподіл сигналів різних антен, і стає можливим збільшення максимальної швидкості передачі даних в 2 або в 4 рази.

У системах, побудованих за принципом просторово-часового кодування, з усіх передавальних антен здійснюється передача одного і того ж потоку даних з використанням схем попереднього кодування з метою забезпечення кращої якості прийому. Так, наприклад, при формуванні сигналу з двох передавальних антен потік комплексних модуляційних символів, які модулюватимуть одну з OFDMA, підносійних-сигналу, розбивається на непарні і парні символи, тобто ці модуляційні символи відповідають одній підносійній, але різним OFDMA - символам. Тоді з урахуванням процедури попереднього кодування, перша антена на двох тактових інтервалах, що відповідають непарному і парному модуляційним символам, на одній піднесійній передаватиме символи і , в той час, як друга антена передаватиме символи. На цих часових інтервалах і на тій і на іншій підносійних на приймальній антені буде присутнім сигнал з наступними значеннями відліків:

$$r_1 = h_1 \cdot x_1 - h_2 \cdot x_2; \qquad r_2 = h_1 \cdot x_2 - h_2 \cdot x_1 \qquad (3.4)$$

де r_1 і r_2 – комплексні коефіцієнти, визначувані значенням передавальної характеристики каналу у нинішній момент часу для кожної з антен.

Після оцінки коефіцієнтів і декодування пари модуляційних символів здійснюється таким чином:

$$x_1 = \frac{r_1 \cdot h_1 + r_2 \cdot h_2}{|h_1|^2 + |h_2|^2}, \qquad x_2 = \frac{r_2 \cdot h_1 + r_1 \cdot h_2}{|h_1|^2 + |h_2|^2}. \qquad (3.5)$$

У системах MIMO, побудованих за принципом TD (Transmit Diversity, просторово-часове кодування) з чотирма передавальними антенами, в який-небудь момент часу ведеться передача сигналу тільки з двох антен. При цьому послідовність комплексних модуляційних символів розбивається на «четвірки» символів, які передаватимуться в порядку, показаному на рис.3.1.

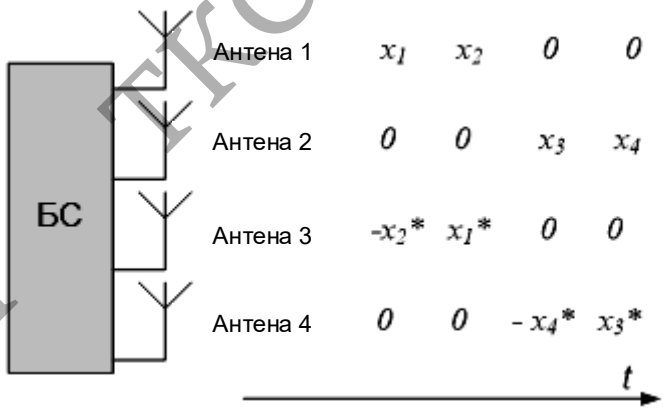


Рисунок 3.1 - Сигнали багатоантенної системи працюючої за принципом TD

Структурна схема MIMO-систем з двома передавальними і двома приймаючими антенами (рис.3.2) побудована за принципом просторового ущільнення, дозволяє підвищити максимальне значення швидкості передачі даних в 2 рази.

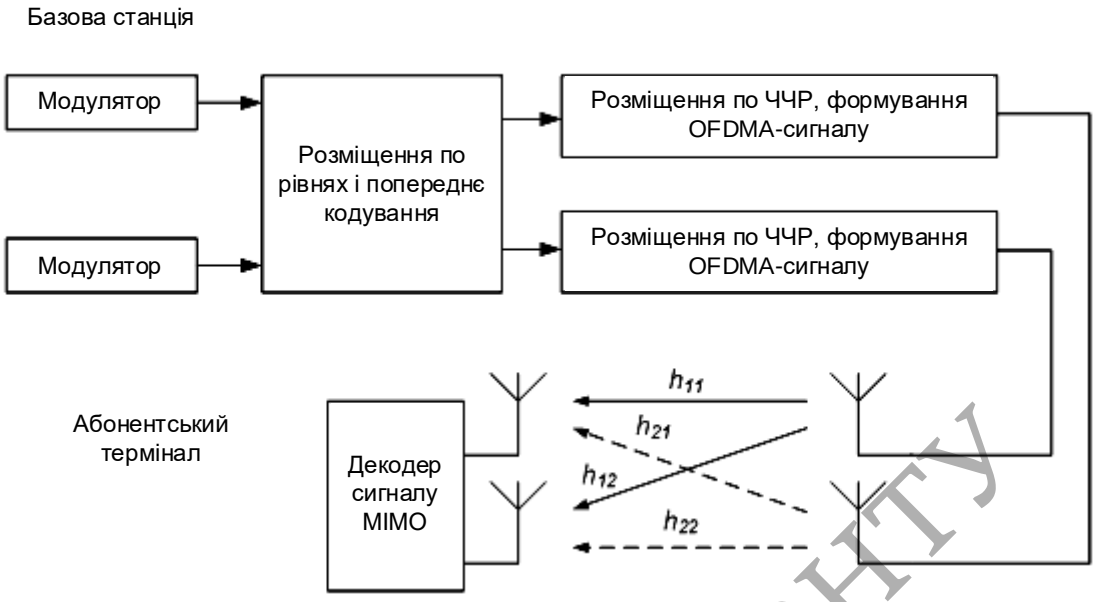


Рисунок 3.2 - Система MIMO з двома передавальними і двома приймаючими антенами (ЧЧР - частотно-часовий розподіл)

Дійсно, якщо в який-небудь момент часу на одній з підносійних перша антена передає комплексний модуляційний символ, друга антена в цей же момент часу на тій же підносійній.

Тоді, аналогічно (3.4) на першій і другій приймальних антенах в даний момент часу на одній підносійній буде присутнім сигнал з відліковими значеннями

$$r_1 = h_{11} \cdot x_1 - h_{21} \cdot x_2; \qquad r_2 = h_{12} \cdot x_1 - h_{22} \cdot x_2 \qquad (3.6)$$

Якщо оцінні значення коефіцієнтів передавальної характеристики відомі, то передавані паралельно символи і можна визначити, вирішивши систему з двох лінійних рівнянь.

Узагальнена структурна схема системи зв'язку, заснована на технології MIMO з STC (Space - Time Coding) і що має передавальні і приймальні антени наведена на рис.3.3.

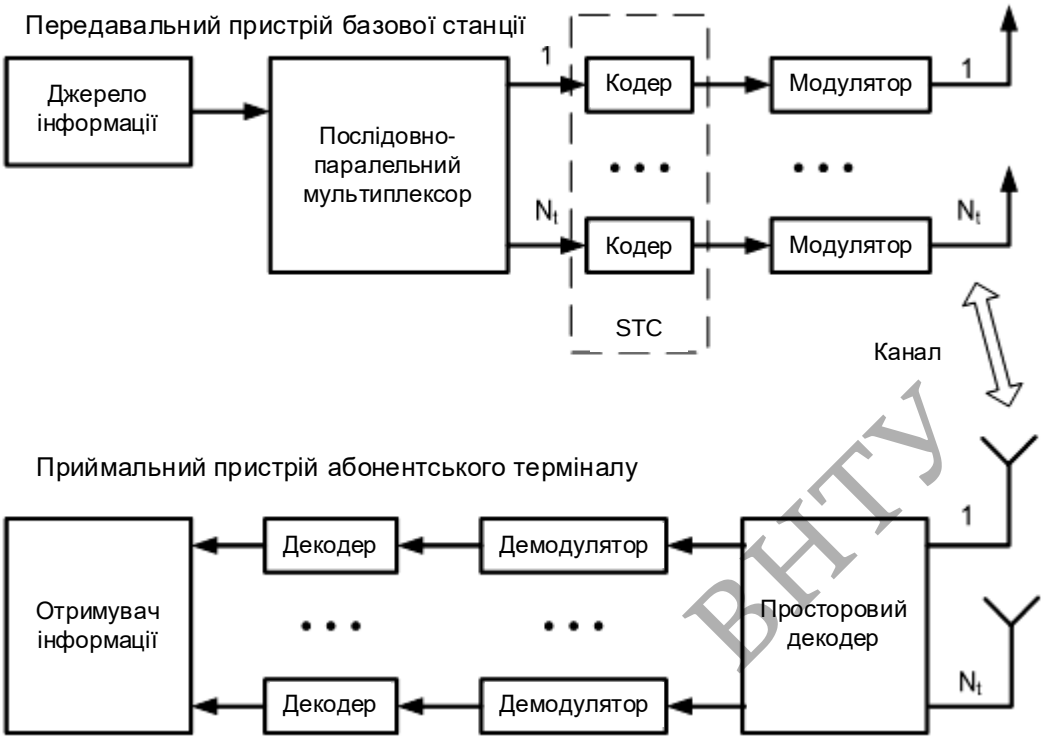


Рисунок 3.3 - Узагальнена структурна схема системи зв'язку заснована на технології MIMO з STC

За цією схемою потік послідовних інформаційних сигналів за допомогою демультиплексора розбивається на паралельні підпотоки. Кожен підпотік кодується просторово-часовим кодом і після модуляції випромінюється просторово відповідною антеною. Усі паралельні підпотоки випромінюються одночасно (синхронно) в одній і тій же смузі частот.

Випромінювальні потоки створюють сумарні сигнали (спостереження) на вході кожної з приймальних антен. Сигнал на вході кожної з приймальних антен є сумішшю сигналів, помножених на комплексні передавальні функції відповідних передавальних антен і каналу зв'язку. Вектор прийнятих сигналів є добутком матриці каналу на вектор сигналів, що випромінюються. Матриця каналу вважається відомою на приймальній стороні. У приймачі вирішується завдання розподілу і оцінки сигналів, що випромінюються, шляхом вирішення системи рівнянь.

Блок MIMO-антен є частковим випадком адаптивних антенних грат (ААР). ААР - тип антени, в якій динамічна зміна параметрів і характеристик антен

змінюється адаптивний до дій зовнішніх або внутрішніх чинників. Останнім часом активно розвивається напрям MIMO систем зв'язку, в яких ААР використовуються як на приймальній стороні, так і на передавальній стороні [16, 17].

Адаптивні антени - це об'єднання антенних грат і цифрової обробки сигналів (digital signal processing, DSP) для формування оптимальної діаграми спрямованості в просторі. Це дозволяє системі міняти напрям випромінювання, адаптуючись до умов передачі сигналу, що призводить до істотного покращення характеристик радіозв'язку. Існують дві основні категорії адаптивних антен (смарт-антен) відповідно до їх функцій:

– з перемиканням променю - з фіксованою кількістю променів певної форми або їх об'єднанням в різних комбінаціях по секторах;

– адаптивні грати - з необмеженою кількістю форм ДН, які настроюються під час роботи на потрібний напрям (рис.3.4)

–

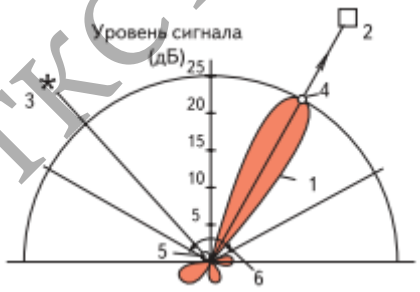


Рисунок 3.4 - ДН адаптивної антени базової станції
з сектором сканування 120°

Адаптація підвищує якість прийому сигналу. У широкому сенсі технологія ААР припускає використання інтелектуальних алгоритмів, реалізованих за допомогою цифрових сигнальних процесорів. Ці алгоритми розділяють сигнали по векторах поширення; потім на їх основі адаптивний коригується ДН передавальних антен.

У адаптивних антенних гратах можлива адаптація не лише діаграми спрямованості, але і інших параметрів, таких як захисний інтервал OFDM сигналу та ін.

Адаптивні приймальні грати застосовуються для зменшення або виключення спрямованих завад за допомогою адаптивного придушення або адаптивного формування нулів, що приводить до поліпшення відношення сигнал-шум. На основі одних видів адаптивних алгоритмів адаптивні приймальні грати можуть «самонастроюватись», тобто автоматично перебудовуватися у бік сигналу при невідомому заздалегідь напрямі його приходу і відділяти цей сигнал від спрямованих завад, поки напрями їх приходу відмінні від напряму приходу сигналу.

3.2 Розрахунок адаптивних антенних грат

Адаптивні антенні грати - це антенна система, що є фазованими антенними гратами (ФАР) і сукупністю аналого-цифрових каналів із загальним фазовим центром. ДН адаптивних антенних грат формується в цифровому виді, без фазообертачів.

Сучасні технології цифрових антенних грат (ЦАР) своїм масовим розвитком зобов'язані інтеграції процесорів цифрової обробки сигналів (у вигляді DSP - digital signal processing або на програмованих логічних інтегральних схемах - ПЛІС) з аналого-цифровими і цифро-аналоговими перетворювачами (АЦП/ЦАП) у рамках одного модуля або навіть чіпа.

Ключова особливість ЦАР - цифрове формування променів діаграми спрямованості (ДН) антени. У завданнях зв'язку це дозволяє динамічно оптимізувати обслуговувану зону покриття, оперативно перенацілюючи цифрові приймально-передавальні промені (рис.3.5) залежно від територіального розподілу абонентів.

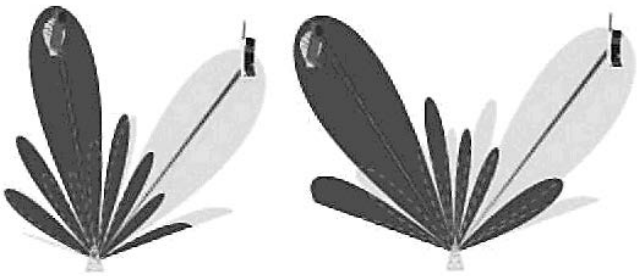


Рисунок 3.5 - Адаптивне управління ДН антени базової станції

Сузір'я променів, що синтезується, наприклад, по алгоритмах швидкого перетворення Фур'є є, по суті, сукупністю просторово-частотних фільтрів, кожен з яких здійснює селекцію строго визначеного набору сигналів і придушує інші, сприйняті як завади.

3.2.1 Постановка завдання

Проектовані адаптивні антенні грати (ААР) призначені для мережі абонентського радіодоступу на робочій частоті 1800 МГц.

ААР повинна складатися з лінійних антенних грат, сформованих з чотирьох антенних елементів. Ширина ДН кожного антенного елементу на рівні - 3 дБ повинна складати близько 30°, в секторі сканування 120°.

Розрахунок АР здійснимий на базі куткової антени [16-20].

3.2.2 Основні співвідношення для розрахунку куткової антени

Куткова антена (рис.3.6) складається з куткового рефлектора, виготовленого з двох плоских металевих пластин, що утворюють деякий кут ψ, і вібратора, розташованого в площині бісектриси цього кута [16, 17]. При належному виборі величини кута Ψ і відстані S від осі вібратора до вершини кута виходить сприятливе складання повної хвилі, відбитої від рефлектора і хвилі, що створюється безпосередньо випромінюванням вібратора. При цьому максимальне випромінювання виходить у напрямі кута ψ.

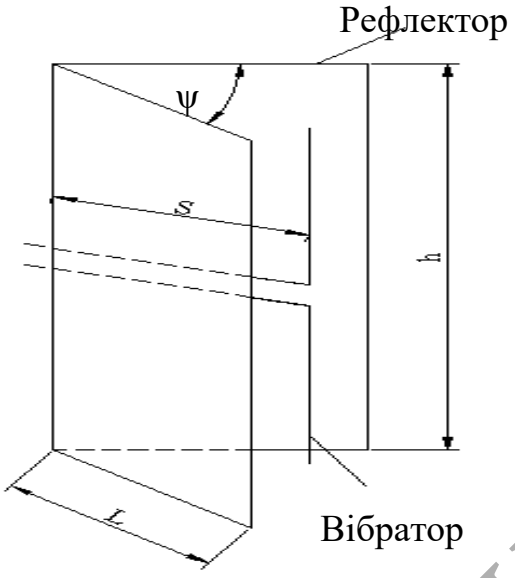


Рисунок 3.6 - Ескіз куткової антени

Розрахуємо основні геометричні розміри антени, виходячи із співвідношень, поміщених в таблицю.3.1. У приведеній таблиці використані наступні позначення:

φ - кут, утворений напрямом променя і бісектрисою кута ψ

E_0 - напруженість поля опромінюючого вібратора в площині, нормальній його осі за відсутності рефлектора;

k - хвильове число.

Таблиця 3.1 - Основні розрахункові співвідношення

Величина	Значення, при куті ψ		
	45	60	90
S/λ	0,5-1	0,35-0,8	0,25-0,75
l	$\geq 2\lambda$	$\geq 1,5\lambda$	$\geq\lambda$
E	$2E_0\{\cos(k_S\cos\varphi)+\cos(k_S\sin\varphi) - \cos[k_S\cos(45 -\varphi)]- \cos[k_S\sin(45+\varphi)]\}$	$2E_0\{\sin(k_S\cos\varphi) - \sin[k_S\cos(60 -\varphi)]- \sin(k_S\cos\theta(60+\varphi)]\}$	$2E_0[\cos(k_S\cos\varphi) - \cos(k_S\sin\varphi)]$

Висота рефлектора одиничної куткової антени визначається по формулі:

$$h = 2 \cdot l + D + 2 \cdot a, \qquad (3.7)$$

де a - відстань від краю рефлектора до крайньої точки проекції опромінюючого лінійного вібратора на рефлектор;

l - довжина вібратора;

D - відстань між вібраторами.

$$a = (0{,}1 - 0{,}15)\lambda. \quad (3.8)$$

Довжина і діаметр вібраторів повинні задовольняти умові: $d/l = (0{,}2 - 0{,}05)$;

Функція спрямованості куткової антени в Н-площині при ψ=90 град. обчислюється за формулою:

$$F(\varphi) = \cos(kS \cdot \cos\varphi) - \cos(kS \cdot \sin\varphi), \quad (3.9)$$

де - відстань від осі вібратора до вершини кута;

φ- азимутний кут, відлічуваний від бісектриси секторного кута, і має діапазон зміни від .

Функція спрямованості куткової антени в Е - площини при град. обчислюється за формулою:

$$F(\theta) = F_{\text{обл}}(\theta) \cdot cos^2\left(\frac{kS \cdot \cos\theta}{2}\right), \quad (3.10)$$

де $F(\theta)$ - функція спрямованості опромінювача (наприклад, у вигляді симетричного електричного вібратора);

θ – меридіональний кут, який лежить в площині опромінювача, і змінюється від 0 до π.

Примітка. Функція спрямованості симетричного вібратора з довжиною плеча l визначається як:

$$F_{\text{обл}}(\theta) = \frac{\cos(kl \cdot \cos\theta) - \cos(kl)}{\sin(\theta) \cdot (1 - \cos(kl))}. \quad (3.11)$$

Функція спрямованості куткової антени в Н-площині при ψ=60 град. обчислюється за формулою

$$F(\varphi) = \sin(kS \cdot \cos\varphi) - \sin\left(kS \cdot \cos\left(\frac{\pi}{3} - \varphi\right)\right) - \sin\left(kS \cdot \cos\left(\frac{\pi}{3} + \varphi\right)\right), \quad (3.12)$$

Для куткової антени при град. функція спрямованості в Е - площині обчислюється за формулою

$$F(\theta) = \cos\left(\frac{kS \cdot \cos\theta}{2}\right) \cdot \cos^2\left(\frac{kS \cdot \cos\theta}{4}\right) \cdot \quad (3.13)$$

КНД куткової антени при град визначається як:

$$D = 4 \cdot D_0 \cdot (1 - \cos kS)^2 \cdot \frac{R_{\Sigma 0}}{R_{\Sigma}}. \quad (3.14)$$

КНД куткової антени при ψ=60 град визначається як:

$$D = 4 \cdot D_0 \cdot \left(\sin kS - 2 \cdot \sin\left(\frac{kS}{2}\right)\right)^2 \cdot \frac{R_{\Sigma 0}}{R_{\Sigma}}. \quad (3.15)$$

У цих виразах D_0 і $R_{\Sigma 0}$ - КНД і опір випромінювання опромінювача у вільному просторі;

R_{Σ} – опір випромінювання опромінювача у складі куткової антени.

3.2.3 Розрахунок параметрів куткової антени

Необхідно розрахувати куткову антену для частоти f=1800 МГц (λ - довжина хвилі, l - довжина плеча вібратора, h - висота рефлектора, L - ширина стінки рефлектора, S - відстань від осі вібратора до вершини кута рефлектора).

$$f = 1{,}8 \cdot 10^9 \text{ Гц}, \qquad c = 3 \cdot 10^8 \frac{\text{м}}{\text{с}}, \qquad \lambda = \frac{c}{f} \text{ м}, \qquad \lambda = \frac{3 \cdot 10^8}{1{,}8 \cdot 10^9} = 0{,}167, \text{м}$$

$$\alpha = 2 \cdot \frac{\pi}{\lambda}, \ \alpha = 37{,}699 \ \ l = 0{,}55 \cdot \lambda, \quad h = 0{,}8 \cdot \lambda, \quad L = 1{,}5 \cdot \lambda$$

При куті розкриву антени 90 град, ДН в площині Н (рис.3.7) розраховується як:

$$FH90(S, \varphi) = \cos(kS \cdot \cos\varphi) - \cos(kS \cdot \sin\varphi). \qquad (3.16)$$

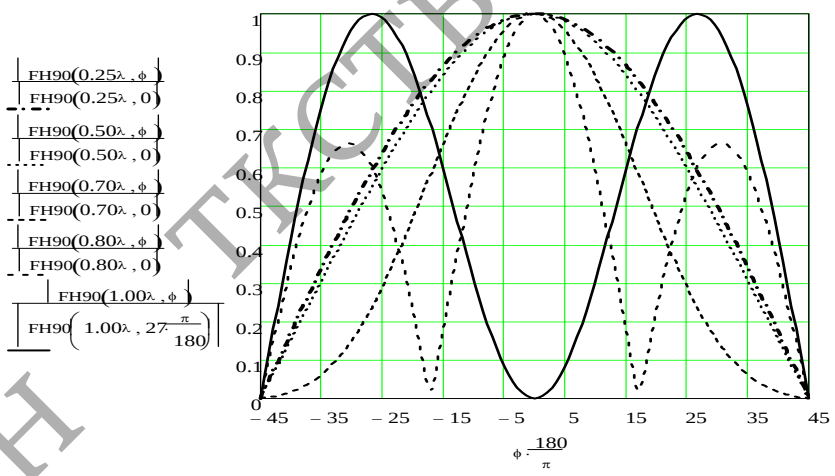


Рисунок 3.7 - ДН куткової антени в площині Н при куті розкриву 90 град

ДН у вигляді півхвильового вібратора (рис.3.8) обчислюється за формулою:

$$F_{\text{обл}}(\theta) = \frac{\cos(kl \cdot \cos\theta) - \cos(kl)}{\sin(\theta) \cdot (1 - \cos(kl))}. \qquad (3.17)$$

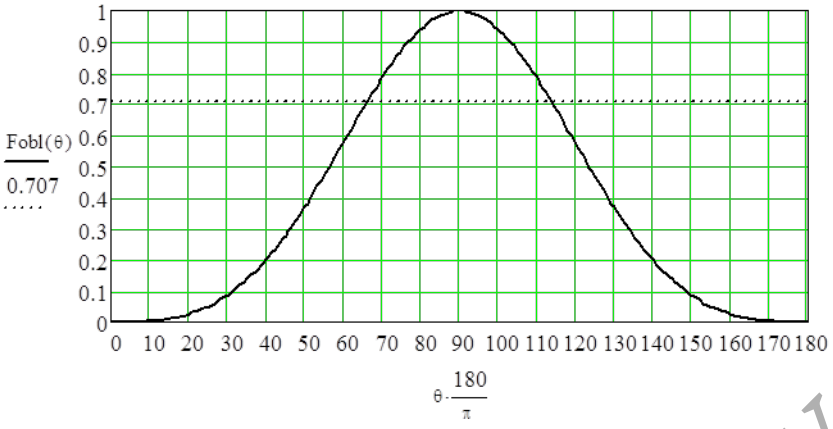


Рисунок – 3.8 ДН півхвильового вібратора

Діаграма спрямованості одиничної куткової антени з опромінювачем у вигляді півхвильового вібратора і куті розкриву антени 90 град в площині Е (рис.3.9) визначається по формулі:

$$FE90(S,\theta) = F_{обл}(\theta) \cdot \left(\cos\left(k \cdot \frac{S \cdot \cos\theta}{2}\right)\right)^2, \qquad (3.18)$$

де θ - кут, відлічуваний від осі вібратора.

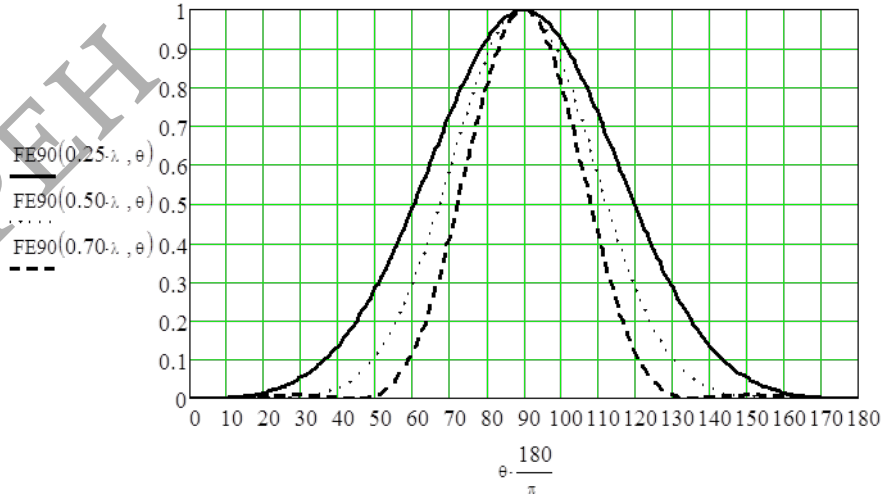


Рисунок 3.9 - ДН куткової антени з кутом розкриву 90 град опромінюваною півхвильовим вібратором в площині Е

Діаграма спрямованості поодинокої куткової антени з опромінювачем у вигляді півхвильового вібратора і куті розкриву антени 60 град в площині (рис. 3.10) визначається по формулі:

$$FH(S,\varphi) = \sin(kS\cdot\cos\varphi) - \sin\left(kS\cdot\cos\left(\frac{\pi}{3}-\varphi\right)\right) - \sin\left(kS\cdot\cos\left(\frac{\pi}{3}+\varphi\right)\right), \qquad (3.19)$$

ДН поодинокої куткової антени з опромінювачем у вигляді півхвильового вібратора і куті розкриву антени 60 град в площині Е (рис. 3.11) визначається по формулі:

$$FE60(S,\theta) = \left|F_{обл}(\theta)\cdot\left(\cos\left(k\cdot\frac{S\cdot\cos\theta}{4}\right)\right)^2\cdot\cos\left(k\cdot\frac{S\cdot\cos\theta}{2}\right)\right| \qquad (3.20)$$

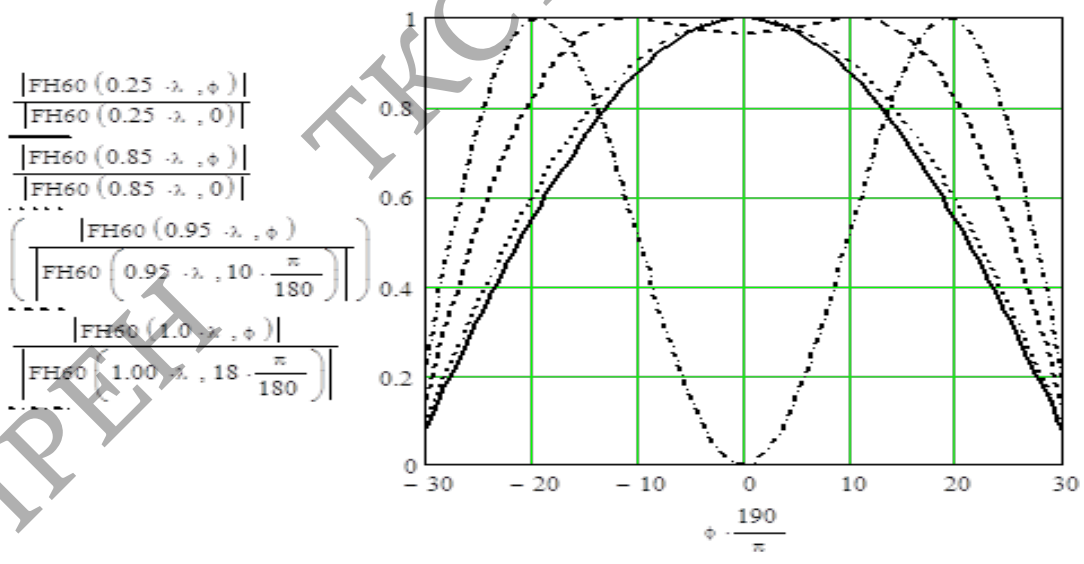


Рисунок 3.10 - ДН куткової антени з кутом розкриву 60 град опромінюваною півхвильовим вібратором в площині Н

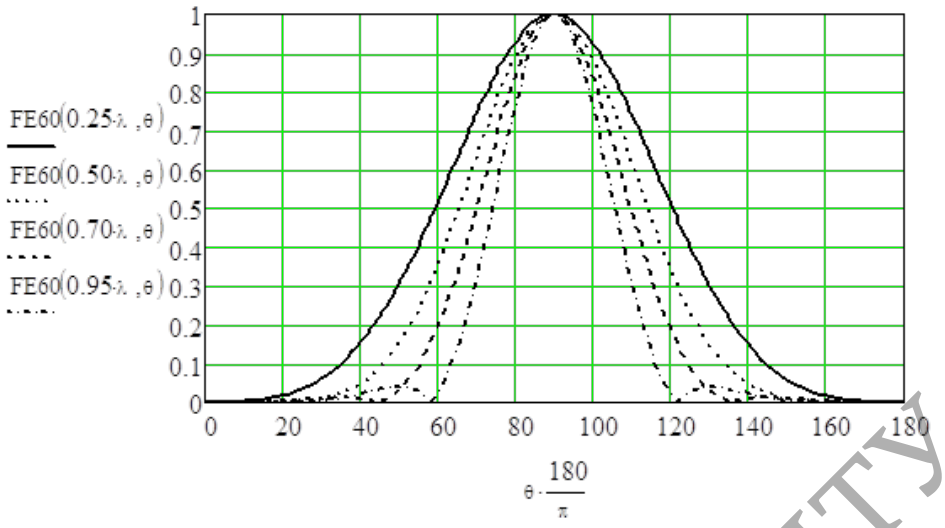


Рисунок 3.11 - ДН куткової антени з кутом розкриву 60 град опромінюваною півхвильовим вібратором в площині Е

Далі розрахуємо опір випромінювання і КНД куткової антени з вібратором для кутів розкриву антени 60 і 90 град. методом наведених ЭДС. Вплив рефлектора приблизно врахований методом дзеркальних зображень [16, 17].

$$D_0 = 1{,}64 \qquad R_{\Sigma 0} = 73{,}1 \text{ Ом.}$$

$$R_{vz}(dl) = 30 \cdot \left[2 \cdot Ci(2 \cdot \pi \cdot dl) - Ci\left(\sqrt{\pi^2 + (2 \cdot \pi \cdot dl)^2} - \pi\right) - Ci\left(\sqrt{\pi^2 + (2 \cdot \pi \cdot dl)^2} + \pi\right)\right]$$

$$R_{\Sigma}90(S\lambda) = R_{\Sigma 0} - 2 \cdot R_{vz}\left(S\lambda \cdot \sqrt{2}\right) + R_{vz}(2 \cdot S\lambda), \quad R_{vz}(0{,}7) = -24{,}863$$

$$R_{\Sigma}60(S\lambda) = R_{\Sigma 0} - 2 \cdot R_{vz}(S\lambda) + R_{vz}\left(S\lambda \cdot \sqrt{3}\right) - R_{vz}(2 \cdot S\lambda), Sl = 0{,}2; 0{,}205 \ldots 1$$

$$D90(S\lambda) = 4 \cdot D_0(1 - \cos(2 \cdot \pi \cdot S\lambda))^2 \cdot \frac{R_{\Sigma 0}}{R_{\Sigma}90(S\lambda)}$$

$$D60(S\lambda) = 4 \cdot D_0\left[\left(\sin(2 \cdot \pi \cdot S\lambda) - 2 \cdot \sin\left(2 \cdot \pi \cdot \frac{S\lambda}{2}\right)\right)^2\right] \cdot \frac{R_{\Sigma 0}}{R_{\Sigma}60(S\lambda)}$$

На рис. 3.12, 3.13 приведені залежності і від співвідношення для різних кутів розкриву антени.

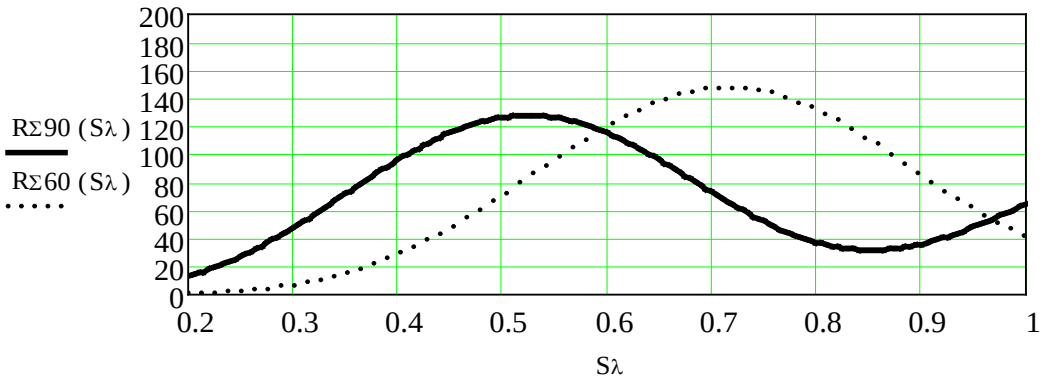


Рисунок 3.12 - Залежність R_Σ від співвідношення S / λ для кутів розкриву антени 60 і 90 град

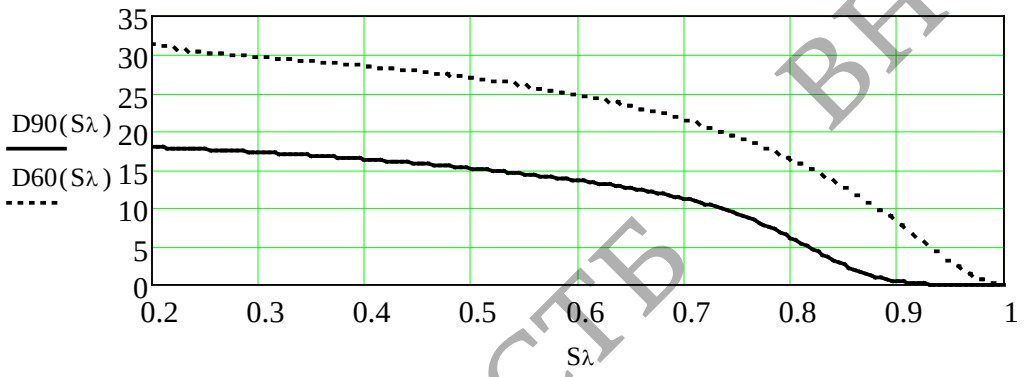


Рисунок 3.13 - Залежність D від співвідношення S / λ для кутів розкриву антени 60 і 90 град

3.2.4 Розрахунок ДН синфазних куткових грат

При розрахунку приймемо наступні позначення:

k – хвилеве число;

N – кількість елементів грат;

d – відстань між вібраторами (крок грат);

a – відстань від краю рефлектора до крайньої точки проекції опромінюючого лінійного вібратора на рефлектор

При побудові лінійної АР зазвичай приймається, що випромінювачі розташовані на одній прямій, віддаленій від кута рефлектора на відстані (у нашому випадку м) і на однакових відстанях один від одного). Вібратори збуджуються синфазно або для відхилення діаграми спрямованості від нормалі з різницею фаз.

ДН прямолінійних однорідних грат з використанням принципу перемножування ДН може бути отримана з виразу:

$$f_{syst}(S,\theta)=F(S,\theta)\cdot f_p(\theta) \qquad (3.21)$$

де $F(S,\theta)$ - ДН одиничної куткової антени;

$f_p(\theta)$ – множник антенних грат (рис.3.14), який визначається як [16, 17]:

$$f_p(\theta)=\frac{\sin\left[\frac{N\cdot k\cdot d\cdot(\cos(\theta)-\alpha)}{2}\right]}{N\cdot\sin\left[\frac{l\cdot k\cdot d\cdot(\cos(\theta)-\alpha)}{2}\right]} \qquad (3.22)$$

Розрахунки виконані для значень:

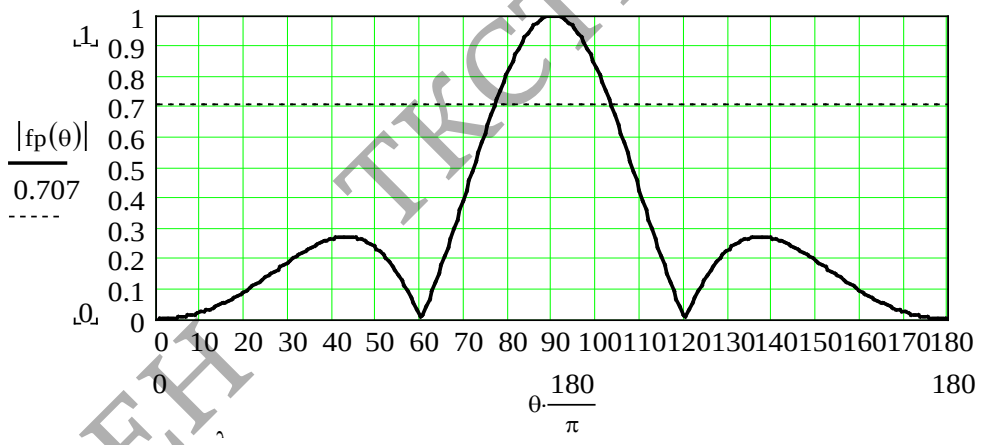


Рисунок 3.14 - ДН множника антенних грат

ДН антенних грат в цілому (з урахуванням ДН куткової антени, кут розкриву 90 град, площина Е, рис.3.15) визначається як [16, 17]:

$$f_{syst}(S,\theta)=FE90(S,\theta)\cdot f_p(\theta) \qquad (3.23)$$

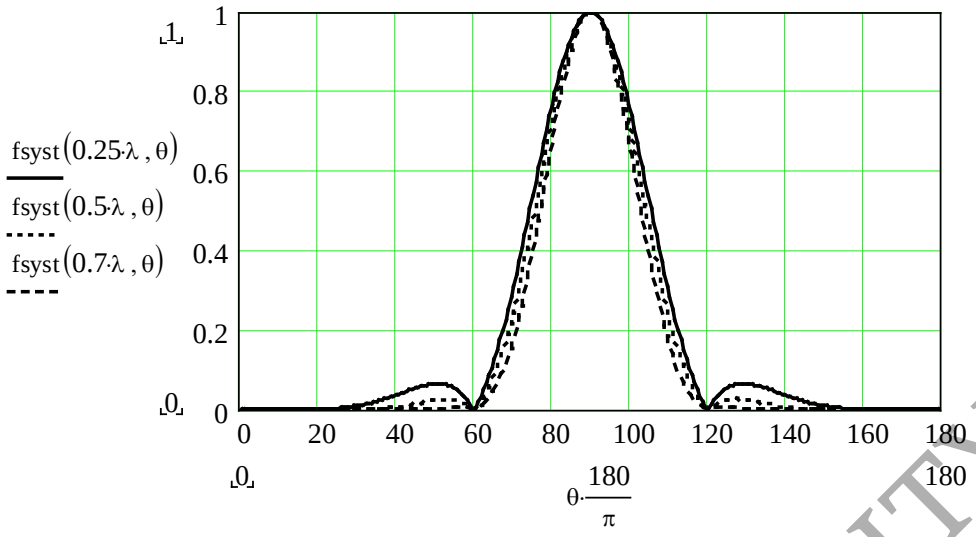


Рисунок 3.15 - ДН антенних грат в площині Е

(кут розкриву 90 град)

Діаграма спрямованості грат в площині Н (рис3.16) - це діаграма спрямованості поодинокої куткової антени в цій площині.

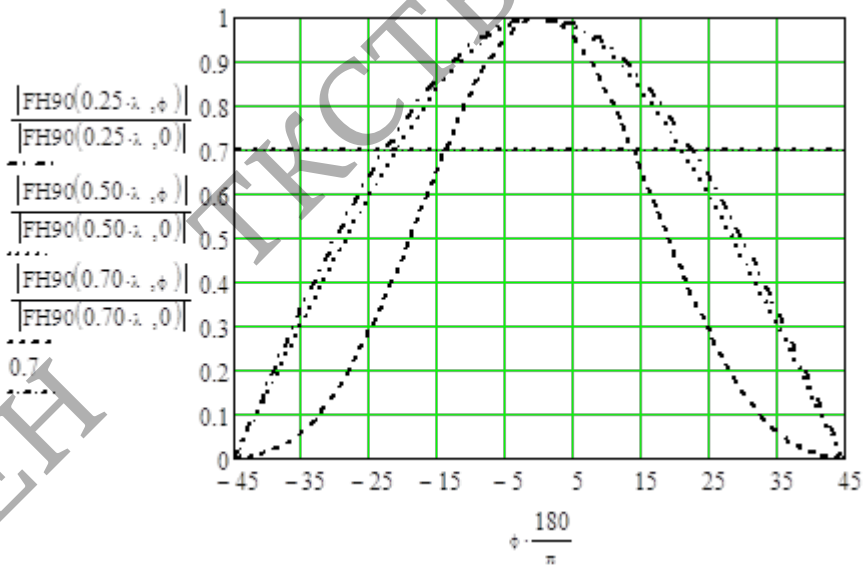


Рисунок 3.16 - ДН антенних грат в площині Н

(кут розкриву 90 град)

ДН антенних грат в площині Е рис.3.17 визначається діаграмою спрямованості куткової антени, кут розкриву 60 град і множником антенних грат.

$f3_{syst}(S,\theta)=FE60(S,\theta)\cdot f_p(\theta)$

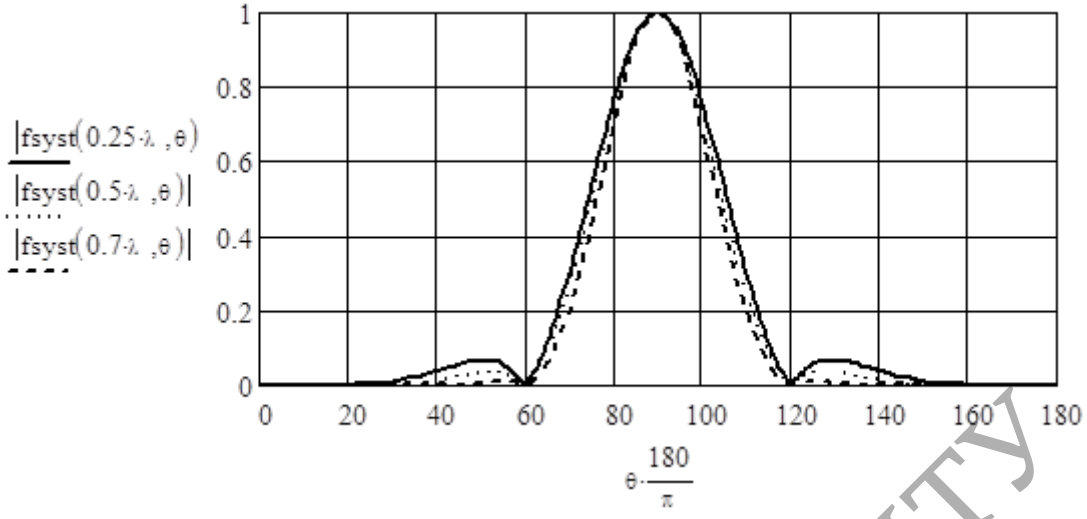


Рисунок 3.17 - ДН антенних грат в площині Е
(кут розкриву 60 град)

ДН грат в площині Н для кута розкриву 60 град. (рис3.18) - це діаграма спрямованості одиничної куткової антени з тим же кутом розкриву і в цій же площині [16, 17].

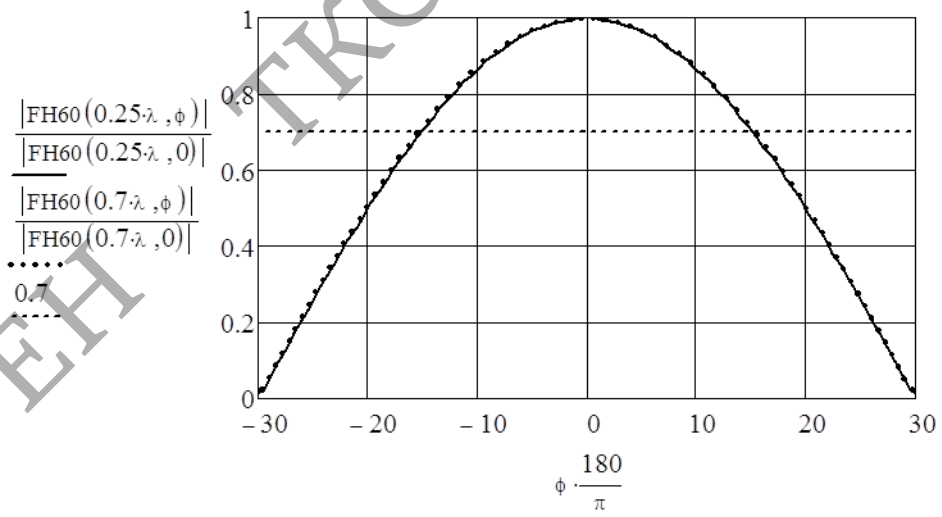


Рисунок 3.18 - ДН антенних грат в площині Н
(кут розкриву 60 град)

3.2.5 Розрахунок розмірів антенних грат

Висота антенних грат визначається як [16, 17]:

$$h = l \cdot 4 + 2a,$$

де l - довжина опромінювача;

$a = 0{,}1 \cdot \lambda$ - відстань від краю рефлектора до крайньої точки проекції опромінюючого лінійного вібратора на рефлектор.

Тогда $h = 0{,}5 \cdot \lambda \cdot 4 + 2 \cdot 0{,}1 \cdot \lambda = 0{,}348$ м.

Ширина бічної площини куткової антени визначається з вираження:

$$L(\psi) := \begin{cases} \lambda & \text{if } \psi = 90 \\ (\lambda \cdot 1.5) & \text{if } \psi = 60 \\ (\lambda \cdot 2) & \text{if } \psi = 45 \end{cases}$$

Тоді розмір бічної площини складає (м) :

- для кута розкриву антени 60 град

- для кута розкриву антени 90 град

Розраховані дані зведемо в таблиці. 3.2.

Таблиця 3.2 - Розраховані розміри куткової антени

Розмір антени	При куті розкриву антени (ψ^o)	
	60	90
Ширина бічної площини антени L, мм	237	158
Висота антени h, мм	348	348
Відстань від ребра куткового екрану антени до вібратора S, мм	95	79
Діаметр вібратора d, мм	4,3	
Довжина поодинокого вібратора l, мм	87	

Для побудови систем зв'язку найбільш підходить антена з кутом розвороту - 60^o, оскільки у неї найменша ширина ДН при найменшому рівні бічних пелюсток і найбільшому коефіцієнті підсилення.

3.3 Побудова адаптивних антенних грат для базової станції

Антенні грати базової станції повинні забезпечувати широку діаграму спрямованості в горизонтальній площині і можливість зміни положення цієї діаграми у вертикальній площині. В ряді практичних випадків необхідно мати у вертикальній площині вузьку діаграму спрямованості. І в тому і в іншому випадках це можна реалізувати [16, 17] за допомогою фазованих антенних грат (рис.3.19).

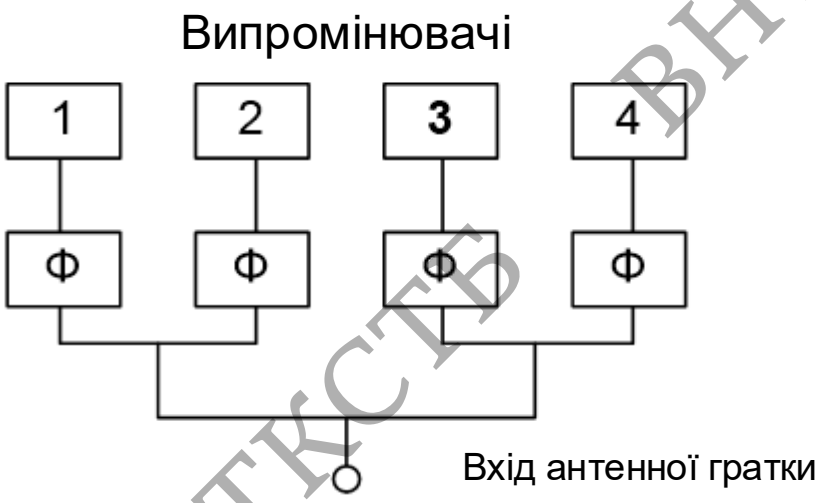


Рисунок 3.19 - Структурна схема антенних грат

При рівних значеннях фазообертачів максимальне випромінювання грат перпендикулярне її осі, а при зміні положень фазообертачів відбувається гойдання ДН антенних грат.

За цією схемою можуть бути реалізовані лінійні антенні грати з керованим положенням ДН на основі куткових антен.

Управління положенням діаграми спрямованості може бути виконане із застосуванням цифрових антенних грат. Цифрові антенні грати - це антенна система, що є фазованими антенними гратами (ФАР) і сукупністю аналого-цифрових каналів із загальним фазовим центром, в якій ДН формується в цифровому виді, без фазообертачів. Структурна схема адаптивних антенних грат з цифровим формуванням променя представлена на рис.3.20. Ця схема дозволяє

реалізувати приймально-передавальні грати. Передавальний канал антенної системи має внутрішній блок (входить до складу внутрішніх блоків базової станції) і зовнішній блок (представлений лінійним підсилювачем потужності, що входить до складу модуля попередньої обробки сигналів). Перемикання антенних грат в режим передачі здійснюється за допомогою диплексера.

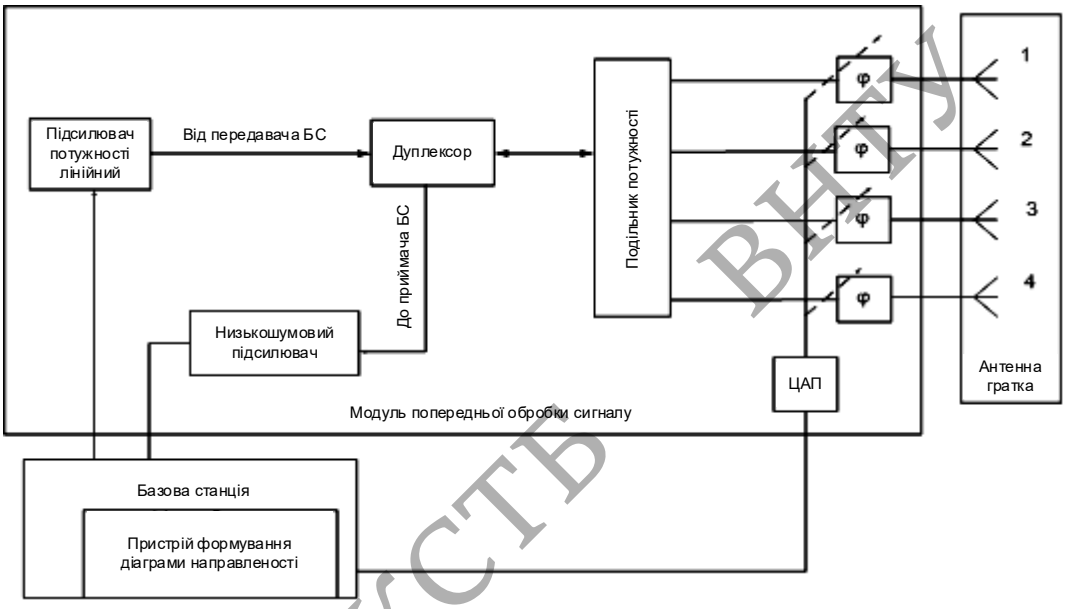


Рисунок 3.20 - Структурна схема проектованої АР

Ця антена по своїх технічних параметрах близька до параметрів антен базової станції Spotlight компанії Metawave. Це дає можливість використовувати побудовану АР у складі базової станції системи абонентського радіодоступу.

4 ЕКОНОМІЧНА ЧАСТИНА

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 «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» 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.

4.1 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 «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» 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. 4.1 та 4.2.

Таблиця 4.1 – 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	0	0	0
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)	40	40	40
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		40,0		

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 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (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	65	0	60
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	0	55	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	60,0		

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 [69]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \quad (4.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 40,0, k_{теор} = 60,0$ балів;

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

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 40,0 + 0,4 \cdot 60,00 = 48,00 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 4.3.

Таблиця 4.3 – 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 «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу», даний рівень становить 48,00 балів і відповідає статусу - достатній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.2.1 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 [69]:

$$З_о = \sum_{i=1}^{k} \frac{М_{ni} \cdot t_i}{T_p}, \quad (4.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

$М_{ni}$ – 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.

$$З_о = 11340{,}00 \cdot 21 / 21 = 11340{,}00 \; грн.$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
1. Керівник проекту	11340,00	540,00	21	11340,00
2. Ст. науковий співробітник	10100,00	480,95	18	8657,14
3. Інженер-програміст в сфері захисту інформації	9570,00	455,71	12	5468,57
4. Фахівець-консультант питань радіотелефонії	10100,00	480,95	7	3366,67
Всього				28832,38

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \qquad (4.3)$$

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:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \qquad (4.4)$$

де $М_М$ – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=2379,00 грн;

$К_і$ – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [69];

$К_с$ – 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.

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

$t_{зм}$ – тривалість зміни, год.

$С_1 = 2379{,}00 \cdot 1{,}10 \cdot 1{,}5 / (21 \cdot 8) = 23{,}37$ *грн.*

$З_{р1} = 23{,}37 \cdot 13{,}50 = 315{,}43$ *грн.*

Таблиця 4.5 – 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
1. Встановлення допоміжного обладнання	13,50	2	1,10	23,37	315,43
2. Інсталяція програмного забезпечення	8,00	4	1,50	31,86	254,89
3. Встановлення радіо-модулів	16,00	5	1,70	36,11	577,76
4. Налагодження системи	1,50	5	1,70	36,11	54,16
Всього					1202,24

Додаткова заробітна плата дослідників та робітників

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

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.5)$$

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

$З_{дод}$ = (28832,38 + 1202,24) · 11 / 100% = 3303,81 грн.

4.2.2 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:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.6)$$

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

Зн = (28832,38 + 1202,24 + 3303,81) · 22 / 100% = 7334,46 грн.

4.2.3 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 «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу».

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 (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \qquad (4.7)$$

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

n – кількість видів матеріалів;

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

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

B_j – маса відходів *j*-го найменування, кг;

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

M_1 = *5,00 · 112,00 · 1,1 - 0,000 · 0,00 = 616,00 грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.6 – 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 білий (80%)	112,00	5,00	0,000	0,00	616,00
Диск оптичний (CD-R)	12,30	5,00	0,000	0,00	67,65
Органайзер офісний BOX-16A	135,00	4,00	0,000	0,00	594,00
Канцелярське приладдя	195,00	4,00	0,000	0,00	858,00
Тонер HP-26 (для заправки картриджа)	6214,00	0,12	0,000	0,00	820,25
FLASH-пам'ять	305,00	2,00	0,000	0,00	671,00
Всього					3626,90

4.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.8)$$

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 … 1,15*).

$К_в = 1 \cdot 5600,00 \cdot 1,1 = 6160,00$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Модуль підтримки цифрового потоку для АТС Zycoo CooVox U50, U80 і U100	1	5600,00	6160,00
Escene ES410PE - телефон	2	2940,00	6468,00
MikroTik - маршрутизатор	1	2240,00	2464,00
Escene ESH12 - професійна гарнітура для телефонів і інтерфейсом RJ9 для підключення телефонної трубки	2	1120,00	2464,00
Всього			17556,00

4.2.5 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:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (4.9)$$

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.

$B_{спец}$ = *1650,00 · 1 · 1,11 = 1831,50 грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Роутер	1	1650,00	1831,50
Термінальне обладнання	1	6300,00	6993,00
CooVox EX16S - шістнадцятиканальний FXS шлюз з підтримкою VoIP і SIP Zyccо	1	12460,00	13830,60
Всього			22655,10

4.2.6 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:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i, \quad (4.10)$$

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.

$B_{прг} = 8200{,}00 \cdot 1 \cdot 1{,}2 = 9840{,}00$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Windows	1	8200,00	9840,00
Microsoft Office	1	5700,00	6840,00
Пакет обробки даних	1	18320,00	21984,00
Всього			38664,00

4.2.7 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:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.11)$$

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.

$A_{обл} = (28700{,}00 \cdot 1) / (3 \cdot 12) = 797{,}22$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Комп'ютеризований програмно-аналітичний комплекс	28700,00	3	1	797,22
Монтажне обладнання	9576,00	5	1	159,60
Програмне забезпечення підтримки радіотелефонії	30568,00	2	1	1273,67
Місце оператора спеціалізоване	9780,00	5	1	163,00
Офісна оргтехніка	12300,00	4	1	256,25
Дослідницька лабораторія	250000,00	25	1	833,33
Всього				3483,07

4.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \qquad (4.12)$$

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

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо Ц$_e$ = 4,05 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

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

$B_e = 0,05 \cdot 40,0 \cdot 4,05 \cdot 0,95 / 0,97 = 8,10$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Модуль підтримки цифрового потоку для АТС Zycoo CooVox U50, U80 і U100	0,05	40,0	8,10
Escene ES410PE - телефон	0,01	40,0	1,62
MikroTik - маршрутизатор	0,03	40,0	4,86
Роутер	0,03	80,0	9,72
Термінальне обладнання	0,32	80,0	103,68
CooVox EX16S - шістнадцятиканальний FXS шлюз з підтримкою VoIP і SIP Zyccо	0,06	40,0	9,72
Місце оператора спеціалізоване	0,42	160,0	272,16
Комп'ютеризований програмно-аналітичний комплекс	0,75	160,0	486,00
Монтажне обладнання	0,04	5,0	0,81
Офісна оргтехніка	0,96	32,0	124,42
Всього			1021,09

4.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» 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:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.13)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 25%.

$B_{св}$ = (28832,38 + 1202,24) · 25 / 100% = 7508,66 грн.

4.2.10 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:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.14)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 40%.

$B_{сп}$ = *(28832,38 + 1202,24) · 40 / 100% = 12013,85 грн.*

4.2.11 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:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.15)$$

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

$I_в$ = *(28832,38 + 1202,24) · 60 / 100% = 18020,78 грн.*

4.2.12 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:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.16)$$

де $H_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$$B_{нзв} = (28832,38 + 1202,24) \cdot 100 / 100\% = 30034,63 \text{ грн.}$$

Витрати на проведення науково-дослідної роботи на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + B_{спец} + B_{прг} + A_{обл} + B_е + B_{св} + B_{сп} + I_в + B_{нзв}. \quad (4.17)$$

$B_{заг}$= 28832,38 +1202,24 +3303,81 +7334,45557 +3626,90 +17556,00 +22655,10 + 38664,00 + 3483,07 +1021,09 +7508,66 +12013,85 +18020,78 +30034,63 = 195256,95 грн.

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

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.18)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,9.

$$ЗВ = 195256,95 / 0,9 = 216952,17 \text{ грн.}$$

4.3 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 «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» 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:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \qquad (4.19)$$

де I – коефіцієнт важливості роботи. Приймемо $I = 3$;

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 $T_C = 2$;

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 $R = 3$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо B =216952,17 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 [69].

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 2{,}99$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

4.4 Висновок до розділу 4

Витрати на проведення науково-дослідної роботи на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» складають 216952,17 грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково-дослідної роботи на тему «Підвищення інформаційної захищеності локальної мережі абонентського радіодоступу» є достатній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Можливість реалізації небезпеки і ступінь несприятливого впливу її на людину залежить відвідповідних факторів. У виробничій сфері фактори поділяються на вражаючі, небезпечні та шкідливі. Вражаючі фактори можуть призвести до загибелі людини. Небезпечні фактори викликають в окремих випадках травми чи раптове погіршення здоров'я (головний біль, погіршення зору, слуху, зміни психологічного та фізичного стану). Шкідливі фактори можуть спричиняти захворювання чи зниження працездатності людини як у явній, так і прихованій формах. Розподіл факторів на вражаючі, небезпечні та шкідливі – досить умовний.

Магістерська робота висвітлює дослідження підвищення інформаційної захищеності локальної мережі абонентського радіодоступу. Небезпечні та шкідливі виробничі фактори, що можуть впливати на розробника мережі (згідно ГОСТ 12.0.003-74 [2]):

1. Фізичні:

підвищена запиленість та загазованість повітря робочої зони;

підвищена чи понижена температура повітря робочої зони;

підвищений рівень шуму на робочому місці;

підвищений рівень електромагнітного випромінювання;

підвищена чи понижена іонізація повітря;

недостатня освітленість робочої зони.

2. Психофізіологічні:

статичне перевантаження;

розумове перевантаження;

емоційні перевантаження.

Відповідно до визначених факторів здійснюємо планування щодо безпечного виконання роботи.

5.1 Технічні рішення з безпечного виконання робіт.

5.1.1 Технічні рішення з організації робочого місця під час проектування

Найбільш вагомим шкідливим фактором який може впливати на працівника, що досліджує підвищення інформаційної захищеності локальної мережі абонентського радіо доступу є електромагнітні випромінювання, тому, надалі, для створення оптимальних умов праці, розглянемо рішення при роботі з джерелами електромагнітних випромінювань.

Приміщення, у яких розміщуються установки, які є джерелами ЕМП, повинні відповідати вимогам діючих санітарних норм щодо проектування промислових підприємств і за своїм планувальним рішенням відповідати характеру виконуваних у них технологічних процесів. Рівні освітлення, опалення і вентиляції приміщень повинні відповідати вимогам будівельних норм і правил.

Метеорологічні умови в приміщеннях, наявність у повітрі робочої зони шкідливих речовин, рівень шуму, а також інших несприятливих факторів виробничого середовища повинні відповідати вимогам, указаним у відповідних нормативних документах, затверджених Міністерством охорони здоров'я України.

Захисні засоби повинні відповідати вимогам правил використання і випробування захисних засобів, які використовуються в електроустановках.

При розміщенні в одному приміщенні декількох установок треба унеможливлювати перевищення ГДР при сумації енергії випромінювання. У разі можливого проходження електромагнітної енергії через будівельні конструкції в сусідні приміщення повинні вживатись заходи, які унеможливлюють опромінювання працівників при рівнях, які перевищують гранично допустимі для відповідних категорій опромінювання.

Допускається при погодженні з органами державного санітарно-епідеміологічного нагляду проведення робіт щодо настроювання і регулювання апаратури, яка є джерелом ЕМП, в екранованих приміщеннях. Робочі площі та об'єми екранованих приміщень повинні встановлюватись, виходячи з габаритів оброблюваних виробів, з урахуванням вимог безпеки при роботі з високою напругою і санітарних норм проектування промислових підприємств. Для унеможливлення перевищення ГДР за рахунок відбитого випромінювання стіни, стелю і підлогу екранованих приміщень необхідно покривати матеріалами, що поглинають ЕМВ до допустимих рівнів.

У разі спрямованого випромінювання допускається застосування поглинальних покриттів тільки на відповідних ділянках стін. В екранованих приміщеннях повинні вживатися заходи з компенсації нестачі природного світла, ультрафіолету, змін газового й аероіонного складу повітря та ін. відповідно до вимог санітарних норм і правил.

Захист персоналу від дії ЕМП досягається шляхом проведення організаційних, інженерно-технічних заходів, а також використання засобів індивідуального захисту.

До організаційних заходів належать: вибір раціональних режимів праці установок, обмеження місця і часу перебування персоналу в зоні опромінювання і т. ін.

Інженерно-технічні заходи включають раціональне розміщення обладнання, використання засобів, які обмежують надходження електромагнітної енергії на робочі місця персоналу (поглинальні матеріали, екранування).

До засобів індивідуального захисту належать захисні окуляри, щитки, шоломи, захисний одяг (комбінезони, халати з металовмісної тканини; окуляри з металовмісним склом).

Засіб захисту в кожному конкретному випадку повинен визначатись з урахуванням робочого діапазону частот, характеру робіт, необхідної ефективності захисту.

Особи (фахівці), які проводять дослідження електромагнітних випромінювань, повинні мати засоби індивідуального захисту від впливу ЕМВ.

На кожний засіб захисту повинна бути складена технічна документація з відміткою про призначення та діапазон частот, у яких цей засіб захисту може бути використаний, допустимої потужності розсіювання, забезпеченої ефективності захисту за всім діапазоном частот, на який розраховано використання даного засобу.

Виключення або обмеження випромінювання від антенних систем або відкритих хвилеводів забезпечується застосуванням:

при налагодженні високочастотної апаратури - еквівалентних навантажень;

при перевірці робіт приймальних, індикаторних, обчислювальних та систем керування - імітаторів мети;

при обробці ліній передачі енергії і антенних пристроїв - хвилеводів з використанням антенно-хвилеводних трактів вимірювальних генераторів.

Випробування установок з випромінюванням на антену повинно проводитись на спеціальних полігонах. В окремих випадках допускається проведення суворо регламентованих за часом і місцем вибіркових випробувань у приміщеннях цехів за умови виключення опромінення персоналу за інтенсивності, яка перевищує граничнодопустиму. У період роботи установок з випромінюванням на антену повинна діяти попереджувальна (звукова або світлова) сигналізація.

Екранування джерел випромінювання або робочих місць здійснюється за допомогою відбивальних екранів (стаціонарних або

пересувних). Відбивальні екрани виготовляються з металевих листів, сітки, бавовняної металовмісної тканини та ін. У поглинальних екранах використовуються спеціальні матеріали, що забезпечують поглинання випромінювання відповідної довжини хвилі. Залежно від потужності випромінювання і взаємного розміщення джерела і робочих місць конструктивне вирішення екранів може бути різним (замкнута камера, щит, чохол, штора та ін).

При випробуванні й експлуатації установок у режимі випромінювання на антену на відкритих територіях полігонів, аеродромів, метеостанціях, суднах морського і річкового флоту слід уживати заходи, спрямовані на обмеження рівня опромінювання території об'єкта, раціональне розміщення на ньому будинків і споруд, забезпечення безпечних умов для проведення робіт і пересування персоналу в зонах випромінювання антен.

Для зниження рівня опромінювання території об'єкта слід:

антени станції розміщувати на насипах (естакадах) або природних пагорбах;

обмежувати використання від'ємних кутів нахилу антени.

Службові приміщення на території об'єкта слід розміщувати переважно в місцях, захищених від ЕМП ("радіотінь", "мертва зона"), орієнтувати так, щоб було унеможливлене опромінювання вікон і дверей, у разі необхідності - екранувати.

Маршрути руху персоналу на території об'єкта слід установлювати таким чином, щоб унеможливити опромінювання при рівнях, що перевищують граничнодопустимі.

5.1.2.Електробезпека приміщення

Приміщення, де буде здійснюватись робота за небезпекою ураження електричним струмом можна віднести до 1 класу, тобто це приміщення без підвищеної небезпеки (сухе, мало запорошене, з нормальною температурою повітря, ізольованими підлогами і малим числом заземлених приладів) [8].

На робочому місці з усього обладнання металевим є лише корпус системного блоку комп'ютера, в якого крім робочої ізоляції передбачений елемент для заземлення та провід з заземлюючий жилою для приєднання до джерела живлення.

Електротехнічне устаткування: апаратури, кабелі й керівництва, розподільні пристрої всіх видів і напруг по своїх номінальних параметрах задовольняє умовам роботи як при нормальних режимах, так і при коротких замиканнях, перенапругах, перевантаженнях.

Для забезпечення безпеки установлюються наступні технічні рішення:

– Забезпечено недоступність струмопровідних частин (застосована схована проводка, кабель прокладений у спеціальних ринвах).

– Забезпечено ізолювання струмопровідних частин з використанням ізоляції, опір якої не нижче 1кОм/В, передбачені постійний контроль і профілактика ізоляції.

– Напруга освітлювальної мережі приймається 220 В із заземленою нейтраллю.

5.2 Технічні рішення з гігієни праці та виробничої санітарії

5.2.1. Мікроклімат

Дослідження підвищення інформаційної захищеності локальної мережі абонентського радіо доступу, згідно гігієнічною класифікацією праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу [1] за енерговитратами відноситься до

категорії І б. Допустимі параметри мікроклімату для цієї категорії наведені в табл.5.1 (відповідно ДСН 3.3.6.042-99 [6]).

Таблиця 5.1 – Параметри мікроклімату

Період року	Допустимі		
	t,°C	W, %	V, м/с
Теплий	22-28	40-60	0,1-0,3
Холодний	20-24	75	0,2

Для збереження допустимих умов праці, потрібно підтримувати вищенаведені параметри мікроклімату.

5.2.2. Склад повітря робочої зони

ГДК шкідливих речовин, які знаходяться в досліджуваному приміщені, наведені в таблиці 5.2.

Таблиця 5.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Формальдегід	0,035	0,03	2
Фенол	0,01	0,01	3
Пил нетоксичний	0,5	0,15	4
Озон	0,16	0,03	1

Для забезпечення складу повітря робочої зони передбачено: механічна вентиляція, регулярне прибирання та заборона заходити у приміщення в верхньому одязі.

5.2.3. Виробниче освітлення

Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні, які необхідно забезпечити під час виконання роботи зазначені у таблиці 5.4 (відповідно ДБН В.2.5-28-2006 [4]):

Таблиця 5.4 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО,%			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або	Бокове	Верхнє або верхнє	Бокове
Дуже високої точності	Від 0,15 до 0,3	II	г	великий	світлий	1000	300	7	2,5	4,2	1,5

Для забезпечення достатнього освітлення передбачені такі заходи:

Система природного освітлення на сьогоднішній день являється другорядним, компенсується загальним штучним освітленням, що створюється за допомогою економічних світлодіодних ламп.

5.2.4 Виробничий шум

Рівні шуму на робочому місці розробника встановлюються згідно ДСН 3.3.6.037-99 [5].

Під час аналізу мереж спостерігався шум непостійний тональний. Допустимі рівні звукового тиску під час виконання роботи повинні відповідати ГС, а рівні звуку L_A не повинні перевищувати 50 дБА (таблиця 5.5).

Таблиця 5.5 – Допустимі рівні звукового тиску і рівні звуку

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах зі середньогеометричними частинами (Гц)									Допуст-мий рівень звуку, дБА
	32	63	125	250	500	1000	2000	4000	8000	
Виробничі приміщення	86	71	61	54	49	45	42	40	38	50

Для забезпечення допустимих параметрів шуму доцільно використовувати засоби індивідуального захисту, якщо відбуватиметься порушення відповідних норм.

5.2.6 Виробничі випромінювання

Джерелом електромагнітного випромінювання під час виконання роботи є ПК.

У результаті дії ЕМП на людину можливі гострі та хронічні форми порушення фізіологічних функцій організму. Ці порушення виникають в результаті дії електричної складової ЕМП на нервову систему, а також на структуру кори головного та спинного мозку, серцево-судинної системи.

Допустимі значення параметрів електромагнітних випромінювань від монітору комп’ютера згідно СанПіН 2.2.4.1191-03 [11] наведені в табл. 5.6.

Таблиця 5.6 – Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні відеомонітору	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні відеомонітору	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати:	для дорослих користувачів 20кВ/м для дітей 15кВ/м

Для захисту людини від дії електромагнітних випромінювань передбачаються наступні способи і засоби: обмеження часу перебування персоналу в робочій зоні; встановлення раціональних режимів експлуатації установок і роботи працюючого персоналу.

5.2.6. Психофізіологічні фактори

Основними показниками важкості праці є: фізичне динамічне навантаження, стереотипні робочі рухи, статичне навантаження, переміщення у просторі. Основними показниками напруженості праці є: тривалість зосередження уваги або щільність сигналів, ступінь ризику для власного життя та життя інших осіб або ступінь відповідальності за життя інших осіб, змінність при роботі виключно в нічну зміну. [1]. Розглянемо деякі нормовані значення до яких потрібно прагнути при організації розпорядку робочого дня та режиму роботи відпочинку для досягнення оптимальних умов. Сенсорні навантаження:

Тривалість зосередження уваги до 50% від загального часу зміни.

Спостереження за екранами відеотерміналів, до2 годин на зміну.

Монотонність виробничої обстановки, час пасивного спостереження за технологічним процесом менше 75 % від часу зміни.

Тривалість робочого дня 6-7 год.

Змінність роботи – однозмінна робота (без нічної зміни).

Емоційне навантаження: є відповідальним за виконання окремих елементів завдання. Вимагає додаткових зусиль в роботі з боку працівника.

5.3 Безпека у надзвичайних ситуаціях. Дослідження безпеки роботи локальної мережі абонентського радіодоступу в умовах дії загрозливих чинників надзвичайних ситуацій

В радіоелектронній апаратурі іонізуючі випромінювання, викликають зворотні і незворотні процеси, внаслідок яких можуть відбуватися порушення роботи електричних елементів схеми, що призводять до виходу з ладу апаратури. Так, проходячи через елементи РЕА, потік гамма-випромінювань створює в них вільні носії електричних зарядів, в результаті переміщення яких виникає помилковий імпульс, який призводить до спрацьовування пристрою. При великих дозах випромінювання втрачають працездатність комплектуючі елементів локальної мережі абонентського радіодоступу. Опромінення у транзисторів змінює обернений струм і коефіцієнт підсилення, у конденсаторах знижує напругу пробою та опір стікання, змінюється провідність і внутрішній нагрів; руйнується електрична ізоляція дротів з полімерних матеріалів.

Одним з загрозливих чинників для бездротових, зокрема, локальної мережі абонентського радіодоступу є електромагнітний імпульс (ЕМІ). Уражаюча дія ЕМІ в приземній області й на землі пов'язана з акумулюванням його енергії довгими металевими предметами, рамними і каркасними конструкціями, антенами, лініями електропередачі та зв'язку, в них виникають сильні наведені струми, які руйнують підключене електронне та інше чутливе устаткування. У районі дії ЕМІ безпосередній контакт людини зі струмопровідними предметами теж є небезпечний.

ЕМІ уражає радіоелектронну і радіотехнічну апаратуру. В провідниках індукуються високі напруги і струми, які можуть призвести до постійних або тимчасових пошкоджень ізоляції кабелів, відключення реле, пошкодження елементів зв'язку, систем передачі даних тощо. Найбільш уразливими елементами обладнання є напівпровідникові прилади — транзистори, діоди, кремнієві

випрямлячі, інтегруючі ланцюги, цифрові процесори, управляючі й контрольні прилади. Чутливі до пошкодження ЕМІ транзистори звукової частоти, перемикаючі транзистори, інтегруючі ланцюги та ін.

Дослідження безпеки роботи локальної мережі абонентського радіодоступу в умовах дії іонізуючих випромінювань

Приймаючи до уваги елементну базу, що використовується для реалізації локальної мережі абонентського радіодоступу, складається таблиця потужностей експозиційної дози опромінення для кожного елемента $P_{зв.і}$, що викликають початок зворотних змін (таблиця 5.1).

Таблиця 5.1 - Максимально допустимі потужності дози γ – випромінювання.

Елементи приладу	$P_{гр,і}$ (Р/год)	$P_{гр}$ (Р/год)
Транзистори КТ	10^5	10^4
Діоди кремнієві	10^5	
Конденсатори електролітичні	10^6	
Резистори	10^6	
Мікросхеми ТТЛШ	10^4	
Прийомо-передавачі	10^4	

За мінімальним значенням $p_{гр}$ (див. табл. 5.1) межа безпеки роботи локальної мережі абонентського радіодоступу складає $p_{гр} = 10^4$ (Р/год). Для дослідження безпеки роботи локальної мережі абонентського радіодоступу визначається граничне значення потужності дози гамма-випромінювання ($p_{гр}$) за наступною формулою:

$$P_{гр} = K \times p_{гр} \times K_{пос} , \qquad (5.1)$$

де: К – коефіцієнт надійності, К = 0,9..0,95;

$p_{гр}$ – рівень радіації, що відповідає початку зворотних зміну найменш стійкого елемента;

$K_{пос}$ – коефіцієнт послаблення радіації ($K_{пос} = 1$),

$$Р_{гр} = 0,9 \times 10^4 \times 1 = 9 \times 10^3 \text{ (Р/год)},$$

З вище наведених розрахунків можна зробити висновок, що безпека роботи локальної мережі абонентського радіодоступу в умовах дії іонізуючих випромінювань буде забезпечуватись, якщо радіація в умовах експлуатації не перевищуватиме $Р_{гр} = 9 \times 10^3$ (Р/год).

Розрахуємо допустимо максимальний час роботи локальної мережі абонентського радіодоступу в умовах дії іонізуючих випромінювань:

$$Д_м = \frac{2P_{гр}(\sqrt{t_К^{\,2}} - \sqrt{t_П^{\,2}})}{1}, \qquad (5.2)$$

де: $\sqrt{t_П^{\,2}}$, дорівнює 1;

$Д_м$ – дорівнює 10^3;

$$t_{доп} = 13,27 \times 10^3 \text{ (год)}.$$

Такий час є достатнім для безпечної роботи системи в цілому.

Дослідження безпеки роботи локальної мережі абонентського радіодоступу в умовах дії електромагнітного імпульсу

Безпека роботи локальної мережі абонентського радіодоступу в умовах дії електромагнітного імпульсу характеризується коефіцієнтом безпечної роботи $К_б$, який визначається по

$$К_б = 20\lg\frac{U_д}{U_{в(г)}} \geq 40[\text{дБ}], \qquad (5.3)$$

де $U_д$ – допустимі коливання напруги живлення системи;

$U_{в(г)}$ – напруга живлення вертикальної (горизонтальної) наводок внаслідок дії електромагнітного вмпульсу.

$$U_д = U_ж + (U_ж/100)*N, \qquad (5.4)$$

де $U_ж$ = 12 В – наруга живлення пристрою;

N = 10% - коливання напруги живлення.

Підставивши значення для $U_ж$ і N в (4.6), одержимо:

$$U_д=12+12/100*10= 13,2 \text{ (В)}.$$

Визначимо *Uв*, для чого формулу (5.3) приведемо до наступного вигляду:

$$lgU_д/U_в=2, \qquad (5.5)$$

звідки $U_в$= 0,6025 В.

Визначимо горизонтальну складову напруженості електромагнітного поля $E_г$:

$$U_в=E_г*l, \qquad (5.6)$$

де l=0,63 м – максимальна довжина струмоведучих частин. Тоді:

$$E_г=0,6025/0,63=20,08 \text{ В/м}$$

Вертикальна складова напруженості електромагнітного поля $E_в$, визначається з формули:

$$E_г=10^{-3}*E_в, \qquad (5.7)$$

звідки

$$E_в=20,08/10^{-3}=20080 \text{ В/м}.$$

Отже, мережа мобільного зв'язку буде стабільно працювати при умові, що вертикальна і горизонтальна складові напруженості електромагнітного поля не будуть перевищувати значень відповідно: $E_в$=20080 В/м і $E_г$=20,08 В/м.

Розробка заходів по підвищенню безпеки роботи локальної мережі абонентського радіодоступу в умовах надзвичайних ситуацій

Найбільш ефективним способом підвищення стійкості роботи локальної мережі абонентського радіодоступу є екранування системи або її елементів. Тому частіше за все в якості захисту проводиться розрахунок екранування. Визначається перехідне затуханні енергії електричного поля стальним екраном:

$$А=К_{бном}-К_{бмін}, \quad (5.8)$$

де $К_{бном}$ – номінальний коефіцієнт безпеки ($К_{бном}$ - 40дБ);

$Кб_{мін}$ – мінімальний коефіцієнт безпеки, отриманий під час розрахунків.

$$А=40+36,6=76,6(дБ)$$

Товщину захисного екрану знаходимо за формулою:

$$t=\frac{А}{5,2\cdot\sqrt{f}}, \quad (5.9)$$

де А – перехідне затухання екрану;

f – найбільш домінуюча частота ЕМІ (15 кГц);

$$t=\frac{76,6}{5,2\cdot\sqrt{15000}}=0,104(см)$$

Підвищення стійкості роботи локальної мережі абонентського радіодоступу можна досягти шляхом посилення найбільш слабких елементів і ділянок мережі, а також завчасним проведенням комплексу інженерно-технічних, технологічних та організаційних заходів, які спрямовані на максимальне зниження дії вражаючих факторів і створений умов для ліквідації наслідків аварійної ситуації. В роботі було проведено дослідження безпеки роботи локальної мережі абонентського

радіодоступу в умовах дії НС, ЕМІ та розробка заходів по підвищенню безпеки роботи її в умовах дії НС.

Отже у розділі були розглянуті причини виникнення НС, що впливають на роботу локальної мережі абонентського радіодоступу під час НС, і, також можливі шляхи їх усунення. Було розраховано граничні значення вертикальної і горизонтальної складових напруженості електромагнітного поля. А також був проведений розрахунок екранування для захисту електроніки локальної мережі абонентського радіодоступу від загрозливих чинників НС.

ВИСНОВКИ

Магістерська робота присвячена актуальним питанням систем абонентського радіодоступу, побудованих на основі різних стандартів, у тому числі LTE, IEEE802.11xx. Предмет дослідження - інформаційна безпека з урахуванням особливостей систем радіозв'язку, забезпечення захисту і високої швидкості передачі даних, а також поодинока куткова антена і антенні грати на її основі.

У першому розділі розглянуті принципи і особливості побудови САРД, сформульовані їх переваги і недоліки, проведені класифікація, аналіз їх складу і основних характеристик. Відзначається, що в системах радіодоступу широко використовуються різні технології організації множинного доступу, зокрема, FDMA, TDMA, CDMA.

У другому розділі розглянуті питання забезпечення безпеки і захищеності САРД. Розглянуті і класифіковані погрози (порушення конфіденційності, цілісності, доступності), а також характерні для безпровідних систем уразливості. Відзначається, що для безпровідних мереж стандарту 802.11n (і інших стандартів) усіх засобів і методи захисту можна розділити на наступні типи [8-10]: а) засоби і методи аутентифікації; б) засоби криптографічного захисту передаваних даних; в) засоби технічного захисту.

Враховуючи випадковий характер, як характеристик каналу зв'язку, так і можливостей порушника по протидії роботи легітимного каналу, критерій захищеності каналу зв'язку можна представити у формі вірогідності складної події, як суми двох елементарних подій: вірогідність потайної роботи і завадозахищеності каналу. Проведений аналіз завадостійкої видів модуляції для стандарту IEEE 802.11n.

Відзначається, що найбільшу завадостійку (чи найменшими енергетичними витратами) при заданій вірогідності помилки мають сигнали BPSK і QPSK.

У третьому розділі розглянуті «антенні проблеми» САРД, рішення яких потрібне для підвищення пропускної здатності. При цьому важливим джерелом підвищення якості безпровідного зв'язку є технологія MIMO. Вона є технологією

передачі даних за допомогою N - антен і прийому інформації M - антенами. Така технологія дозволяє зменшити число помилок при радіообміні даними без зниження швидкості передачі в умовах множинних переотражений сигналів.

Відмічено, що перевагою антенної системи побудованої за технологією MIMO, є можливість формування порівняно вузької спрямованості передачі даних, усунення дій завад, що заважають, за рахунок їх компенсації в приймальному пристрої. Це дає можливість підвищити завадостійку каналу зв'язку і збільшити ефективність використання спектру за рахунок передачі даних в паралельних променях. Крім того, технологія MIMO дозволяє зменшити число помилок при радіообміні даними без зниження швидкості передачі в умовах множинних переотражений сигналів. Як наслідок, використання цієї технології забезпечує збільшення пікової швидкості передачі даних за рахунок поліпшення завадостійкої.

У роботі проведений машинний експеримент по дослідженню можливостей зміни спрямованих параметрів куткової антени (як поодинокою, так і у складі антенних грат для базової станції) в двох основних площинах. Показано, що при зміні ряду конструктивних параметрів, можлива зміна ДН антени, необхідне для відповідної зміни завадостійкої САРД.

У четвертому розділі розглянуті економічні розрахунки доцільності та ефективності науково-дослідної роботи із аналізу, дослідження та розробки мережі радіодоступу.

У п’ятому розділі розглянуті небезпечні та шкідливі фактори, які діють на людину під час роботи в приміщенні де здійснюються дослідження та розробка елементів мережі радіодоступу.

Завдання по магістерській роботі виконане в повному об'ємі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Janevski, T. QoS for Fixed and Mobile Ultra-Broadband / T. Janevski. - John Wiley & Sons Ltd, 2019. - 326 p.

2. Recommendation ITU-T Y.2021. IMS for Next Generation Networks. - 2006.

3. Recommendation ITU-T Y.2011. General principles and general reference model for Next Generation Networks. - 2004.

4. Recommendation ITU-T X.210. Open System Interconnection Layer Service Definition Conventions. - 1988.

5. Recommendation ITU-T Y.1223. Interworking guidelines for transporting assured IP flows. - 2008.

6. Recommendation ITU-T G.8010/Y.1306. Architecture of Ethernet layer networks.- 2004.

7. Recommendation ITU-T P.10/G.100. Vocabulary for performance, quality of service and quality of experience. - 2017.

8. Recommendation ITU-T P.800.2. Mean opinion score interpretation and reporting. - 2016.

9. Recommendation ITU-T P.913. Methods for the subjective assessment of video quality, audio quality and audiovisual quality of Internet video and distribution quality television in any environment. - 2016.

10. Recommendation ITU-T G.107. The E-model: a computational model for use in transmission planning. - 2015.

11. Recommendation ITU-T P.862. Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs. - 2001.

12. Recommendation ITU-T I.350. General Aspect of Quality of Service and Network Performance in Digital Networks, including ISDNs. - 1993.

13. Recommendation ITU-T E.360.1. Framework for QoS routing and related traffic engineering methods for IP-, ATM-, and TDM-based multiservice networks. - 2002.

14. Recommendation ITU-T Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters. - 2019.

15. Recommendation ITU-T Y.1541. Network performance objectives for IP-based services. - 2011.

16. Recommendation ITU-T M.2301. Performance objectives and procedures for provisioning and maintenance of IP-based networks. - 2002.

17. Recommendation ITU-T E.492. Traffic Reference Period - 1996.

18. Recommendation ITU-T E.500. Traffic Intensity Measurement Principles. - 1988.

19. Recommendation ITU-T Q.544. Digital Exchange Measurements. - 1993.

20. Recommendation ITU-T E.600. Terms and Definition of Traffic Engineering. - 1993.

21. Recommendation ITU-T G.1010. End-user multimedia QoS categories. - 2001.

22. Гольдштейн, Б. С. Сети связи : учебник для ВУЗов / Б. С. Гольдштейн, Г. Г. Яновский, Н. А. Соколов. - СПб. : БХВ-Петербург, 2010. - 400 с.

23. Гольдштейн, Б. С. Сети связи пост-NGN / Б. С. Гольдштейн, А. Е. Кучерявый. - СПб. : БХВ-Петербург, 2014. - 160 с.

24. Кучерявый, Е. А. Управление трафиком и качество обслуживания в сети Интернет / Е. А. Кучерявый. - СПб. : Наука и Техника, 2004. - 336 с.

25. Кучерявый, А. Е. Сети связи общего пользования: тенденции развития и методы расчета / А. Е. Кучерявый, А. И. Парамонов, Е. А. Кучерявый. - М. : ФГУП ЦНИИС, 2008. - 296 с.

26. Степанов, С. Н. Основы телетрафика мультисервисных сетей / С. Н. Степанов. - М. : Эко-Трендз, 2010. - 392 с.

27. Битнер, В. И. Нормирование качества телекоммуникационных услуг : учебное пособие / В. И. Битнер, Г. Н. Попов ; под ред. профессора В. П. Шувалова. - М. : Горячая линия - Телеком, 2004. - 312 с.

28. Битнер, В. И. Принципы и протоколы взаимодействия телекоммуникационных сетей : учебное пособие для студентов высших учебных

заведений, обучающихся по специальности 210406 - "Сети связи и системы коммутации" / В. И. Битнер. - М. : Горячая Линия - Телеком, 2008. - 272 с.

29. Шувалов, В. П. Обеспечение показателей надежности телекоммуникационных систем и сетей / В. П. Шувалов, М. М. Егунов, Е. А. Минина. - М. : Горячая линия -Телеком, 2015. - 168 с.

30. Нетес, В. А. Основы теории надежности : учебное пособие для вузов / В. А. Нетес. - М. : Горячая Линия - Телеком, 2019. - 102 с.

31. Попков, Г. В. Математические основы моделирования сетей связи : учебное пособие для вузов / Г. В. Попков, В. К Попков, В. В. Величко. - М. : Горячая линия - Телеком, 2014. - 183 с.

32. Модели для анализа качества обслуживания в сетях связи следующего поколения: учеб. пособие / Г. П. Башарин, Ю. В. Гайдамака, К. Е. Самуйлов, Н. В. Яркина - М. : РУДН, 2008. - 137 с.

33. McCabe, J. D. Network Analysis, Architecture, and Design / J. D. McCabe - 3-ed. - USA, Burlington : Morgan Kaufmann, 2007. - 473 p.

34. Claise, B. Network Management: Accounting and Performance Strategies / B. Claise, R. Wolter. - USA, Indianapolis : Cisco Press, 2007. - 672 p.

35. Ackerley, R. Telecommunications Performance Engineering / R. Ackerley. - UK, London : Institution of Electrical Engineers, 2004. - 288 p.

36. Cole, R. G. Wide-Area Data Network Performance Engineering / R. G. Cole, R. Ramaswamy. - USA : Boston, Artech House, 2000. - 417 p.

37. Recommendation ITU-T E.800. Definitions of terms related to quality of service. - 2008.

38. Recommendation ITU-T E.802. Framework and methodologies for the determination and application of QoS parameters. - 2007.

39. Конахович, Г. Ф. Сети передачи пакетных данных / Г. Ф. Конахович, В. М. Чуприн. - К. : «МК-Пресс», 2006. - 272 с.

40. Recommendation ITU-T E.419. Business oriented key performance indicators for management of networks and services. - 2006.

41. Recommendation ITU-T X.140. General Quality of Service Parameters for

Communication via Public Data Networks. - 1992.

42. Recommendation ITU-T X.213. Information technology – Open Systems Interconnection – Network service definition. - 2001.

43. Moller, S. Quality of Experience : Advanced Concepts, Applicationsand Methods /S. Moller, A. Raake. - Springer International Publishing, 2014. - 434 p.

44. Recommendation ITU-T G.1011. Reference guide to quality of experience assessment methodologies. - 2016.

45. Technical Report ETSI TR 102 643 V1.0.2 (2010-01). Human Factors (HF); Quality of Experience (QoE) requirements for real-time communication services. - 2010.

46. Recommendation ITU-T E.502. Traffic measurement requirements for digital telecommunication exchanges. - 2001.

47. Recommendation ITU-T Y.1543. Measurements in Internet protocol networks for inter-domain performance assessment. - 2018.

48. Recommendation ITU-T E.800 Supplement 8. Guidelines for inter-provider quality of service. - 2009.

49. Multimedia Quality of Experience (QoE): current status and future requirements / C. W. Chen, P. Chatzimisios, T. Dagiuklas, L. Atzori. - John Wiley & Sons Ltd, 2016. - 192 p.

50. Recommendation ITU-T G.1030. Estimating end-to-end performance in IP networks for data applications. - 2014.

51. Recommendation ITU-T Y.1562. Framework for higher-layer protocol performance parameters and their measurement. - 2007.

52. Recommendation ITU-T G.1031. QoE factors in web-browsing. - 2014.

53. Recommendation ITU-T G.1080. Quality of experience requirements for IPTV services. - 2008.

54. Recommendation ITU-T G.114. One-way transmission time. - 2003.

55. Recommendation ITU-T G.1020. Performance parameter definitions for quality of speech and other voiceband applications utilizing IP networks. - 2006.

56. ETSI Guide ETSI EG 202 009-2 V1.3.0 (2014-09). User Group; Quality of telecom services; Part 2: User related indicators on a service specific basis. - 2014.

57. Recommendation ITU-T Y.110. Global Information Infrastructure Principles and Framework Architecture. - 1998.

58. Бабкин, В. А. Методы оценки качества передачи данных в пакетных сетях связи / В. А. Бабкин, Е. П. Строганова // T-Comm: Телекоммуникации и транспорт. - 2019. - №11. - С. 25-31.

59. Recommendation ITU-T Y.1564. Ethernet service activation test methodology. - 2016.

60. RFC 5357. A Two-Way Active Measurement Protocol (TWAMP). - 2008.

61. RFC-6802. Ericsson Two-Way Active Measurement Protocol (TWAMP) Value- Added Octets. - 2012.

62. Sholomon, A. Enterprise Network Testing / A. Sholomon, T. Kunath. - USA, Indianapolis : Cisco Press, 2011. - 599 p.

63. Recommendation ITU-T O.211. Test and measurement equipment to perform tests at the IP layer. - 2006.

64. RFC 3416. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP). - 2002.

65. Мауро, Д. Основы SNMP / Д. Мауро, К. Шмидт ; пер. с англ. - 2-е издание - СПб. : Символ-Плюс, 2012. - 520 с.

66. Clemm, A. Network Management Fundamentals / A. Clemm. - USA, Indianapolis: Cisco Press, 2007. - 510 p.

67. RFC 3432. Network performance measurement with periodic streams. - 2002.

68. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Олифер, Н. Олифер. - 5-е изд. - СПб. : Питер, 2016. - 992 с.

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

Додаток А
(обов’язковий)

ВНТУ

ЗАТВЕРДЖУЮ
Зав.кафедри ТКСТБ ВНТУ,
докт. техн. наук, професор
В.М. Кичак
. “__” _____ 2021 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ЛОКАЛЬНОЇ МЕРЕЖІ АБОНЕНТСЬКОГО РАДІОДОСТУПУ
08-34.МКР.008.00.000 ТЗ

Керівник роботи
к.т.н., доц. кафедри ТКСТБ ВНТУ
Стальченко О.В.

Виконавець: ст. гр. ТКС-19м
Мирончак В.М.

Вінниця-2021

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “24” 09 2021 року № 277 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 01.09.2021 р.

Дата закінчення: 20.12.2021 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою дослідження є підвищення захищеності передачі інформації по системах абонентського радіодоступу, побудованих на основі різних технологій.

Задачами магістерської кваліфікаційної роботи є:

- аналізу сучасного стану безпровідних систем;
- класифікації САРД;
- порівняльного аналізу різних САРД;
- безпеці і захищеності безпровідних систем передачі інформації;
- аналізу завадостійкої різних видів модуляції, використовуваних в САРД;
- проектування антени і лінійних антенних грат на її основі.

Об’єктом дослідження є система абонентського радіодоступу, побудована на основі різних стандартів, у тому числі стандарту IEEE 802.11n с технологією MIMO.

Предметом дослідження є захищені системи абонентського радіодоступу, побудовані на основі теорії скритності і завадозахищеності систем передачі інформації і теорії електродинаміки антен. Кількісні оцінки параметрів САРД проводилися за допомогою розрахунків і моделювання в середовищі Mathcad..

Основними завданнями роботи є:

- техніко-економічне обґрунтування доцільності даної розробки;
- аналіз принципів побудови САРД
- аналіз безпеки і захищеності безпровідних систем передачі інформації
- розрахунок антени і антенної гратки для базової станції;

- аналіз економічної ефективності проведеної розробки;
- дослідження питань безпеки життєдіяльності.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Робота базується на результатах попередніх досліджень.

Список використаних джерел розробки:

3.1. Recommendation ITU-T E.600. Terms and Definition of Traffic Engineering. - 1993.

3.2. Recommendation ITU-T G.1010. End-user multimedia QoS categories. - 2001.

3.3 Гольдштейн, Б. С. Сети связи : учебник для ВУЗов / Б. С. Гольдштейн, Г. Г. Яновский, Н. А. Соколов. - СПб. : БХВ-Петербург, 2010. - 400 с.

3.4 Гольдштейн, Б. С. Сети связи пост-NGN / Б. С. Гольдштейн, А. Е. Кучерявый. - СПб. : БХВ-Петербург, 2014. - 160 с.

3.5 Кучерявый, Е. А. Управление трафиком и качество обслуживания в сети Интернет / Е. А. Кучерявый. - СПб. : Наука и Техника, 2004. - 336 с.

3.6 Кучерявый, А. Е. Сети связи общего пользования: тенденции развития и методы расчета / А. Е. Кучерявый, А. И. Парамонов, Е. А. Кучерявый. - М. : ФГУП ЦНИИС, 2008. - 296 с.

3.7 Степанов, С. Н. Основы телетрафика мультисервисных сетей / С. Н. Степанов. - М. : Эко-Трендз, 2010. - 392 с.

3.8 Битнер, В. И. Нормирование качества телекоммуникационных услуг : учебное пособие / В. И. Битнер, Г. Н. Попов ; под ред. профессора В. П. Шувалова. - М. : Горячая линия - Телеком, 2004. - 312 с..

3.9 Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – В.: ВДТУ, 2003.

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

3.11 Разработка и оформление конструкторской документации радиоэлектронной аппаратуры. Справочник. Под ред. Э.Т.Романычевой.- М: Радио и связь, 1989.

3.12 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.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи ТКС-20м Мирончак В.М.

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати дослідження методів і алгоритмів оцінки параметрів якості сигналів і каналу зв'язку мультисервісної мережі

Технічні вимоги, яким повинна відповідати розробка, наступні:

- технологія рознесення сигналів – MIMO,
- робоча частота – 1800 МГц;
- висота рефлектора – 0,13м;
- ширина стінки рефлектора – 0,25м;
- сектор сканування антени – 120°.

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)	01.09.2021р.	10.09.2021р.	Розроблене ТЗ	Додаток А
2.	Аналіз принципів побудови САРД	11.09.2021р.	17.09.2021р.	Проведений аналіз	Вступ. Розділ 1.
3.	Аналіз безпеки і захищеності безпровідних систем передачі інформації	18.09.2021р.	01.10.2021р.	Проведений аналіз	Розділ 2
4.	Розрахунок антени і антенної гратки для базової станції	02.10.2021р.	19.11.2021р.	Характе-ристики і параметри	Розділ 3
5.	Аналіз економічної ефективності	20.11.2021р.	30.11.2021р.	Економічна частина МКР	Розділ 4

6.	Охорона праці та безпека в надзвичайних ситуаціях	01.12.2021р.	06.12.2021р.	Частина ОТ та БНС	Розділ 5
7.	Оформлення пояснювальної записки (ПЗ) та графічної частини	07.12.2021р.	13.12.2021р.	Оформлена документація	ПЗ та графічна частина
8.	Нормоконтроль, попередній захист, опонування МКР	14.12. 2021р.	17.12.2021р.	Позитивні відзиви	Відгуки
9.	Захист МКР ЕК		20.12.2021р.	Позитивний захист	Протокол ЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- представлена розробка моделі загроз для мережі на основі обладнання сімейства стандартів IEEE 802.11xx.
- питання безпеки та захищеності САРД.
- критерії оцінки скритності та завадозахищенності систем, побудованих на основі цих стандартів.
- виконано конструктивний розрахунок кутової антени та антенної решітки, розрахунок їх параметрів.

Теоретична і практична значущість роботи. полягає в тому, що сформовані критерії оцінки скритності та завадозахищенності систем, побудованих на основі стандартів систем радіодоступу. Виконано конструктивний розрахунок кутової антени та антенної решітки, розрахунок їх параметрів та здійснено моделювання.

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

- Регіональний Центр експлуатації телекомунікаційної мережі України шляхом впровадження широкосмугового ІКМ;

- ПАТ “Укртелеком” шляхом впровадження нових методик контролю характеристик ІКМ.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується підвищення точності та зменшення обчислювальної здатності.

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 магістерської кваліфікаційної роботи відбувається на відкритому засіданні ЕК.

10 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

Документація, що розробляється в процесі виконання досліджень повинна містити:

- модель загроз і забезпечення безпеки САРД;
- розрахунок адаптивних антенних грат;
- економічну частину та розділ БЖД і ЦЗ;
- рекомендації щодо подальшого використання отриманих методів.

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

Типова структура і склад мереж абонентського доступу

Додаток В

Архітектура САРД

Додаток Г

Методи доступу і розширення спектру

Додаток Д

Залежності ВБП для видів модуляції САРД

Додаток Е

Структурна схема відвідного каналу в режимі перехоплення

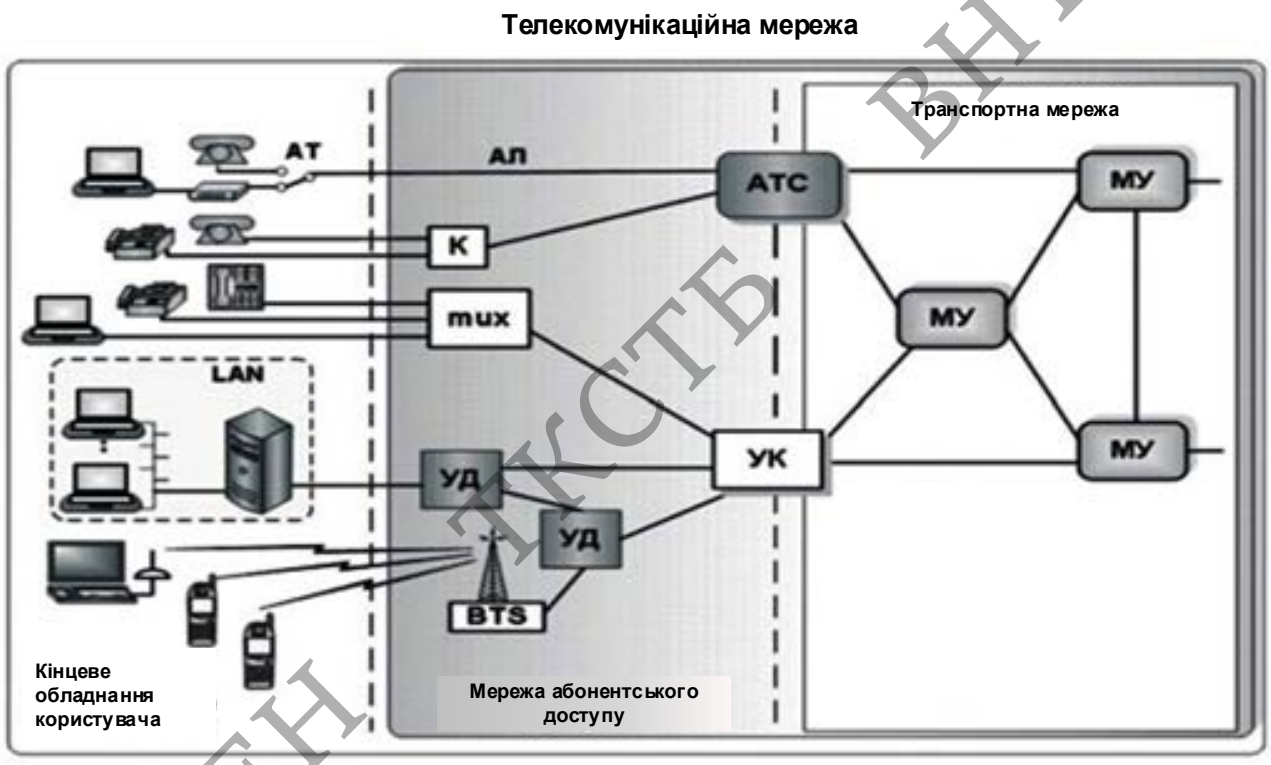
Додаток К

Система MIMO з двома передавальними і двома приймаючими антенами

Додаток Л

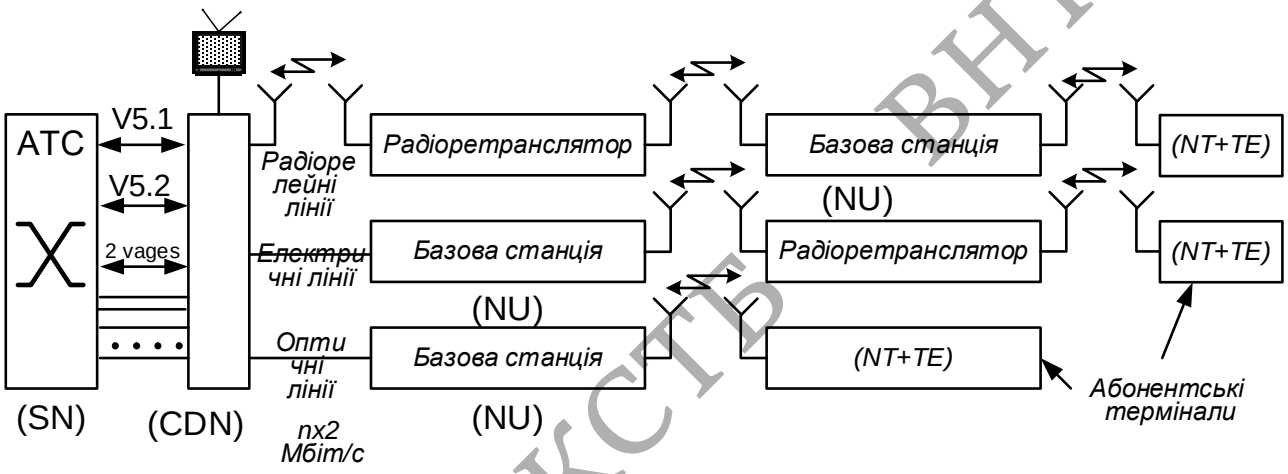
Моделювання параметрів антени

Типова структура і склад мереж абонентського доступу



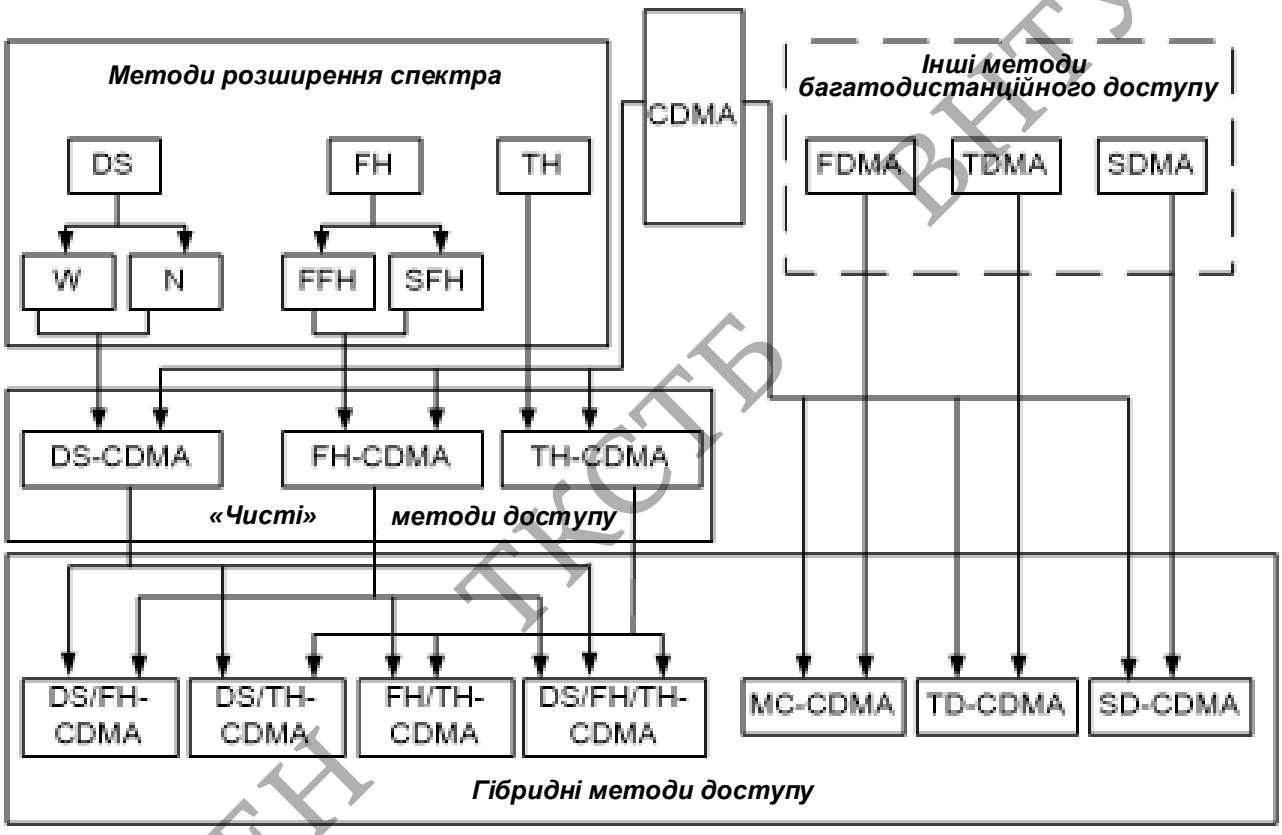
					08-34.МКР.008.00.000		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Мирончак В.М.			Типова структура і склад мереж абонентського доступу	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Семенов А.О.				ВНТУ, гр. ТКС-20м	
Н. Контр.		Стальченко О.В.					
Затверд.		Кичак В.М.					

Архітектура САРД



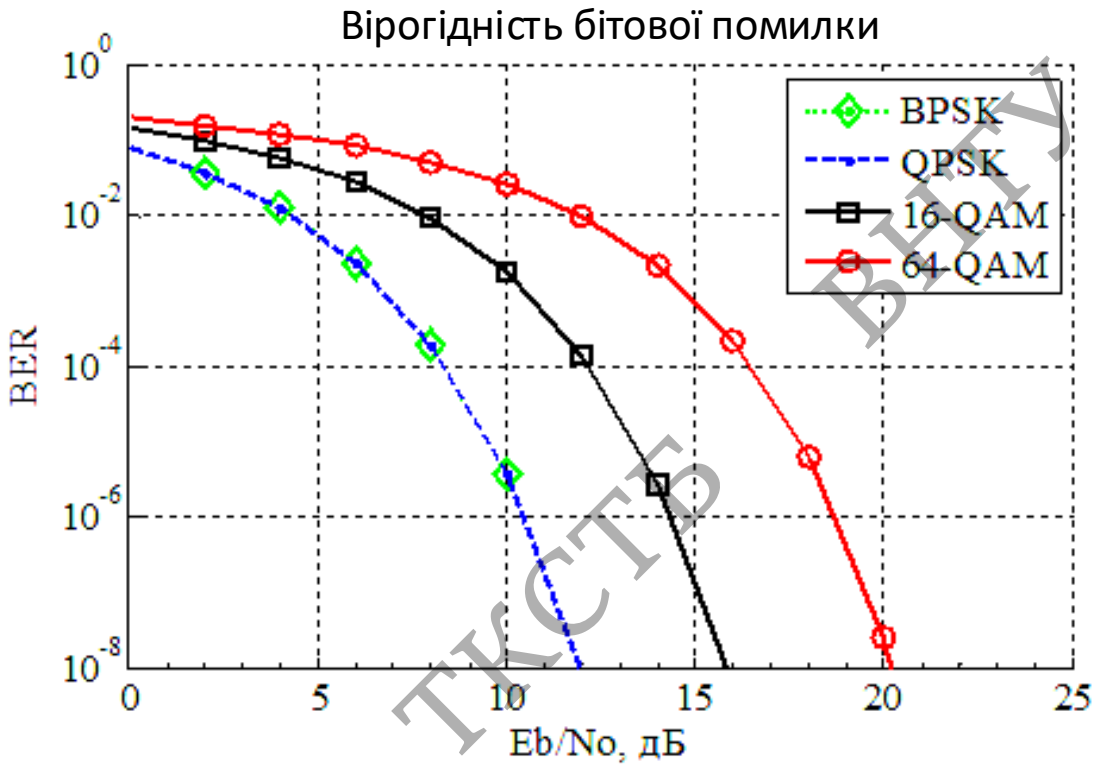
					08-34.МКР.008.00.000	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Мирончак В.М.			Архітектура САРД	Літ. / Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.				
Реценз.		Семенов А.О.				ВНТУ, гр. ТКС-20м
Н. Контр.		Стальченко О.В.				
Затверд.		Кичак В.М.				

Методи доступу і розширення спектру



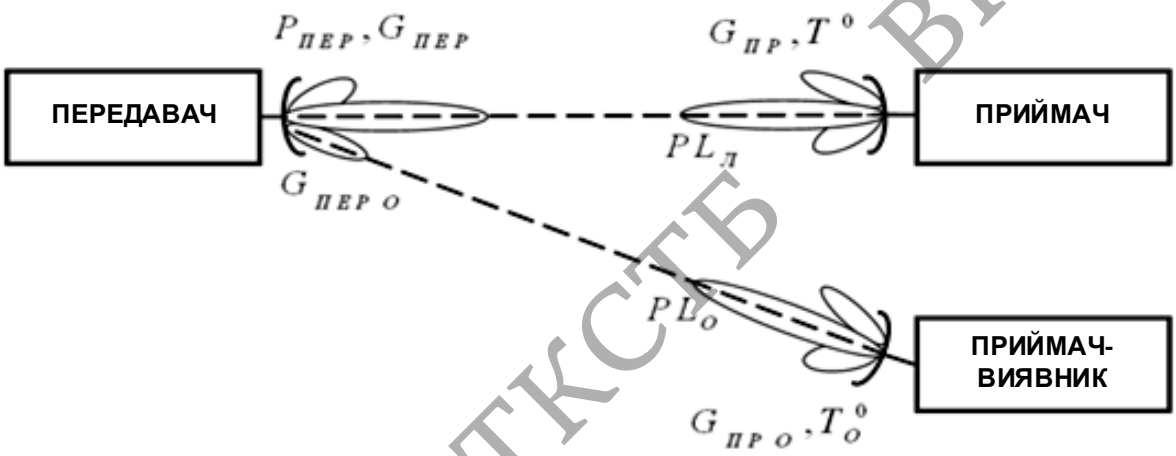
					08-34.МКР.008.00.000	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Мирончак В.М.			Методи доступу і розширення спектру	Літ. / Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.				
Реценз.		Семенов А.О.				ВНТУ, гр. ТКС-20м
Н. Контр.		Стальченко О.В.				
Затверд.		Кичак В.М.				

Залежності ВБП для видів модуляції САРД



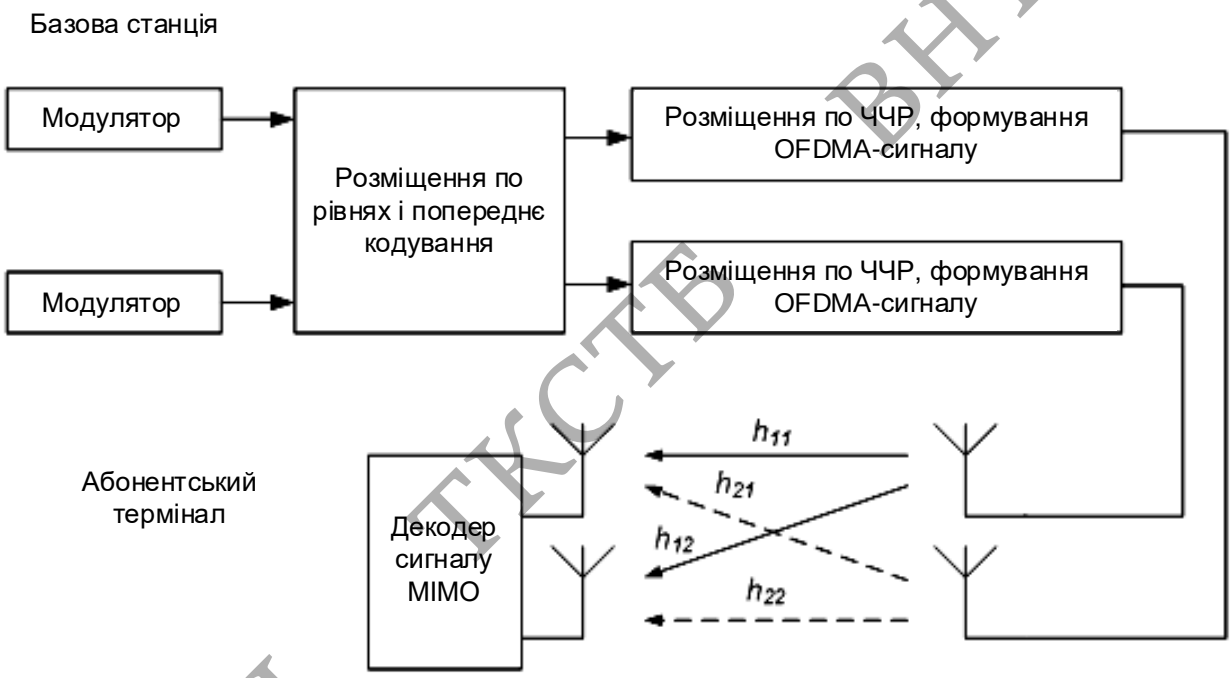
					08-34.МКР.008.00.000		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Мирончак В.М.			Залежності ВБП для видів модуляції САРД	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Семенов А.О.				ВНТУ, гр. ТКС-20м	
Н. Контр.		Стальченко О.В.					
Затверд.		Кичак В.М.					

Структурна схема відвідного каналу в режимі перехоплення



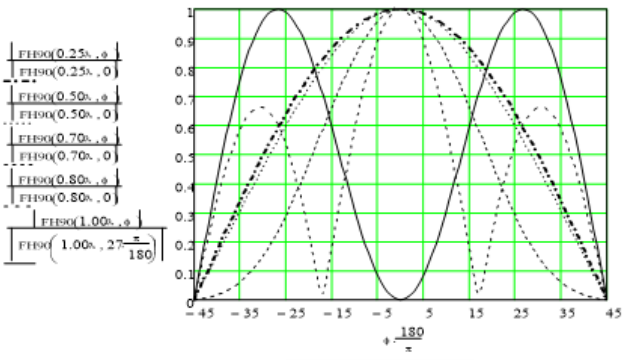
					08-34.МКР.008.00.000		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Мирончак В.М.			Структурна схема відвідного каналу в режимі перехоплення	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Семенов А.О.				ВНТУ, гр. ТКС-20м	
Н. Контр.		Стальченко О.В.					
Затверд.		Кичак В.М.					

Система MIMO з двома передавальними і двома приймаючими антенами

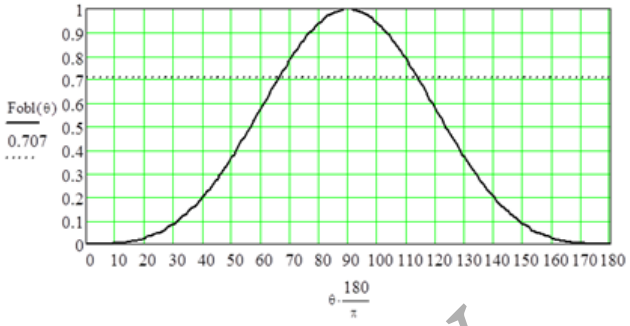


					08-34.МКР.008.00.000	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Мирончак В.М.			Система MIMO з двома передавальними і двома приймаючими антенами	Літ. / Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.				
Реценз.		Семенов А.О.				ВНТУ, гр. ТКС-20м
Н. Контр.		Стальченко О.В.				
Затверд.		Кичак В.М.				

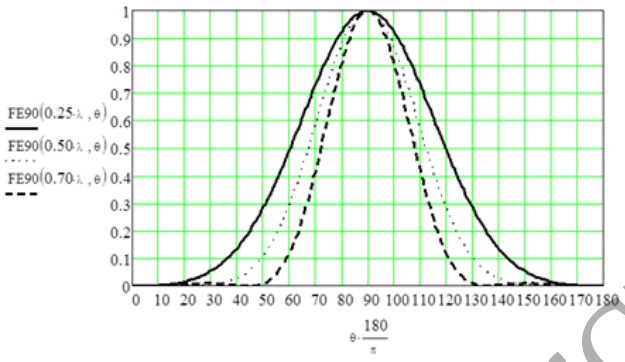
Моделювання параметрів антени



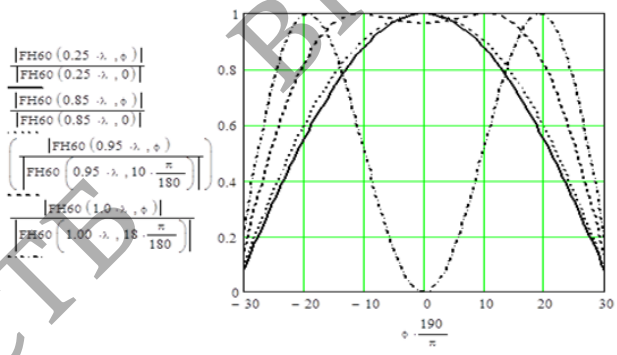
ДН куткової антени в площині Н при куті розкриву 90 град



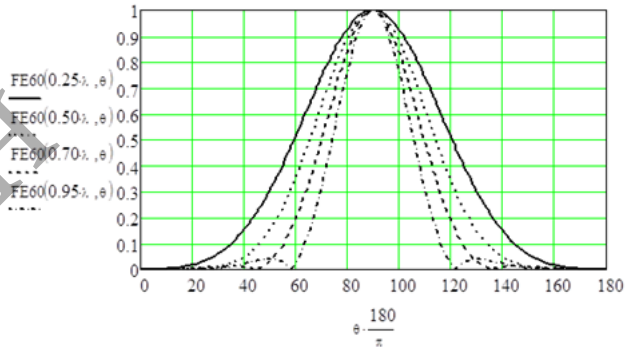
ДН півхвильового вібратора



ДН куткової антени з кутом розкриву 90 град опромінюваною півхвильовим вібратором в площині Е



ДН куткової антени з кутом розкриву 60 град опромінюваною півхвильовим вібратором в площині Н



ДН куткової антени з кутом розкриву 60 град опромінюваною півхвильовим вібратором в площині Е

					08-34.МКР.008.00.000	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Мирончак В.М.			Моделювання параметрів антени	Літ. / Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.				
Реценз.		Семенов А.О.				ВНТУ, гр. ТКС-20м
Н. Контр.		Стальченко О.В.				
Затверд.		Кичак В.М.				