Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній рівень)

на тему: *«Дослідження методів первинного захисту інформаційних каналів для супутникових систем зв'язку»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Криванич Є.М.
підпис (прізвище та ініціали)

Керівник *Баран І.О.*
підпис (прізвище та ініціали)

Нормоконтроль *Кареліна О.В.*
підпис (прізвище та ініціали)

Рецензент *Пасічник В.В.*
підпис (прізвище та ініціали)

м. Тернопіль – 20*19*

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет *комп'ютерно – інформаційних систем і програмної інженерії*
Кафедра *кібербезпеки*
Освітній рівень *магістр*
Спеціальність *125 «Кібербезпека»*
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри *Загородна Н.В.*

«_____» _____ 20*19* р.

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Криваничу Євгенію Михайловичу
(прізвище, ім'я, по батькові)
1. Тема проекту (роботи) *«Дослідження методів первинного захисту інформаційних каналів для супутникових систем зв'язку»*

Керівник проекту (роботи) *Баран Ігор Олегович, к.т.н., доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом по університету від «_____» _____ 20*19* року №____
2. Термін подання студентом проекту (роботи)
3. Вихідні дані до проекту (роботи) *Дослідження методів, які є первинними для цілісності та достовірності переданої інформації супутниковими системами*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ.
Розділ 1 Аналіз первинного захисту інформаційних супутникових каналів
Розділ 2 Методи захисту інформаційних мереж
Розділ 3 Науково-технічне значення отриманих результатів та рекомендації із застосування
Розділ 4 Спеціальна частина
Розділ 5 Обґрунтування економічної ефективності
Розділ 6 Охорона праці та безпека в надзвичайних ситуаціях
Розділ 7 Екологія
Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Рис. 1.1 – Варіант структури мережі супутникового зв'язку типу VSAT;
Рис. 2.2 – Можливі завади між системами супутникового зв'язку; Рис. 2.3 – Варіанти можливих завад між супутниковими лініями зв'язку з радіорелейними лініями; Рис. 2.5 – Схема просторової режекції завад; Рис. 3.3 – Топологія мережі «крапка-крапка»; Рис. 3.4. – Топологія мережі «зірка»

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина			
Обґрунтування економічної ефективності			
Охорона праці та безпека в надзвичайних ситуаціях			
Екологія			

7. Дата видачі завдання *« 01 » жовтня 2019 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	**Примітка**

Студент _____ *Криванич Є.М.*
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ *Баран І.О.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження методів первинного захисту інформаційних каналів для супутникових систем зв'язку // Дипломна робота ОР «Магістр» // Кривanич Євгеній Михайлович // Тернопільський національний технічний університет імені Івана Пулюя // факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // С. -102, рис. – 26, табл. – 8, додат. – 3.

Ключові слова: АЛГОРИТМ, МЕТОД ПЕРЕДАЧІ ІНФОРМАЦІЇ, ОЦІНЮВАННЯ, СУПУТНИКОВА СИСТЕМА ЗВ'ЯЗКУ, ДУАЛЬНИЙ МЕТОД, VSAT СТАНЦІЯ.

Мета роботи – аналіз відомих і розробка нового методу первинного захисту передачі інформаційних каналів для систем супутникового зв'язку. Основні результати роботи – розроблений метод захисту інформаційних каналів супутникової мережі ґрунтується на дуальній передачі інформації одночасно на два штучні супутники Землі, які не мають між собою зв'язку. Розроблено алгоритм роботи такого комплексу «абонент – супутник – абонент – базова станція». Проведено модельні дослідження розробленого алгоритму.

У першому розділі описані основні конфігурації алгоритму роботи супутникової мережі типу VSAT з точки зору інформаційної безпеки та завадостійкості.

У другому розділі розглядаються методи захисту інформаційних мереж, створених на основі систем зв'язку типу VSAT.

У третьому розділі – експериментальному – порівнюються існуючі системи з безпеки інформативних каналів зв'язку; створений власний гібридний метод з захисту інформаційних каналів передачі.

У результаті підготовки дипломної роботи проведені експерименти та всебічний аналіз для виявлення факторів, що впливають захист інформаційних каналів з точки зору зовнішнього несанкціонованого втручання та завадного середовища.

ANNOTATION

Research of methods of primary protection of information channels for satellite communication systems // Diploma work of the Master's degree program // Evgeny M. Kryvanich // Ivan Puluj Ternopil National Technical University // Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security group SBm-61 // Ternopil, 2019 // P. –102, fig. – 26, tab. – 8, add. – 3.

Keywords: ALGORITHM, INFORMATION TRANSMISSION METHOD, EVALUATION, SATELLITE COMMUNICATION SYSTEM, DUAL METHOD, VSAT STATION.

The purpose of the work is to analyze the known and develop a new method of primary protection of transmission of information channels for satellite systems. The main results of the work – the developed method of protection of information channels of the satellite network is based on the dual transmission of information simultaneously to two artificial satellites of the Earth, which are not interconnected. The algorithm of work of such complex "subscriber - satellite - subscriber - base station" is developed. Model researches of the developed algorithm are carried out.

The first section describes the basic configurations of the VSAT satellite network algorithm for information security and noise immunity.

The second section describes how to protect information networks that are based on VSAT communications systems.

The third section is experimental. It compares existing information feed security systems. Own hybrid method for protection of transmission information channels was created.

As a result of the preparation of the thesis, experiments and a comprehensive analysis were conducted to identify the factors that influence the protection of information channels in terms of external unauthorized interference and interfering environment.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ЕІВП	еквівалентно ізотропна випромінююча потужність
МККР	Міжнародний консультативний комітет по радіочастотах при ООН
ЕМЕ	електромагнітна енергія
ПК	персональний комп’ютер
ССЗ	супутникова система зв’язку
МСЕ	Міжнародний союз електрозв'язку
ЦКС	центральна керуюча станція
ШСЗ	штучний супутник Землі
СПРЗ	система просторової режекції завад
GEO	геостаціонарна орбіта, «Geostationary Earth Orbit»
LEO	низькі колові орбіти, «Low Earth Orbit»
MEO	середньовисотні колові орбіти, «Medium Earth Orbit»
EEO	еліптичні навколоземні, «Elliptical Earth Orbit»
VSAT	Very Small Aperture Terminal
USAT	Ultra Small Aperture Terminal
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
DVB	Digital Video Broadcasting
FDMA	Frequency Division Multiple Access
VLAN	Virtual Local Area Network, стандарт IEEE 802.1Q
DSCS	Defense Satellite Communications System

ВСТУП

Актуальність теми дослідження. Надшвидкими темпами розвиваються інформаційно-телекомунікаційні системи, які паралельно надають поштовх для розвитку систем зберігання, захисту та достовірності переданої інформації. Це відбувається на основі розвитку цифрових технологій. Захист інформації має як зовнішні так і внутрішні складові.

Кібербезпека – це технологія, яка є основою захисту внутрішніх інформаційних каналів на основі програмного забезпечення. Зовнішні чинники захисту інформаційних каналів при організації передачі на основі бездротових технологій ґрунтуються на технічних характеристиках антенних систем та вхідних ланок радіотехнічних систем, комплексів.

Один із таких поширених систем бездротового зв’язку – супутниковий зв’язок на основі технологій VSAT, передача даних, телебачення, радіолокація.

Епоха розвитку супутникового зв’язку почалась у 50-60 роки XX століття і на теперішній час є альтернативою наземного зв’язку, а у багатьох випадках і переважає з точки зору доступності та покриття території.

Враховуючи вищесказане, технічні характеристики різного роду терміналів, систем повинні відповідати заявленим даним та бути максимально адаптованими до електромагнітної сумісності, завадостійкості з другими системами. Завадне середовище може суттєво змінити структуру інформаційних каналів, внести завади, зменшити рівень.

На сьогднішній час є багато методів для боротьби з завадним середовищем, зовнішнім несанкціонованим втручанням, але вони в повній мірі не забезпечують на 100 % захист інформації, яка передається системами зв'язку.

Метою дипломної роботи є аналіз, систематизація існуючих методів боротьби з завадними інформаційними полями, які створюються як природнім шляхом так і штучним, створення нового методу гібридного типу для підвищення первинного інформаційного захисту каналів зв’язку, достовірності та ідентичності переданого й прийнятого сигналів.

Основні завдання дослідження:

- провести аналіз архітектурних топологій існуючих систем супутникового зв’язку, які функціонують на різних штучних орбітах навколо Землі:
- розглянути існуючі методи захисту інформаційних каналів зв’язку;
- дослідити алгоритми роботи систем супутникового зв’язку з точки зору захисних функцій зі зменшення впливу дестабілізуючих факторів завадного середовища;
- здійснити оцінку достовірності організаційних та енергетичних методів захисту інформаційних каналів зв’язку;
- дослідити методи режекції для зменшення завадного шкідливого інформаційного поля;
- створити новий гібридний дуальний метод з покращеними кількісними та якісними характеристиками переданої інформації супутниковими каналами зв’язку;
- розробити алгоритм роботи гібридного методу;
- оцінити технічні характеристики систем передачі інформації;
- порівняти даний метод з існуючими.

Об’єктом дослідження є система супутникового зв'язку за технологією типу VSAT та методи первинного захисту інформаційних каналів зв'язку від зовнішнього завадного середовища.

Предметом дослідження є системи супутникового зв’язку геостаціонарного типу, засоби аналізу параметрів інформаційних каналів зв'язку, просторових параметрів електромагнітних хвиль, методи подалення паразитних завадних сигналів.

Теоретико-методологічною базою дипломної роботи є сучасна теорія та фундаментальні концепції створення систем з первинного захисту інформаційних каналів супутникового зв'язку, кібербезпеки.

Інформаційну базу дипломної роботи склали: вітчизняна і закордонна література, міжнародні Регламенти радіозв'язку, норми та законодавчі акти міжнародного консультативного комітету по радіо при ООН, законодавчі акти,

ТСЗІ, закони України (РНБО України) з точки зору інформаційної та кібербезпеки.

Наукова новизна отриманих результатів. У дипломній роботі отримані наступні наукові результати:

– створено гібридний дуальний метод ефективної боротьби з завадним середовишем при передачі інформаційних каналів супутникових систем зв'язку;

– створено алгоритм роботи методу при первинному захисті інформації;

– виконано порівняльну характеристику параметрів сигналу з ідентичності та достовірності переданої інформації у порівнянні з другими методами з подавлення завадних сигналів.

Практичне значення одержаних результатів. Впровадження гібридного дуального методу підвищення безпекового первинного рівня у боротьбі з завадним середовищем природного та штучного характеру дасть можливість більш ефективно виконувати сеанси зв'язку та передачу інформації супутниковими каналами зв'язку, а саме:

- збільшення коефіцієнту достовірності та ідентичності переданої інформації каналами зв'язку;

- збільшення рівня подавлення завадних сигналів, особливо штучного походження;

- покращення ефективності роботи системи.

Апробація результатів роботи та публікації. Результати проведеного дослідження опубліковано у матеріалах VIII Міжнародної науково-технічної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ», 27-28 листопада 2019 року, м. Тернопіль.

Структура та обсяг дослідження. Дипломна робота складається зі вступу, семи розділів, висновків, списку використаних джерел і додатків. Загальний обсяг основної частини дипломної роботи складає 102 сторінок комп’ютерного тексту.

Дипломна робота містить 8 таблиць, 26 рисунків, 2 додатки на 3 сторінках. Перелік бібліографічних джерел нараховує 42 найменування.

РОЗДІЛ 1 АНАЛІЗ ПЕРВИННОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ СУПУТНИКОВИХ КАНАЛІВ

1.1 Супутникова мережа передачі даних типу VSAT

У даний час розвиваються активно наземні (дротові та бездротові) та системи супутникового зв'язку. Останні в порівнянні з наземними бездротовими та кабельними мережами мають багато істотних переваг:

- використовують значно більш широкі охоплюючи площі земної поверхні. Вони не залежить від інфраструктури наземних мереж комунікаційних, а це значить, що в віддалених і малонаселених соціорегіонах є найбільш технічно оптимальними і економічно виваженими рішеннями.

- наявність систем супутникового зв'язку дозволяє забезпечувати телекомунікаційним зв'язком і об'єднати внутрішні регіональні комунікації населених пунктів, участків правоохоронних органів різних структур, таких як міністерство внутрішніх справ, податкові фіскальні служби, пограничні структури та термінали та ін. у одну інформаційно-телекомунікаційну мережу.

Отже, супутниковий зв’язок на теперішній час є практично однією з найбільш затребуваною технологією, яка дозволяє здійснювати: телефонний і факсимільний зв'язок, доступ до міжнародних світових мереж таких як Інтернет, ретрансляція відеоконференцій та ін. Для створення таких мереж зв'язку широко використовують системи супутникових технології, типу VSAT, USAT (рис.1.1).

Позначення та ідентифікація «VSAT» була введена термінологію супутникового зв’язку в 1983 році з метою ідентифікації абонентських та корпоративних станцій з антенами невеликих діаметрів рефлекторів робочих поверхонь наземних станцій до (2,4-3,0) м із антенами (рефлекторами дзеркальних поверхонь) великих розмірів, більше 3,0 м.

В основі мереж супутникового зв'язку за такими технологіями. Типу VSAT будуються на основі космічних супутників-ретрансляторів, які розміщаються на геостаціонарній орбіті, у площині екватора Землі. Одним з найбільш суттєвих істотних переваг такого виду супутникового зв'язку за технологіями VSAT,

USAT є їх майже повна мережева незалежність від наявності регіональних місцевих наземних провайдерів Інтернет послуг.

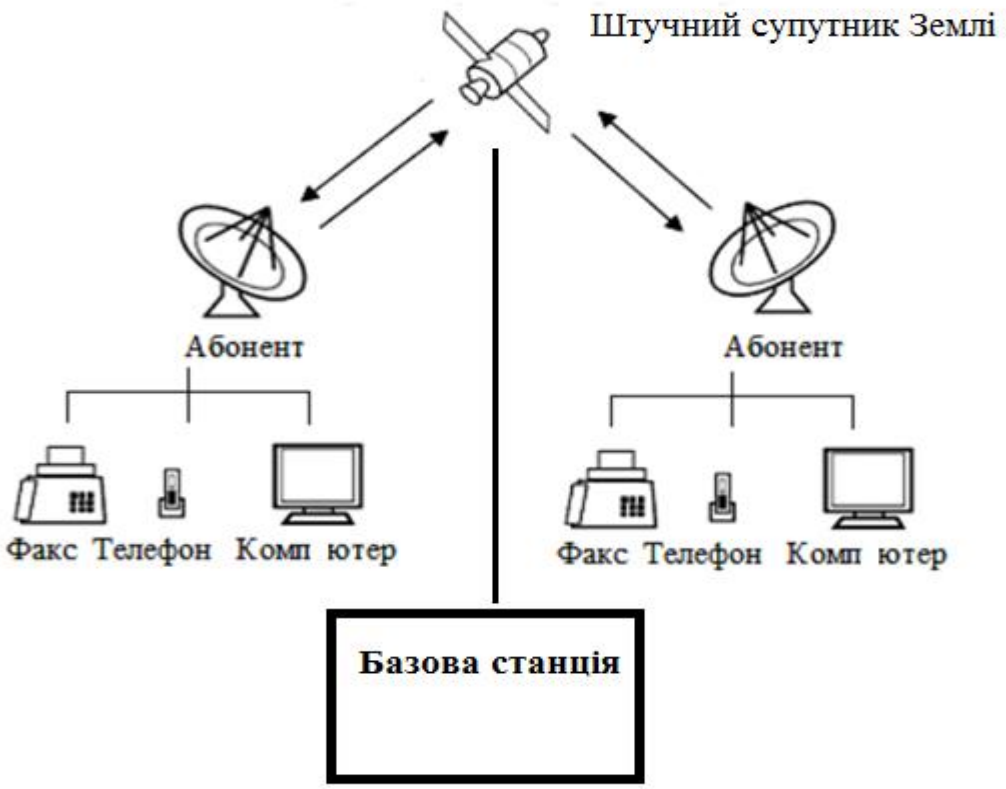

Рисунок 1.1 – Варіант структури мережі супутникового зв’язку типу VSAT

Для можливості здійснення зв'язку в мережах з використанням технології VSAT необхідно забезпечити тільки пряму видимість на супутник - ретранслятор.

Крім космічного супутникового апарату в мережу супутникового зв'язку входять такі об’єкти, як: центральна управляюча станція (ЦКС), операторська супутникового зв'язку і абонентські регіональні віддалені термінали VSAT, USAT. ЦКС комплектується приймально-передавальною апаратурою, антенними системами з фідерними пристроями, комплексом контрольно-діагностичного та контрольно-вимірювального обладнання, для виконання функцій контролю, діагностики, керування, аналізу роботи всієї регіонально - абонентської супутникової мережі, з можливістю перерозподілу її ресурсів при повному завантаженні однієї з ланок, виявлення несправностей, спряження з

мережами наземних ліній зв'язку.

На рис. 1 показана спрощена структурна схема «абонент – абонент – базова станція» мережі супутникового зв'язку за типовою технологією VSAT.

VSAT – регіонально-абонентські термінали з малою апертурою робочих поверхонь антен.

USAT – абонентські термінали з дуже малими робочими діаметрами дзеркальними антенами, менше 0,6 м.

Відповідно до міжнародного Регламенту Міжнародного союзу електрозв'язку (МСЕ), де вказані виділені діапазони частот для систем супутникового зв'язку приведено у таблиці 1.1.

Таблиця 1.1 – виділені частоти для систем супутникового зв’язку

№ п/п	Назва діапазону	Смуги частот, ГГц	Діаметр антени, м	Область використання
1.	L -	1.452 – 1,550 1,610 – 1,710		Рухомий супутниковий зв’язок
2.	S -	1,93 – 2,70		
3.	C -	3.40 – 5.25 5,725 – 7,075	2.4 – 2,5	Факсимільний супутниковий зв'язок
4.	Ku-	10,70 – 12,75 12,75 – 14.80	0,6 – 1,5	Факсимільний супутниковий зв'язок, телетрансляція
5.	Ka	15.40 – 26,50 27,00 – 30,20	0,3 – 0,9	Факсимільний супутниковий зв'язок, міжсупутниковий зв'язок

Такі канали передачі інформації передбачають досить високий рівень кодування, дешифрування, збереження та захисту переданих і отриманих даних.

Системи зв'язку за технологією типу VSAT «транспортують» і оберігають

передану інформацію досить надійно у порівнянні з іншими технології зв'язку, Це дає можливість вибирати регіональними абонентами - користувачами для резервування власних наявних каналів як більш безпечні з безпековою та достовірної технічної точок зору для максимального можливого захисту інформації від ушкоджень, завад, несанкціонованого втручання і можливих збоїв.

Передача інформації цифрового або аналогового типів в мережах VSAT характеризуються досить низькими рівнями помилок - не більше однієї на 10 млн.

При дослідженні різних комунікаційних мереж, таблиця 1.2, можна прослідкувати високу достовірність інформаційних потоків переданої інформації.

Таблиця 1.2 – якісні характеристики комунікаційних мереж зв’язку

Назва мережі	Рівень помилок при передачі інформації	Достовірність переданої інформації, %
Кабельна	2×10^{-5}	93
Наземна стільникова	9×10^{-5}	81
Наземна радіорелейна	5×10^{-5}	92
Супутникова факсимільна	2×10^{-5}	93
Супутникова VSAT	1×10^{-6}	97
Міжсупутникова	1×10^{-7}	99
Іоносферна	3×10^{-5}	87
Тропосферна	2×10^{-5}	85

При перерахунку на передані біти інформації (майже орієнтовно одна помилка на 500 текстових сторінок).

Надійність роботи такої системи (статистично) – до 100 тис. год., що у перерахунку майже понад 10 років круглодобового безперебійного супутникового зв'язку.

Швидкість трафіку такими супутниковими каналами для абонентських терміналів VSAT складає 16 Кбіт/с … 100 Мбіт/с, що дорівнює швидкості передачі інформації в наземних мережевих каналах, крім волоконно - оптичних.

Супутникові сигнали, так як і сигнали радіорелейних зв’язкових ліній мають схильність до суттєвого послаблення у вологому атмосферному кліматі (дощ, туман, велика хмарність), тому для конкретної місцевості, при врахуванні багаторічних цілодобових кліматичних спостережень, необхідно враховувати вплив погодних умов при проектуванні систем при оптимальному виборі встановлення антенної системи.

Технологія VSAT спочатку орієнтувалась в основному на надання операторам даного зв'язку закріплених одиночних каналів SCPC для організації систем віддаленого доступу супутникових мереж телефонії. Потім оператори перейшли з пропозиції голосових послуг до інтегрально - комбінованих телематичних послуг, які в свій склад включають послуги з передачі спочатку аналогових а тепер цифрових даних.

Орієнтація системи VSAT направлена на використання протоколів IP і Frame Relay, які є на транспортному рівні цих систем. Спеціалізовані програми, які необхідні для використання при передачі даних з одного комп'ютера і прийому їх інший комп'ютер споживача (абонента). Транспортний рівень - TL (Transport Layder) – це є рівень мережі супутникового зв'язку, який відповідає за організацію доставки інформативних потоків без помилок, з мінімальними завадами у межах допустимих. втрат і дублювання в переданій послідовності пакетів. Протокол IP – це один із самих основних протоколів передачі даних, який об'єднав окремі регіональні комп'ютерні мережі в загальну мережеву сітку. Цей протокол входить у загальний стек (набір) протоколів TCP / IP.

Протокол управління TCP (Transmission Control Protocol) – це є протокол управління передачею даних. У міру розвитку та функціонування глобальних мереж супутникового та наземного зв'язків з'явилася нагальна потреба в передачі достовірної інформації та її захисті.

1.2 Основні методи інформаційної безпеки супутникової мережі

На основі вище приведеного можна визначити основні методи забезпечення інформаційної безпеки передачі пакетів інформації бездротовим супутниковим каналом від одного абонента до наступного або кількох абонентів є:

- обмеження доступу на фізичному рівні до каналу зв'язку;
- використання апаратно-програмних засобів із захисту інформації, де застосовується протокол SCPC (Single Channel Per Carrier) – це один інформаційний канал на несучу частоту;
- протокол IP (Internet Protocol) – який є міжмережевим протоколом;
- технологія передачі даних Frame Relay (ретрансляція кадрів) – яка є високошвидкісною, створена на алгоритмі комутації пакетів, для передачі цифрових даних між високоінтелектуальними крайніми пристроями типу маршрутизаторів або FRAD, які мають можливість працювати зі швидкостями 56 Кб/с - 1.544 Мб/с.

Реалізація цього першого методу забезпечується безпекою супутникового мережевого зв'язку і передбачає здійснення цілого комплексу організаційних і науково - адміністративних заходів з метою захисту регіонального та базового вузла зв’язку. Сама безпека об'єкту (система супутникового зв’язку) забезпечується основними заходами як на фізичному так і на інженерному рівнях захисту інформації:

- забезпечення фізичної охорони об'єкту зв’язку;
- встановлення загальної огорожі навколо об'єкту системи зв’язку;
- встановлення сигналізації, яка є частиною пакетної передачі інформації;
- встановлення та ведення цілодобового відеоспостереження;
- дія режиму автоматизованих перепусток з інтелектуальною фіксацією.

До технічних засобів інформаційного захисту від перешкоджання несанкціонованого доступу можна також віднести:

- ідентифікація – розпізнавання, або ототожнення потенційного користувача за його унікальним зареєстрованим іменем та шифром доступу;
- аутентифікація – це встановлення та підтвердження автентичності

користувача (абонента), який представив власний ідентифікатор або загальна перевірка того, що дана особа, чи її використовуваний пристрій є тим інструментом, на основі якого він себе видає, Це є найбільш поширений спосіб. Крім цього при аутентифікації використовується власний пароль;

- авторизація – це є ідентична перевірка повноважень і прав абонента (користувача) при виконанні доступу до конкретних інформаційних ресурсів. Авторизація здебільшого проводиться з метою проведення розмежування прав доступу споживача до мережевих ресурсів систем зв’язку та комп'ютерних ресурсів локальної мережі.

Крім цих процедур технічним персоналом виконуються регламентні роботи з резервного архівування та копіювання баз даних та збереження конфігурацій всіх ключових серверів.

Ці системи захисту використовують від зовнішнього фізичного та інженерного захисту при проникненні на об’єкт.

Проти несанкціонованого навмисного доступу всередині об'єкту зв’язку, використовують до каналів зв'язку логіни, ключі, шифри, паролі.

Другий метод забезпечення інформаційної безпеки системи, що працює у супутниковій мережі та переданої інформації за технології VSAT, пов’язаний з програмно – апаратними засобами з точки зору захисту інформації у супутникових каналах зв'язку. Рівень безпеки забезпечується завдяки виконанню кодування, створення спеціальних видів цифрової модуляції та шифруванню переданих даних. Кодування пакетів інформації – це є процес перетворення переданих цифрових пакетів даних з форми, зручної для попереднього використання інформації, у спеціальну форму, яка є зручною для передачі, архівування, зберігання та автоматичного перетворення у двійковий код і обробки.

Шифрування даних, які передаються – це є процес перетворення пакетів інформації за допомогою шифрів, ключів так, щоб на другому приймальному кінці мережі її не зміг прочитати сторонній споживач. Крім розроблених відкритих протоколів, які є необхідними для передачі пакетованих даних з одного комп'ютера споживача (абонента) та прийому їх другим комп'ютером

абонента, в процесі удосконалення систем передачі даних були розроблені стандарти захищеності протоколів, Один із таких протоколів є протокол IPsec. Він забезпечує без пекову роботу системи на мережевому рівні.

NL (Network Layer) – це є мережевий рівень, який визначає можливі шляхи передачі даних, адреси, встановлену маршрутизацію. На теперішній час існують 12 стандартизованих протоколів IPsec: RFC2401, ..., RFC2412.

Протокол IPsec, або повний набір цих протоколів забезпечує у мережі:

- загальну цілісність віртуального з'єднання;

- проведення аутентифікації джерела інформації за протоколом AH (Authentication Header);

- шифрування переданої інформації за протоколом ESP (Encapsulating Security Payload);

- первинне налаштування можливого віртуального з'єднання, виконання взаємної аутентифікацію та обмін при сеансі передачі даних конфіденційними ключами.

Ці протоколи є основними апаратно-програмними способами та методиками за відповідними алгоритмами з захисту інформації. Вони входять у апаратно-програмний метод із захисту інформаційних пакетів, і є спеціалізованими програмними продуктами. Реалізуються вони за допомогою апаратно - технічних засобів, а саме: блоки живлення, вузли пам'яті, частотні генератори, приймально-передавальні модульні пристрої та ін.

У теперішній час сучасні двохсторонні супутникові мережі за технологією передачі даних VSAT використовують потужні системи шифрування на програмному та апаратному рівнях. Такі комбінації роблять перехоплення інформації радіоканалами майже неможливими і зводяться до нульової відмітки. Супутниковий канал передачі інформації в напрямі від базової станції до терміналу абонента (користувача) вважаються прямими супутниковими каналами стандартів модуляції та шифрування, типу DVB-S, DVB-S2, Frame Relay.

Ці канали всієї супутникової мережі з абонентських терміналів є єдиними і однаковими для всіх операторів. Цими каналами здійснюється передача

конфігураційних параметрів та команди керуючих команд абонентів (регіональних операторів). Крім цього цими каналами передаються призначені для користувача конфіденційні дані. Вся ця інформація пакетується і передається супутниковими каналами. Передаючі дані проходять багатоступеневу перевірочну систему з перетворень і шифрування. У результаті цих процесів здійснюється:

- застосування для передачі фірмових алгоритмів шифрування, модулювання даних;

- перевірка ідентичності терміналу при його початковій реєстрації у супутниковій мережі з перевіркою апаратного ключа;

- проведення шифрування спочатку всього сеансу роботи системи з програмним ключем, так і створення сеансових ключів кожного сеансу окремо;

- використання та застосування фірмових алгоритмів при перетворенні вихідних даних пакетів у внутрішні структурні формати цих даних, які потім будуть передаватись через супутникові канали зв'язку. На основі цього вирішуються завдання виконання додаткового захисту інформаційних каналів, проведення доставки службової конфіденційної інформації і проведення постійної корекції помилок;

- можливості прискорення трафіку передачі даних згідно протоколу TCP/IP;

- у створюваних на основі цього віртуальних каналах вихідні пакетні цифрові дані групуються у сеансах TCP, компресуються (стискаються) і отримують загальні пріоритети.

У напрямах від абонентських терміналів до базової станції або інтегрованого абонентського терміналу супутникові канали є зворотними каналами. Супутникові ланки окремої мережі терміналів інтегрованого оператора можуть працювати відразу з багатьма, в залежності від конфігурації мережі та алгоритмів роботи зворотними каналами. Така система роботи цих пристроїв методи роботи дозволяють констатувати факт захищеності даної супутникової мережі.

Метод підвищення скритності при передачі угрупування вузькосмугових

сигналів, який полягає у випромінюванні двох ідентичних сигналів: корисного і маскуючого. Сигнали додаються, перетворюється маскуючий сигнал і в подальшому усувається (фільтрується). Випромінювання групи корисних сигналів відбувається незалежно від маскуючих, причому паралельне випромінювання маскуючих сигналів відбувається у діапазоні робочих частот для всієї групи корисних сигналів. Маскуючий сигнал формується на основі з вузькосмугового корисного сигналу шляхом завідомо розширеного його спектру частот за рахунок однієї з модуляцій (частотної або фазової), варіант модуляції відомий власним приймаючим пристроям. Перетворення всіх вхідних сигналів та маскуючих відбувається таким чином, що загальний спектр маскуючого сигналу спочатку звужують, а спектри інших корисних вхідних сигналів розширюють. Потім відбувається режекція маскуючи сигналів і такі сформовані пакети даних передають. На приймальній стороні проводять зворотні процедури і тим самим відновлюють інші вхідні сигнали.

Метод спеціального радіозв'язку теж використовується при інформаційній безпеці. Він ґрунтується на формуванні, передачі та наступному прийомі вузькосмугового інформаційного сигналу передавальним та приймальним пристроями на одній частоті несучого коливання. Основна відмінність від системи стандартного передавально – приймального варіантів полягає у тому, що додатково з вузькосмуговим корисним інформаційним сигналом паралельно замішують та випромінюють завадний сигнал гребневої структури. Спектральна та енергетична характеристики складових частин гребня такого сигналу є аналогічна до спектральної та і енергетичної характеристик цього ж вузькосмугового корисного інформаційного сигналу. На приймальній стороні системи здійснюють фільтруваннявузькосмугового корисного інформаційного сигналу від завадого сигналу гребеневої структури.

Розглянуті методи – це групові випромінювання корисних вузькосмугових та маскуючих сигналів, використання з вузькосмуговим корисним інформаційним сигналом завадного гребеневого сигналу досить ефективно використовуються у системах зв’язку.

Методи модуляції параметрів змішаних за певним законом (алгоритмом)

хаотичного сигналу та корисного цифрового сигналу.

Такі сигнали формують та передають цілісним пакетом каналами зв'язку, на приймальній стороні їх поділяють на два ідентичних сигнали з подальшою обробкою. Системою синхронізації є аналогічний генератор хаотичних сигналів на передаючій стороні. Враховуючи режим узагальненої синхронізації, і знятий з виходу генераторів хаотичних сигналів ругого та третього порядку на різницевому пристрої виділяють наявний корисний цифровий сигнал. Корисний цифровий сигнал створюють на основі та у вигляді двійкового коду.

Метод використання шумоподібних інтегрованих сигналів є серед різних методів для захисту цілісності інформації на теперішній час широко відомий. Він характеризується підвищенням пропускної спроможності каналів передачі та високого рівня завадо захищеності каналів зв'язку.

Даний метод є широко використовуваний такими технологіями як VSAT системи та CDMA.

Технологія CDMA це є зв'язкові наземні системи з кодовим поділом каналів. Вони мають найбільший рівень критеріїв завадо захищеності. Крім цього така технологія CDMA дозволяє забезпечувати високі якісні характеристики передачі інформації при суттєвому зниженні випромінюваної потужності. Високу енергетична скритність інформаційних каналів та конфіденційність переданих даних відбувається внаслідок використання шумоподібного сигналу, який є переносником інформації. Одна із переваг такого методу – це є зменшення (придушення) інформації в каналах зв'язку при кодовому поділі каналів шляхом постійного відновлення кодових комбінацій у кожному переданому інформаційному імпульсі.

До цих методів використання шумоподібних сигналів в якості переносника інформації можна також віднести кодування корисного сигналу за допомогою генератора хаотичних детермінованих сигналів.

Метод передачі інформативних каналів з нелінійним підмішуванням шуму також відносять до вище приведених методів боротьби з інформаційною безпекою. Алгоритм передачі інформації ґрунтується на нелінійному підмішуванні інформаційного сигналу при допомозі функціонального суматора

із з використанням дискретних відображень.

Зазначені відображення, при відповідних значеннях керуючих параметрів, здатні створювати складну періодичну та хаотичну структуру або хаотичну послідовність. Отже, така генерація хаотичної послідовності може бути вибором значення керуючого параметру. Це кожне конкретне значення керуючого параметра створює закритий «ключ» для каналу передачі інформації.

1.3 Способи конфігурації та функціонування мереж VSAT терміналів

Найбільш поширеними способами конфігурації функціонування терміналів у таких каналах зв'язку є можливість створення принципів доступу з тимчасовим і тимчасово - частотним поділом каналів зв'язку TDMA / FDMA, а саме:

TDMA – це є спосіб використання відведених радіочастот, коли в одному частотному інтервалі створена можливість використання кількох абонентів;

FDMA – це спосіб використання заданих радіочастот, де в одному відведеному частотному діапазоні працює тільки один користувач (абонент);

DVB – стандарт цифрового відео трансляції;

TDMA – це технологія множинного доступу з поділом за часовими проміжками;

FDMA – це множинний доступ з поділом за частотою.

Кожен зворотний абонентський канал працює у власній відведеному певному частотному проміжку (смузі) із власною несучою модульованою частотною складовою та з створеним спеціальним алгоритмом кодування з метою виявлення та корекції помилок, які можуть передаватись пакетами даних у Turbo Coding.

Кожний конкретний абонентський термінал здатний здійснювати передачу інформації тільки в одному зворотному каналі.

Але у багатьох можливих випадках на спеціалізованому обладнанні вже

реалізована можливість зміни несучих смуг частот цих зворотних каналів. На цей час термінали здійснюють передачу за технологією FDMA від одного абонента (користувача) сеансу до іншого. Такий спосіб дозволяє, з одного боку, створювати перерозподіл всіх можливих передавальних абонентських терміналів за зворотніми каналами у середині їх групи (балансування загальним навантаженням мережі), а з іншого боку це значно ускладнює можливість перехоплення переданих інформаційних даних.

Кожен абонентський зворотний канал поділяється на часові складові інтервали. Він у терміналі не є безперервним, а є послідовністю створених імпульсних сигналів, де тривалість кожного імпульсу не перевищує значення кількох мілісекунд.

Метод багатостанційного доступу з TDMA дає можливість працювати в режимі передачі з великою кількістю терміналів. Дані цифрових пакетів передаються у виділені методом тимчасові інтервали для кожного одного каналу або для групи каналів. Шифрування пакетованих даних у супутниковому каналі передачі даних відбувається за участі як у терміналах супутникового зв'язку на стороні одного абонента (користувача), так і на спеціальних високопродуктивних серверах базової станції або оператора.

На спеціалізоному сервері користувача-оператора встановлюється захищена системна база ключів шифрування та сеансних ключів для всіх супутникових терміналів. Щоб даний термінал зміг працювати в мережі оператора, вся інформація від бази ключів основного оператора повинна співпадати з апаратним ключем, який зберігається на базовому сервері терміналу.

Така структура має можливість виключити несанкціоноване підключення до терміналів "чужого" користувача. Генерація ключів та їх поширення відбувається за початковим алгоритмом, який встановлений у обладнання виробником. Всі термінали виготовляють з врахуванням повної захищеності від вилучення цих ключів шифрування, будь-якого впливу зовнішніх сигналів та дестабілізуючих факторів, а також від можливого демонтажу та розбирання обладнання з метою дослідження та аналізу.

На серверах базових чи центральних станцій оператори часто для міжсерверної мережевої взаємодії між собою використовують модифіковані транспортні спеціалізовані протоколи для забезпечення повного контролю за мережевими серверними інтерфейсами, а крім цього для захисту від несанкціонованого програмного та апаратного доступу до них.

Кожен сервер має дублюючий, віртуальний окремий ідентичний сервер. Цей сервер сам виконує всю роботу при можливому виході з робочого стану основного пристрою базової станції чи серверу оператору. Мережева взаємодія серверного обладнання логічно розділена на умовно віртуальні мережі за спеціалізованою технологією VLAN (IEEE 802.1Q), де дані для керування та контролю повинні бути ізольовані від тих даних, які призначені для другого абонента (користувача).

У результаті використання таких методів застороги всі можливі атаки на мережу «оператор – мережа – оператор» як з боку потенційних чи несанкціонованих користувачів або з боку міжнародної мережі Інтернету стають практично неможливими, а поширення вірусів у мережу та в самій мережі блокується.

Таким чином супутникові абонентські користувацькі термінали мають весь необхідний набір засобів на апаратному та програмному рівнях для забезпечення безпеки, так і для захисту всіх підключених терміналів до цих мереж. Одним із головних інструментів, який виконує захисну функцію є мережевий фільтр. Для виконання цих функцій його функціоналу досить, щоб знешкодити, заблокувати та виключити більшість атак на порти і протоколи мереж користувачів - клієнтів через канали супутникового зв'язку.

Реєстрацію різних помилок, завад, можливості спроб несанкціонованого доступу та навмисного злому надає такий сервіс мережі як генерація подій, які відбуваються на протязі сеансів.

Метод завадо захищеності при кодуванні – це програма Turbo Coding.

VLAN – це віртуальна комп'ютерна локальна мережа. Вона описана у стандарті IEEE 802.1Q.

При сенсі зв’язку інформація про події автоматично має можливість

передаватись на центральне управління базової станції оператора. Більш деталізований аналіз роботи абонентського терміналу також аналізується при допомозі записів у журналі подій.

Інформаційна безпека в мережах супутникового зв’язку за технологією VSAT, USAT підвищується також за можливу складність всіх використовуваних методів з метою організації функціонування абонентських зворотних каналів та застосування власних фірмових алгоритмів при роботі з ними.

Застосування спеціальних шифрувальних засобів апаратури дає можливість використовувати супутникові канали зв’язку також для передачі конфіденційної та закритої інформації, яка має найвищі пріоритетні рівні грифу.

Такі засоби підключаються через стандартизовані пóрти. Порти є з синхронними та асинхронними інтерфейсами, які з’єднуються між абонентським комп'ютером або другим пристроєм обробки оперативної інформації та другим абонентським терміналом VSAT. Крі цього вони забезпечують криптографічну складову захисту інформації.

Таке телекомунікаційне рішення здійснюється при виконанні всього комплексу заходів з можливого захисту інформативних каналів.

Воно відповідає технічним вимогам з забезпечення інформаційної безпеки переданої інформації мережею супутникового зв’язку за допомогою технології VSAT.

З модернізацією та розширенням розвитку технологій такого супутникового зв'язку також розширюються можливості та удосконалюються методи захисту інформації.

1.4 Методи віртуального розширення смуги пропускання та збільшення пропускної спроможності каналів супутникового зв’язку

Технічні характеристики любого фізичного каналу супутникового зв'язку відрізняються від ідеальних. Зважаючи на це, канал зв'язку варіює (змінює) сигнали передачі. Для стійкості та синхронізації мережі зв’язку необхідно

враховувати топологію, за якою відбувається передача даних. Такими технологіями можуть служити наступні: Ethernet, PDH, dwdm, token ring та інші.

Одна із головних характеристик, яка впливає дуже суттєво на передачу даних – це смуга пропускання. Вона має постійний діапазон частот, у якому загасання сигналу не перевищують певний рубіж. В основному крайніми частотами є ті частоти, де потужність вихідного сигналу зменшується на 3 dB порівняно з вхідним. Ширина каналу (смуга) пропускання суттєво впливає на максимальний трафік транспортування даних лініями любого виду зв'язку. Смуга пропускання в основному залежить від технічних характеристик каналу та довжини або частотної смуги пропускання. На рис.1.2 продемонстровано смуги пропускання каналів різних типів зв'язку і частотні діапазони.

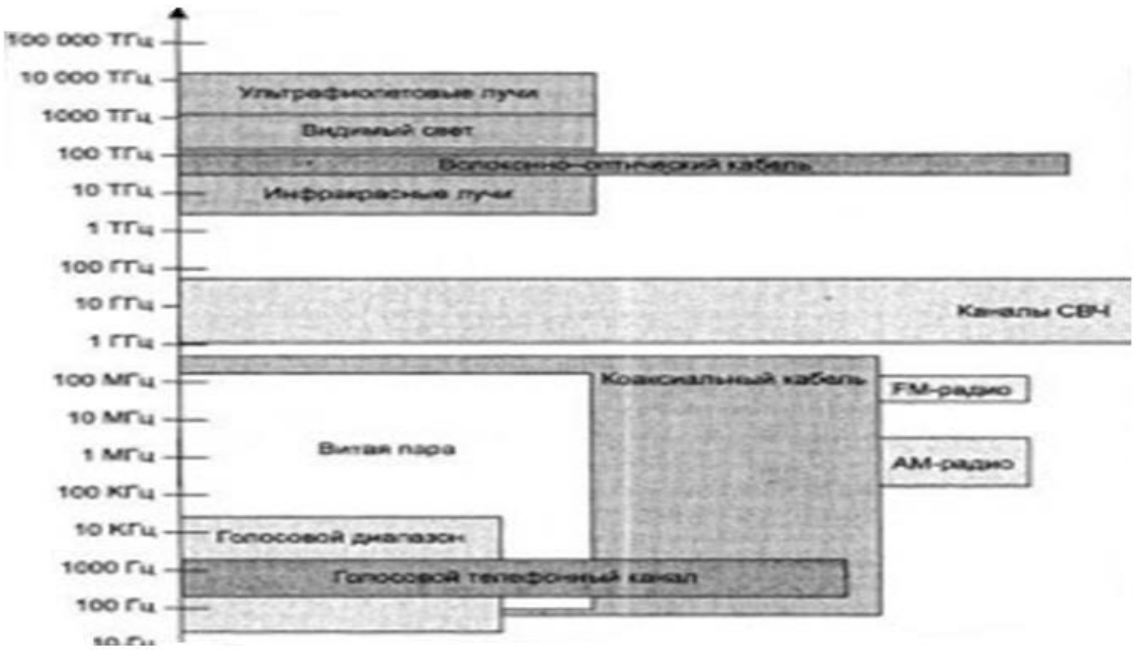

Рисунок 1.2 – Схема смуг пропускання систем зв’язку різних типів.

Пропускна здатність каналу зв’язку вказує на максимально допустиму швидкість (трафік) транспортування інформації, яка максимально розвивається на каналі. Особливістю пропускної здатності – це те,що параметр залежить від різних характеристик та дестабілізуючих факторів фізичного середовища та визначається загальним способом передачі інформації.

Отже, якшо не визначено протокол фізичного рівня, то не можна оцінити

пропускну здатність каналу зв'язку.

Вибір використовуваного протокол визначається політикою інформативної безпеки. Низька або недостатня пропускна здатність каналу може спровокувати проблеми та загрози з інформаційного захисту в мережах.

Для цифрових ліній необхідно враховувати, якщо відомий протокол фізичного рівня:

- бітову швидкість трафіку передачі інформації (64 Кбіт/с, 2 Мбіт/с та ін.);
- перехресні наведення,
- смуга пропускання каналу;
- стійкість перед завадами;
- технічні характеристики провідних ліній зв'язку;
- варіанти комутації каналів і пакетів.

Інформація в мережі зв’язку транспортується послідовно, по бітово.

У середині ПК інформативні потоки працюють паралельно. Це відрізняє ПК від мережі зв’язку на протокольному рівні.

Також пропускна здатність каналу залежить від самого спектру сигналу. Якщо необхідні гармоніки сигналу, ті де амплітуда вносить свій вклад в вихідний сигнал, і потрапляють в смугу пропускання, то даний сигнал буде добре транспортуватись даним каналом зв'язку, а приймаючий пристрій буде відмінно розпізнавати ці дані. Це рішення показано на рис. 1.3.

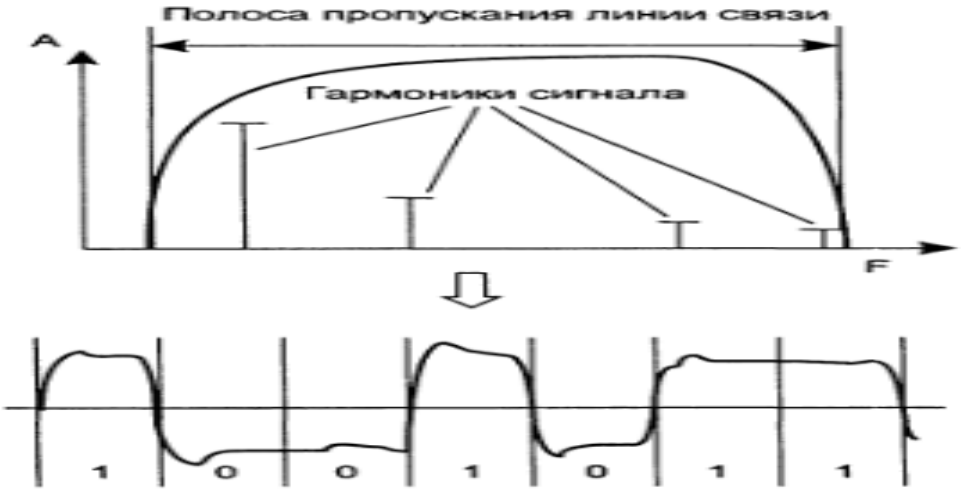

Рисунок 1.3 – Структура сигналів у каналі зв’язку з гармоніками у межах пропускної смуги каналу

Якщо основні гармоніки сигналу будуть виходити за межі пропускної смуги каналу зв'язку, то даний сигнал буде спотворений. Приймаючий пристрій буде постійно помилятися при декодуванні інформації, що показано на рис.1.4.

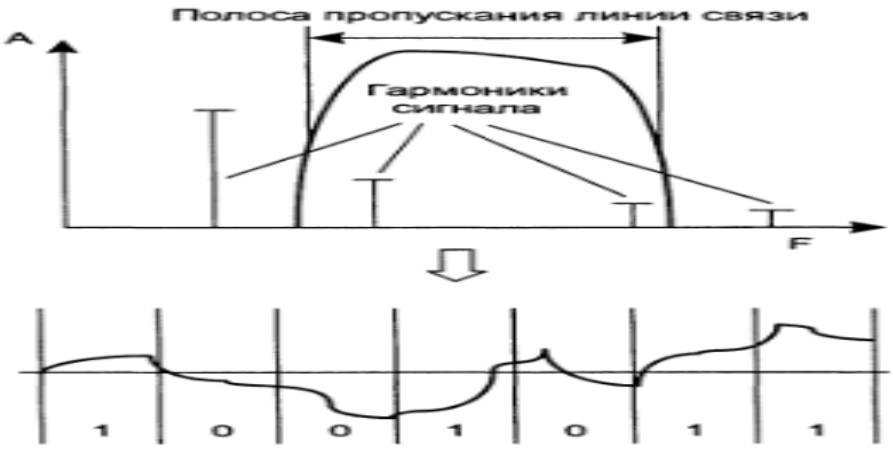

Рисунок 1.4 – Структура сигналів у каналі зв’язку з гармоніками за межами пропускної смуги каналу

Будь-які непередбачувані і мало помітні модифікації структури сигналу спотворюють загальну інформацію.

У результаті приймаючи синусоїдальний сигнал, де фаза, амплітуда і частота є незмінними, дані не змінюються і модифікація сигналу якщо мало відбувається, але кінцевий сигнал є достовірним і мала ймовірність його спотворення.

Якщо у модифікованому стані сигналу можна проаналізувати лише його два стани, то любий модифікований стан буде визначатись бітом - найменшою одиницею інформації.

Якщо сигнал має більше двох станів, то люба модифікація буде передавати кілька біт інформації.

Пропускна здатність лінії передачі залежна від мережевого адаптера та варіанту логічного кодування.

Логічне кодування передує фізичному і характеризується заміною бітів початкової інформації новою ланкою бітів, що несуть загальну інформацію і наділені додатковими характеристиками.

Логічне кодування вихідну ланку бітів модифікує у більш довгу ланку. Пропускна здатність лінії за відношенню до первинної корисної інформації зменшується.

Такий метод логічного кодування є одним з варіантів захисту інформації.

Біти інформації можна кодувати не тільки на фізичному та прикладному рівнях при передачі інформації.

Можна використовувати стандартизовані методи шифрування – RSA разом з другими методами шифрування. Це збільшить якість інформаційних сигналів.

Висновки до розділу 1

У першому розділі виконаний аналіз інформаційних джерел з точки зору інформаційної безпеки супутникових мереж та каналів зв’язку. Визначений пріоритет однієї із технологій передачі інформаційних каналів – VSAT станції, які на теперішній час є досить гнучкими, адаптованими до збільшення об’ємів інформації, захищеності від несанкціонованих втручань як ззовні так із середини мережі, мають можливість модернізовуватись, розширювати смуги частот, пропускну здатність сигналів.

Визначені та проаналізовані основні засади з захисту інформаційних каналів та протоколи передачі інформації, а саме:

- модернізація антенних систем з точки зменшення бокових пелюсток для підвищення завадостійкості системи;
- логічне кодування;
- завадо захищеність при кодуванні (Turbo Coding);
- багатостанційний доступу з TDMA;
- технологія множинного доступу з поділом за часовими проміжками;
- правильний вибір пов'язаний з програмно - апаратними засобами з точки зору захисту інформації
- кодування пакетів інформації у спеціальну форму;
- ідентифікація, аутентифікацію, авторизація пакетів переданої інформації

- технологія передачі даних Frame Relay.

У сукупності дані засади захисту інформації у мережах супутникового зв’язку підвищують ступінь переданої достовірної інформації без спотворень, завад та несанкціонованого впливу.

РОЗДІЛ 2 МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ МЕРЕЖ

2.1 Захист від завадного середовища

Враховуючи дуже швидкий розвиток різного роду систем зв’язку як наземного так і супутникового спрямування суттєво ускладнюється радіоелектронна обстановка особливо в регіонах міст.

Діючі процедури при розподілі радіочастотного ресурсу в Україні мають обмеження і тому не гарантують роботу станції без завад та помилок. Вирішення цієї проблеми потрібує високоефективні засоби завадозахисту для систем наземного супутникового зв'язку. Одне з найбільш перспективним, рішенням цієї проблеми є застосування систем просторової режекції для подолання завад на основі адаптивних антен, які можуть забезпечувати, враховуючи просторові відмінності технічних характеристик корисного сигналу та можливої завади, автоматичну адаптацію радіоліній до ймовірної завадної обстановки.

Враховуючи те, що завади є природного та штучного походження, то одна із основних проблем проектування та функціонування телекомунікаційних систем – це є захист каналів зв'язку від цих дестабілізуючих факторів. Перші методи захисту від радіозавадного середовища були створені в середині XX ст. та систематизовані у спеціальній літературі [2, 3]. Застосування цих методів завадного захисту систем зв’язку визначаються їх доцільністю та технічними можливостями при реалізації.

Широко ці методи використовуються у спеціальних та військових системах зв'язку. Тепер досить часто і оператори цивільних систем зв'язку мусять вдаватися до різних методів захисту від радіозавадного середовища.

Так як радіоелектронна обстановка суттєво ускладнюється особливо у багатонаселених пунктах (містах), та одночасно розвиваються радіоелектроніка і системи зв’язку, то ці ключові фактори спонукають реалізовувати технічно складні, але досить ефективні системи завадного захисту інформаційних каналів.

Рівні завадного шумового спектру можна визначити за допомогою формули 2.1,

$$\Psi = 20\lg(U_{сигн.}/U_{еф.ш.}) \qquad (2.1)$$

де, $U_{сигн.}$ – амплітуда розмаху сигналу;

$U_{еф.ш.}$ – ефективне значення вагомого шуму.

Амплітудно- частотні характеристики сигналів показані на графіку рис 2.1.

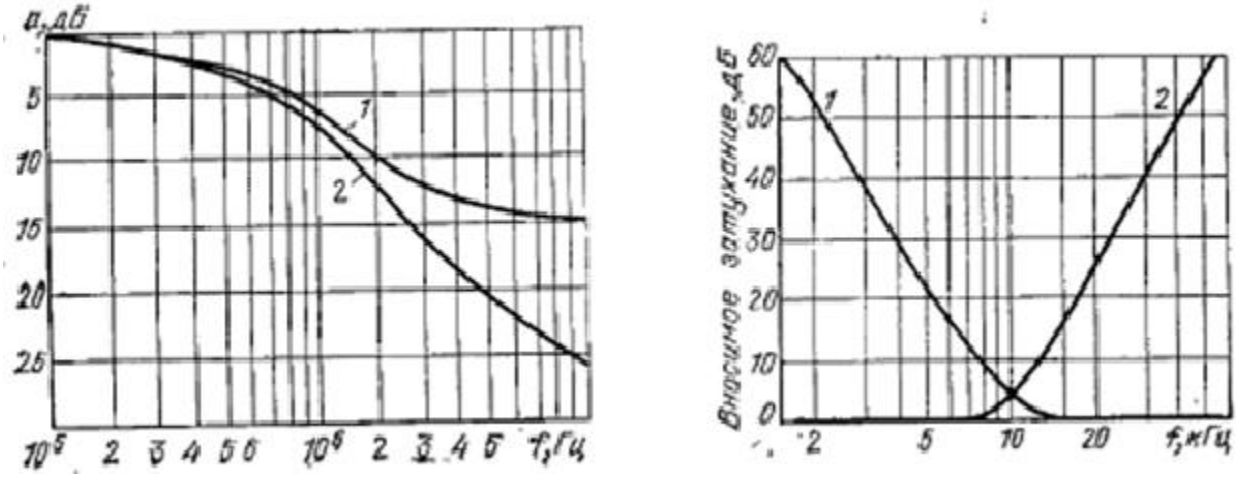

Рисунок 2.1 – Амплітудно частоні характеристики сигналів та флуктуаційних шумів (завад)

Між супутниковими системами зв’язку наземного базування та наземними системами зв’язку (радіорелейні лінії, стільниковий зв'язок та телефонія та ін.) часто виникають взаємні завади системного характеру. Структура завадного середовища та можливі варіанти завадної обстановки в одному секторі супутникового зв’язку показано на рис. 2.2. Допустимі рівні завадного середовища прийняті на рівні міжнародних рекомендацій на XVI Пленарній асамблеї МККР.

При визначенні умов існування наземних та супутникових систем зв’язку можна виділити 4 основні види завадного середовища:

- від передавача космічної станції у робочих смугах частот для радіоліній « космос – Земля»;

- від передавачів наземних станцій зв’язку на приймачі земних станцій у робочих смугах частот для радіоліній «космос – Земля»;

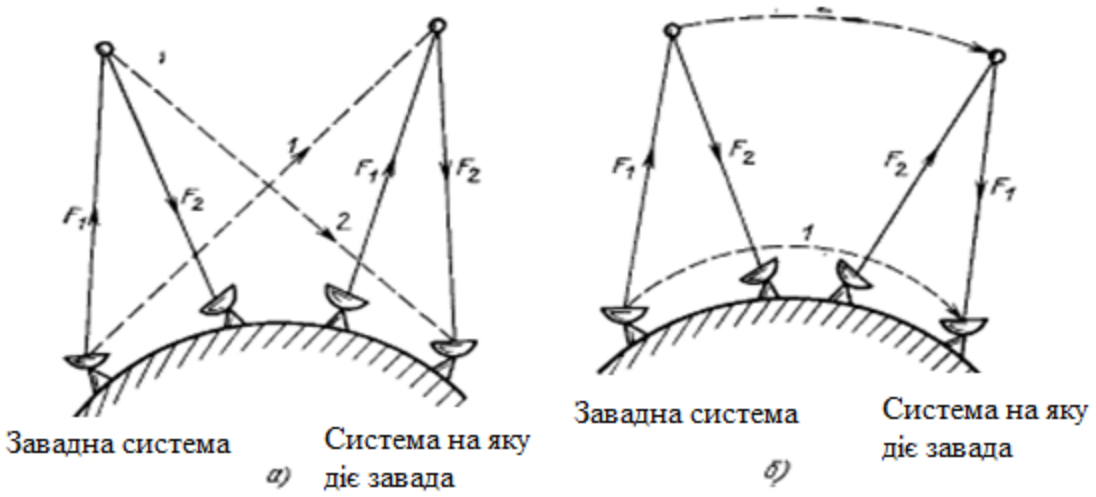

Рисунок 2.2 – Можливі завади між системами супутникового зв’язку:

а) при співпадінні напрямів передачі;

б) при реверсному використанні частого спектру.

- від передавачів наземних станцій зв’язку на приймачі космічних станцій у робочих смугах частот для радіоліній «Земля – космос»;

- від передавачів земних станцій на приймачі наземних станцій у робочих смугах частот для радіоліній «Земля – космос», рис.2.3.

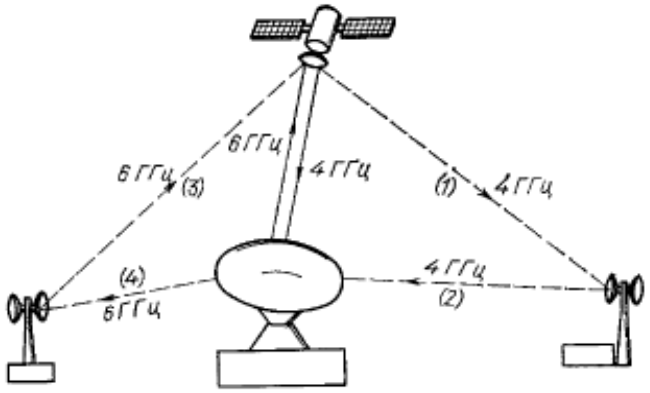

Рисунок 2.3 – Варіанти можливих завад між супутниковими лініями зв’язку з радіорелейними лініями

При використанні одного із варіантів первинного захисту інформативних каналів на вході антенної системи необхідно проаналізувати завадне середовище двома етапами, а саме:

- розрахунком відношення потужності корисного сигналу до завади на вході приймальної системи земної станції зв'язку, $(P_c/P_ш)_{вх.}$;

- або порівняти отримані дані з нормативними, або перерахувати шумову потужність завадного сигналу і потім порівняти з нормативним значенням. Це можна достовірно виконати, коли співпадають робочі смуги частот.

$$(P_c/P_ш)_{КС} = P_{ЗС} + G_1 - \Delta L_{ЗК} - \Delta L_0 - P_{з.п} - G_1(\theta) + \Delta G_2 + Y_{ЗК},$$
$$(P_c/P_ш)_{ЗС} = E + G_4 + \Delta L_{КЗ} - e - G_4(\theta) + Y_{КЗ}. \quad (2.2)$$

де, $(P_c/P_ш)_{кс}$, $_{зс}$ – відношення корисний сигнал – завада на лініях Земля – космос, та космос – Земля, dB;

$P_{з.с.}$, $P_{ш.}$ – потужність корисної та завадної складових, які підводяться до станції земної станції, dBBm;

G_1,G_4 – коефіцієнти підсилення передаючої та приймальної антен земної станцій;

$G_1(Q)$ – коефіцієнт підсилення передаючої антени на ШСЗ, на який впливає завада;

$G_4(Q)$ - коефіцієнт підсилення приймальної антени земної станції, на яку впливає завада;

е – ЕІВП корисного та завадного сигналів ШСЗ у напрямі на земну станцію;

ΔG_2 – різниця у коефіцієнті підсилення приймальної антени корисного ШСЗ у напрямі на завадну та корисну земну станцію;

ΔLзк, кз – різниця у втратах корисного сигналу та завади на відстані в лініях вверх та вниз відповідно [4].

Дані нормативні значення завадного середовища у системах супутникового зв'язку прописані у звітах МККР 455-2. Завадне середовище необхідно враховувати при використанні ліній зв'язку як вверх, так і ліній зв'язку вниз (реверсною зв'язкою).

Такий розрахунок дасть можливість врахувати максимально всі складові завадного середовища у бездротових супутникових системах а також дасть

пріоритети при правильному плануванні розміщення абонентських супутникових VSAT станцій.

$$(P_c/P_п)_{КС} = P_{ЗС} + G_1 - \Delta L_0 + \Delta G'_2 - e' + Y + 20 \lg \theta - 35{,}2, \quad (2.3)$$

де, $\Delta G'_2$ – різниця коефіцієнта підсилення приймальної антени ШСЗ у напрямі на передаючу земну станцію та завадну станцію ШСЗ;

е’ – ЕІВП завадного сигналу ШСЗ у напрямі на ШСЗ, на який впливає завадне середовище.

Виходячи з вищесказаного, можна визначити еквівалентне відношення корисних сигналів та завадного середовища у інформаційному супутниковому каналі зв’язку. Потім ці значення можна порівняти з стандартним значенням, які описані у Звіті 388-4 МККР.

$$(P_c/P_п)_{экв} = 10 \lg \left[1/\left(10^{-0,1(P_c/P_п)ЗС} + 10^{-0,1(P_c/P_п)КС}\right)\right]. \quad (2.4)$$

На рис.2.4. приведені загальні співвідношення сигналів до завади та сигналів до шумів при роботі систем супутникового зв’язку, зокрема, за технологією VSAT.

2.2 Методи завадозахисту

Виходячи з принципів реалізації методи захисту від завадного середовища, можна виділити наступні методи захисту від радіозавад:

- організаційні,
- енергетичні,
- сигнальні
- просторові.

2.2.1. Організаційний метод боротьби з завадним середовищем

Організаційний метод у первинному передбачає таке просторове

розміщення джерел радіосигналів та вибір робочих частот, при яких спроектовані та встановлені системи зв'язку не створюватимуть взаємних завад.

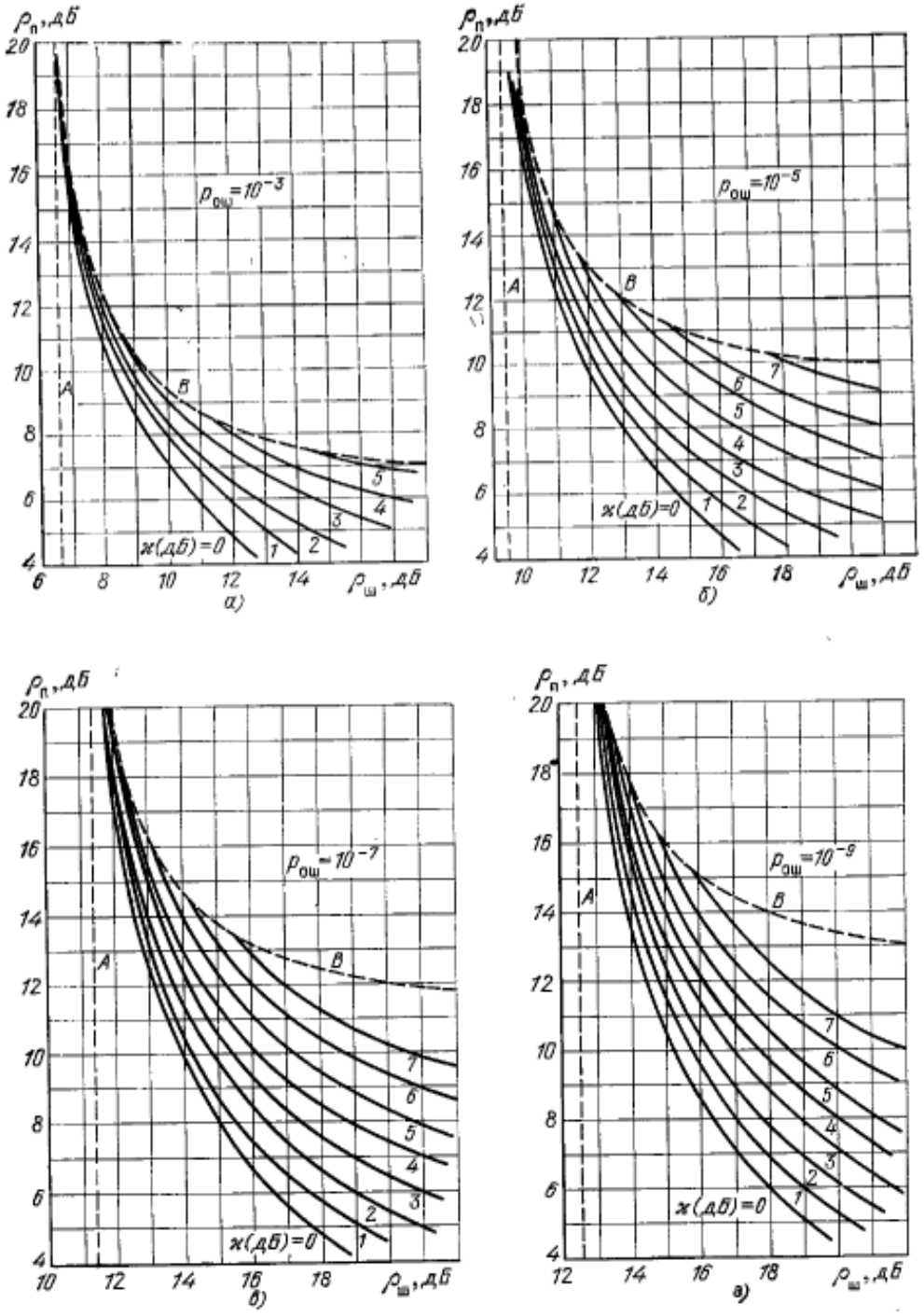

Рисунок 2.4 – Необхідні співвідношення сигнал – завадне ($Р_з$) середовище та сигнал – шум ($Р_ш$) при заданій ймовірності похибки при прийомі сигналів у системах супутникового зв'язку (χ – пік – фактор завадного сигналу).

Враховуючи складні умови мегаполісів та промислово розвинені регіони,

які надто насичені різного роду радіоелектронними засобами, стає очевидно, що метод частотно-територіального розносу систем зв’язку стає не дуже ефективним. Однак, враховуючи просторове планування та використання цифрових карт території мегаполісів з нанесенням діаграм спрямованості антен робочих систем різнопланового зв’язку, цей метод утвердився і постійно застосовується у формах, які вимагають беззаперечного виконання обов'язкових, визначених міжнародними та національними регуляторами та Регламентами основних процедур, які зв’язані з взаємної координацією та реєстрацією робочих смуг радіочастот для різних мереж зв’язку як супутникового так і наземного сегментів.

При виконанні зазначених процедур з постійної координації оператори зв’язку повинні підписати та виконувати угоди про взаємоприйнятні співвідношеннях сигнал/завада, сигнал/шум і в кінцевому варіанті досягти необхідних рівнів електромагнітної сумісності та завадостійкості власних систем.

Для реалізації цієї мети широко також застосовується метод поляризаційної та крос поляризаційних розв'язок як просторово так і в трактах самих систем. При необхідності може також використовуватись метод частотного сегментування. Він має можливість обмежувати використовуваний частотний спектр ресурсів робочих смуг, але оператори зв’язку змушені йти на цей вимушений крок з метою досягнення координаційних угод між собою та системою частотного нагляду на взаємоприйнятних умовах.

Суворе виконання регламентних міжнародних процедур і дотримання взаємних угод між операторами 20-30 років тому здавалося, що ці процедури забезпечать з високою ймовірністю функціонування супутникових та наземних систем зв'язку без можливих взаємних неприйнятних завад. Однак щодо радіочастотного забезпечення тепер вважається , що в системах супутниковому зв'язку особливо на низьких орбітах настає кризова ситуація, яка пов'язана з самою системою радіочастотного розподілу ресурсного потенціалу. Дана проблема може ще більше усугубитись, коли на низьких навколоземних орбітах буде виведено та розміщено ще понад 12 тис. телекомунікаційних ШСЗ для

обслуговування міжнародної мережі Інтернет, IP телефонії супутникового стільникового мобільного зв’язку.

Багато супутникових операторів констатують факти та визнають, що сучасні мережі супутникового телекомунікаційного зв'язку, пройшовши етапи координації, верифікації та реєстрації, отримують все більші рівні потужностей неприйнятних для систем зв’язку як хаотичних так і направлених завад.

Це означає, що раніше ефективний організаційний метод захисту від завадного середовища, який базується на постійно діючих міжнародних регламентних процедурах, частково вичерпав свої можливості втратив ефективність. Але цей зазначений метод з розподілу частотного ресурсу, який заснований на міжнародних і національних Регламентах, на теперішній час є одним із основних інструментів при радіочастотному регулюванні та недопущенності "радіочастотної анархії" у системах зв’язку.

2.2.2 Енергетичний метод боротьби з завадним середовищем

Другий метод, який є досить ефективним з точки зору ефективності роботи систем зв’язку – це енергетичний метод боротьби з завадним середовищем. Він передбачає збільшення потужності передаючих пристроїв до тих рівнів, які гарантовано перевищують потенційно можливі завади та штучні шуми у робочому спектрі робочих частот. Даний метод досить широко використовується у спеціалізованих та військових системах як супутникового так і наземного зв'язків, Але його застосування та повноцінне використання входить у протиріччя з точки зору необхідності забезпечення максимальної електромагнітної сумісності систем, міжнародними Регламентними обмеженнями і, цей метод є досить енергетично витратним.

Швидкий розвиток цифрової техніки надав поштовх для можливості реалізувати практично ефективні методи боротьби з завадним середовищем - це сигнальні методи завадозахисту, які ґрунтуються та засновані на цифровій обробці сигналів. Дані методи дозволяють забезпечувати зниження динамічних

рівнів впливу завадного середовища на рівнях мінус (20 ... 30) dB.

Вони базуються на використанні псевдовипадкових, багато частотних, широкосмугових, надширокосмугових та шумоподібних сигналах, паралельно використовуючи методи завадостійкого кодування корисних сигналів.

Ці методи широко використовуються у теперішніх сучасних системах супутникового зв'язку та демонструють задовільну ефективність роботи. Головний недолік таких методів – це є необхідність розширення (в деяких конкретних випадках досить істотного) робочого радіочастотного спектру для надійного забезпечення захисту системи від радіозавад. У високошвидкісних системах цей істотний недолік суттєво знижує ефективність при застосуванні таких методів враховуючи обмеженість радіочастотного ресурсу.

При дослідженнях застосування сигнальних методів стало відомо, що це призводить до зниження коефіцієнтів завадозахисту особливо із збільшенням трафіків потоків інформації. Не зважаючи на ці недоліки, сигнальні методи вс ж таки є досить ефективними. Вони постійно удосконалюються, і поки що є затребувані в ближній перспективі. Дослідження показують, що їх ефективність зростає у поєднанні з деякими другими методами просторового завадозахисту.

Наступні найбільш прості методи з завадо захисту - це- екранування радіоелектронних засобів особливо в напрямі можливого впливу ймовірних завад.

Досить ефективний метод боротьби з завадами на первинному рівні – це застосування радіо поглинаючих матеріалів та покриттів у певних секторних зонах робочих поверхонь рефлекторів дзеркальних параболічних антен з метою зниження впливу при прийомі завади бічними пелюстками діаграми спрямованості антенної системи. Вони використовуються і в системах супутникового зв’язку за технологіями VSAT.

Ці методи займають своє відповідне місце в загальній ієрархії методів боротьби з завадним середовищем, але не отримали широкого поширення виходячи з того, що вони не завжди спроможні забезпечити відповідний рівень захисту. Наприклад, метод екранування не повністю забезпечує надійного завадо захисту при поширенні завад з невизначеного напрямку. Крім цього

забезпечення відповідного рівня завадо захищеності призводить до створення досить громіздких конструкцій. Радіо поглинаючі покриття все-таки мають обмеження за рівнем зниження завадного середовища при залежності від частотних діапазонів.

Метод компенсації завад радіоелектронної компоненти, або ще друга назва просторова режекція перешкод є найбільш складний у порівнянні з другими методами та при технічній реалізації. Метод заснований на відтворенні та порівнянні копії сигналу, що заважає корисному сигналу при придушенні. Коефіцієнт завадозахисту даного методу, при відміні від сигнального, майже не залежить від трафіку передачі інформації. Його ефективність залежить від максимальної точності відтворення копій сигналів завад. За деякими оцінками, які враховані статистично при роботі систем зв'язку з цими методами може досягати значення придушення завади до мінус 40 dB.

Такі результати були отримані в процесі проведення лабораторних досліджень. Практично системи зв'язку з методом просторової режекції завад, яка працює у реальних умовах з впливом завадного середовища з 2-3 напрямків, досягає рівня зменшення завад на рівні мінус (20 ... 25) dB. Для покращення існуючих результатів подавлення завадного середовища можна суттєво зменшити при застосуванні принципово нового математичного апаратного інструментарію та функціонального програмного забезпечення.

2.2.3 Просторова режекція завад

Системи просторової режекції завад створюються у основному на основі просторового або просторово - часового створення та формування мінімумів у діаграмі спрямованості робочої антени за напрямом дії завадного середовища із сигналів та з обробкою вхідних корисних сигналів на робочих чи проміжних частотах.

Моделювання впливу завадного середовища від різних джерел, які впливають на наземні станції супутникового зв'язку показує, що вплив завадного середовища на основну пелюстку діаграми спрямованості антени

малоймовірно.

Більш ймовірно і досить небезпечно мають вплив сигнали завад на бічні пелюстки. Отже, при використанні методу просторової режекції сигнали завадного середовища потрапляють та приймається бічними пелюстками ДС антени на захищену станцію та приймаються на головну пелюстку на одну із компенсаційних антен СПРЗ. Схема такої системи СПРЗ показана на рис. 2.5.

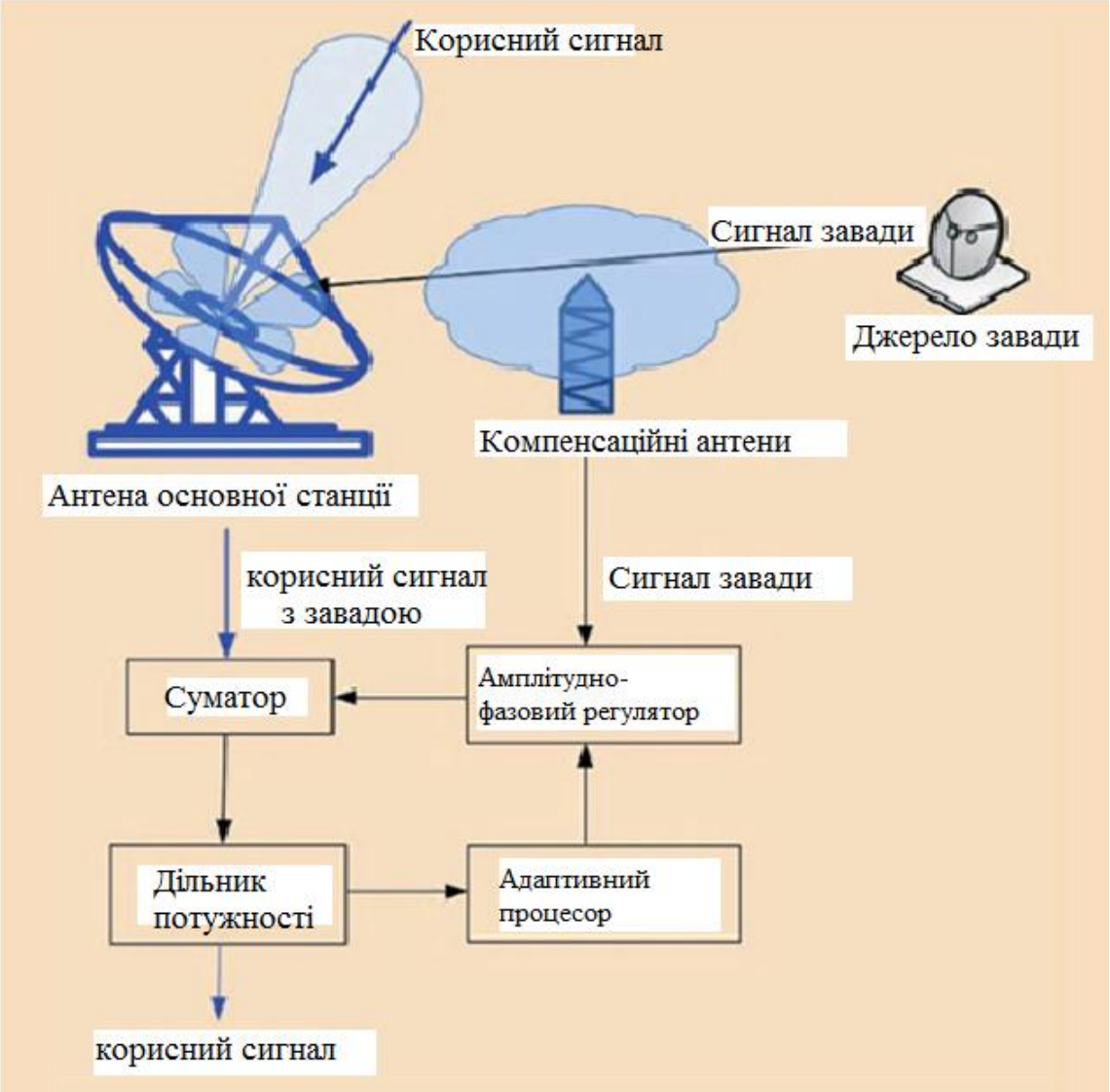

Рисунок 2.5 – Схема просторової режекції завад

Сигнали завадного середовища, прийняті компенсаційною антеною, посилюється та передаються на один із входів фідерного амплітудно - фазового регулятора. Тут амплітуда та фаза комплексної напруги сигналу, що є завадним, змінюється у відповідності до вибраного алгоритму адаптації.

Отримана таким методом копія завадного сигналу подається на компенсаційний вхід фідерного синфазного суматора потужності, а на лругий вхід якого надходить аддитивна компонентна суміш корисного сигналу і завадного. З виходу фідерного суматора потужності корисний сигнал передається на вхід апаратури захищеної станції та через вхід адаптивного процесору на другий інформаційний вхід фідерного амплітудно - фазового регулятора, Тут відбувається чергове перетворення амплітуди і фази завадного сигналу.

Внаслідок кількох ітераційних процесів на компенсаційному інформаційному вході синфазного фідерного суматора з'являється виділена напруга завадного сигналу, яка рівна за амплітудою та протилежна за фазою до напруги первинної завади, що надійшла на основний вхід фідерного суматора приймальним каналом захищеної станції системи зв’язку.

У результаті цих перетворень на виході фідерного суматора потужності з’являється корисний сигнал і незначний, який відповідає рівневі шумів, залишковий завадний сигнал. Внаслідок цього сукупний коефіцієнт завадо захисту збільшується на (20 ... 25) dB у сантиметровому діапазоні частот та до (25 ... 30) dB у дециметровому діапазоні частот, де відносна робоча смуга частот знаходиться у межах 50%.

На рис. 2.6. показана зміна діаграми спрямованості робочої антени наземної станції супутникового зв'язку при використанні методу режекції завади та формування умовного "нуля" діаграми спрямованості за напрямом завадного середовища.

При проектуванні систем просторової режекції завадного середовища слід враховувати фізичні та технічні принципи реалізації виробів. Основні вимоги, які необхідно враховувати до СПРЗ зводяться до наступного:

- основна кількість компенсаційних антен або каналів повинна бути не менше загальної кількості діючих завад, які діють одночасно;

- діаграми спрямованості основної антени та додаткових компенсаційних антен або каналів повинні мати просторову розв'язку з значеннями не менше 20 dB;

- якісні характеристики компенсаційного приймального каналу або антени повинні бути не нижче якісних характеристик основного каналу за напрямом дії завадних сигналів.

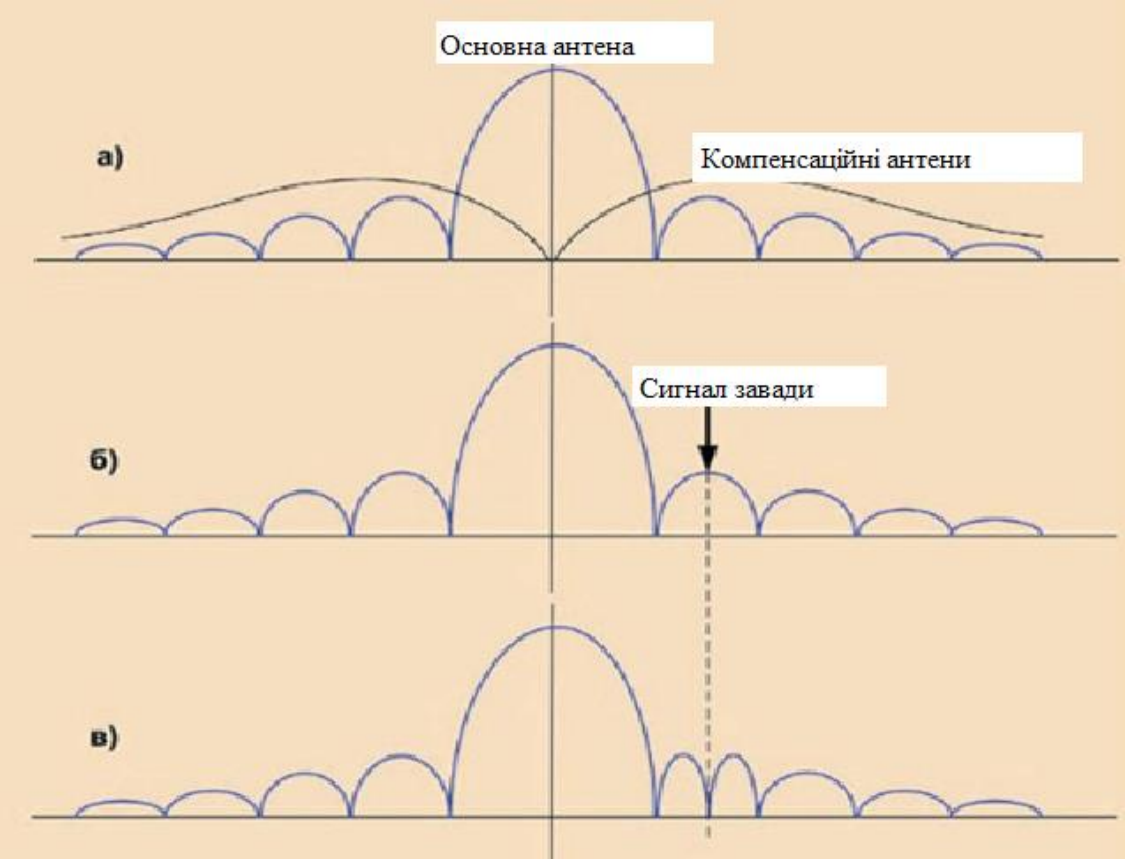

Рисунок 2.6 – Формування «нуля» діаграми спрямованості основної антени за завадним напрямом:

а) взаємне розміщення діаграм спрямованості основної антени та компенсаційних антен;

б) діаграма спрямованості до адаптації;

в) діаграма спрямованості після адаптації.

У просторово-часовому методі з боротьби з потенційним завадним середовищем сигнали завад можна при обробці розділити на вузькосмугові і широкосмугові. Даний поділ передбачає принципово нові та різні алгоритми обробки та технологію обробки сигналів.

Для прикладу, якщо в разі роботи з короткими радіоімпульсами тривалістю

$$\tau = 1 / \Delta f \qquad (2.5)$$

де, Δf – смуга частот, яка заповнена цим імпульсом,

то зменшення підсилення антеною даної системи відбувається тому, що для різних спектральних значень складових формується промінь діаграми спрямованості, який зміщений на кут, прийому корисного сигналу.

У результаті цього діаграма спрямованості антени або антенної градки для такого імпульсного сигналу ширша за стандартну діаграму спрямованості для центральної частоти. Якщо ввести таке поняття, як час заповнення імпульсу, це є час, коли фронт хвилі, який поширюється під кутом Q, проходить через весь проміжок L:

$$T = \frac{L}{c} \sin \Theta \qquad (2.6)$$

де, c – це є швидкість поширення ЕМ енергії,

то при процесі зменшення підсилення антенної градки у межах до 1 dB, загальна тривалість радіоімпульсу має бути рівною часу заповнення розкриття, отже

$$\frac{1}{\Delta f} = \frac{L}{c} \sin \Theta \qquad (2.7)$$

У загальній системі "СПРЗ - наземна станція" повний розмір розкриття Lo повинен визначатись, як максимальна відстань між центрами суміщених фазових нулів основної та додаткової антен.

Нижче приведена нерівність вказує на вузькосмуговість сигналу завади.

$$\frac{Lo}{c} \sin \Theta \ll \frac{1}{\Delta f} \qquad (2.8)$$

Для цього типу сигналу просторова й часова обробки розділені. За допомогою антена виконується функцію просторової обробки, а часова обробка проводиться в приймальному тракті.

Якщо вищенаведені нерівності не виконуються, то сигнал – широкосмуговий у просторово-часовому контексті. Факторизація такого

сигналу практично неможлива, і функції самої антени не будуть зведені тільки до методу просторової обробки сигналів. У цьому випадку здійснюється загальна просторово-часова обробка прийнятих сигналів.

Ця просторово-часова обробка прийнятих сигналів за допомогою вище приведеного методу пов'язана з необхідністю часткової зміни вагових коефіцієнтів у відповідності до обвідної прийнятого корисного сигналу. Тому ще виникає суттєва необхідність застосування трансверсальних фільтрів. Враховуючи те, що реалізація широкосмугового функціонального амплітудно-фазового регулятора, який створений на основі трансверсальних фільтрів потребує складні технологічні проблеми, тому потрібно створювати такий допоміжний антенний пристрій, який зможе забезпечити факторизацію прийнятого сигналу та відповідну факторизацію всіх вагових коефіцієнтів. Тому функції основної антени в цьому випадку зводяться тільки до просторової обробки сигналів.

Для реалізації вище приведеної нерівності при впливі вузько смугових сигналів завадного середовища під постійним тілесним кутом на відстані $L_{0,}$ який виникає між фазовими центрами основної антени та допоміжної антени необхідно зменшувати шляхом підбору однакових фазових набігів прийнятих сигналів у основному та компенсаційних каналах при допомозі окремих відрізків недисперсійних ліній передачі, таких як приклад можуть бути використані відрізки фазостабільного радіотехнічного кабелю.

У випадку прийому разом з корисними сигналами широкосмугову заваду, система повинна змінювати просторові координати вузькосмугового завадного середовища при необхідності можливого застосування трансверсальних фідерних фільтрів на основі, як приклад може бути регульована багатовідвідна лінія групової затримки.

У кожному окремому відведенні лінії затримки повинен встановлюватись вузькосмуговий фідерний амплітудно-фазовий регулятор на основі квадратурних розщеплень прийнятих сигналів. Ефективність роботи такої системи при використанні трансверсальних фільтрів з кількома відводами (три, п'ять), як демонструють дослідження, практично однакова. Для відносної

частотної робочої смуги сигналу до 40 % вистачає встановлення трьохвідвідних трансверсальних фільтрів.

2.2.4 Реалізація практичного застосування СПРЗ

Один із варіантів вищеописаної загальної системи просторової компенсації завадних сигналів реалізована практично на штучному супутнику геостаціонарних орбіти DSCS, рис.2.7.

Антенна система цього штучного супутника розподілена на 2 ідентичні підсистеми: приймальну і передавальну. Приймальна антенна підсистема включає в себе:

- 2 рупорні антени з глобальним покриттям земної поверхні;
- 61 променева антенна градка, яка дає можливість забезпечити повне керування за амплітудою та фазою кожного променя.

Така конфігурація дозволяє сформувати контурну діаграму і "нуль" спрямованості основної антени за напрямом на можливе джерело завад (навмисне та ненавмисне).

Така система може досить успішно боротись з впливом потужного ненавмисного завадного середовища, яке поширюється від наземних станцій супутникового зв'язку та телеметричного керування великими антенами.

Крім цього були розроблені технічні компоненти для захисту від впливу потужної радіозавади на самих супутникових станціях зв'язку. Це є системи просторової компенсації завадного середовища на основі антенного компенсатора завад, який є допоміжним варіантом антенної градки адаптивного типу та є когерентною схемою зменшення завадних та шумових сигналів. Ці сигнали в основному приймаються бічними пелюстками діаграми спрямованості антени. Антенні компенсатори дозволяють зменшити завадні сигнали на величину до мінус 15 dB, що дає можливість проводити впевнений прийом корисних сигналів з штучних супутників.

Рисунок 2.7 – Система просторової режекції завад у дециметровому діапазоні частот.

Прототипи СПРЗ у наукових розробках створювались на основі синтезу копії завадних сигналів на основній робочій, так на проміжній робочих частотах.

Технічна реалізація у першому випадку в якості фідерного амплітудно-фазового регулятора використовувалась система ланок фазоповертачів з зміною фазової складової від 0 до 360 град. і керування відбувалось при допомозі адаптивного процесора. У другому випадку технічна реалізація виконувалась за допомогою автоматичного регулятора комплексних амплітуд та на основі ланок фазових детекторів.

Такі конфігурації систем просторової режекції у супутникових системах зв'язку дециметрового частотного діапазону показали стійкого зв'язку регіональних наземних станцій з низькоорбітальними штучними супутниками при можливому впливі однієї або зразу кількох просторово рознесених та одночасно впливаючих завадах них сигналів. Величина завадних сигналів була встановлена до рівня 25 dB над верхнім рівнем шумів. Величина корисного сигналу складала не більше 7 dB. Час адаптації системи при таких експериментах становив не більше (2 ... 3) сек.

У дециметровому спектрі частот використовують такі СПРЗ, які представляють собою шестигранні призми. На кожну грань такої системи встановлюють антенні градки, рис. 2. Ширина діаграм спрямованості основної пелюстки таких антенних градок в азимутальній площині має 60 град., у площині кута місця має не більше 10 град. Таке технічне рішення дає можливість знизити ймовірність приймання корисного сигналу головною пелюсткою діаграми спрямованості парціальної антенної градки СПРЗ. Це практично унеможливлює розвал діаграми спрямованості антенної градки захищеної приймальної станції і, збої або можливий зрив сеансів зв'язку.

У сантиметровому діапазоні частот будуються СПРЗ на основі автоматичних фідерних регуляторів комплексних амплітуд. Таке рішення дозволяє завершувати процеси адаптації сигналів протягом (50 ... 100) мсек та реалізовувати зменшення (придушення) кількох одночасно прийнятих завад на рівні, не менше мінус 20 dB.

Отже, виходячи з вище приведеного, антенна система може виконуватись у двох або одному варіантах, а саме:

- на основі антенної системи захищеної приймальної станції;
- на основі восьмигранної приймальної антенної градки.

У першому варіанті додаткові приймальні компенсаційні антени можуть реалізовуватись на основі рупорних опромінюючих структур, які винесені з фокусної точки уздовж фокальної вісі та розміщені перпендикулярно до фокальної вісі. Фазові характеристики в розкриві такої двохдзеркальної антени мають відповідну квадратичну складову, яка забезпечує можливість розширення діаграми спрямованості. Лінійна складова антени забезпечує відхилення на певний кут діаграми спрямованості. Головна пелюстка діаграми спрямованості такої приймальної антени захищеної станції знаходиться у захисній зоні просторової воронки, яка обмежена цими головними пелюстками діаграм спрямованості приймальних компенсаційних антен системи.

У другому варіанті антенна система реалізується на основі 8 парціальних приймальних антенних градок, які розташовані на гранях призми. У просторі дальньої зони формується дискова діаграма спрямованості, яка дозволяє

успішно блокувати завадні сигнали а азимутальній площині від 0° до 360° та у площині кута місця секторно в межах 10°.

Висновки до розділу 2

У даному розділі розглянуто деталізовано різні методи захисту інформативних каналів, які є досить успішними при використанні. Однак вини самостійно не в повній мірі здатні захистити цілісність, достовірність, правдоподібність переданої та прийнятої інформації.

Також існує досить велика частина супутникових інформаційних каналів зв'язку, передачі даних, які є відритими для прийому досить великою кількістю абонентів.

Такі канали є досить вразливі від несанкціонованого доступу (спотворення, придушення, зашумлення, зменшення рівня потужності з порушенням і перебоями у зв'язку, підробка, знищення та ін.), впливу дестабілізуючих факторів, як кліматичних, так і від завадної компоненти других супутникових та наземних систем зв'язку.

Тому, незважаючи на велику кількість існуючих методів, які бажано використовувати паралельно, проблема забезпечення цілісності інформації існує і супутникові канали залишаються практично найбільш вразливими.

РОЗДІЛ 3 НАУКОВО-ТЕХНІЧНЕ ЗНАЧЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ ТА РЕКОМЕНДАЦІЇ ІЗ ЗАСТОСУВАННЯ

3.1 Практична реалізація супутникових системи захисту інформаційних каналів

Мережі VSAT встановлюються на базі геостаціонарних штучних супутників-ретрансляторів. Таке технічне рішення дає можливість максимально спрощувати абонентські термінали і проектувати фіксованими дзеркальними офсетними або симетричними параболічними антенами без системи стеження за штучним супутником. Вихідна потужність абонентських станцій типу VSAT орієнтовно складає (30 – 50) Вт., що дає можливість забезпечення стабільної роботи при різних катаклізмах та дестабілізуючих кліматичних факторах

Та як дані станції типу VSAT є складовими фіксованої супутникової служби, то на їх основі будуються супутникові зв’язкові мережі з метою:

- надання послуг за критеріями цією служби;
- передача даних;
- передача голосової інформації;
- передача зображень (цифрових, аналогових);
- організація відеоконференцій;
- доступ до всесвітніх мереж типу Інтернет;
- мультимедійний сервіс.

Одна із центральних станцій моніторингу та контролю даних телеметрії обслуговуючих супутників показана на рис. 3.1.

Мережі таких встановлених станцій у світовому масштабі налічується сотні тисяч, а число абонентів – це сотні мільйонів.

В Україні на теперішній час понад 1000 станцій, які об'єднані в корпоративні зв’язкові системи.

Рисунок 3.1– Центральна станція системи VSAT

Наземні VSAT станції супутникового зв'язку відповідають технічним характеристикам згідно міжнародних вимог (Рекомендації MCE-P S.725-S.729).

Структура таких терміналів показана на рис 3.2.

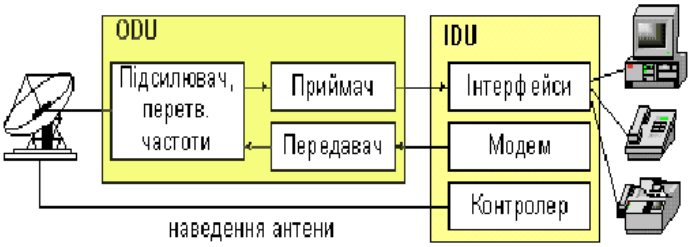

Рисунок 3.2 – Загальна структура VSAT станції

Термінал VSAT складається з антенної системи, де на антені встановлюється зовнішній блок (ODU) та внутрішній блок (IDU) всередині приміщення користувача (абонента).

Особливість таких систем полягає у тому, що від діаметрів рефлекторів антен залежать наступні технічні характеристики каналів зв’язку, а саме:

- діапазонами частотного спектру;
- трафіки передачі інформації;
- робоча потужність радіоканалів;
- кліматичні умови експлуатації системи.

У зовнішній блок входять система підсилення, приймання та перетворення частотного діапазону. Внутрішній блок укомплектований супутниковий модемом, цифровим контролер та інтерфейсами, які дають можливість підключати різне периферійне обладнання для обробки даних, захисту інформації, забезпечення зв’язку та спряження з телефонними мережами.

Перелік основних технічних вимог наступний:

- станції є складовими фіксованої супутникової служби (ФСС) та відповідають технічним міжнародним вимогам або вимогам орієнтованим супутниковим операторам згідно Регламенту Радіозв'язку;

- для сеансів зв’язку використовують спектри діапазонів частот, які виділені для ФСС: (14 і 6) ГГЦ – вверх на супутник, а (10-13) і 4 ГГЦ вниз на земну станцію;

- еквівалентні діаметр рефлекторів антен є в межах (0.9... 3.5) м;

- трафік передачі інформації зі станції - від 1.2 кбіт/с до 2,048 Мбіт/с;

- висока щільність розміщення приймально-передавальних станцій на земній території;

- станції зв’язку встановлюються безпосередньо на об’єктах у користувачів;

- робочі абонентські станції мають можливість експлуатуватись автономно;

- здійснення централізованого контролю та керування станцією, яка знаходиться у складі мережі;

- цифрова передача даних, IP телефонія функціонують у режимі прийому в симплексному режимі, у режимі прийом/передача – у дуплексному режимі;

- використовуються малопотужні радіопередавачі, які мають можливість збільшувати потужність передачі при дестабілізуючих кліматичних факторах з метою компенсації втрат сигналу.

На теперішній час використовують чотири покоління терміналів.

VSAT першого покоління – тільки режими мовного асиметричного діапазону в С-діапазоні

Друге покоління підтримує дуплексний (двосторонній) зв'язок особливо

для банківських і фінансових організацій. Робота в С - та Ku-діапазонах.

Термінали третього покоління, де діаметри антен до 1,2 м і менше. Використовуються у великих мережах у Ku-діапазоні.

Четверте покоління VSAT – для мультимедійних додатків, таких як USAT. Термінали працюють у Ku- і Ка - діапазонах. Швидкість передачі даних – декілька мегабіт у секунду. У Ка - діапазоні) еквівалентні діаметри антен є в межах (0,4-0,9)м. Дане покоління оснащене кількома методами із захисту інформаційних каналів системи зв’язку.

3.2 Архітектура мереж VSAT з метою безпеки інформаційних каналів

При формуванні конфігурацій компоновки та архітектури мереж супутникового зв'язку необхідно максимально враховувати захист інформаційних каналів. За конфігурацією трафіку розрізняють кілька структурованих топологічних варіантів систем зв’язку за VSAT технологіями, а саме:

- топологія «крапка – крапка», рис.3.3.;
- топологія «зірка»;
- топологія «кожний з кожним».

Такий варіант топології мережі, типу "крапка - крапка" дає можливість створювати та забезпечувати прямий дуплексний зв'язок між двох абонентів (абонентських станцій), які віддалені між собою на значну відстань виділеними каналами. Ефективність схеми топології такого зв'язку визначається завантаженням каналів на рівнях, не менше (30-40) %.

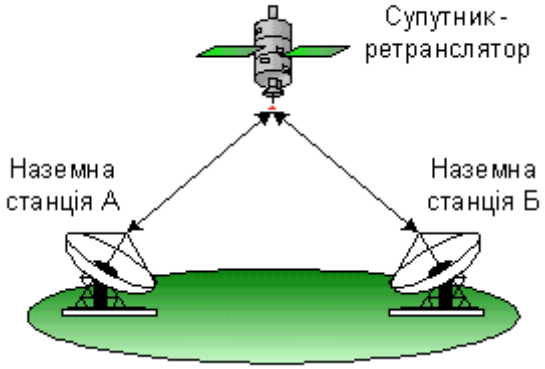

Рисунок 3.3 – Топологія мережі «крапка-крапка»

Перевагою такої топології архітектурного рішення є простою при організації каналів зв'язку, надає повну прозорість до роботи з протоколами обміну та безпеки. Дана мережа зв’язку не вимагає особливої системи керування.

Топологія мережі типу «зірка», рис. 3.4 досить розповсюджена при архітектурній компоновці супутникових систем зв’язку з віддаленими абонентськими станціями типу VSAT.

Дана мережа забезпечує направлений різносторонній радіальний трафік, включаючи центральну наземну станцію (HUB), та регіональними віддаленими периферійними терміналами (станціями).

Недолік такого архітектурного рішення - подвійний стрибок зв'язку між всіма терміналами мережі, який приводить до затримки сигналів.

Спряження з телефонними лініями у мережу загального користування відбувається через центральну станцію, яка має наземні канали зв’язку з центрами комутації або АТС.

Функції контролю і керування у такій мережі виконують централізовано і з допомогою центральної керуючої станції. Ємність периферійних абонентів у такій мережі - до 10 тис. терміналів.

Рисунок 3.4 – Топологія мережі «зірка»

Повнозв’язна мережа або топологія мережі «кожен з кожним» (рис. 3.5) надає можливості прямого зв’язку з будь-якими абонентом, або ще називають цю топологію «односкачковим» режимом.

Кількість дуплексних радіоканалів дорівнює

$$A = N \times (N - 1) \qquad (3.1)$$

де, N – число станцій абонентів у мережі.

Кожна станція абонента повинна виконувати умову - кількість каналів прийому-передачі повинна дорівнювати (N-1). Така технічна конфігурація є оптимальним архітектурним рішенням мережі для телефонних мереж, які використовуються у у важкодоступних або віддалених регіональних районах. Також така мережа ефективно працює з мережами, де відносно невелика кількість віддалених терміналів.

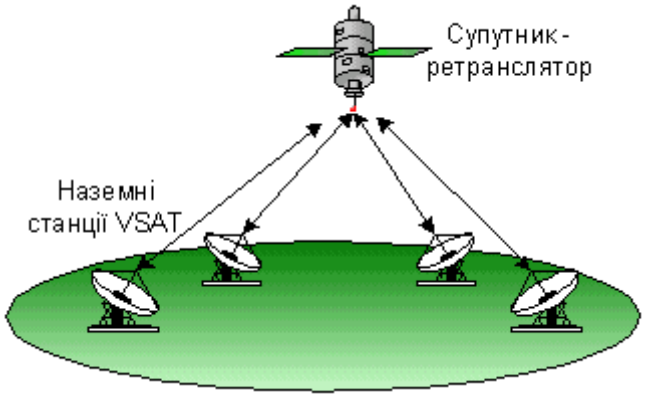

Рисунок 3.5 – Топологія мережі «кожен з кожним».

Та як для роботи між малими двома або більше абонентами потрібні відносно великі енергетичні ресурси та затрати , то у порівнянні з першим варіантом у даній топології потрібно використовувати більш потужні передавачі і антени з рефлекторами більшого діаметру, що має місце впливу на завадне середовище та шумові характеристики. Це впливає на загальну безпеку інформаційних каналів.

Так як система керування терміналами носить децетралізований характер, то такі системи доцільно використовувати при проектування малих мереж, до 30 абонентів з високим трафіком передачі даних, невеликі корпоративні закриті мережі.

Кожна з цих описаних архітектурних топологій має свої переваги і недоліки. Для різних мереж, враховуючи відповідний спектр послуг бажано вибирати відповідний варіант топології.

Для оцінки ефективності роботи системи зв’язку з точки зору протидії загрозам та загальної безпеки інформативних каналів, процедури розпізнавання переданої та достовірності прийнятої інформації використовують метод ковзного контролю.

Ймовірність розпізнавання загрози та рівня інформаційної безпеки обчислюється за виразом

$$P_{рз} = \Omega\left(\frac{0{,}5 \cdot \sum_{i=1}^{N_{pa}}\left[1 + \Omega(\mathrm{IZ}_{\mathrm{p_{axj}}} / 2) \cdot \log_2 n_i\right]}{2 \cdot N_{pa}}\right) \quad (3.2)$$

де, Ω – інтеграл ймовірності;

N – кількість ознак ймовірного нападу на інформацію;

IZ – інформативність значення ознак ймовірної атаки;

n – число градацій ймовірних ознак нападу на інформацію.

3.3 Дуальний метод захисту інформаційних каналів

Враховуючи вище приведені архітектурні рішення топологій супутникового зв'язку, створено новий гібридний тип топології зв'язку, оснований на методі дуальності.

Дуальний метод захисту інформативних каналів системи супутникового зв'язку типу VSAT ґрунтується на передачі інформації двома незалежними каналами на два різні штучні супутники Землі геостаціонарної орбіти, рис.3.6.

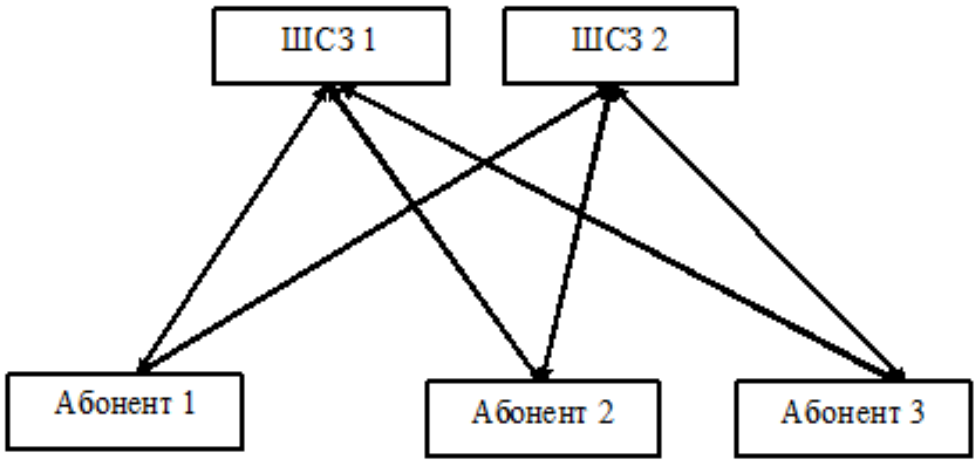

Рисунок 3.6 – Структурна схема передачі інформації через два ШСЗ

Таке технічне рішення має наступні переваги над існуючими системами:

- більша достовірність переданої інформації;
- малі енергетичні затрати;
- високий рівень інформаційної безпеки та захищеність при передачі та прийому інформаційних потоків двома паралельними каналами та на два різні супутники, які між собою не зв’язані;
- Враховуючи різні комбінації переданої інформації та кодових ключів можна розширити ширину смуги пропускання каналу у частотному спектрі та збільшити трафік передачі інформації, а також розширити мультимедійну сервісну складову.

3.4 Захист інформації при передачі даних та супутниковому зв’язку

Мережі VSAT мають можливість отримувати по загальних периферійних мережах аналогові та цифрові дані, які в результаті перетворення передають другим абонентам мережі. Способи перетворення та передачі залежать від конфігурації мережі рівня захищеності мережі, варіантів модуляції та других технічних характеристик.

Аналіз каналів передачі даних вказує на те, що в основному відсотковому значенні на передачу припадають мультимедійні та пакетовані інформативні дані. В основному використовують наступні формати та способи кодування даних:

1. при передачі документів:

- doc формат графічного редактора MsWord6.0 (7.0) for Windows;
- pdf - формат переносимого документа. Основоположником є фірма ADOBE;
- ps, eps - мови опису сторінок Postscript, Encapsulated Postscript;
- vsd, dwg, dxf, ai, cdr - формати технічної документації;
- dp - формат електронних документів;
- fpk, fr *, fa * - формати електронних форм;
- max - формат MaxMate;

- ppt - формат файлів презентацій, електронних слайдів;

- htm, html - формат гіпертексту.

2. утиліти кодування даних, які використовують для специфікації MIME:

- UUENCODE, XXENCODE, BINHEX, BASE64 (для передачі двійкових файлів).

3. формати відео даних:

- avi - video for Windows;

- mpg, mpeg;

- dat - формат запису відео інформації на CD-ROM;

- mov - Quick Time for Windows;

- viv, vdo, avs.

4. формати аудіо даних:

- av, aiff, aif, wav, mid, midi, snd.

5. формати графічних даних:

- gif, jpeg, jpg, tif, tga, wrl (тривимірна графіка);

6. формати баз даних:

- dbf, db - формати файлів баз даних dBase, dBase3 +, dBase4;

- mdb - MsAccess for Windows 2.0 і 7.0.

7. формати стиснення файлів:

- ZIP, Z, Z, GZ, TAR, TGZ, CAB, SIT.

8. виконувані програми:

- CLASS - файл скрипта (мова JAVA);

- exe - саморозкривні архіви.

Основні способи кодування:

- код Хафмана;

- код Read;

- код MRC;

- код UMRC.

Кодовані факсимільні повідомлення у процесі формування перетворюються в аналогову форму і потім передаються у канал зв'язку. З метою ущільнення повідомлень у цифрові стандартизовані потоки на основі

методів ІКМ або АДІКМ відбувається перетворюються у цифровий пакет.

Для збільшення пропускної здатності засобів DCME з передачі повідомлень 3-ї групи є розроблені і запропоновані різні модифікації для обробки даних, вони отримали назву - це «факсимільний компресор». На МККТТ прийнята рекомендація G.766 для можливого використання DCME «факсимільного компресора» в засобах зв'язку.

Для сигналів високошвидкісних типу V.17 (12 кбіт/с, 14.4 кбіт/с) використовується коефіцієнт ущільнення 4:1.

Технічні вимоги до обвідної діаграми спрямованості антени наступні у відповідності до стандарту IESS, п.1.2, визначені формулами:

$$\begin{aligned} &G(q)=29-25\lg q \text{ (дБи)}, && \text{при } 1^0<q<20^0 \\ &G(q)= -3{,}5 \text{ (дБи)}, && \text{при } 20^0<q<26{,}3^0 \\ &G(q)= 32-25\lg q \text{ (дБи)}, && \text{при } 26{,}3^0<q<48^0 \\ &G(q)= -10 \text{ (дБи)}, && \text{при } q>48^0 \end{aligned} \qquad (3.3)$$

Також зважаючи на вище приведені дані дозволяється у межах вимог:

- допускається збільшення рівня, який вказаний, до 10 % піків для основної та крос поляризаційної ДС;

- при $D/\lambda > 100$ замість

$$q = 1° \rightarrow \quad q_{min}=[(100\lambda)/D]°, \qquad (3.4)$$

де. D-діаметр рефлектору;

- вимоги стосуються прийому та передачі.

Вимоги з точки зору захисту інформаційних каналів супутникових систем згідно міжнародних Рекомендацій 580-5 и 465-5 МСЭ-Р визначено формулами:

$$\begin{aligned} &G(q) =29-25 \lg q \text{ (дБи)}, && \text{при } 1^0<q<20^0 \\ &G(q)= -3{,}5 \text{ (дБи)}, && \text{при } 20^0<q<26{,}3^0 \\ &G(q)= 32-25\lg q \text{ (дБи)}, && \text{при } 26{,}3^0<q<48^0 \\ &G(q)= -10 \text{ (дБи)}, && \text{при } 48^0<q<180^0 \end{aligned} \qquad (3.5)$$

де. q - кут, який відраховується від вісі головної пелюстки

$q_{min}=10$ $[100\lambda/D]^0$, якщо $100\lambda/D>1$

D – діаметр рефлектора;

λ – довжина хвилі.

- кросполяризаційна розвязка в тракті передачі ≥ 30 dB, при прийомі ≥25 дБ
- послаблення у тракті - 0,5 dB.

У відповідності до міжнародних Рекомендацій МСЭ – Р 524 густина потужності випромінювання розраховується за формулою, а саме:

$$EIBП =[32 – 25log] \quad (3.6)$$

Висновки до розділу 3

У даному розділі виконаний опис та приведені характеристики архітектурних топологій створення супутникових систем зв’язку з врахування системи безпеки та захисту інформаційних каналів передачі даних.

Надані рекомендації з практичної реалізації даних мереж.

Описаний створений новий дуальний метод передачі інформативних каналів, який має значно вищий рівень ймовірнісної інформаційної безпеки переданих даних.

Надані рекомендації при використанні протоколів даних та програмного забезпечення для максимального рівня безпеки та достовірної обробки, перетворення інформації, переданої мережею супутникового зв’язку.

Приведені формули, за допомогою яких можна розрахувати ймовірнісний характер та параметри завад та визначити їх рівень у інформаційній складовій.

Приведені технічні рекомендації у відповідності до міжнародного Регламенту Радіозв’язку для антенних систем з точки зору запобігання інформаційної безпеки абонентських терміналів, зменшення шумових складових від навколишнього середовища та несанкціонованого спливу на передану інформаційну складову у загальному інформаційному полі каналу зв’язку.

РОЗДІЛ 4 СПЕЦІАЛЬНА ЧАСТИНА

4.1 Програма HFSS Ansoft v. 9-11. Загальна характеристика.

Дана програма використовується для моделювання електродинамічних процесів у системах телекомунікацій, розрахунку характеристик окремих НВЧ структур, моделювання електромагнітних полів у різних зонах випромінювання: ближня, проміжна, дальня, моделювання систем електромагнітної сумісності та завадостійкості систем.

У даний час основною тенденцією розвитку програм проектування радіоелектронних систем та процесів можна вважати інтеграцію підсистем проектування орієнтованих на розробку вузьких класів радіоелектронної апаратури в єдину систему, яка підтримує процес розробки всіх пристроїв від цифрових схем обробки і формування сигналів до НВЧ схем і антен. У рамках цієї тенденції засоби проектування різних з фізики функціонування і методів математичного аналізу пристроїв об'єднуються разом на базі єдиної платформи, що дозволяє інтегрувати результати роботи різних програм з метою створення проекту всієї радіоелектронної системи в цілому.

Особливий інтерес викликає можливість інтеграції засобів проектування цифрової та аналогової апаратури, яка здебільшого є НВЧ апаратурою. Останнім часом спостерігається зростання пропозиції на ринку програмних засобів автоматизованого проектування як в області цифрової, так і аналогової техніки. Говорячи про розробку цифрових пристроїв, слід зазначити створення нових методів моделювання пристроїв обробки і формування цифрових потоків даних. Група таких підходів отримала назву косимуляції. Ці методи успішно реалізовані в програмі Ptolemy1, яка є прибутковим частиною найпотужнішого середовища проектування радіосистем ADS – Advanced Design System (компанія Agilent).

Аналогічне завдання вирішується програмою VSS, що входить в найбільш поширену систему проектування НВЧ пристроїв MWO – Microwave Office2.

Що стосується програм розрахунку аналогової частини радіосистем, то тут

відбувається перехід від програм, які розраховують НВЧ структури методами теорії ланцюгів (до яких відноситься метод Олінера, www.agilent.com, www.moffice.com мають в ряді випадків досить високу для практики проектування точність) до програм, що виконують повноцінний розрахунок тривимірного електромагнітного поля.

Ця тенденція пояснюється, в першу чергу тим, що багато частин реальних пристроїв не піддаються декомпозиції на елементи, які є в бібліотеці моделей.

Наприклад, навіть в найпростішому випадку аналізу плавного повороту багатошарової мікросмужкової структури, важко визначити, де мікросмужкова лінія, а де структура з підвішеною підкладкою.

У програмах електродинамічного моделювання використовується велика різноманітність математичних методів.

Метод моментів, реалізований у MWO, призначений для моделювання багатошарових схем. Він значно вдосконалений у системі IE3D3 – системі тривимірного електродинамічного моделювання НВЧ пристроїв.

Програма IE3D дозволяє, зокрема, розраховувати антенні системи складної конфігурації і аналізувати їх діаграми спрямованості. Вона включає до десяти утиліт, які значно розширюють її можливості, аж до аналізу нелінійних НВЧ пристроїв у тимчасовій області.

Інша програма цієї ж компанії (Zeland) Fidelity вирішує завдання електродинамічного моделювання методом FDTD (Finite Difference Time Domain). Цей метод дозволяє аналізувати більш складні структури, довільної конфігурації. Він також реалізований у програмі FDTD, яка дозволяє аналізувати невзаємні НВЧ пристрої (наприклад, феритові вентилі, циркулятори і ін.).

У даний час великий розвиток отримала програма High Frequency System Simulator (HFSS) компанії AnSoft, яка призначена для аналізу тривимірних НВЧ структур, в тому числі, антен і навзамін пристроїв, що містять ферити. Наслідуючи кращі можливості, реалізовані в однойменних програмах компаній Hewlett Parcard і Agilent, зроблено значний крок вперед.

Серед нових можливостей Ansoft HFSS можна відзначити:

- періодичні граничні умови, призначені для аналізу антенних градок;

- систему макросів, яка значно розширює можливості програми;

- підпрограму аналізу власних коливань і власних хвиль (eigenmode solver);

- нові можливості візуалізації результатів аналізу, зокрема, анімації картин поля, побудова тривимірних діаграм спрямованості і ін.;

- адаптивний алгоритм рішення електродинамічних задач, що забезпечує високу ефективність моделювання складних структур;

- можливість аналізу багатополюсників з багатомодовими портами;

- великі бази даних з НВЧ матеріалами та компронентами;

- можливість параметричного аналізу і оптимізації параметрів структури.

В останні роки саме HFSS, в розробці якої взяли участь фірми Hewlett Packard, Agilent і Ansoft, зайняла лідируючу позицію в світі проектування НВЧ та телекомунікаційних пристроїв і ЕМ полів. Інші програми, що використовують електродинамічні методи розрахунку - IE3D, Microwave Office, Microwave Studio призначені для своїх класів задач.

HFSS показала в повну силу широкі можливості суворого електродинамічного моделювання.

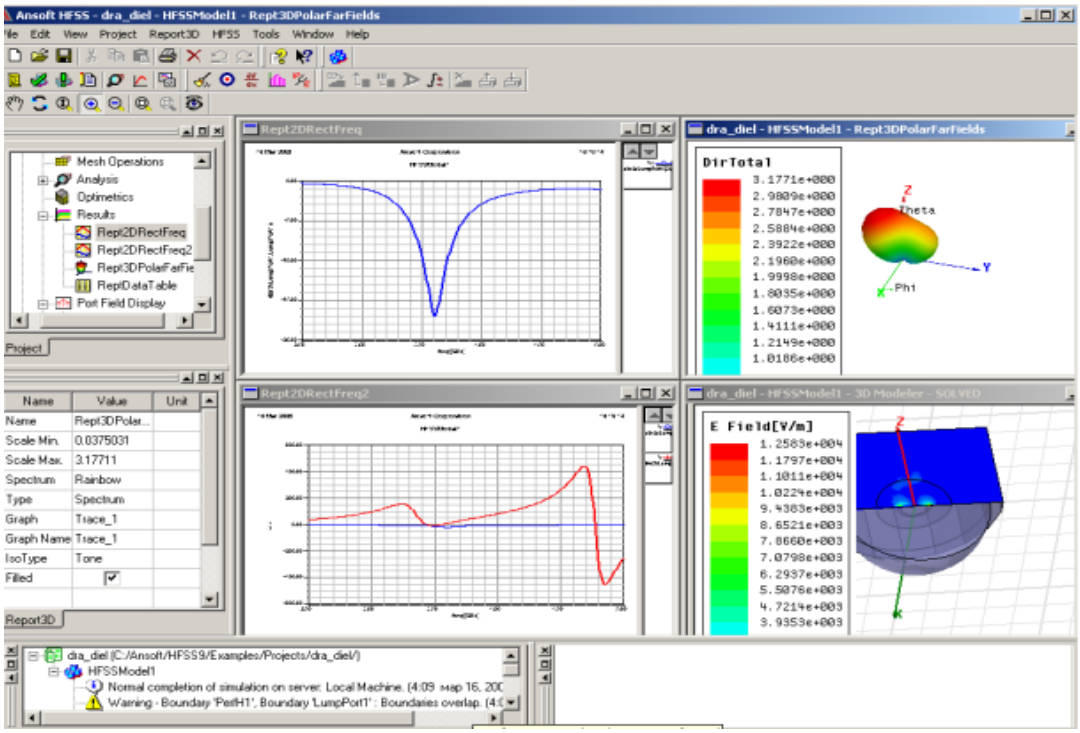

Рисунок 4.1 – Інтерфейс програми HFSS

Даний інтерфейс, рис.4.1, повністю інтегрований з Ansoft Designer і показує випромінюючу структуру, її діаграму спрямованості при порушенні структури дискретним джерелом енергії (напруги), частотні залежності вхідного опору. Електродинамічне моделювання у HFSS засноване на використанні методу скінчених елементів (Finite Element Method, FEM).

Рішення граничної задачі шукається у частотній області. Використання методу скінчених елементів забезпечує високу ступінь універсальності чисельних алгоритмів, які виявляються досить ефективними для широкого кола завдань від аналізу хвилеводних і смужкових структур до моделювання антен і складних навзамін пристроїв, що містять гіротропне середовище, моделювання електромагнітних полів та завадні середовища.

HFSS дозволяє з високою точністю розраховувати зовнішні параметри НВЧ багатополюсників: матриці розсіювання, матриці імпедансів і адмітансів. Це служить основою для інтегрування HFSS з іншими програмами проектування, які реалізують рішення нелінійних задач.

Розраховані S-параметри можуть використовуватися далі в програмах аналізу лінійних і нелінійних схем, систем, зокрема, в програмі Microwave Office, Serenade Ansoft або ADS. HFSS повністю сумісний з платформою Ansoft Designer, яка призначена для наскрізного проектування радіоелектронних систем.

Процес проектування за допомогою HFSS включає в себе ряд стандартних кроків:

1. Створення моделі аналізованої структури, в тому числі:

- створення тривимірної графічної моделі структури (кресленик);
- задання параметрів матеріалів, з яких складається структура.

2. Визначення електродинамічних параметрів структури, що включає:

- завдання граничних умов на поверхнях, які формують об'єкт;
- визначення і калібрування портів;
- завдання параметрів рішення.

3. Електродинамічний аналіз досліджуваного об'єкта, в тому числі:

- аналіз об'єкту в смузі частот;

- параметричний аналіз об'єкту;

- параметрична оптимізація об'єкту.

4. Візуалізація результатів електродинамічного аналізу, що включає:

- побудова графіків у декартових, полярних координатах, діаграм Сміта, діаграм спрямованості і ін.;

- анімація розподілів електромагнітного поля і електричного струму;

- збереження результатів аналізу в файлах даних.

Всі етапи проектування повністю відображають можливості HFSS.

4.2 Бібліотека моделей

Система HFSS включає велику бібліотеку стандартних структур, яка прискорює процес креслення складних об'єктів. До їх числа відносяться:

- мікросмужкове Т розгалуження;

- мікросмужкові та смужкові лінії, пов'язані з широкою та вузькою сторонами;

- зрізані та незрізані повороти мікросмужкових ліній;

- радіальні і несиметричні вигини ліній;

- коаксіальні лінії із заданим Zo;

- кругла і квадратна 3D спіраль;

- магічний Т-міст;

- плоскі антени;

- стандартні трьохмірі моделі;

- стандартні моделі уявних електромагнітних полів;

- спіральні конфігурації і ін.

Трьохмірна модель діаграми випромінювання антени показана на при.4.2., яка створена за допомогою програмного забезпечення HFSS.

Проектування антен HFSS дозволяє розраховувати основні характеристики, в тому числі: коефіцієнт посилення, тривимірні діаграми спрямованості (ДН) в дальній зоні, перетину ДН в далекій зоні ширини променя за рівнем 3 дБ, спрямованість антени, коефіцієнт еліптичності і ін.

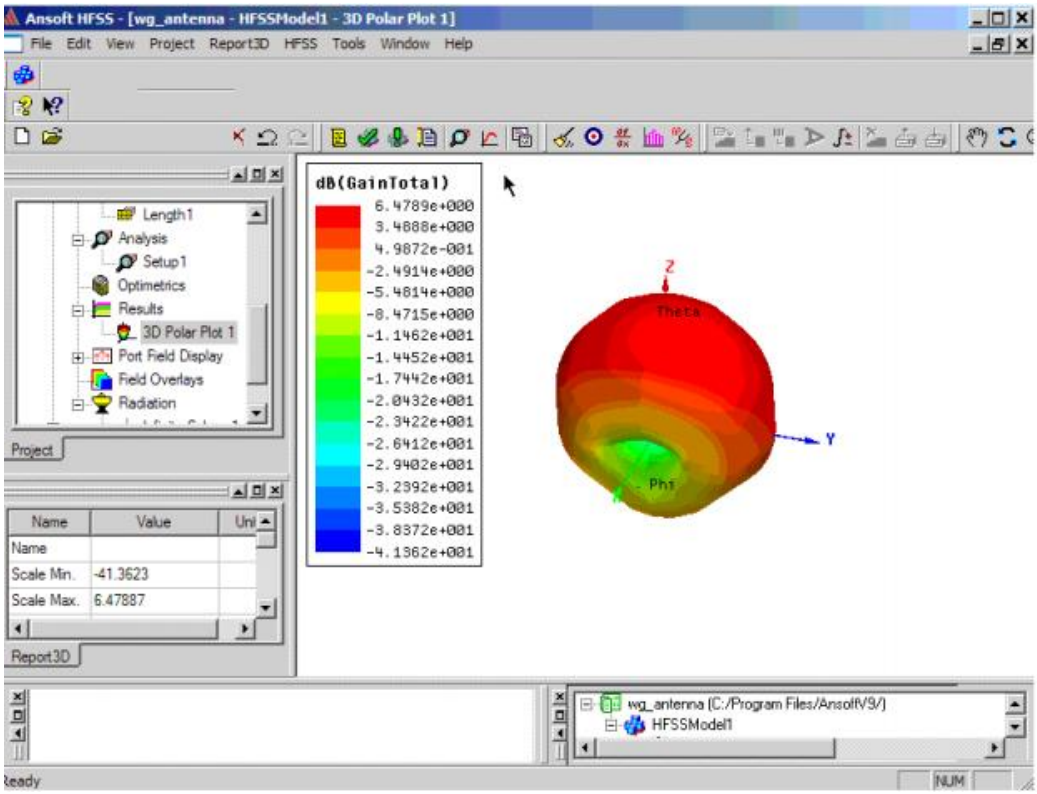

Рисунок 4.2 – Тримірна модель ДС антени

Розраховуються поляризаційні характеристики, включаючи компоненти поля у сферичних координатах і вектори поляризації поля. Крім цього розраховуються НВЧ компоненти, рис. 4.3.

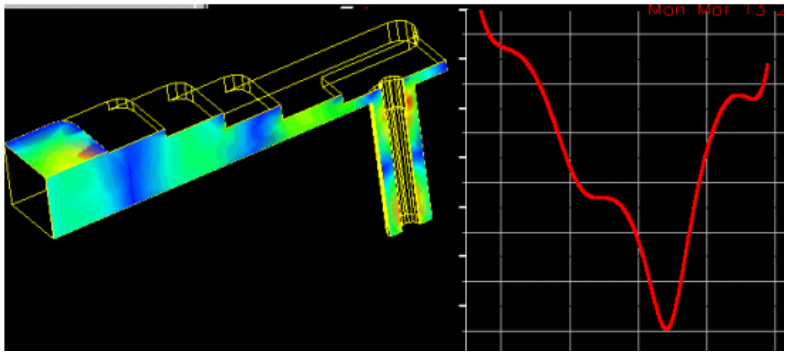

Рисунок 4.3 – Хвилевідно коаксіальний перехід

4.3 Постпроцесор поля

Постпроцесор HFSS - це спеціальна програма, яка:

- забезпечує анімацію для будь-якого поля і його візуалізацію у вигляді

векторів, контурів або заштрихованих контурів;

- обробляє статичні та анімаційні креслення на будь-якій поверхні, включаючи поверхні перетину об'єктів, тривимірних поверхонь об'єктів і на тривимірних просторових поверхнях;

- виконує анімацію векторів поля, скалярного поля або будь-якої заданої величини, пов'язаної з полем, використовуючи постпроцесорну обробку даних розрахунку, рис.4.4.

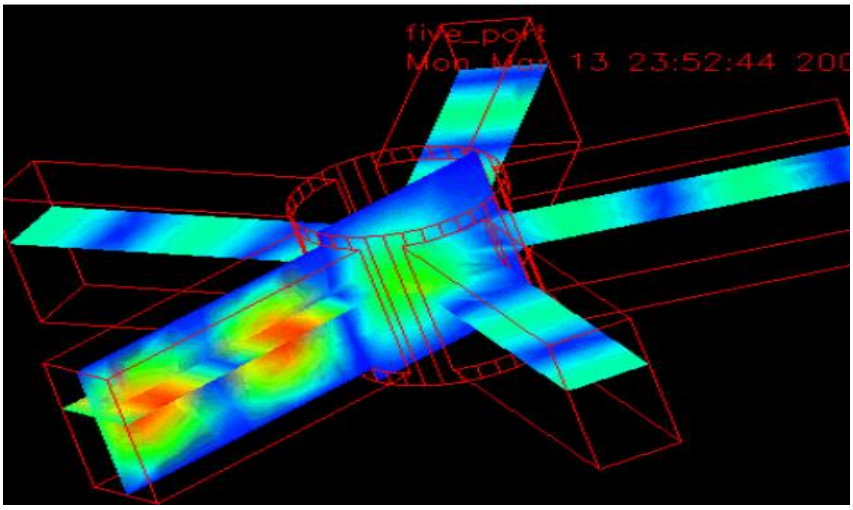

Рисунок 4.4 – Зображення електричних і магнітних полів, ближнє реактивне і далеке поле випромінювання у різних перетинах

Візуалізація поля тривимірної діаграми спрямованості, використовують м'які колірні переходи, дозволяють вивчити ближні поля і поля випромінювання з високою точністю. Користувачі можуть обертати структуру в реальному масштабі часу з миттєвими модифікаціями графіків. Постпроцесор також виконує обробку даних, після розрахунку поля. З його допомогою можна обчислити такі характеристики як потужність розсіювання, поглинання енергії, добротність, S-параметри і пов'язані з ними характеристики. Також можуть бути розраховані абсолютні значення полів. У кожній точці простору можна вивести модуль і фазу векторів E і H електромагнітного поля.

Унікальні можливості надає аналіз поля у всіляких перетинах, а також анімація розподілу поля за рахунок зміни фази збудження генератора, що

створює враження проходження поля через структуру. Після накопичення певного досвіду, цю анімовану картину можна використовувати для оптимізації структури, і для аналізу якості конструкції. Картини рушійного поля приносять неоціненну допомогу розробнику з точки зору наглядності.

4.4 Калькулятор поля

Калькулятор поля - це підпрограма, призначена для обробки результатів рішення граничної задачі у вигляді розподілів векторів електричного і магнітного полів. Калькулятор може обчислити похідні від векторів поля і їх компоненти, перетворити і записати отримані дані в файл і багато іншого. Калькулятор не виконує розрахунки, поки вони не потрібні для подальшого використання або виведення на графік.

Параметричний аналіз і оптимізація HFSS має потужну макрокомандну мову з можливістю автоматичного запису і модифікації. Ці можливості реалізовані в програмі Optimetrics, яка виконує параметричний аналіз і оптимізацію структури, змінюючи форму і розміритих елементів, які входять в неї.

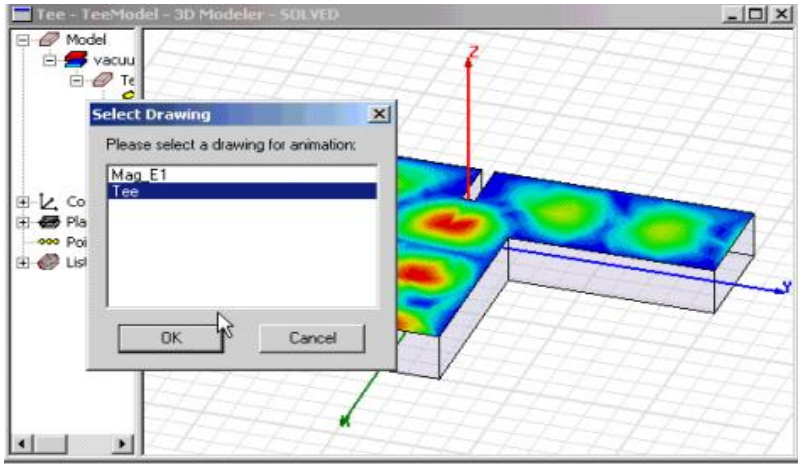

Рисунок 4.5 – Тестова структура хвилеводного дільника потужності і оптимізація положення структури

У якості цільової функції при оптимізації можуть використовуватися як окремі S-параметри, так і інші характеристики, включаючи діаграму

спрямованості і параметри антени. Наприклад, діаграма спрямованості чотирьохспіральної антени, яка широко використовується, наприклад, у приймачах GPS. Її випромінювання мають кругову поляризацію і діаграму спрямованості з дуже малими задніми пелюстками. Антена моделювалася на HFSS. Використовуючи розширені макрокоманди, проектувальник здатний швидко зробити десятки розрахунків, щоб зрозуміти, які параметри сильніше впливають на ширину променя антени, коефіцієнт посилення і рівень бічних пелюсток. HFSS враховує вплив корпусу на випромінюючі властивості антени. Використовуючи оптимізацію за допомогою утиліти Optimetrics, можна мінімізувати цей вплив і оптимізувати структуру за критерієм максимуму коефіцієнта посилення і мінімуму крос - поляризаційного випромінювання.

4.5 Інтерфейс програми Ansoft HFSS v.9-11

HFSS - це пакет програм, призначений для розрахунку параметрів і моделювання електромагнітних полів у складних НВЧ пристроях. Перед рішенням електродинамічної задачі необхідно накреслити аналізований пристрій, задати матеріали для кожного об'єкту, вказати порти і граничні умови на поверхнях. Потім HFSS розрахує електромагнітне поле в кожній точці досліджуваної структури і знайде за цими даними S-параметри та інші характеристики. HFSS включає в себе програму розрахунку власних хвиль структур і власних коливань НВЧ резонаторів Eigenmode. Ця програма обчислює резонансні частоти власних коливань і постійні поширення власних хвиль структури на підставі її геометрії, властивостей матеріалів і граничних умов. HFSS може отримати рішення для фіксованої частоти або для ряду частот.

Системні вимоги є наступними:

процесор: Pentium III, 500 MHz, 1 GHz;

вільний простір на жорсткому диску (для програми HFSS v.9) - 200 Mb;

оперативна пам'ять (RAM) - 256 MB, 2 GB.

Для вирішення складних завдань, які включають оптимізацію проекту,

рекомендуються використовувати більш потужний комп'ютер.

Операційні системи, які підтримують HFSS Ansoft версії 9- 11: Windows NT 4.0 Workstation, Windows NT 4.0 Server, Windows 2000 Professional, Windows XP Professional.

4.6 Інтерфейс HFSS Ansoft

Інтерфейс HFSS складається з декількох вікон, лінійки меню, лінійки інструментів, і лінійки стану.

HFSS містить наступні пункти меню, які розташовані у верхній частині головного вікна.

File Команди в меню File призначені для управління файлами проекту і для виведення на друк.

Edit Команди в меню Edit призначені для редагування геометричних об'єктів, а також для скасування і повторення дій над об'єктами.

View Команди в меню View призначені для відображення частин робочого столу і об'єктів моделі, для зміни параметрів вікна 3D Modeler, і для зміни вигляду моделі.

Project Команди в меню Project служать для додавання проекту нової конструкції, для перегляду і завдання набору даних, змінних проекту.

Draw Команди в меню Draw призначені для креслення одно-, дво-, і тривимірних об'єктів, а також для операцій перетворення одно- і двовимірних об'єктів в тривимірні.

3D Modeler Команди в меню 3D Modeler використовуються для імпорту, експорту, і копіювання файлів Ansoft 2D Modeler і файлів 3D Modeler, завдання матеріалів об'єктів, для керування розбивкою простору на елементарні осередки в 3D Modeler.

HFSS Команди в меню HFSS управляють усіма параметрами активного проекту. Більшість цих параметрів є дерева проекту.

Tools Команди меню Tools використовуються для зміни бібліотеки матеріалів активного проекту, упорядкування бібліотеки матеріалів, запуску і

записи сценаріїв розрахунку (скриптів).

Window Команди меню Window використовуються для впорядкування вікон 3D Modeler і кнопок на панелі інструментів.

Help Команди меню Help служать для отримання контекстно-залежної довідкової інформації.

4.7 Дерево хронології

Дерево хронології, рис. 4.6, у вікні 3D Modeler перераховує всі моделі структури, площини і деталі проекту. Дерево хронології складається зі списку всіх команд, які застосовувалися до об'єктів моделі.

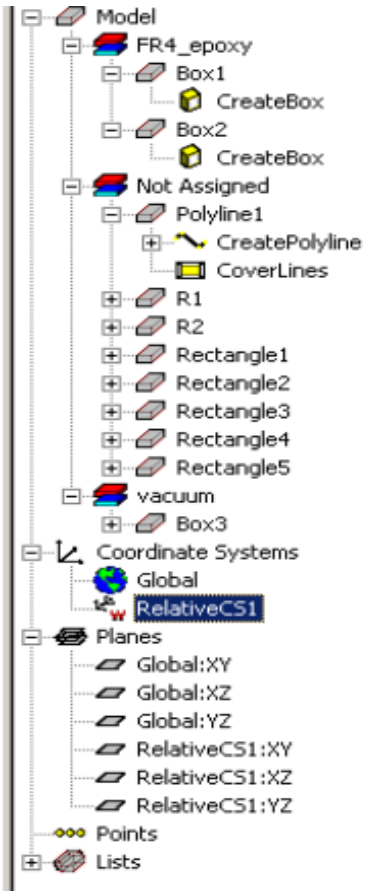

Рисунок 4.6 – Дерево хронології проекту

Щоб розглянути виконану команду в дереві хронологій потрібно натиснути ім'я пункту в дереві хронологий. Опції цієї команди з'являються у вікні Properties. При створенні системи координат, за замовчуванням, задаються площині xy, yz і xz. Створення списку - зручний спосіб об'єднувати групу

об'єктів для виведення, наприклад, графіків полів на декількох площинах.

4.8 Послідовність етапів роботи в HFSS

Для вирішення завдання необхідно послідовно виконати ряд операцій: накреслити об'єкт, запустити розв'язок граничної задачі, виконати аналіз конструкції.

Алгоритм рішення задачі, представлений на рис. 4.7. Виконання наступних операцій: креслення геометричній моделі, редагування параметрів моделі, призначення змінних для зміни моделі, задання параметрів для вирішення електродинамічної задачі, перевірка правильності установок проекту, виконання моделювання, висновок графіків S-параметрів, створення графіка поля у просторі або на площині, виконання результатів анімації.

Для оптимізації конструкції застосовується програма Оптіметрік (Optimetrics).

Рисунок 4.7 – Алгоритм рішення задачі

Можна автоматично створити нову поверхню CS, кожен раз, коли креслите на поверхні об'єкту. Об'єкти, які потрібно креслити, орієнтується згідно нової

поверхні CS. Це прискорює процес створення складних конструкцій, рис. 4.8.

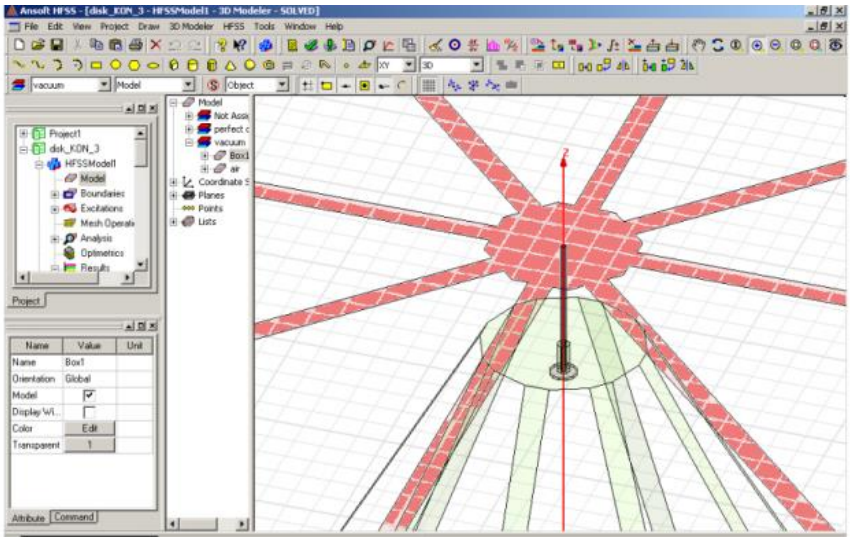

Рисунок 4.8 – Кресленик складної антенної структури з установленими робочими системами координат

4.9 Розрахунок параметрів максимуму ближнього поля

Для обчислення max поля у ближній зоні, необхідно задати межі випромінювання або PML. Для тих частин ліній ближнього поля, які виходять за межі моделюється області, ближнє поле розраховується наближено.

Якщо частини лінії лежать всередині області моделювання, використовуються інтерпольовані значення обчислюваних полів. Таблично задаються компоненти точок максимуму поля і нормалізована відстань уздовж ліній, при яких вони досягаються. При обчисленні максимальних значень дального поля, відстань r виноситься як загальний множник, за дужки E-поля. Орієнтовна модель такого поля показана на рис. 4.9.

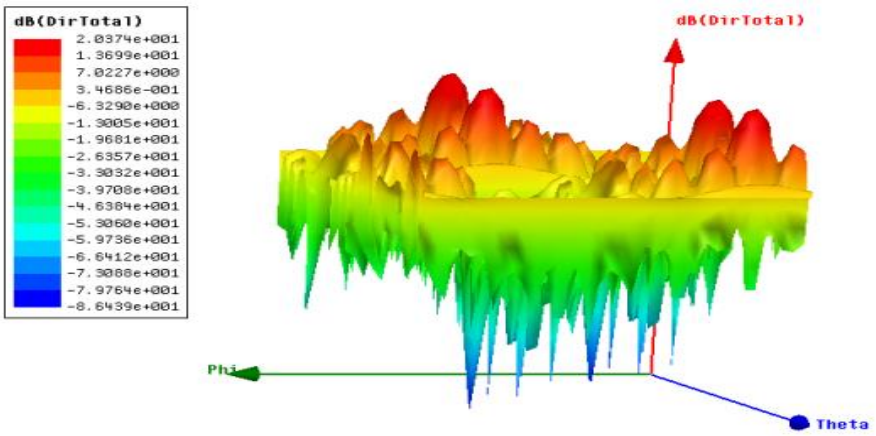

Рисунок 4.9 – Направленість антенної структури в системі координат Phi, Theta

РОЗДІЛ 5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою дипломної роботи є порівняння існуючих методів первинного захисту інформаційних каналів у супутникових мережах та створення власного гібридного дуального методу для захисту інформації від зовнішніх несанкціонованих втручань та завадного середовища.

5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального його використання.

Аналіз алгоритмів роботи розділено поетапно, що дозволяє полегшити і структурувати виконання завдання.

Основні етапи наступні:

1. пошук літературних джерел з області дослідження;

2. дослідження наборів даних;

3. порівняльний аналіз алгоритмів анонімізування за різними параметрами.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу.

Виконавцем усіх операцій по розробці системи первинного захисту інформаційних каналів на основі систем супутникового звязку є інженер.

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час, год.
1.	Пошук літературних джерел з області дослідження.	інженер	26
2.	Дослідження наборів даних.	інженер	44

3.	Порівняльний аналіз алгоритмів анонімізування за різними параметрами.	інженер	48
Разом			118

Загальні затрати часу на реалізацію даної роботи становить 118 години, найбільш трудомістким є сам порівняльний аналіз – 48 годин.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні потреби

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”. Розмір заробітної плати залежить від складності, умов виконуваної роботи, професійно-ділових якостей працівника, результатів його. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. при тривалості робочого дня – 8 год.

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2019 рік», зокрема у статті 8 min заробітна погодинна плата становить 25,13 грн. Рекомендовані тарифні ставки: керівник дипломної роботи – (30,00...50,00) грн./год., інженер – (25,13...30,00) грн./год., консультант – (25,13...30,00) грн./год., технік – (25,13...30,00) грн./год., лаборант – (25,13...26,00) грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \times К_г \,, \quad (5.1)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт виконує розробник, то основна заробітна плата буде розраховуватись тільки за формулою

$$З_{осн.} = 25{,}13 \times 118 = 2965{,}34 \text{грн.}$$

Додаткова заробітна плата становить (10–15) % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \times К_{допл.}, \quad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод} = 2965{,}34 \times 0{,}15 = 444{,}8 \text{грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (5.3)$$

$$В_{о.п.} = 2965{,}34 + 444{,}8 = 3410{,}14 \text{грн.}$$

Відрахування на соціальні заходи:

- єдиний соціальний внесок ЄСВ (прибутковий податок) – 22%;
- військовий збір – 1,5%.

Зазначені сумарні відрахування становлять 23,5 %.

Сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \times 0{,}235 \quad (5.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$В_{с.з.} = 3410{,}14 \times 0{,}235 = 801{,}38 \text{грн.}$$

Проведені розрахунки витрат на оплату праці зведені в таблицю 5.2.

Таблиця 5.2 – Розрахунки витрат на оплату праці

з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Відрахування $Ф_{ОП}$, грн.	Всього витрати на плату праці, грн. (3+4+5)
		Тарифна ставка, грн.	Кількість відпрацьованих год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1.	Інженер (розробник)	25,13	118	2965,34	444,8	801,38	4211,52

Отже, загальні витрати на оплату праці становить 4211,52 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{ві} = q_i \times p_i \,, \tag{5.5}$$

де: q_i – кількість витраченого матеріалу і–го виду;

p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{ві} \,. \tag{5.6}$$

Розрахунки занесемо у таблицю 5.3.

Таблиця 5.3 – Розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Один. виміру	Норма витрат	Ціна за один., грн.	Затрати матер., грн.	Транс-портно-заготівель-ні витрати, грн.	Загальна сума витрат на матер., грн.
1. Основні матеріали						
Використання мережі Internet	години	120	–	120	–	120
2. Допоміжні витрати						
Папір формату А4	шт.	160	0,3	48	–	48
Разом:						168

Загальні матеріальні витрати на Internet і папір ф. А4 становлять 168,0 грн.

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \times T \times S, \quad (5.7)$$

де, W – необхідна потужність, кВт;

T – кількість годин на реалізацію розробки;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 1,68грн.

Потужність комп'ютера для створення дипломної роботи – 90 Вт, кількість годин роботи обладнання згідно таблиці 6.1 –118 год.

$$З_в = 0{,}09 \times 118 \times 1{,}68 = 17{,}84 \text{грн.}$$

Загальна вартість витрат на використану електроенергію 17,84 грн.

5.5 Розрахунок амортизаційних відрахувань

Особливість застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їхнього повного відновлення.

Визначення амортизаційних відрахувань відбувається за формулою:

$$A = \frac{Б_В \cdot H_A}{100\%}, \quad (5.8)$$

де, A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

H_A – норма амортизації.

Засоби розрахунків (комп'ютер) та оргтехніка належать до четвертої групи основних фондів. Річна норма амортизації для них є 60 % (квартальна – 15 %).

У нашому випадку засобом розробки є комп'ютер. Його вартість становить 11500 грн. Амортизаційні відрахування будуть рівні:

$$A = 11500 \times 5/100 = 575{,}00 \text{ грн.}$$

Оскільки робота виконувалась 118 год., або менше одного місяця (60%), то

амортизаційні відрахування будуть становити:

$$A = 575{,}00 \times 0{,}6 = 345{,}00 \text{ грн.}$$

5.6 Розрахунок накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, адміністративні витрати та створення необхідних умов праці.

У залежності від організаційно-правової форми діяльності суб'єкту господарювання, накладні витрати становлять (20–60) % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \times (0{,}2 \ldots 0{,}6) , \qquad (5.9)$$

де $H_в$ – накладні витрати.

Отже, накладні витрати становлять:

$$H_в = 4211{,}52 \times 0{,}2 = 842{,}3 \text{грн.}$$

5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків зведено в таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	у % до загальної суми
Витрати на оплату праці $B_{о.п}$	3410,14	61,06
Відрахування на соціальні потреби $B_{с.з}$	801,38	14,35
Матеріальні витрати $З_{м.в}$	168,00	3,01
Витрати на електроенергію $З_в$	17,84	0,32
Амортизаційні відрахування A	345,00	6,18
Накладні витрати $H_в$	842,3	15,08
Собівартість $C_в$	5584,66	100,00

Собівартість ($С_в$) роботи розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_в + А + Н_в \text{ .} \quad (5.10)$$

Отже, собівартість дослідницької роботи дорівнює:

$С_в$ = 3410,14+801,38+168,0+17,84+345,00+842,3= 5584,66грн.

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 5584,66 грн.

5.8 Розрахунок вартості науково-дослідної роботи

Вартість науково-дослідної роботи визначається за формулою:

$$Ц = С_В \cdot (1 + Р_{рен}) \cdot (1 + ПДВ) \quad (5.11)$$

де, $Р_{рен.}$ – рівень рентабельності, 30 %,

ПДВ – ставка податку на додану вартість, (20 %).

Вартість на науково - дослідницьку складе:

$Ц$ = 5584,66× (1 + 0,3) × (1 + 0,2) = 8712,07грн.

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене повне відображення кінцевих результатів використання робочої сили, засобів, технологічного оснащення та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$Е_р = \frac{П}{С_В}, \quad (5.12)$$

де, $П$ – прибуток;

$С_В$ – собівартість.

Плановий прибуток ($П_{пл}$) визначається за формулою:

$$П_{пл} = Ц - С_в \text{ .} \quad (5.13)$$

Отже, плановий прибуток буде складати:

$$П_{пл} = 8712,07 – 5584,66 = 3127,41грн.$$

Згідно формули 6.12 економічна ефективність буде складати,

$$E_p = 3127,41 / 5584,66 = 0,56.$$

Термін окупності капітальних вкладень (T_p) розраховують:

$$T_p = \frac{1}{E_p}, \qquad (5.14)$$

Термін окупності дорівнює:

$$T_p = 1 / 0,56 = 1,79 років$$

Отже:

плановий прибуток від розробки становить 3127,41грн.,

економічна ефективність дорівнює 0,56

термін окупності становить 1,79 років.

Виходячи з вище розрахованих економічних та фінансових показників, можна вважати, що така науково-дослідницька робота є доцільною, економічно обґрунтованою та вигідним.

РОЗДІЛ 6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Безпека праці при використанні інформаційно-телекомунікаційних технологій

Теперішній розвиток та використання інформаційно-телекомунікаційних технологій – це технологічна система, раціональне та ефективне використання якої можливе лише при відповідній технічній, методичній та фаховій підготовці тих, хто буде її використовувати.

Перехід сучасного суспільства до ери глобальної комп'ютеризації та цифрових технологій вимагає від сучасної людини володіння знаннями новітніх інформаційних технологій та вміння безпечного використання комп'ютерної техніки. Наразі визріла необхідність підвищення рівня безпеки праці при використанні інформаційно-телекомунікаційних технологій, особливо в освітніх установах.

Здатність педагогічних працівників до запровадження сучасних засобів навчання в освітню практику стає обов'язковою компонентою підвищення якісних показників освітньої діяльності, а формування цієї здатності – одне з головних завдань освітньої установи. Проаналізовані можливості безпечного використання інформаційно-комп'ютерних технологій у навчальному процесі, що сприяє урізноманітненню предметної діяльності студентів, надає можливість для різнобічного саморозвитку особистості, підвищує мотивацію для отримання якісної освіти.

Під час будівництва, капітального ремонту будівель закладів освіти, лабораторних та лекційних приміщень бажано використовувати мінімальну кількість легкозаймистих матеріалів (дерева, пінопласту), а також легкозаймистого пластика в ізоляції. Рекомендується віддавати перевагу цеглі, склу та металу. Приміщення, де знаходяться технічні засоби повинно добре вентилюватися і охолоджуватися в жарку пору року. Досить важливим є своєчасний відвід надлишкового тепла від технічних пристроїв.

Безпека використання мультимедійної техніки в установах передбачає наявність загальнодоступної інструкції, в якій мають бути вказані обов'язкові

вимоги до облаштування робочого місця і процесу використання техніки. Ці правила єдині для всіх організацій, їх виконання контролюється керівними органами.

Для працівників, які працюють в кабінетах, що обладнані інформаційно-телекомунікаційними засобами, повинен бути проведений усний базовий інструктаж, в подальшому у друкованій формі інструкція повинна надаватися для докладного вивчення. В обов'язковому порядку така інформація розміщується в кабінетах та лабораторіях на видному місці. Інструктаж має охоплювати повний цикл контакту людини з комп'ютером, телекомунікаційним засобом, лабораторним стендом, засобами зв’язку та вимірювальна база.

Перед початком роботи, перед тим, як включити комп'ютер, необхідно переконатися в тому, що в зоні досяжності відсутні оголені дроти і різні шнури. Вони не тільки заважатимуть роботі, але й будуть нести потенційну небезпеку в разі короткого замикання. Не можна розпочинати роботу з технічними засобами які мають видимі пошкодження. У разі виявлення тріщини на корпусі або пошкоджень іншого роду, потрібно звернутися за допомогою до фахівців з обслуговування техніки. Це саме стосується і комп’ютерних засобів. Предмети на столі, лабораторному стенді не повинні заважати огляду, перешкоджати користуватися мишкою і клавіатурою, а поверхня екрану мусить бути абсолютно чистою.

Неприпустимо включати персональний комп'ютер в подовжувачі і розетки, в яких відсутня заземлювальна шина. Під час відключення пристроїв забороняється руками тягнути за жили кабелю.

Забороняється працювати в приміщеннях з підвищеною вологістю, а також, якщо поруч присутні відкриті джерела вологості (калюжі на поверхні столу чи мокра підлога, настил.

Інформаційні технології в навчанні – це педагогічні технології, що використовують технічні і програмні засоби. Сучасні інформаційні технології це потужний інструмент для розвитку прогресу в усіх сферах суспільного розвитку та освіті. Стрімке впровадження комп’ютерів у сфері управління виробництвом, на транспорті, в банківській системі, бізнесі, системі освіти та

інших сферах призвело до того, що мільйони людей виявились задіяними у взаємодію людини з комп'ютером.

Будь-яка взаємодія людини та засобів праці – є двостороння. Сучасні технології та техніка, до яких належать інформаційно-телекомунікаційні технології, несуть у собі певні потенційні небезпеки та шкідливий вплив. В зв'язку з цим набуває актуальності вивчення фізіологічних, психологічних, соціальних та виробничих наслідків у системі «людина-комп'ютер-середовище» та розробка і впровадження заходів щодо нормалізації праці та збереження здоров'я працівників під час роботи за комп'ютером та засобами телекомунікацій.

Ймовірність негативних наслідків від використання персонального комп'ютера така ж, як і при експлуатації інших технічних пристроїв та обладнання. Нехтування елементарними рекомендаціями має серйозні наслідки для їх користувачів. Комп'ютер – це таке ж потенційне джерело загроз для здоров'я, майна і навіть життя користувача. Непряма шкода, яка непомітна відразу, це є шкода здоров'ю.

Вже ні у кого не викликає сумнівів щодо існування величезного негативного навантаження на зір, яке стає причиною його незворотного погіршення, почервоніння і синдрому «сухого ока». Неправильна поза при роботі з комп'ютером викликає численні захворювання суглобів, грудної клітки і регулярні болі різного характеру. Бомба уповільненої дії – надмірне навантаження на психіку користувача.

Небезпека ПК як електроприладу полягає у виникненні збоїв в електричному живленні і можливість загоряння всієї системи. Основні правила організації простору навколо робочого місця стверджують, що при тривалій та інтенсивній роботі, на поверхні складових комп'ютера виникають невеликі розряди струму. Ці заряди активізуються під час дотиків до них і призводять до виходу техніки з ладу. Потрібно регулярно використовувати нейтралізатори, зволожувачі повітря та антистатичні засоби.

Неприпустимо знімати корпус будь-якої із складових частин ПК чи другого обладнання під час його роботи. Розбирання та ремонт техніки мають

здійснюють тільки працівники, які мають відповідну підготовку.

Своєчасна пильність допоможе уникнути небезпечних ситуацій для життя і зберегти цілісність техніки. В аварійних ситуаціях, при неполадках в електропостачанні пристрою необхідно відразу відключити комп'ютер від мережі. Якщо виявлено оголений провідник, то необхідно оперативно сповістити всіх працівників, не допускаючи будь-чийого контакту з ним. У кожній установі повинні знаходитися вогнегасники (вуглекислотні або порошкові), а також інші вогнегасні засоби в необхідній кількості. Персонал зобов'язаний знати де знаходяться засоби для гасіння вогню і куди потрібно телефонувати в разі пожежі.

При ураженні людини електричним струмом, перш за все, надається перша допомога (штучне дихання і зовнішній непрямий масаж серця), і відразу викликається швидка допомога. По закінченню роботи потрібно правильно закрити всі програми і вікна. В комп’ютері не можна залишати активні периферійні носії інформації (диски, «флешки», чи другі носії інформації).

Розглядаючи вимоги до робочого місця слід пам’ятати, що мінімальна площа робочого місця для однієї людини – 6 $м^2$. Світло у приміщення, де розміщені інформаційно - телекомунікаційні засоби, повинно надходити від штучних і природних джерел. Лампи освітлення не мають утворювати відблиски на екрані, а надлишок сонячних променів необхідно перекривати за допомогою штор або жалюзів.

При виконанні протягом дня робіт, які належать до різних видів трудової діяльності, за основну роботу з комп’ютерною технікою слід вважати таку, що займає не менше 50% часу впродовж робочої зміни чи робочого дня. Відповідно до санітарних правил встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з комп’ютером при 8-годинній денній робочій зміні в залежності від характеру праці:

для розробників програм із застосуванням комп’ютерної техніки, слід призначити регламентовану перерву для відпочинку тривалістю 15 хв. через кожну годину роботи;

для операторів із застосуванням комп’ютерної техніки, слід призначити

регламентовані перерви для відпочинку тривалістю 15 хв. через кожні 2 години роботи;

для операторів комп'ютерного набору, слід призначити регламентовані перерви для відпочинку тривалістю 10 хв. після кожної години роботи.

Поряд з технічними, організаційними та іншими заходами і засобами щодо збереження здоров'я та підвищення працездатності працівників значна увага повинна приділятись медичним профілактичним заходом щодо збереження здоров'я та підвищенні працездатності користувачів комп'ютерів. До вказаних заходів належать: медичні огляди (попередні та періодичні); раціональне і профілактичне харчування; спеціальні вправи, самомасаж та психофізіологічне розвантаження.

Перехід сучасного суспільства до ери глобальної комп'ютеризації вимагає від сучасної людини вміння користуватись комп'ютерною технікою, володіти певними знаннями новітніх інформаційних технологій і безпечного застосовувати їх у різних сферах життєдіяльності [9; 10]. Організована таким чином трудова діяльність та навчальний процес дозволяє гарантувати безпеку працівників та користувачів при використанні інформаційно-телекомунікаційних технологій навчання та зберегти здоров'я та працездатність як педагогічних працівників так і студентів.

6.2 Захист від електромагнітного випромінювання радіочастотного та оптичного діапазонів

Джерелами випромінювання електромагнітної енергії є різні установки, починаючи від потужних телевізійних, радіомовних станцій, промислових установок високочастотного нагрівання і закінчуючи вимірювальними, контрольними і лабораторними приладами різного призначення. Джерелами випромінювання можуть бути будь-які елементи, що ввімкнені в високочастотне коло.

Робочі місця обслуговуючого персоналу можуть бути в наступних зонах електромагнітного поля: ближній, проміжний і дальній у залежності від частот

електромагнітних полів (ЕМП), параметрів і типів систем, які випромінюють на віддалі від джерела випромінювання до робочого місця. На характер розподілу поля по приміщенню впливають обладнання, прилади і металеві конструкції будинків, які утворюють ЕМП вторинного випромінювання.

Первинним проявом дії електромагнітної енергії є нагрівання, яке може призвести до змін і навіть до пошкоджень тканин і органів. Механізм поглинання енергії – складний. У тканинах, які опромінюються є іонна дисперсія, дипольне і резонансне поглинання. Теплова дія характеризується загальним підвищенням температури тіла або локальним нагріванням тканин.

При загальному опроміненні підвищення температури тіла більше ніж на 1^0С недопустиме. Нагрівання особливо небезпечне для органів зі слабкою терморегуляцією, які мають невелику кількість кровоносних судин або недостатньо інтенсивний кровообіг (мозок, очі, нирки, шлунок, жовчний міхур). Електромагнітна енергія довжиною хвилі (1-20)см шкідливо діє на очі, викликаючи катаракту. Під впливом магнітного поля частотою 50 Гц з'являється "магнітний фосфен" (відчуття миготіння). У результаті довготривалого перебування в зоні дії ЕМП наступає передчасна стомлюваність, сонливість або порушення сну, болі голови, наступає розлад нервової системи. При систематичному опроміненні спостерігається зміна кров'яного тиску, сповільнення пульсу, нервово-психічні захворювання і трофічні явища (випадіння волосся, ламкість нігтів).

Дослідженнями встановлено, що біологічна дія одного і того ж за частотою ЕМП залежить від напруженості його складових або густини потоку потужності для діапазону більше 300 МГц. Це є критерієм для визначення біологічної активності електромагнітних випромінювань. Для цього електромагнітні випромінювання з частотою до 300 МГц розбиті на діапазони, для яких установлені гранично допустимі рівні напруженості електричної і магнітної складової поля. Для населення ще враховують місцезнаходження випромінювача в зоні забудови або житлових приміщень. Для електромагнітних випромінювань з частотою від 300 до 300 000 МГц встановлена граничнодопустима густина потоку потужності з врахуванням часу

опромінення і режиму роботи установки.

На стадії проектування радіоелектронної апаратури необхідно виконувати попередній розрахунок можливої інтенсивності ЕМП на робочому місці.

Для зменшення впливу електромагнітного випромінювання застосовуються такі ж засоби захисту, як і при НВЧ – випромінюванні, тобто: захист часом, захист віддаллю, зменшення потужності безпосередньо в джерелі. Екранування джерел випромінювання використовується для зменшення інтенсивності ЕМП на робочому місці. У цьому випадку застосовують заземлені екрани з металевих листів або сіток у вигляді замкнутих камер або кожухів. Ефективність екранування являє собою відношення параметра ЕМП в даній точці при відсутності екрана (E,H) до цього ж показника в цій же точці при наявності екрану. Товщину екрану δ, виготовленого з суцільного матеріалу, який забезпечує задане послаблення інтенсивності поля.

При виборі конструкції екрана або камери необхідно враховувати ступінь їх герметичності (наявність отворів). Якщо отвори рівні або кратні цілому числу півхвиль, тоді різко зросте потужність випромінювання, оскільки така щілина є антеною. У цьому випадку послаблення ЕМП досягається насадкою на отвір спеціального патрубка, який являє собою граничний хвилевід. Вентиляційні, оглядові та інші отвори затягуються металевими сітками, які щільно припаяні по периметру. Застосовують граничні хвилеводи з сітками на обох кінцях, щільникову конструкцію або патрубки. Контактуючі поверхні частин екрана повинні мати антикорозійне покриття, (лудіння, цинкування, міднення) і щільно прилягати один до одного по всьому периметру. Екранування робочого місця застосовують, якщо неможливо здійснити екранування джерел випромінювання. Для цього споруджують невеликі кабіни або металевих ширм з радіо поглинаючим покриттям. Індивідуальні засоби захисту застосовують у тому випадку, коли інші засоби недопустимі або неефективні. Як засоби захисту застосовують халати, комбінезони, капюшони, захисні окуляри. Для захисту від постійного магнітного поля застосовують шапки і спідниці з пермалою. Для захисту очей від НВЧ - випромінювання застосовують сіткові або скляні окуляри, покриті шаром двооксиду олова.

До випромінювання оптичного діапазону відносяться інфрачервоні й ультрафіолетові хвилі, видиме світло, лазерне випромінювання.

По фізичній природі інфрачервоні промені мають хвильові (довжина хвилі 0,78-540 мкм) і квантові властивості. Генератором випромінювання є будь-яке тіло, температура якого вище абсолютного нуля. За законом Стефана-Больцмана інтегральна густина випромінювання, Вт/м^2, абсолютно чорного тіла пропорційна четвертому ступеню його абсолютної температури.

З підвищенням температури тіла змінюється спектральний склад його випромінювання. Чим вища температура тіла, тим коротша довжина хвилі, максимального випромінювання.

Інфрачервона енергія, яка потрапляє на тіло людини, діє передусім на незахищені його частини (лице, руки, шию, груди), причому конвективне тепло впливає на зовнішній шкіряний покрив, тоді як інфрачервоне випромінювання може проникнути на деяку глибину в тканину. При довготривалому перебуванні людини в зоні інфрачервоного випромінювання, як і при систематичній високій температурі наступає різке порушення теплового балансу в організмі. Для вимірювання густини потоку випромінювання на робочому місці застосовують актинометр – прилад, який дозволяє вимірювати густину потоку інфрачервоного випромінювання у діапазоні від 0 до 14кВт/м^2 . Основні види захисту від інфрачервоного випромінювання – захист часом, захист віддалю, усунення джерела тепловиділення, теплоізоляція, охолодження гарячої поверхні, забезпечення тепловіддачі тіла людини та індивідуальні засоби захисту. Потужність випромінювання можна знизити за рахунок конструкторських і технологічних рішень (зміною нагрівання виробів у нагрівальних пічках індукційним нагріванням та ін.) і за рахунок покриття поверхні, яка нагрівається, тепло ізолювальним матеріалом. Для захисту очей застосовують світлофільтри зі спеціального жовто-зеленого або синього скла.

Ультрафіолетове випромінювання змінює склад виробничої атмосфери. Утворюється озон, оксиди азоту і пероксид водню. Короткохвильове випромінювання іонізує повітря, утворює в атмосфері ядра конденсації, які зменшують освітленість робочих місць і призводять до утворення туманів.

Основні засоби захисту. Першочергові заходи – це конструкторські і технологічні рішення, які виключають генерацію або понижують інтенсивність випромінювання. Спеціальні засоби захисту (екранування джерел випромінювання, фарбування стін у світлі кольори) попереджують розповсюдження і знижують інтенсивність цих випромінювань у виробничих приміщеннях. Очі захищають окулярами або щитками зі склом – світлофільтром. Для захисту шкіри використовують мазі з речовинами – світлофільтрами для цих променів (салол, саліцилово-метиловий ефір та ін.), а також спецодяг з бавовняних тканин і грубововняного сукна. Руки захищають рукавицями.

Діапазон довжин хвиль які випромінюють оптичні квантові генератори (ОКГ) – лазери, охоплює видимий спектр і розповсюджується в інфрачервоній і ультрафіолетовій областях.

Найбільш чутливими до дії випромінювання ОКГ є очі. Випромінювання викликають опіки і пошкодження сітківки ока, це може призвести до сліпоти. Небезпечне не тільки пряме випромінювання, але й відбите від стін, обладнання.

Існують “Санітарні норми і правила улаштування і експлуатації лазерів”, до яких ввійшли організаційні та інженерно-технічні заходи, які можуть забезпечити зменшення густини потоків енергії (потужності) на робочих місцях до величин, значно менших від допустимих. ОКГ розміщують в окремих або відгороджених приміщеннях. Саме приміщення і обладнання не повинні мати дзеркальної поверхні. Стіни, стелі, обладнання й інші предмети фарбують матовою фарбою з малою сорбційною здатністю. Приміщення повинно мати високу освітленість, а також припливно-витяжну вентиляцію. При розміщенні в одному приміщенні декількох ОКГ їх огороджують ширмами, шторами або екранами, що не пропускають випромінювання. Надійним захистом від випадкового попадання випромінювання на людину є світловод, який екранує промінь на усьому шляху його дії (від ОКГ до мішені).

РОЗДІЛ 7 ЕКОЛОГІЯ

7.1 Захист інформаційних управляючих систем від ушкоджень, що викликані дією ЕМІ ядерних вибухів

У воєнних доктринах багатьох країн світу важлива роль відводиться застосуванню зброї масового ураження (хімічної, ядерної, бактеріологічної), як зброї великої вражаючої здатності, призначеної для нанесення масових втрат та руйнувань. Особливе значення приділяється ядерній зброї, що є одним з самих руйнівних засобів ведення війни.

Ядерна зброя – це зброя масового ураження вибухової дії, яка заснована на використанні внутрішньоядерної енергії, що виділяється при ланцюгових реакціях розподілу важких ядер деяких ізотопів урану і плутонію або при термоядерних реакціях синтезу легких ядер у більш важкі. Один із основних вражаючі фактори ядерної зброї - електромагнітний імпульс.

Внаслідок іонізації повітря і руху електронів з великими швидкостями виникають електромагнітні поля, які утворюють імпульсні електричні розряди і струми. Електромагнітний імпульс (ЕМІ), який утворюється в атмосфері подібно блискавиці, може наводити сильні струми в антенах, електромережах (антени довгих та наддовгих ЕМ хвиль), інформаційно-управляючих системах, тощо. ЕМІ уражає, перш за все, електронну і радіотехнічну апаратуру, яка знаходиться на озброєнні, військовій техніці та інших об'єктах. Радіус дії ЕМІ при повітряних вибухах потужністю 1 Мт може поширюватися до 32км, при вибуху потужністю 10 Мт - до 115 км.

Технічні характеристики ЕМІ наступні:

- довжина хвиль (1 – 1000) м, частота – (10 кГц - 100 МГц);
- час наростання імпульсу 10 nsec, тривалість імпульсу ≥ 230 nsec;
- інтенсивність електричного поля ≥50 кВ/хв., магнітного поля - 130 А/хв.;
- напруженість ЕМ поля, створюваного ЕМІ, досягає 50 000 В/м (тоді як у радіолокації вона не перевищує 200 В/м, а у зв'язку – 10 В/м).

Виходячи з вище приведених характеристик в момент приходу ЕМІ чутливе електронне обладнання одержить дуже велике перевантаження,

відбувається пробій ізоляції, виходять з ладу розрядники, запобіжники, відключаються реле та ін.

Особливо чутливими до впливу ЕМІ є 6 основних груп об'єктів і систем:

1) системи передачі електроенергії: повітряні ЛЕП, кабельні лінії, різні види з'єднувальних ліній і повітряна електропроводка;

2) системи виробництва, перетворення і накопичення енергії: електростанції, генератори постійного і змінного струму, трансформатори, перетворювачі струмів і напруг, комутатори і розподільні пристрої, електричні батареї і акумулятори, паливні, сонячні й термоелементи;

3) системи регулювання і управління: електромеханічні й електронні датчики та інші елементи автоматики, комп'ютерні установки, мікропроцесори;

4) системи споживання електроенергії: електродвигуни, нагрівальні, холодильні, вентиляційні, освітлювальні установки та кондиціонери;

5) системи електротяги: електроприводи, напівпровідникові та ін.;

6) системи радіозв'язку, передачі, зберігання і накопичення інформації: антенні системи, приймально-передавальні пристрої, АТС.

Найбільш стійкі до ЕМІ вакуумні електронні прилади, які виходять із ладу при енергії 1 Дж.

Більшість систем зв'язку працюють у діапазоні частот від середніх до ультрависоких і можуть буди пошкоджені залежно від робочого діапазону частот. Радіолокаційні системи менше вразливі до ЕМІ, тому що працюють у тих діапазонах частот, де щільність енергії ЕМІ невелика, рис.7.1.

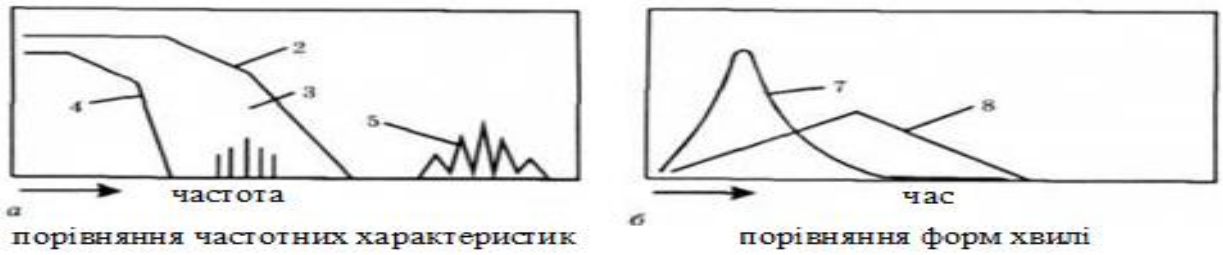

Рисунок 7. 1 Характеристика ЕМІ: 2,7 – ЕМІ; 3 – засоби зв'язку; 4, 8 – розряд атмосферної блискавки; 5 – РЛС

Сучасні технічні підходи дають можливість розробити різні рівні та системи захисту від ЕМІ до яких входять схеми, стійкі до електромагнітної інтерференції, радіоелектронні елементи стійкі до ЕМІ, екранування окремих пристроїв або цілих електронних систем, використання стійких радіотехнічних вузлів до потужних ЕМІ.

7.2. Організація оповіщення та зв'язку у надзвичайних ситуаціях техногенного та природного характеру

Сповіщення про загрозу виникнення або виникнення надзвичайних ситуацій — доведення сигналів і повідомлень органів управління цивільного захисту про загрозу та виникнення надзвичайних ситуацій техногенного та природного характеру, аварій, катастроф, епідемій, пожеж тощо до центральних і місцевих органів виконавчої влади, підприємств, установ, організацій і населення.

Рішення про оповіщення виникнення надзвичайної ситуації приймають на рівнях:

- загальнодержавному – Прем'єр-міністр України;
- територіальному – голови обласних, міських держадміністрацій;
- місцевому – голови органів місцевого самоврядування;

об'єктовому – керівники об'єктів.

Оповіщення – доведення сигналів і повідомлень органів управління цивільного захисту про загрозу та виникнення надзвичайних ситуацій, аварій, катастроф, пожеж, епідемій тощо до центральних і місцевих органів виконавчої влади (керівників об'єднаних територіальних громад), підприємств, установ, організацій та населення. Оповіщення здійснюється на рівнях: загальнодержавному – оперативно-черговою службою на пункті управління ДСНС; територіальному – оперативно-черговими службами на пунктах управління обласних, міських держадміністрацій; місцевому – черговими службами місцевих органів виконавчої влади; об'єктовому – диспетчерськими

(черговими) службами об’єктів, на яких створено спеціальні, локальні та об’єктові системи оповіщення.

З метою створення умов для побудови в Україні автоматизованої системи централізованого оповіщення нового покоління, яка б відповідала сучасним світовим стандартам, Урядом прийнято рішення щодо вдосконалення нормативно-правової бази у сфері організації оповіщення про загрозу виникнення або виникнення НС і привести її у відповідність до чинного законодавства. Постановою Кабінету Міністрів України від 27 вересня 2017 року № 733 затверджено Положення з організації оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту.

Положення визначає порядок організації оповіщення, забезпечення функціонування апаратури і технічних засобів оповіщення та технічних засобів телекомунікацій.

Керівники всіх рангів зобов'язані встановлювати у населених пунктах, на підприємствах сигнально – гучномовні пристрої, електронні інформаційні табло, радіотрансляційні точки для передачі інформації з питань цивільного захисту.

Системи оповіщення (програмно-технічні комплекси) за рівнями поділяються на: загальнодержавну, територіальну, місцеву автоматизовані системи, спеціальну, локальну, об'єктову системи оповіщення.

Система оповіщення це комплекс організаційно-технічних заходів, апаратури і технічних засобів оповіщення, апаратури, засобів та каналів зв’язку, призначених для своєчасного доведення сигналів та інформації про виникнення надзвичайних ситуацій до центральних та місцевих органів виконавчої влади.

Організація та забезпечення оповіщення про загрозу у надзвичайних ситуаціях здійснюється через:

- ПАТ "Національна суспільна телерадіокомпанія України";
- державні, публічні, комунальні, громадські телерадіокомпанії;
- операторів телекомунікаційних мереж загального користування;
- Інтернет-ресурси (сайти, соціальні мережі).

ВИСНОВКИ

Проаналізувавши та дослідивши системи супутникового зв’язку за технологією VSAT з точки зору захисту інформаційних каналів та безпеки передачі даних каналами зв’язку можна зробити наступні висновки у відповідності до перших трьох розділів роботи:

1. Проаналізовані типові системи супутникового зв’язку за технологією VSAT.

2. Проведений ґрунтовний аналіз схемних рішень з точки зору організації зв’язку та організації методів захисту інформаційних каналів.

3. Проаналізовані всі основні методи захисту інформаційних каналів на основі програмних та апаратних засобів.

4. Описані способи конфігурації функціонування мереж за технологією VSAT.

5. Проаналізовані методи віртуального розширення смуг пропускання та трафіків супутникових каналів зв’язку.

6. Досліджений та описаний захист від завадного середовища та наведені методи захисту від таких факторів.

7. Приведені та докладно проаналізовані організаційний, енергетичний, режективний методи боротьби з завадним середовищем під час проведення сеансів системами зв’язку.

8. Приведена практична реалізація даних методів боротьби з завадами.

9. Описана архітектура створення мереж типу VSAT для віддалених абонентів.

10. Розроблений власний дуальний метод захисту інформаційних каналів зв’язку під час проведення сеансів зв’язку.

11. Надані рекомендації з захисту інформації у каналах зв’язку при передачі та у процесі формування цифрових пакетів інформації та обробки після прийому.

БІБЛІОГРАФІЯ

1. Камнев В. Е. Спутниковые сети связи: учеб. пособие / В.Е. Камнев, В.В. Черкасов, Г.В. Чечин. – М.: Альпина Паблишер, 2004. – 536 с.

2. Максимов М.В., Бобнев М.П., Кривицкий Б.Х. и др. Защита от радиопомех / М.В. Максимов, М.П. Бобнев, Б.Х. Кривицкий. – М.: Советское радио, 1976. – 496 с.

3. Диксон Р.К. Широкополосные системы. Пер. с англ./Под ред. В.И. Журавлева – М.: Связь, 1979. – 304 с

4. Кантор Л.Я. Расцвет и кризис спутниковой святи // Электросвязь. – М. – 2007. – № 7.

5. Ганзий Д.Д., Егоров И.П. Адаптивный компенсатор помех. Патент № 2307488 от 25.04.2006 г.

6. Егоров И.П., Русаков П.В., Павлов В.В., Ганзий Д.Д. Система пространственной режекции помех на основе когерентного весового суммирования // Радиотехника. – М. – 2007. – № 11. – С. 3-5.

7. Криванич Є.М., Химич Г.П. Метод первинного захисту інформаційних каналів супутникового зв'язку / Є.М. Криванич, Г.П. Химич // Збірник тез VIII Міжнародної науково-технічної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ», том І. – Тернопіль, ТНТУ ім. Івана Пулюя. – 27-28 листопада 2019 р. – С. 99.

8. Технологии и средства связи: периодическое издание. – № 6. – 2008

9. Каганов В.І. Радіотехніка, комп'ютер / В.І. Каганов MATHCAD, Телеком, 2001.

10. Постанова КМУ від 27.09.2017 р. № 733 «Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку у сфері цивільного захисту»

11. НРБУ-97/Д-2000 «Норми радіаційної безпеки України; доповнення: Радіаційний захист від джерел потенційного опромінення»

12. Мендерецький В.В. Місце та роль інформаційно-телекомунікаційних технологій в системі освіти України / В.В. Мендерецький // Сучасні проблеми

математичного моделювання, прогнозування та оптимізації: тези доповідей VII міжнародної наукової конференції. – Кам'янець-Подільський: Кам'янець-Поділ. Нац. ун-т ім. Івана Огієнка, 2016. – с. 145-146.

13. Атаманчук П.С. Охорона праці в галузі: навчальний посібник / П.С. Атаманчук, В.В. Мендерецький, О.П. Панчук, Р.М. Білик. − К. : Центр учбової літератури, 2013. – 322 с.

14. Браїловський В.В. Охорона праці в телекомунікаціях та системах ТЗІ: навч. посібник / В.В. Браїловський, І.М. Зушман, В.Б. Русин. – Чернівці: Чернівецький нац. ун-т, 2018. – 82 с.

15. Вараксін О.О. Кібербезпека мереж наступних поколінь: навч. посібник / О.О. Вараксін, Є.В. Василіу, С.М. Горохов, В.Й. Кільдішев, В.Г. Кононович; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2012. – 240 с.

16. Конахович Г.Ф. Захист інформації в телекомунікаційних системах: навчальний посібник / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, В.М. Чуприн, О.О. Горбунов. – К.: НАУ, 2009. – 380 с.

17. Курушин А.А. Ansoft HFSS / А.А. Курушин. – М, 2013. – 736 с.

18. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификации сигналов радио закладных устройств / Г.А. Максименко, В.А. Хорошко. – К.: ООО «Полиграф консалтинг», 2004. – 317 с.

19. Конахович, Бабак В.П., Фисенко В.М. Специальный радиомониторинг / Г.Ф. Конахович, В.П. Бабак, В.М. Фисенко. – К.: "МК-Пресс ", М.: Издательский дом "Додэка-XXI ", 2007. – 384 с.

20. Юдін О., Конахович Г., Корченко О. Захист інформації в мережах передачі даних: підручник / О. Юдін, Г. Конахович, О. Корченко. – К.: Вид-во ТОВ НВП "ІНТЕРСЕРВІС", 2009. – 714 с.

21. Швець І.П. Компенсаційні методи захисту від завад у безпроводовій локальній мережі / І.П. Швець // Телекомунікаційні та інформаційні технології. – 2017. – № 4. – С. 94-102

22. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика / А.В. Петраков, В.С. Лагутин. – М.: Радио и связь, 2001. – 499 с.

23. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник / Уклад. Пількевич І.А., Лобанчикова Н.М., Молодецька К.В. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

24. Зеркалов Д.В. Охорона праці в галузі. Загальні вимоги: навчальний посібник / Д.В. Зеркалов. – К.: «Основи», 2011. – 551 с.

25. Тарасова В.В. Екологічна статистика: підручник / В.В. Тарасова. – Київ: Центр учбової літератури, 2008. – 392 с.

26. Сакевич В.Ф., Поліщук О.В. Цивільна оборона. Теоретичні основи: навчальний посібник / В.Ф. Сакевич, О.В. Поліщук. – Вінниця: ВНТУ, 2009. – 136 с.

27. Пат. 2232475, МПК H04 K1/02. Способ повышения скрытности группы узкополосных сигналов / В. В. Прилепский, А. В. Гармонов, С. В. Фурсов, В. М. Усачев; Воронежский научно-исследовательский институт связи. – № 2003110893/09; заявл. 16.04.2003. Опубл. 10.07.2004.

28. Грибанов А.С., Невзоров Ю.В. Помехозащищённость систем спутниковой связи с кодовым разделением каналов / А.С. Грибанов, Ю.В. Невзоров // Журнал радиоэлектроники. – 2013. – № 4.

29. Байбурин В.Б., Мантуров А.О. Перспективные методы защиты информации при передаче по открытому каналу святи / В.Б. Байбурин, А.О. Мантуров // Информационная безопасность регионов. – 2008. – № 1. – С. 33-37.

30. Определение координат источников сигналов в системах спутниковой связи : дис. канд. техн. наук : 05.12.04 / В. В. Сухотин ; рук. работы С. П. Пань-ко ; Краснояр. гос. техн. ун-т. Красноярск, 2003. – 127 с.

31. Модель А.М. Фильтры СВЧ в радиорелейных системах, 1967.

32. Kaganov V.I. Radiotexnika Kompjuter Mathcad, 2001.

33. Кантор Л.Я. Спутниковая связь и вещание. Справочник (1988).

34. Высоцкий Г. Услуги сетей VSAT и их потребители // Теле-Спутник. – 201. – № 3. – С. 20-28.

35. Гладченков А. Спутниковые технологии VSAT и информационная безопасность сети / А. Гладченков // Журнал сетевых решений LAN. – № 9. – 2007. – С. 40-44.

36. Колюбакин В. Что такое VSAT / В. Колюбакин // Теле-Спутник. – № 7. – 2015. – С. 6-8.

37. Мальцев Г.Н. Сетевые информационные технологии в современных спутниковых системах святи / Г.Н. Мальцев // Информационно-управляющие системы. – № 1. – 2007. – С. 33-39.

38. Patent 2232475, MPK N04 K1/02. Sposob povyshenija skrytnosti gruppy uzkopolosnyh signalov / V. V. Prilepskij, A. V. Garmonov, S. V. Fursov, V. M. Usachev. – Federal'noe gosudarstvennoe unitarnoe predprijatie Voronezhskij nauchno-issledovatel'skij institut svjazi. № 2003110893/09; Zajav. 16.04.2003; Opubl. 10.07.2004.

39. Gribanov A.S., Nevzorov Ju. V. Pomehozashhishhjonnost' sistem sputnikovoj svjazi s kodovym razdeleniem kanalov // Zhurnal radiojelektroniki. – 2013. – №4.

40. Егоров И.П., Русаков П.В., Ганзий Д.Д. Реализация широкополосных систем пространственной режекции помех / И.П. Егоров, П.В. Русаков, Д.Д. Ганзий // Радиотехника. – М., 2008. – № 2.– С. 90-92.

41. Военные системы спутниковой связи (из справочника "Техника связи за рубежом", 1990 г.). – Режим доступа: http://www.radioscanner.ru/info/article189/

42. Егоров И.П., Русаков П.В., Павлов В.В., Ганзий Д.Д. Система пространственной режекции помех на основе когерентного весового суммирования / И.П. Егоров, П.В. Русаков, В.В. Павлов, Д.Д. Ганзий // Радиотехника. – М., 2007. – № 11. – С 3-5.

ДОДАТКИ

ДОДАТОК А

Вимоги до параметрів антенних пристроїв систем супутникового зв’язку з точки зору електромагнітної сумісності та захисту від впливу загроз ззовні

Вимоги регламентовані документом для супутникових систем зв’язку, які здійснюють роботу в діапазоні частот 6/4 ГГц (документ РСІ-302, «Регламент системи»). У цьому документі приведені основні вимоги до характеристик антен та високочастотної частини земної станції (ЗС), які призначені для роботи через геостаціонарні штучні супутники Землі типів "Горизонт", "Експрес", LMI-1та ін. У Регламенті приведена класифікація ЗС, таблиця 1.

Таблиця 1

Стандарт ЗС	Значення G/T, дБ/К	Типовий Ø антени, м	Ga_{max} антени (Тх)., дБ
С1	31,0	9,0…12,0	54,0
С2	28,0	6,5…7,5	51,0
С3	23,5	3,5…5,0	
С4	19,3	2,0…3,0	42,0

Шумова температура визначається при куті місця 50 град. і повинна бути приведена до входу опромінювача антени.

Вимоги до обвідної діаграми спрямованості:

- для стандартів земних станцій С1 і С2, які працюють через супутники "Горизонт", "Експрес", вимога щоб коефіцієнт підсилення Ga у 90% , бокових пелюсток не переважав наступні значення:

$$G(q) = 29-25 \log q \text{ (дБі)} , \text{ при } 1^0<q<48^0$$

$$G(q) = -10 \text{ (дБі)}, \quad \text{при } q>48^0$$

Рівень першої бокової пелюстки повинен бути не нижче на 14 дБ від рівня основної пелюстки діаграми спрямованості антени, для стандартів С3 і С4

$$G(q) = 49-10\log(D/\lambda)-25\log q \text{ (дБі)} \quad \text{при } 1^0<q<48^0$$

$$G(q) = 10-10\log (D/\lambda)\ (\text{дБі}) \qquad \text{при } q>48^0$$

Для стандартів С1, С2, С3, С4 при роботі через супутники LMI – 1 для основної та кросполяризаційної ДС у режимах передачі та прийому коефіцієнт підсилення у 90% піків не повинен перевищувати значень:

для D/l>50

$$G(q) = 29-25\log q\ (\text{дБі}),\ \text{при } 1^0<q<20^0$$

$$G(q) = -3{,}5\ (\text{дБі}),\ \text{при } 20^0<q<26{,}3^0$$

$$G(q) = 32-25\log q\ (\text{дБі}),\ \text{при } 26{,}3^0<q<48^0$$

$$G(q) = -10\ (\text{дБі}),\ \text{при } q>48^0$$

для D/λ<50

$$G(q) = 32-25\log q\ (\text{дБі})\ \text{при } 1^0<q<48^0$$

$$G(q) = -10\ (\text{дБі}),\ \text{при } q>48^0$$

ДОДАТОК Б

Вимоги до поляризаційних характеристик

При роботі земної станції ЗС через супутники "Горизонт", "Стаціонар" у діапазоні 6/4 ГГц антена повинна забезпечувати у режимі передачі та прийому сигнали з круговою поляризацією:

при передачі – лівого обертання, при прийомі – правого обертання. Коефіцієнт еліптичності (аксіальне відношення) повинен бути не більше 1,06 (що відповідає поляризаційній розв'язці 30,7 дБ) для антен з діаметром рефлектору більше 3,5м. При роботі через супутники «LMI – 1» затухання для сигналів перехресної поляризації в електричній вісі антени повинно складати не менше 33 дБ для земних станцій стандартів С1, С2, С3 і не менше 30 дБ для С4. Затухання перехресної поляризації при відхиленні від вісі повинно бути не гірше:

$$G(q)= 19-25\log q \text{ (дБі) при } 1{,}8^0<q<7^0$$

$$G(q)= -2 \text{ (дБі), при } 7^0 <q<9{,}2^0$$

Загасання для сигналу перехресної поляризації на будь-якій частоті передачі і прийому при відхиленні від осі по контуру - 1 дБ повинно становити не менше 28 дБ для стандартів С1 - С3, і не менше 25 дБ для С4.

Вимоги на параметри антен для земних станцій супутникового зв'язку входять до складу більш загального документа, що регламентує «Загальні технічні вимоги» на земні станції для ліній супутникового зв'язку, що працюють зі штучними супутниками Землі, які знаходяться на геостаціонарній орбіті в діапазонах частот 6 / 4,14 / 11 ... 12 ГГц.

Такі вимоги затверджені міжнародним консультативним комітетом при ООН, погоджені супутниковими операторами і є обов'язковими для виконання як з точки зору інформаційної безпеки так і з точки зору електромагнітної сумісності та завадостійкості систем зв'язку. Частотні діапазони для супутникових систем приведені у таблиці 2.

Таблиця 2

Частотні діапазони ЗС, МГц	
Режим передачі	Режим прийому
5725…6725	3400…4200
6725…7025	4500…4800
12750…13250	10700…11700
14000…14500	10950…11200
11450…11700	
12500…12750	