ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО
ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Виявлення Bluetooth передавачів
у контрольованій зоні»

на здобуття освітнього ступеня магістра
зі спеціальності __125_____
Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Андрій ШОКОДЬКО

Виконав: здобувач вищої освіти групи СЗДМ-62

_____ШОКОДЬКО Андрій

Керівник: _____ПЕПА Юрій_____
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Систем інформаційного та кібернетичного захисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ШОКОДЬКУ Андрію Андрійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Виявлення Bluetooth передавачів у контрольованій зоні».
Керівник кваліфікаційної роботи: ПЕПА Юрій, к.т.н., доцент.
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

Затверджена наказом Державного університету інформаційно-комунікаційних технологій від «____» 2023 р. №_____.

2. Строк подання кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
__Аналіз загроз при роботі Bluetooth.
__Оцінка ефективності методів пошуку Bluetooth пристроїв.
__Способи і методи виявлення робочих Bluetooth пристроїв у контрольованій зоні.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Огляд протоколу Bluetooth та Bluetooth пристроїв і сценаріїв їх застосування зловмисником.
2. Огляд методів пошуку радіозакладних пристроїв.
3. Розробка методу пошуку, що базується на особливостей протоколу Bluetooth.
4. Вибір пошукової антени.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах
_____

6. Дата видачі завдання 15.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз літературних джерел		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання четвертого розділу роботи		
6	Написання висновків по роботі		
7	Підготовка демонстраційних матеріалів		
8	Підготовка доповіді		

Здобувач вищої освіти _____ Андрій ШОКОДЬКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій ПЕПА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи містить: 74 стор., 41 рис., 1 табл. та 14 джерел.

Об'єкт дослідження – пристрої що використовують Bluetooth технологію для передачі інформації.

Предмет дослідження – методи пошуку працюючих пристроїв Bluetooth.

Мета роботи – аналіз можливостей використовування Bluetooth пристроїв для витоку інформації та розробка методу виявлення таких пристроїв.

Методи дослідження: математичні, аналітичні.

В рамках роботи проведено огляд технології Bluetooth. Проведено аналіз сценаріїв застосування зловмисником Bluetooth пристроїв. Виконано аналіз методів виявлення Bluetooth пристроїв. Здійснено розрахунок антени та смугового фільтру.

Галузь використання – забезпечення безпеки інформаційної системи.

Ключові слова: BLUETOOTH ПРИСТРІЙ, РЕЗОНАНС, ЗАКЛАДНИЙ ПРИСТРІЙ, ПРОТОКОЛ, АНТЕНА, СМУГОВИЙ ФІЛЬТР, ТРИАНГУЛЯЦІЯ.

ABSTRACT

The text part of the master's qualification work contains 74 pages, 41 figures, 1 tables and 14 sources.

Object of research – devices that use Bluetooth technology for information transfer.

Subject of research – methods of searching for working Bluetooth devices.

Purpose – to analyze the possibilities of using Bluetooth devices for information leakage and to develop a method for detecting such devices.

Research methods: mathematical, analytical.

As part of the work, an overview of Bluetooth technology was conducted. An analysis of scenarios for the use of Bluetooth devices by an attacker is carried out. The analysis of methods for detecting Bluetooth devices is carried out. The calculation of the antenna and bandpass filter is carried out.

Field of application – ensuring the security of the information system.

Keywords: BLUETOOTH DEVICE, RESONANCE, EMBEDDED DEVICE, PROTOCOL, ANTENNA, BANDPASS FILTER, TRIANGULATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ

AoA – Angle of Arrival

ACL – Asynchronous Connectionless

FHSS – Frequency Hop Spread Spectrum

GPS – Global Positioning System

ISM – Industry, science, medicine

RSSI – Received signal strength indicator

SCO – Synchronous Connection Oriented

ToF – Time of Flight

ИХК – Інтерфейс хост-контролера

ВСТУП

Технологія Bluetooth (стандарт IEEE 802.15) стала першою технологією, що дозволяє організувати бездротову персональну мережу передачі даних (WPAN — Wireless Personal Network). Вона дозволяє здійснювати передачу даних і голосу по радіоканалу на невеликі відстані (10-100 м) у неліцензованому діапазоні частот 2,4 ГГц і з'єднувати ПК, мобільні телефони й інші пристрої при відсутності прямої видимості.

Своєму народженню Bluetooth зобов'язана фірмі Ericsson, яка в 1994 році почала розробку нової технології зв'язки. Спочатку основною метою була розробка радіоінтерфейсу з низьким рівнем енергоспоживання й невисокою вартістю, що дозволяв би встановлювати зв'язок між стільниковими телефонами й бездротовими гарнітурами. Однак згодом роботи з розробки радіоінтерфейсу плавно переросли в створення нової технології.

У цей час на ринку працює велика кількість фірм, що пропонують модулі Bluetooth, а також компоненти для самостійної реалізації апаратної частини Bluetooth-пристрою.

Основне призначення Bluetooth - забезпечення економічної (з погляду споживаного струму) і дешевого радіозв'язку між різними типами електронних пристроїв, причому чимале значення надається компактності електронних компонентів, що дає можливість застосовувати Bluetooth у малогабаритних пристроях розміром з наручний годинник.

За рахунок шифрування даних отримання доступу до пристрою без дозволу користувача майже неможливо. Для того щоб почати обмінюватися даними між мобільними пристроями необхідно, щоб користувачі пройшли процедуру авторизації на цих пристроях, тобто обмінятися кодами доступу [1, 4]. Стандарт Bluetooth має більше 10 профілів, тобто наборів функції для пристрою Bluetooth. Основними профілями які були затверджені групою розробників SIG є:

- Advanced Audio Distribution Profile (A2DP) даний профіль призначений для передачі музики в бездротові навушники; – Audio / Video Remote Control Profile (AVRCP) профіль для управління функціями телевізора;

- File Transfer Profile (FTP_profile) профіль для обміну даними між пристроями;

- Hands-Free Profile (HFP) профіль призначений для з'єднання мобільних пристроїв та бездротових навушників з функцією розмови по телефону;

- LAN Access Profile (LAP) профіль що забезпечує доступ до мереж LAN, WAN чи Internet засобами іншого Bluetooth пристрою;

- SIM Access Profile (SAP, SIM) профіль дозволяє отримати доступ до SIM картки мобільного пристрою та використовувати одну SIM картку на декількох пристроях;

- Wireless Application Protocol Bearer (WAPB) профіль який випростовує протокол для організації (Point-to-Point) з'єднання через Bluetooth та багато інших профілів [1 – 4].

Підсумовуючи можна сказати, що перевагами даної технології є:

– мобільність;

– досить висока швидкість передачі даних;

– доступність;

– безпечність передачі даних;

– низька чутливість до перешкод (залежить від товщини та матеріалу перешкоди).

Усі ці властивості дозволяють зловмиснику використовувати Bluetooth для організації несанкціонованого каналу витоку інформації.

1 ВИТІК ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ РАДІОТЕХНОЛОГІЇ BLUETOOTH

1.1 Опис стандарту Bluetooth

Технологія Bluetooth покликано забезпечити універсальну мережу для:

- організації каналів передачі даних і мови;
- заміщення кабельних з'єднань;
- повсюдного застосування вбудованих у всілякі засоби зв'язку, комп'ютери й побутові прилади компактних і фантастично дешевих мережних адаптерів.

Технологія Bluetooth визначається наступними ключовими параметрами:

1. Частотний діапазон – 2,44 ГГц. Це смуга ПНМ – промислові, наукові й медичні застосування (ISM – industry, science, medicine);

2. FHSS – стрибкоподібна перебудова частоти з розширенням спектра. Радіопередавач здійснює передачу сигналу, перескакуючи з однієї робочої частоти на іншу по псевдовипадковому алгоритму. Дуплексний режим з часовим поділом (TDD) використовується для повнодуплексної передачі;

3. Підтримуються ізохронні й асинхронні послуги передачі інформації й забезпечується проста інтеграція з TCP/IP. Слоти (тимчасові інтервали) розгортаються для синхронних пакетів. Кожний пакет передається на своїй частоті радіосигналу;

4. Топологія локальної радіомережі організована за принципом множинних пікомереж, що взаємодіють між собою по стандартному радіоканалу. Пікомережа завжди включає одну майстер-станцію, яка синхронізує внутрішній трафік у пікомережі.

Спрощена блок-схема Bluetooth-Зв'язку представлена на рис. 1.1.

На прикладі Bluetooth-зв'язку по типу "точка - точка" показане інформаційну взаємодію двох хостів. Кожний Bluetooth-модуль містить

формуючу й приймально-передавальну апаратуру, а також вбудоване або "зашите" програмне забезпечення (Firmware). До останнього ставиться інтерфейс хост-контролера (HCI), менеджер зв'язку (Link Manager), а також контролер несучої частоти (Baseband).Зв'язок модуля з хостом на фізичному й канальному рівнях здійснюється за допомогою шин USB, UART, PC Card і відповідного вбудованого ПО. До фізичного рівня ставиться також радіолінія між модулями [1].

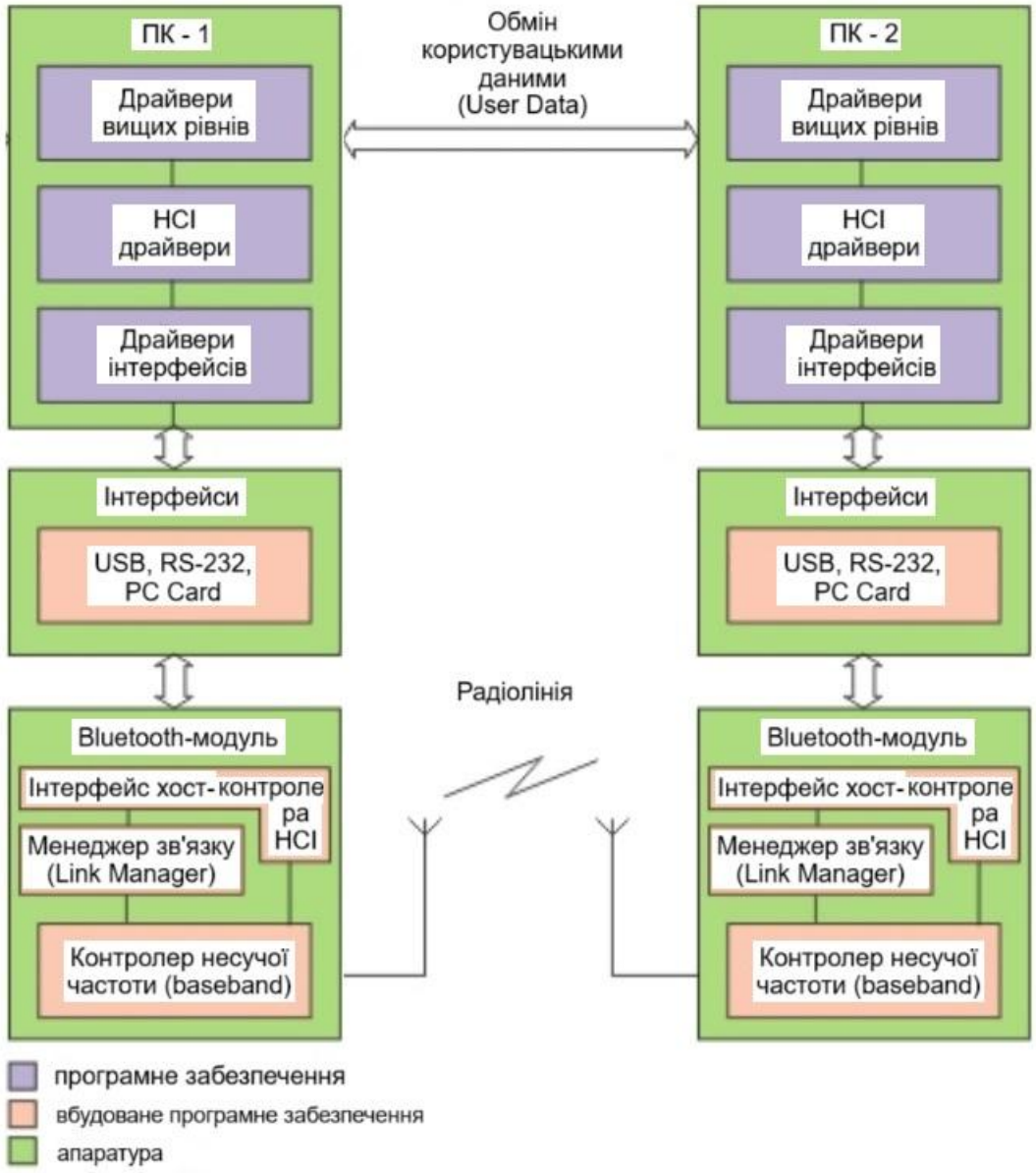


Рисунок 1.1 – Спрощена блок-схема Bluetooth-зв'язку

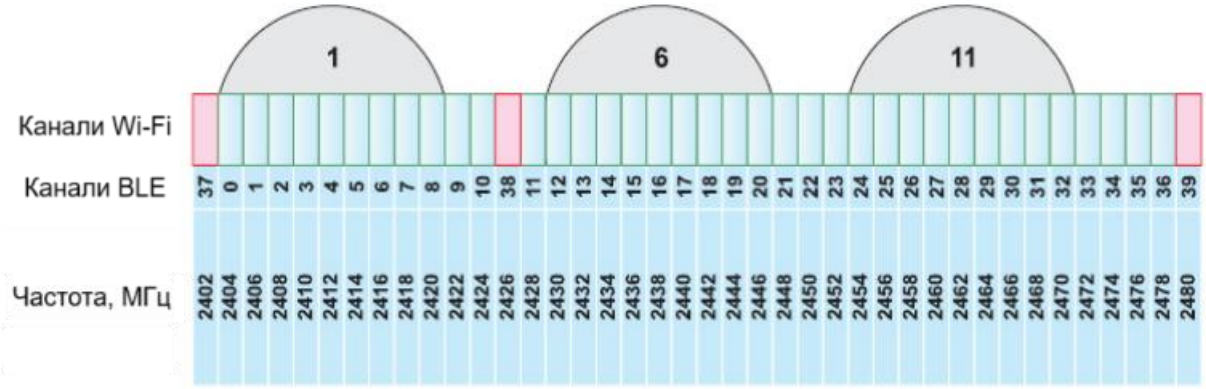
Модуль підтримує приймання – передачу даних і мовних сигналів. Зв'язок між модулем і хост-контролером проводиться за допомогою

високошвидкісного USB-Інтерфейсу або UART/ PCM-Інтерфейсу. Коли використовується USB -Інтерфейс, модуль є USB -відомим приладом і тому не вимагає ресурсів персонального комп'ютера.

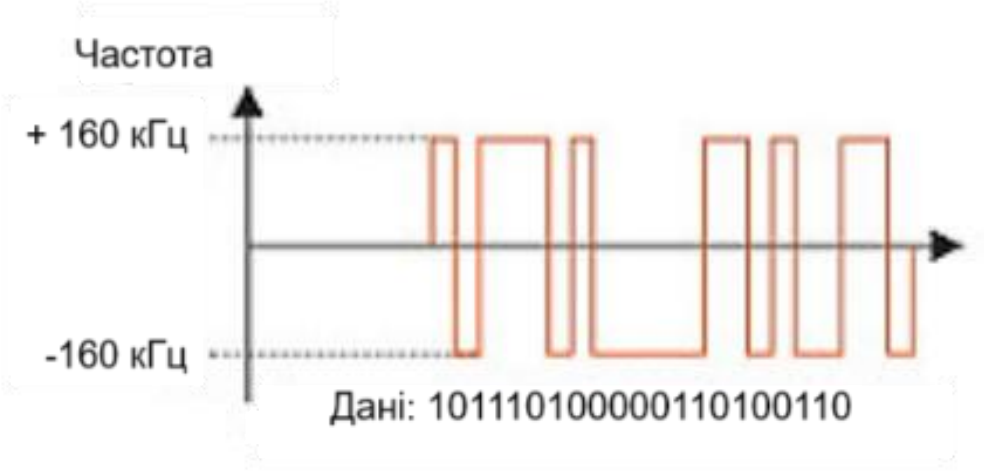
Інтерфейс хост-контролера (ІХК) у модулі є командним інтерфейсом. Хост через ІХК направляє команди, а у відповідь ухвалює від модуля повідомлення про їхнє виконання. Менеджер зв'язку встановлює необхідну конфігурацію ІХК.

Технологія Bluetooth припускає два види зв'язку: синхронну – SCO (Synchronous Connection Oriented) і асинхронну – ACL (Asynchronous Connectionless). Перший вид, SCO, розрахований на встановлення симетричного з'єднання "точка - точка" і служить переважно для передачі мовних повідомлень. Швидкість передачі інформації SCO рівна 64 Кит/с. Другий, ACL, призначений для пакетної передачі даних. Він підтримує симетричні й асиметричні з'єднання типу "точка - багато крапок". Швидкість передачі пакетної інформації при ACL складає порядку 721 Кбит/с. Пакети даних мають фіксований формат. На початку блоку перебуває 72-біт код доступу. Він може застосовуватися, зокрема, для синхронізації пристроїв. За ним іде 54-біт заголовок пакета, що містить контрольну суму пакета й інформацію про його параметри (наприклад, про повторну передачу блоку даних). Замикає пакет область, що безпосередньо містить інформацію, що пересилається. Розмір цієї області варіюється від 0 до 2745 біт.

Основним принципом побудови систем Bluetooth є використання методу розширення спектра при стрибкоподібній зміні частоти (FHSS - Frequency Hop Spread Spectrum). Увесь виділений для Bluetooth-Радіозв'язку частотний діапазон 2,402…2,480 ГГц розбитий на N частотних каналів (рис. 1.2 а). Кількість каналів становить 79. Смуга кожного каналу 1 МГц, рознос каналів – 140…175 кГц. Для кодування пакетної інформації використовується частотна маніпуляція (рис. 1.2 б) [1].



а)



б)

Рисунок 1.2 – а) частотний діапазон Bluetooth;
б) спосіб кодування пакетної інформації

Зміна каналів проводиться за псевдовипадковим законом із частотою 1600 Гц. Постійне чергування частот дозволяє радіоинтерфейсу Bluetooth транслювати інформацію із усього діапазону ISM і уникнути впливу перешкод з боку пристроїв, що працюють у цьому ж діапазоні. Якщо даний канал зашумлено, то система перейде на інший, і так буде відбуватися доти, поки не виявиться канал, вільний від перешкод. На рис. 1.3 показана частотно-часова площина, що ілюструє одночасну роботу трьох Bluetooth-модулів. Модулі працюють тактами (слотами), тривалістю 625 мкс. Кожному модулю в межах кожного такту призначається відповідний частотний канал і режим передачі або прийому [1].

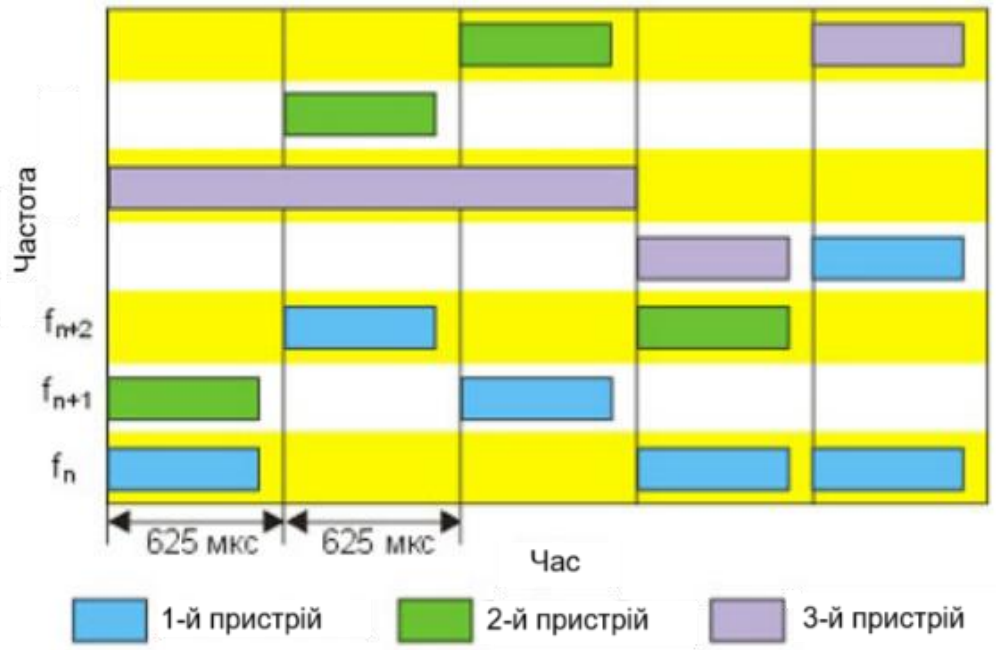


Рисунок 1.3 – Частотно-часова діаграма роботи модулів Bluetooth

Коли пари будь-яких Bluetooth-пристроїв з'єднується, то вони утворюють пікомережу. Апарат, що ініціює зв'язок, є ведучим (host, master), а інші – відомими (slaves). Звичайно ведучим є той модуль, який розміщений у найбільш потужному пристрої, такому, як персональний комп'ютер або плата CPU міні-ЕОМ. Число модулів у пікомережі не обмежується, але в будь-який момент часу активні повинні бути не більше восьми. Не існує різниці, як в апаратній, так і в програмній частині між ведучими й відомими пристроями. Кожне з них може бути й тем і іншим. Ведуче формує пікомережу (у кожній мережі воно тільки одне) і повністю контролює трафік. Відомі можуть відсилати повідомлення тільки в інтервалі "відомі - ведучому" після того, як до них звернувся в попередній слот "ведучий - відомим". Якщо в цьому інтервалі в ведучого немає ніякої інформації для відправлення відомим, то він передає пакет тільки з кодом доступу й заголовком. Якщо в мережі виявляється більш 8 пристроїв, то буде сформована друга пікомережа і так далі. ПередБачена координація трафіка й між мережами.

Безліч пікомереж, здатних взаємодіяти один з одним, формують розподілену мережу (Scatternet) (рис. 1.4).

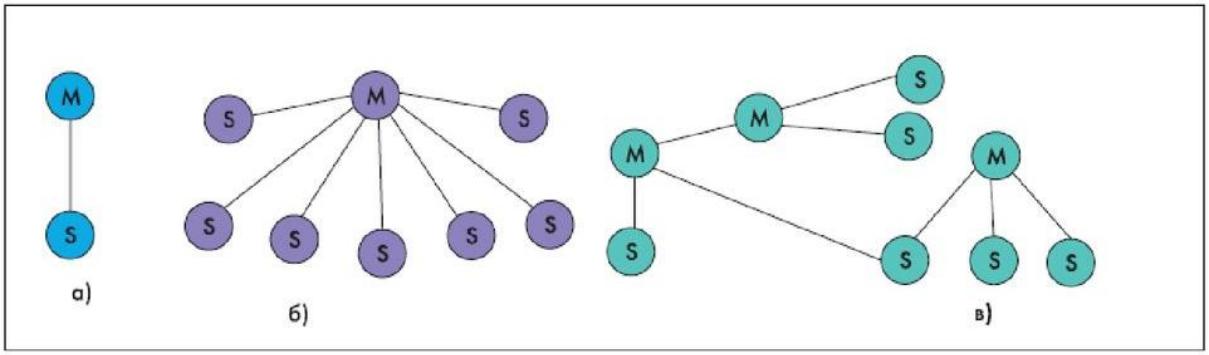


Рисунок 1.4 – Пікомережа й розподілена мережа Bluetooth

Незважаючи на FHSS, пристрої Bluetooth не завжди можуть виключити проблеми, пов'язані із впливом перешкод у діапазоні 2,4 ГГц. Тому крім FHSS використовується спеціальне кодування сигналів. По-перше, кодування трафіка помітно підвищує рівень захищеності зв'язку. По-друге, кодування дозволяє за допомогою спеціальних алгоритмів виявляти й коректувати помилки передачі даних. Крім того, щоб бути впевненим у тому, що пристрої вступають у зв'язок тільки з авторизованими на те пристроями, передбачена також вбудована процедура аутентифікації. Цим припиняє несанкціонований доступ до даних.

На рис. 1.5 показана структурна схема Bluetooth модуля STBT 3.0 [2].

STBT 3.0 - Bluetooth модуль містить радіочастотну схему й блок обробки. Модуль підключається через послідовний порт UART по протоколу HCI і може використовуватися в різних додатках.

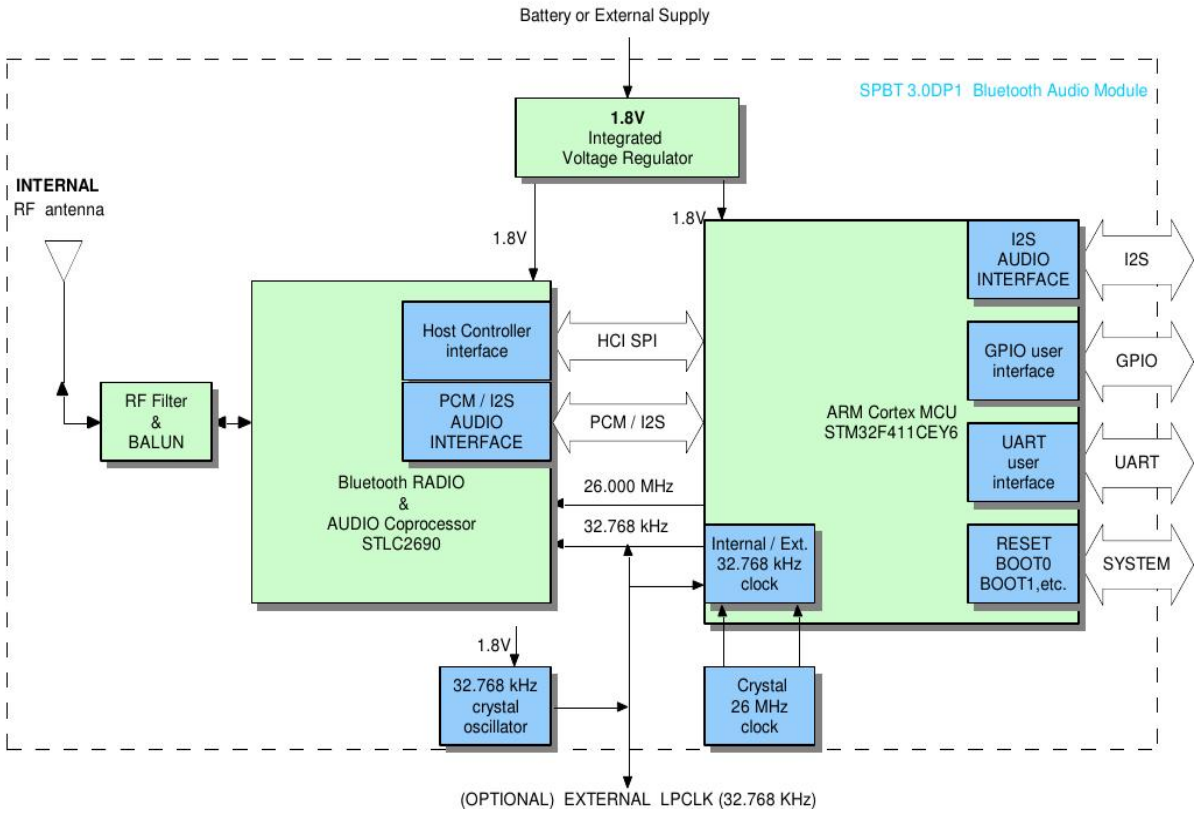


Рисунок 1.5 – Структурна схема Bluetooth модуля STBT 3.0

1.2 Аналіз сценаріїв використання Bluetooth у ролі закладного пристрою

Висока популярність протоколу Bluetooth не обмежує сферу застосування пристроїв для витоку інформації. Доступність модулів Bluetooth, низька їхня вартість (менш 3$), компактні габарити, висока енергоефективність дозволяє їх вбудовувати в різні предмети інтер'єру й передавати різну інформацію в тому числі й конфіденційну.

Наприклад, Bluetooth модуль CC2541 (рис. 1.6) має компактні габаритні розміри й може бути вбудований у провідну клавіатуру й використовуватися для перехоплення тексту, що вводиться, в тому числі й паролів. Недолік такого методу – досить складне й не занадто швидке підключення такого модуля усередині клавіатури сторонньою особою, що в принципі може бути трохи нівельоване шляхом заміни такою ж клавіатурою.

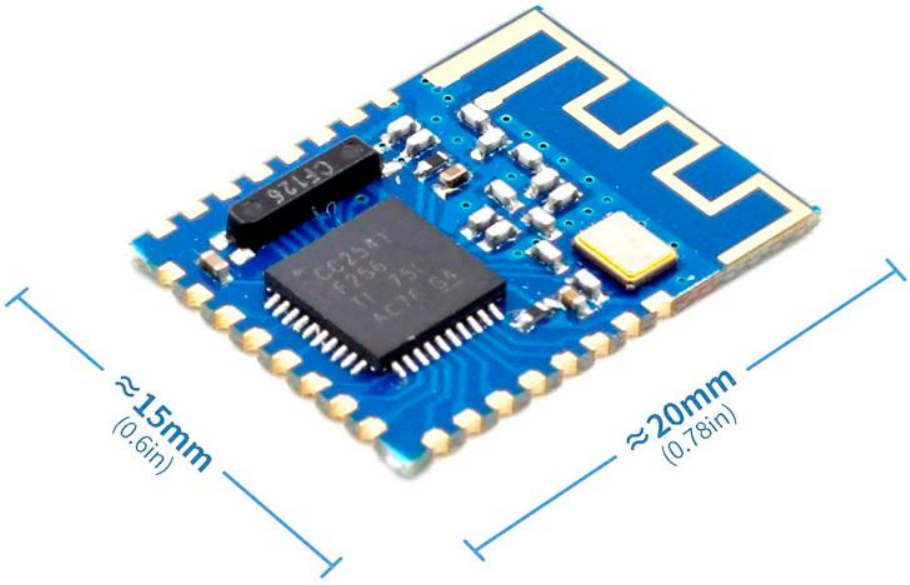


Рисунок 1.6 – Bluetooth 4.0 модуль на базі CC2541

Наступний метод, яким може скористатися зловмисник це використання USB приймально-передавача Bluetooth (рис. 1.7). у цьому випадку при підключенні такого пристрою до USB порту комп'ютера й установки відповідного ПО в зловмисника може з'явиться доступ до будь-якої інформації, що обробляється на цьому комп'ютері. Складності застосування цього методу можуть виникнути якщо комп'ютер буде заблокований паролем, що ускладнить інсталяцію зловмисного ПО. Однак пароль може бути зламаний методом описаним вище.

Рисунок 1.7 – USB Bluetooth трансмітер

Наступним сценарієм використання Bluetooth пристроїв для несанкціонованого доступу до конфіденційної інформації є застосування

Bluetooth-гарнітури (рис. 1.8) або менш популярного пристрою Bluetooth – мікрофона. Після з'єднання Bluetooth-гарнітури зі смартфоном, гарнітура встановлюється в непримітному місці приміщення де проводяться конфіденційні розмови. Недоліком такого методу є обмежена автономність пристрою приблизно добою, яка може бути збільшена до декількох діб (до 10) за допомогою використання системи VOX.

Рисунок 1.8 – Bluetooth-гарнітура

Також необхідно відзначити такий варіант використання як локалізація персоналу із включеним Bluetooth у смартфонах за допомогою Bluetooth міток (рис. 1.9) які заздалегідь установлені зловмисником у різних приміщеннях будинку.

Необхідно відзначити що дальність каналу витоку при використанні стандарту Bluetooth нижче версії 5.0 обмежена 100м за умови прямої видимості. Для стандарту 5.0 і вище довжина каналу може бути більш 1км за умови прямої видимості. У більшості випадків дистанції більш 60 метрів досить для зловмисника.

Рисунок 1.9 – Bluetooth-мітки

У більш складних випадках зловмисником може бути організована MESH мережа (для протоколів вище 5.0) або організований маршрутизатор або міст наприклад Blutooth–GSM, Bluetooth-Lorawan, Bluetooth-Ethernet й ін.

2 АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ПОШУКУ BLUETOOTH ПРИСТРОЇВ

Пошук і виявлення закладних пристроїв може здійснюватися візуально, а також з використанням спеціальної апаратури: детекторів диктофонів і відеокамер, індикаторів поля, радіочастотомірів і інтерсепторів, скануючих приймачів і аналізаторів спектра, програмно-апаратних комплексів контролю, нелінійних локаторів, рентгенівських комплексів, звичайних тестерів, а також спеціальної апаратури для перевірки провідних ліній і т.д.

Метод пошуку закладних пристроїв багато в чому визначається використанням тієї або іншої апаратури контролю.

2.1 Традиційні методи пошуку закладних пристроїв

До основних методам пошуку закладних пристроїв можна віднести [3]:

- спеціальне обстеження виділених приміщень;
- пошук радіозакладок з використанням індикаторів поля, радіочастотомірів і інтерсепторов;
- пошук радіозакладок з використанням скануючих приймачів і аналізаторів спектру;
- пошук радіозакладок з використанням програмно-апаратних комплексів контролю;
- пошук портативних звукозаписних пристроїв з використанням детекторів диктофонів (по наявності їх побічних електромагнітних випромінювань генераторів підмагнічування й електродвигунів);
- пошук портативних відеозаписувальних пристроїв з використанням детекторів відеокамер (по наявності побічних електромагнітних випромінювань генераторів підмагнічування й електродвигунів відеокамер);

- пошук закладок з використанням нелінійних локаторів;
- пошук закладок з використанням рентгенівських комплексів;
- перевірка з використанням ВЧ-пробника (зонда) ліній електроживлення, радіотрансляції й телефонного зв'язку;
- вимір параметрів ліній електроживлення, телефонних ліній зв'язку і т.ін.;
- проведення тестового "прозвону" усіх телефонних апаратів, установлених у приміщенні, що перевіряється, з контролем (на слух) проходження всіх викличних сигналів АТС.

Найпростішими й найбільш дешевими виявлячами радіовипромінювань закладних пристроїв є індикатори електромагнітного поля, які світловим або звуковим сигналом сигналізують про наявність у точці розташування антени електромагнітного поля з напруженістю вище граничної (фонової). Більш складні з них - частотоміри забезпечують, крім того, вимір несучої частоти найбільше "сильного" у точці приймання сигналу.

Для виявлення випромінювань закладних пристроїв у близькій зоні можуть використовуватися й спеціальні прилади, що називають інтерсепторами. Інтерсептор автоматично настроюється на частоту найбільш потужного сигналу й здійснює його детектування. Деякі інтерсептори дозволяють не тільки робити автоматичне або ручне захоплення радіосигналу, здійснювати його детектування й прослуховування через динамік, але й визначати частоту виявленого сигналу й вид модуляції.

Чутливість виявлювачів полю мала, тому вони дозволяють виявляти випромінювання радіозакладок у безпосередній близькості від них.

Суттєво кращу чутливість мають спеціальні (професійні) радіоприймачі з автоматизованим скануванням радіодіапазону (скануючі приймачі або сканери). Вони забезпечують пошук у діапазоні частот, що перекриває частоти майже всіх існуючих радіозакладок - від десятків кГц

до одиниць ГГц. Кращими можливостями по пошуку радіозакладок мають аналізатори спектру. Крім перехоплення випромінювань закладних пристроїв вони дозволяють аналізувати і їх характеристики, що немаловажне при виявленні радіозакладок, що використовують для передачі інформації, складні види сигналів.

Можливість з'єднання скануючих приймачів з переносними комп'ютерами послужило підґрунтям для створення автоматизованих комплексів для пошуку радіозакладок (так званих програмно-апаратних комплексів контролю). Крім програмно-апаратних комплексів, побудованих на базі скануючих приймачів і переносних комп'ютерів, для пошуку закладних пристроїв використовуються й спеціально розроблені багатофункціональні комплекси, такі, наприклад, як "OSCOR-5000".

Спеціальні комплекси й апаратура для контролю провідних ліній дозволяють проводити вимірювання параметрів (напруг, струмів, опорів і т.п.) телефонних, слабкострумових ліній і ліній електроживлення, а також виявляти в них сигнали закладних пристроїв.

Виявлювачі порожнеч дозволяють виявляти можливі місця установки закладних пристроїв у порожнечах стін або інших дерев'яних або цегельних конструкціях.

Більшу групу утворюють засоби виявлення або локалізації закладних пристроїв по фізичних властивостях елементів електричної схеми або конструкції. Такими елементами є: напівпровідникові прилади, які застосовуються в будь-яких закладних пристроях, металеві деталі конструкції і т.д. Із цих засобів найбільш достовірні результати забезпечують засобу для виявлення напівпровідникових елементів по їхніх нелінійних властивостях - нелінійні радіолокатори.

Принципи роботи нелінійних радіолокаторів близькі до принципів роботи радіолокаційних станцій, широко застосовуваних для радіолокаційної розвідки об'єктів. Істотна відмінність полягає в тому, що якщо приймач радіолокаційної станції ухвалює відбитий від об'єкта

зондувальний сигнал на частоті випромінюваного сигналу, то приймач нелінійного локатора приймає 2-у й 3-ю гармоніки відбитого сигналу. Поява у відбитому сигналі цих гармонік обумовлене нелінійністю характеристик напівпровідників.

Металодетектори реагують на наявність у зоні пошуку електропровідних матеріалів, насамперед металів, і дозволяють виявляти корпуси або інші металеві елементи закладки.

Переносні рентгенівські установки застосовуються для просвічування предметів, призначення яких не вдається виявити без їхнього розбирання насамперед тоді, коли вона неможлива без руйнування знайденого предмета.

2.2 Методи пошуку Bluetooth пристроїв засновані на особливостях протоколу

Виділяють два основні методи визначення відносного місця розташування мобільного вузла: трилатерація й тріангуляція (рис. 2.1). При тріангуляції визначається відстань між опорними вузлами й цільовим вузлом. Можливе місце розташування цільового вузла – на перетинанні окружностей з радіусами, рівними відстані до відповідних вузлів. Звичайно потрібні три опорні вузли. При тріангуляції визначається напрямок від опорних вузлів до цільового, і положення цільового вузла буде на перетинанні променів, проведених від опорних вузлів у напрямку цільового. Для локалізації цільового вузла досить двох вузлів опорних точок.

У бездротових системах реалізуються звичайно два методи, що допомагають визначити місце розташування вузла: визначення кута приймання отриманого пакета (Angle of Arrival, Aoa) і визначення часу доставки пакета (Time of Flight, Tof), дослівно – визначення «кута прибуття» і «часу польоту» пакета.

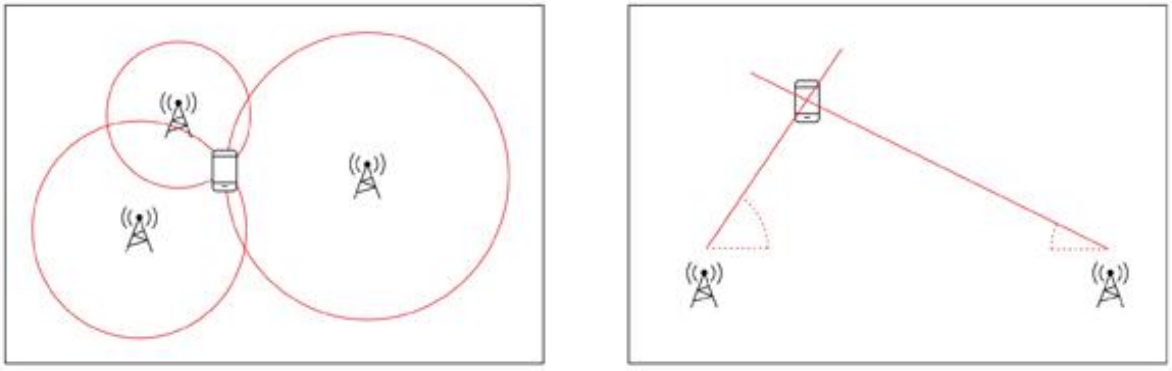


Рисунок 2.1 – Два основні методи для визначення відносного місця розташування мобільного вузла: а) трилатерація; б) тріангуляція

У бездротових системах реалізуються звичайно два методи, що допомагають визначити місце розташування вузла: визначення кута приймання отриманого пакета (Angle of Arrival, Aoa) і визначення часу доставки пакета (Time of Flight, Tof), дослівно – визначення «кута прибуття» і «часу польоту» пакета.

2.2.1 Bluetooth-маячки

Bluetooth-маячки – це невеликий, простий і економічний спосіб встановити зв'язок між пристроєм і мобільним додатком. Використання маяків для push-повідомлень і виявлення присутності досить просто. Але якщо необхідно створити точне позиціонування в приміщенні за допомогою маяків, усе стає небагато складніше. необхідно взяти до уваги ряд речей як з боку розробки програмного забезпечення, так і з погляду розміщення маяків. При цьому при ретельній підготовці можна досягтися точності позиціонування в 1-2 метра також і за допомогою маяків Bluetooth [4].

Радіомаяк Bluetooth не має вбудованого засобу визначення місця розташування. Як видно з назви, вони схожі на маяки, що передають сигнал Bluetooth навколо себе, очікуючи, що поблизу розумні пристрої, що перебувають, уловлять його й зрозуміють його значення. Залежно від того,

чи використовується протокол ibeacon, Eddystone або який-небудь інший протокол, маяки будуть або передавати свої UUID, основні й другорядні значення, або їх простори імен і ідентифікатори екземплярів. Щоб перетворити ці значення в реальні координати, необхідно призначити кожному із цих маяків фізичні координати або усередині додатка, або в зовнішній базі даних. Зрівнявши значення отриманих сигналів із зареєстрованими радіомаяками і їх координатами, з'являється можливість одержати першу приблизну оцінку місця розташування через RSSI. RSSI означає індикатор рівня прийнятого сигналу, який представляє значення потужності прийнятого радіосигналу. Чим більше відстань, тем нижче сигнал RSSI.

Тріангуляція (рис. 2.2). Друга важлива річ, яку необхідно знати, - це те, що в маяків немає спрямованої антени - тому можна одержати тільки оцінку відстані до маяка, а то, з якого напрямку йде сигнал. Щоб реалізувати це, необхідно мати пряму видимість трьох або більш маяків і порівнювати значення RSSI для кожного з них. Коли маяки розташовані правильно, розрахункова точка вказує на одне конкретне місце в кімнаті. Як говорить цей термін, для визначення точного положення знадобиться як мінімум три маяки. Виключенням є вузькі коридори або інші ситуації, коли можна розрахувати положення між двома маяками.

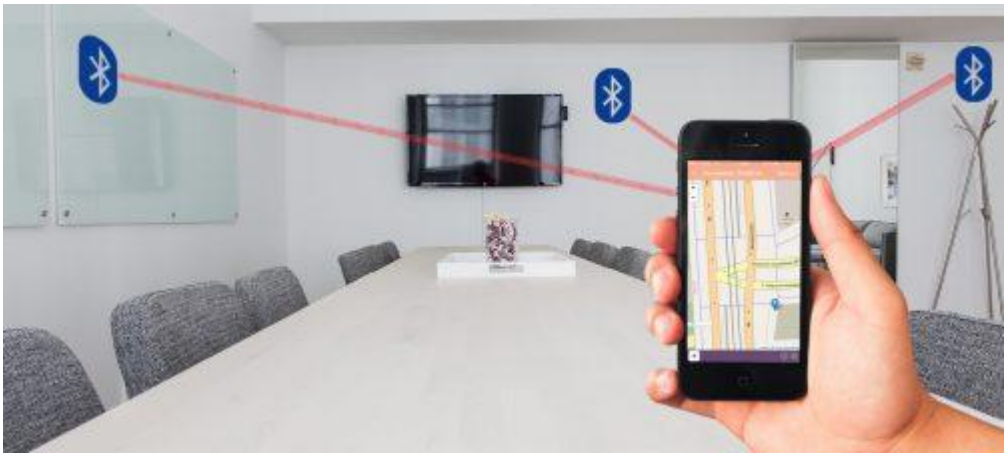


Рисунок 2.2 – Тріангуляція за допомогою Bluetooth-маячків

На жаль, навіть із кращими моделями радіомаяків у переданому сигналі спостерігаються викривлення, і на нього може додатково впливати небажаний шум. Тому розповсюдженим розв'язком є додавання набору фільтрів і алгоритмів поверх розрахунків тріангуляції. Коротенько, фільтри Калмана - це алгоритм, який враховує історію вимірів. З ними можна виключити багато позиційних стрибків.

При використанні платформи Proximi.io, немає необхідності турбуватися ні про яку з вищезгаданих проблем із програмним забезпеченням. Двома словами, платформа Proximi.io надає доступ до всіх позиційних технологій через об’єднання SDK і API. Ці бібліотеки автоматично обробляють усю логіку позиціонування маяків, тріангуляції й фільтрації у фоновому режимі. Крім маяків, є можливість комбінувати Indooratlas, Wi-Fi, GPS і стільникове позиціонування [5].

Що стосується використовуваних фізичних пристроїв, то існують десятки виробників маяків Bluetooth. Що стосується використовуваного протоколу, з можливістю використовувати кожний з доступних варіантів позиціонування. Однак, якщо використовуєте платформу Proximi.io, потрібно вибрати ibeacon або Eddystone, які підтримуються майже всіма маяками.

Якщо переслідується мета до високої точності визначення місця розташування, найкраще розміщати маяки на стінах на висоті близько 2 метрів. Коли сигнал іде зверху, інтелектуальному пристрою легше його прийняти. Рекомендується розміщати їх на видному місці.

На рис. 2.3 приклади розташування маяків у приміщенні квадратної форми. Це зображення являє собою велику кімнату, де потрібно більш одного маяка на кут.

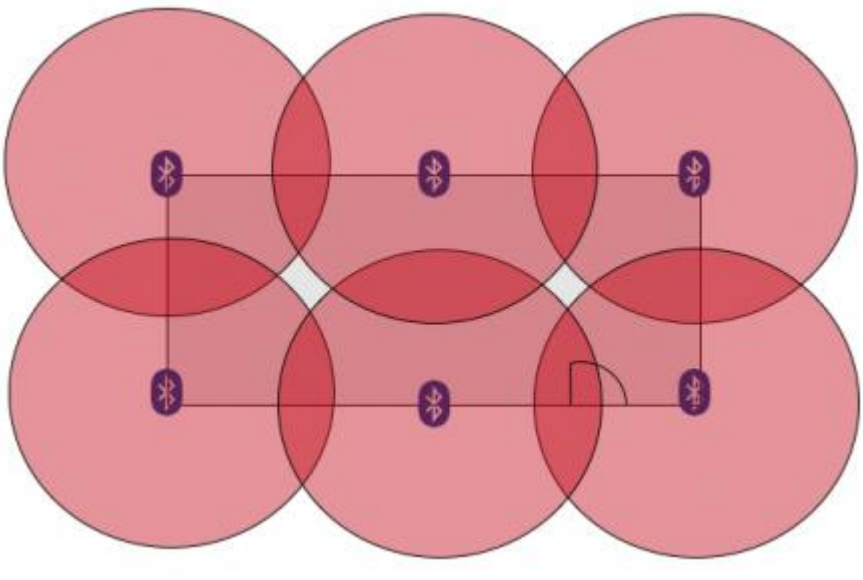


Рисунок 2.3 – Приклад розташування Bluetooth-маячків

2.2.2 Визначення місця розташування по RSSI

Показник рівня прийнятого сигналу, RSSI (англ.*received signal strength indicator*) – повна потужність прийнятого приймальником сигналуа) [6].

Для пристроїв, що працюють по стандартах Wi-Fi і Bluetooth 4.0, RSSI є одним з параметрів, що дозволяють виміряти відстань від пристрою до базової станції або маяка. Рівняння для обчислення відстані (за межами ближній зони передавача) має такий вигляд:

$$P_d = P_0 - 10 \cdot n \cdot \lg\left(\frac{d}{d_0}\right),$$

де:

d – відстань від пристрою до передавача, м;

d0 – відстань від пристрою до крапки, на якій виконувався вимір потужності сигналу пристрою, м (обране одиничне (каліброване) відстань, наприклад, 1 м);

P0 – потужність сигналу пристрою, обмірювана на одиничній відстані від пристрою, dBm;

n – коефіцієнт втрат потужності сигналу при поширенні в середовищі, безрозмірна величина (для повітря ; збільшується при наявності перешкод);

Pd – RSSI, dBm.

Можна помітити зміну значення RSSI навіть у фіксованому місці або на фіксованій відстані. Одним з факторів зміни може бути обладнання/радіомодема. Наприклад, на пристроях IOS, де не так багато різних наборів мікросхем, значенням RSSI може точно відображати відповідна відстань.

Значення RSSI для iphone A, імовірно, означає таке ж значення рівня на iphone B. Однак на пристроях Android, де є велика різноманітність пристроїв і наборів мікросхем, абсолютне значення RSSI не допоможе легко зіставити відповідне місце розташування.

Те саме значення RSSI на двох різних телефонах Android із двома різними наборами мікросхем може означати два різні рівні сигналу. У результатах дослідження [7] видно, що для тій самій відстані й того самого джерела різні смартфони показали рівень RSSI одмінний на 30дБ (рис 2.4).

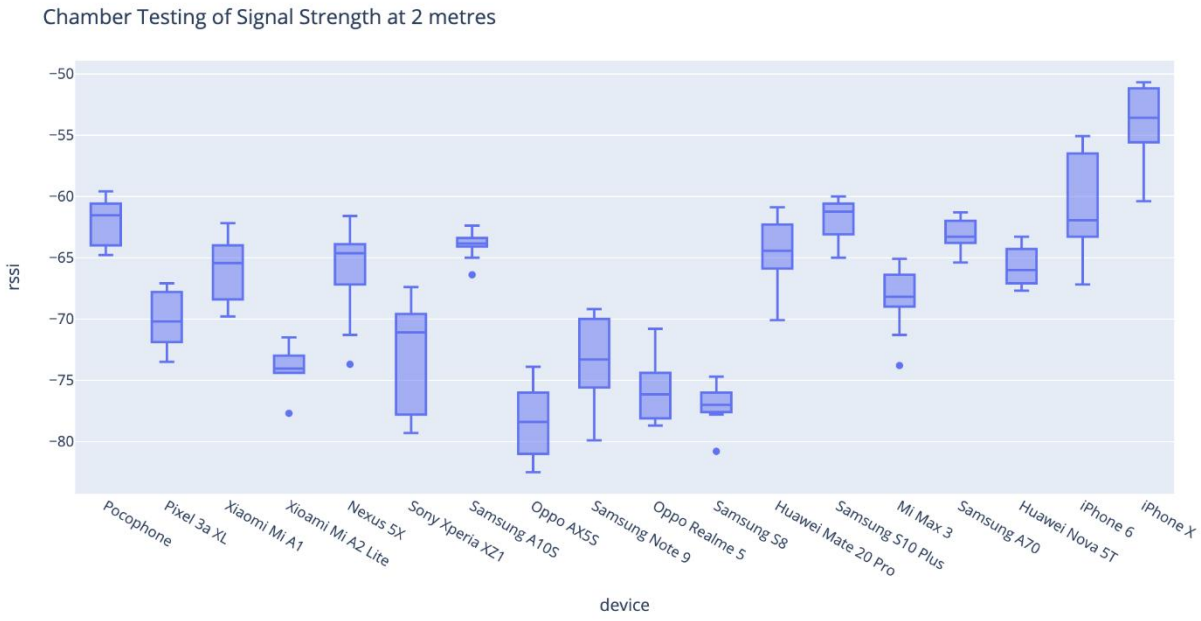


Рисунок 2.4 – Розкид рівня RSSI вимірюваного різними смартфонами в безеховій камері

Крім того, на рівень RSSI впливають:

- поглинання сигналу тілом людини ~ 15 дБ;
- багатопроменеве поширення сигналу ~ 10 дБ;
- орієнтація антени ~ 5 дБ;

Однак значення RSSI усе ще може бути дуже корисним у додатках визначення близькості, якщо використовувати його для визначення тенденції зміни значення RSSI. Ця тенденція може надати необхідні дані.

2.2.3 Визначення місця розташування по часовим затримках між запитами

Послуги на основі визначення місця розташування (LBS) відродилися в останні роки завдяки декільком важливим подіям, таким як поява мобільних пристроїв з підтримкою GPS, впровадження платформи Web 2.0 і розгортання бездротових широкосмугових бездротових послуг [8]. Є також ряд зрушень парадигми, які сприяли відродженню LBS, а саме: від реактивного до проактивному (тобто спровоковані визначеними подіями), від одиночної мети до множинної мети (тобто взаємозв'язок декількох цілей один з одним), від саме-посилання до перехресного посилання (тобто інші користувачі запитують місце розташування користувача) і від контент-орієнтованого до орієнтованого на додатки [8].

Визначення місця розташування є основним компонентом систем LBS. Для зовнішніх середовищ Global Positioning System (GPS) забезпечує ефективний розв'язок для визначення місця розташування мобільних пристроїв з підтримкою GPS. Однак для приміщень такого ефективного розв'язку не існує. У результаті визначення місця розташування в приміщенні є активною областю досліджень.

Більшість розв'язків на основі Bluetooth залежать від мережних характеристик, таких як потужність прийнятого сигналу (RSS). Bluetooth RSS, обумовлений як індикатор RSS (RSSI) і якість зв'язку (LQ), не є

надійним показником, враховуючи неоднорідність устаткування Bluetooth у доступних пристроях.

Частково це є результатом неточного визначення RSS у стандарті Bluetooth [9]. Крім того, одержання RSS по Bluetooth звичайно вимагає встановлення зв'язку між відповідними пристроями. Це вимагає, щоб користувачі підтримували свої пристрої в режимі підключення, який більшістю користувачів уважається небезпечним.

Методика “Час польоту” Time-of-Flight (Tof) реалізована в конфігурації «ведучий-відомий» (“master-slave”). Ведучий пристрій посилає пакет, який відоме пристрій повертає назад пристрою, що й веде, обчислює час його шляху між вузлами, віднімаючи час на обробку пакета (фіксоване й відоме).

Через малу швидкість роботи радіомодуля Bluetooth щодо швидкості світла кожний окремий вимір дає дуже грубий результат. Але, виконуючи безліч вимірів, звичайно кілька сотень протягом декількох миллисекунд, можна одержати середній результат із прийнятною точністю.

Швидкість поширення радіохвиль постійна, а це означає, що час, необхідне для їхнього поширення, прямо пропорційно відстані. Щоб знайти відстань до об'єкта, необхідно записати оцінку часу, коли пакет переданий, зрівняти її з міткою часу в повернутому пакеті (урахувати час обробки пакета), розділити на два й помножити на швидкість світла. Принцип виміру подібний із принципом роботи радара (рис. 2.5) з тим виключенням, що пакет не відбивається фізично, а приймається й відсилається назад відомим вузлом.

Далі для сигналу, що відсилається, буде використане позначення PING, для відповідного сигналу – PONG або ACK.

У реалізації методу виміру часу прольоту пакета є дві складності:

- час на приймання й формування відповідного пакета відомим пристроєм впливає на виміри;

- для подолання відстані в один метр світла потрібно всього лише 3,3 нс, таким чином, для одержання дозволу в 1 метр потрібна частота роботи таймера виміру часу як мінімум 303 МГц.

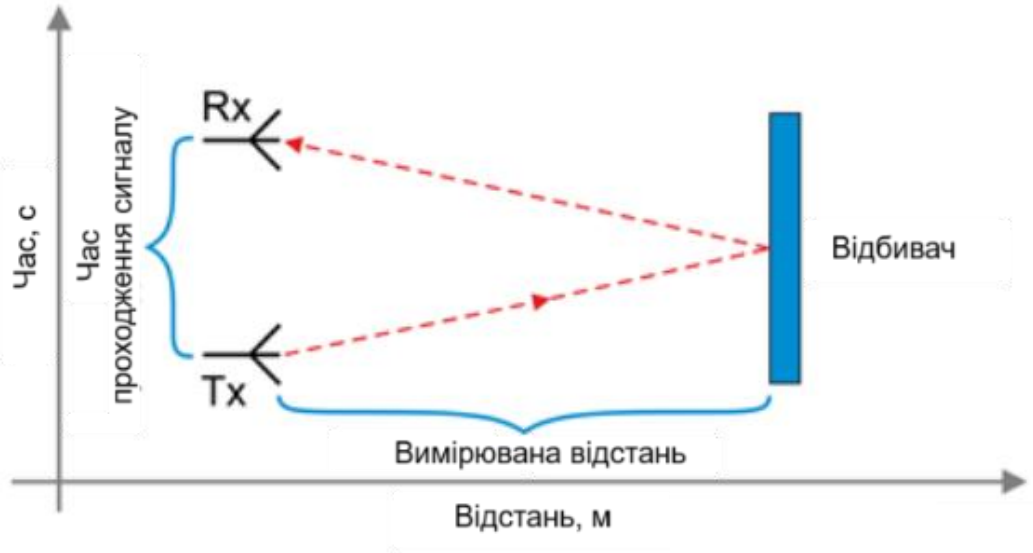


Рисунок 2.5 – Ілюстрація принципу роботи радара

Перша вирішується шляхом точного визначення часу, який відомий вузол затрачає на формування й відправлення відповідного пакета.

Друга проблема трохи складніше, але, проте, може бути вирішена. Частота демодулятора в радіотракте в режимі ToF становить 8 МГц, що дає тимчасовий дозвіл 125 нс. Цей результат може бути поліпшений за рахунок передискретизації при періодичних вимірах часів проходження досить великої кількості пакетів.

ToF-протокол.

Для роботи додатка потрібні як мінімум два пристрої: ведучий, або майстер (Master), і відомий (Slave). Обоє пристрою будуть взаємодіяти в певному діапазоні частот (точніше – частотних каналів) і працювати з певним додатком – списком синхрослів.

Спочатку відомий пристрій перебуває в стані приймання на першій із заданих частот і очікує передачі першого в списку синхрослова. Якщо відомий одержує відповідний пакет, він відповідає пакетом ACK/PONG і міняє частотний канал і синхрослово за списком, заданому додатком.

Провідний пристрій передає пакет з першим синхрословом, після чого переходить у режим приймання, очікуючи відповіді від відомого із другим синхрословом.

Аналогічно цьому, майстер, що прийняв пакет ACK/PONG у відповідь на свій початковий PING, буде випливати тій же схемі перебудови частоти (рис. 2.6) [10].

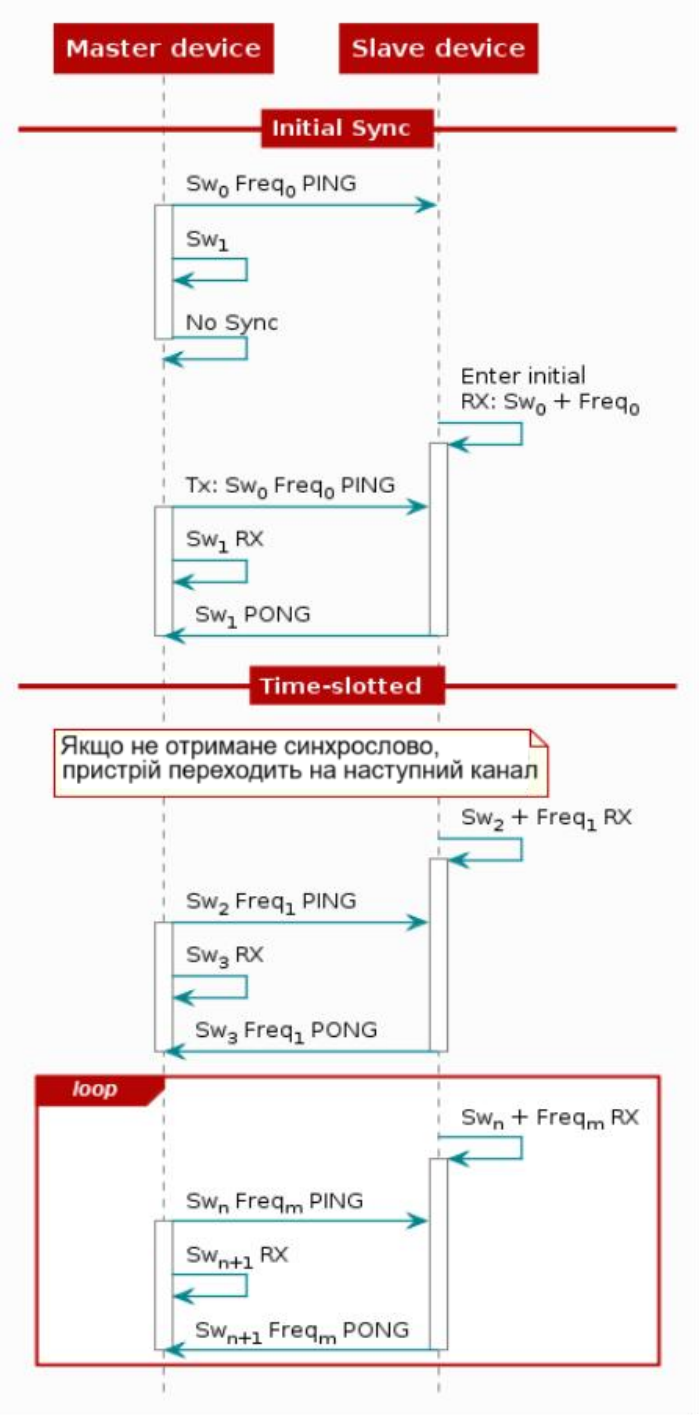


Рисунок 2.6 – Послідовність вимірів ToF

Схематично процес обміну пакетами й етапи обчислення ToF представлені на рис. 2.7. На цьому рисунку:

- TA – ведучий посилає пакет PING;
- TB – ведучий переходить у режим приймання;
- TC – ведучий ухвалює відповідний пакет;
- TD – відомий одержує потрібний пакет від відомого;
- TE – відомий переходить у режим передачі;
- TF – відомий посилає відповідь PONG.

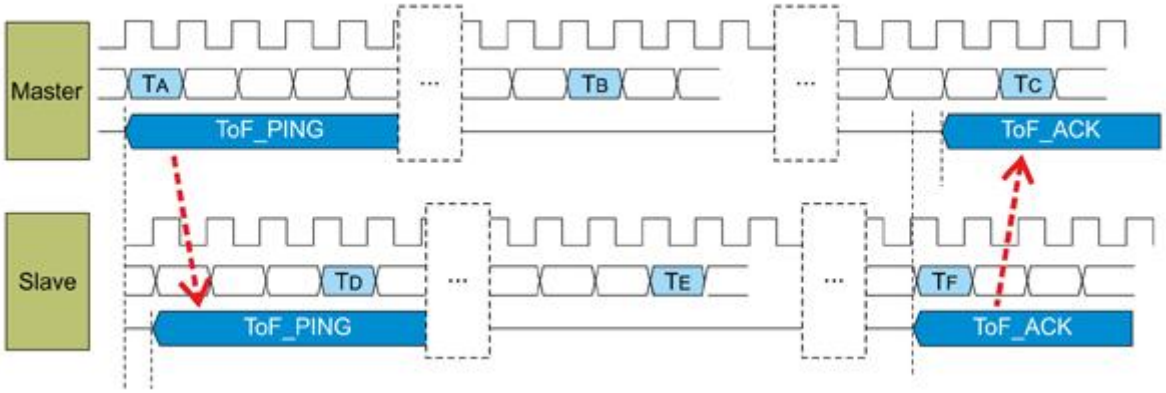


Рисунок 2.7 – Схема обміну пакетами й етапи обчислення ToF

При старті додатка ведучий і відомий повинні погоджувати порядок перемикання частот і проходження синхрослів.

Додаток повинний погодити з одноранговим пристроєм (пристроями), які частоти слід використовувати, який повинен бути порядок частот і що повинен містити список синхрослів.

Це також може бути показане у вигляді спрощеної діаграми послідовності.

Часова діаграма роботи додатка – взаємодія додатка, драйверів і радіочастини – представлена на рис. 2.8.

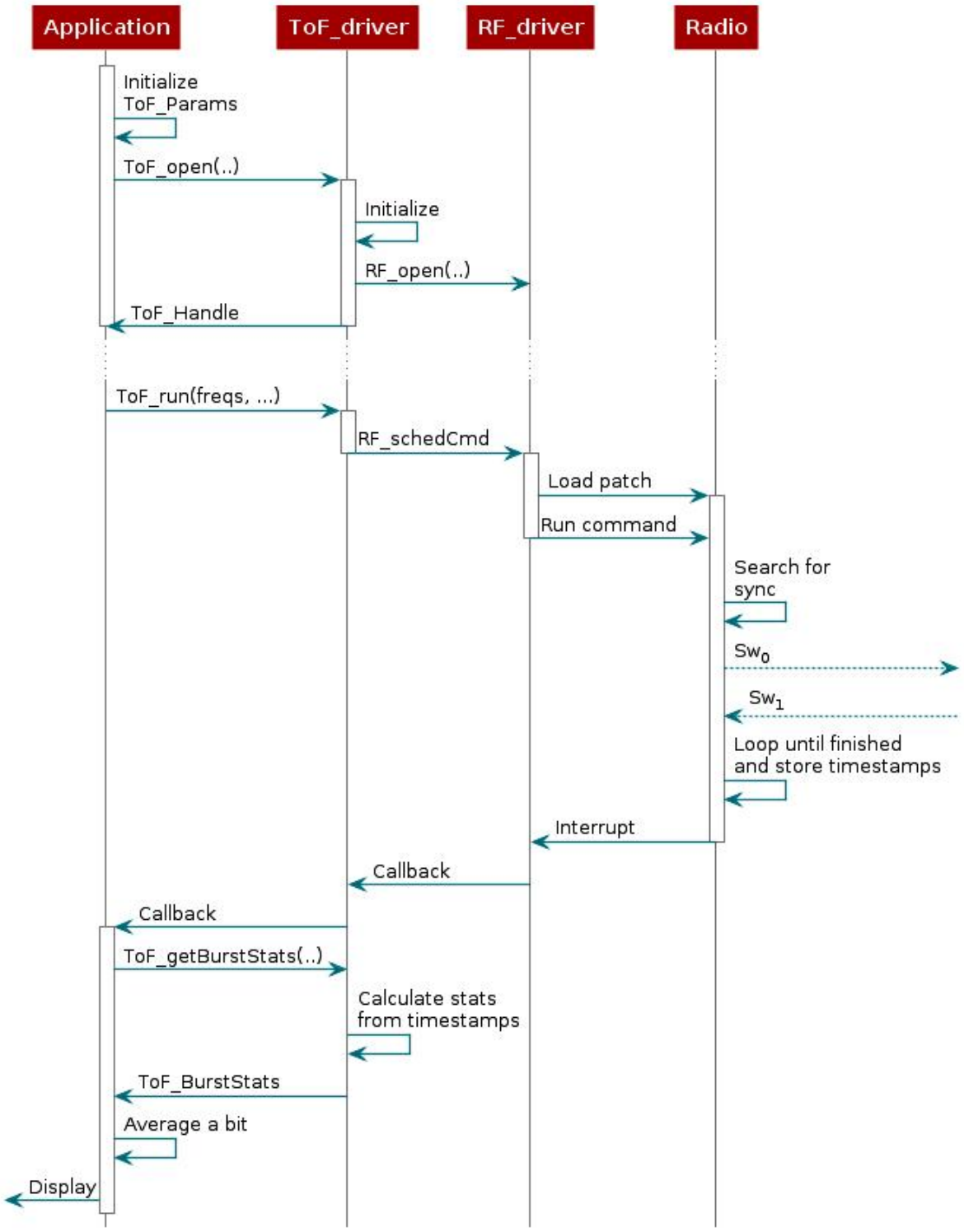


Рисунок 2.8 – Часова діаграма роботи додатка

З боку додатка послідовність дій виглядає досить просто:

1. ініціалізація;
2. запуск;
3. збір результатів;

4. калібрування.

Результати експериментального дослідження методики ToF наведені на рис. 2.9.

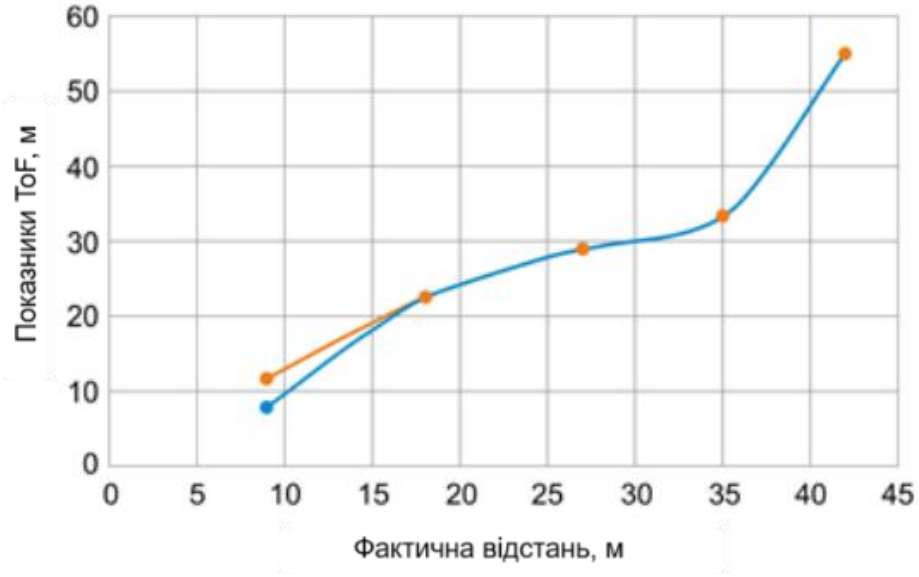


Рисунок 2.9 – Точність визначення відстані за методикою ToF

Метод визначення місця розташування, описаний в [11] - це розв'язок для локалізації на основі відбитків пальців і є модифікацією методу TOF, яке покладається тільки на швидкість відгуку (RR) запитів Bluetooth. Це просто вимагає, щоб мобільні пристрої були в режимі виявлення. Згідно із цим підходом, кожне місце відслідковується за допомогою RR запиту (IRR) датчиків Bluetooth, установлених у багатоповерховому будинку.

Після одержання IRR цільового пристрою, що підлягає локалізації, система використовує відносний захід ентропію (функція Кульбака-Лейблера) і її розширення (тобто вимір відстані Дженсена-Шеннона) для оцінки місця розташування цільового пристрою.

У роботі [11] оцінена продуктивність розв'язку, виконавши кілька експериментів з інфраструктурою, розгорнутої в офісному будинку. Точність оцінки місця розташування склала майже 98% у кімнаті.

Необхідно привернути увагу, що ця продуктивність була отримана, коли для зняття відбитків пальців використовувалися різні типи пристроїв,

а цільовий пристрій, який потрібно локалізувати, відрізнявся від цих пристроїв.

Даний розв'язок спрямований на визначення місця розташування на рівні приміщення, що є значимим ступенем деталізації для широкого спектра внутрішніх додатків.

Таким чином, розв'язок не вимагає відновлення мобільних пристроїв, а тільки вимагає, щоб ці пристрої перебували в режимі виявлення.

Результати тестування показали, що розв'язок досягає точності оцінки 98% і 75%, коли було повне покриття датчика й часткове покриття датчика відповідно.

2.2.3 Визначення кута приходу Bluetooth сигналу

Методика Angle of Arrival (AoA) полягає у визначенні напрямку, з якого був прийнятий Bluetooth-пакет щодо орієнтації прийомного вузла. AoA звичайно застосовується при реалізації методу тріангуляції.

Для реалізації технології використовується набір антен з певними характеристиками, приймач повинен буде швидко перемикатися між окремими антенами, одночасно вимірюючи фазове зрушення прийнятого сигналу, що обумовлено невеликими відмінностями в довжині шляху сигналу для різних антен.

Ці відмінності в довжині траси будуть залежати від напрямку вхідних радіочастотних хвиль щодо антен у решітці. Щоб полегшити вимір фази, пакет Bluetooth повинен мати специфічний вигляд: містити ділянку безперервного тону (CT), у якому немає фазових зрушень, викликаних модуляцією [10].

В AoA-пакетах у корисному навантаженні пакета (PDU) передається секція послідовних одиниць, що формує синусоїду на піднесучій частоті 250 кГц (рис. 2.10). Це дає демодулятору час на синхронізацію, щоб потім вибрати I- (реальна складова) і Q- (уявна складова) компоненту сигналу, записати їх у буфер і передати додатку для подальшого аналізу.

Рисунок 2.10 – Структура AoA-пакету

При роботі з AoA-пакетами передавальне радіоядро поміщає тоновий сигнал у секцію PDU-пакета й формує коректну контрольну суму. Прийомна сторона аналізує пакет і починає фіксувати відліки сигналу в потрібний час, синхронізуючи перемикання антен. Відліки зберігаються в пам'яті радіоядра й аналізуються згодом основним ядром.

Вибірка й буферізація відліків відбуваються без участі основного ядра. Завдяки спеціальній попередній обробці додаток на основному ядрі може починати визначення зрушення фаз у сигналі без таких етапів як фільтрація постійної складової й проміжної частоти. Схема взаємодії основного ядра й радіоядра представлена на рис. 2.11.

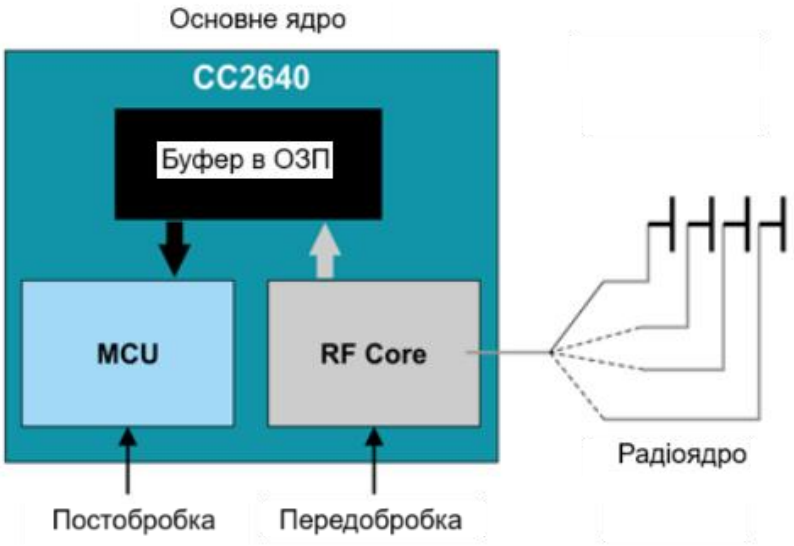


Рисунок 2.11 – Схема взаємодії основного ядра й радіоядра

I/Q-відліки можуть вибиратися із частотою до 4 МГц при дозволі 16 біт. При 32 бітах на комплексний відлік сигналу (пари I + Q) виходить потік в 128 біт у секунду, у підсумку буфер розміром 1 кбайт зберігає 64

мікросекунди сигналу (при необхідності розмір буфери може бути збільшений до 2 кбайт).

Радіоядро контролює сигнали, що керують перемиканням антен за допомогою виводів CC2640, і тим самим розділяє загальний прийнятий сигнал на слоти, що належать до кожної з антен. Тривалість слота (antenna dwell time) буде визначати точність визначення зсуву фази сигналу, за замовчуванням ця тривалість становить 4 мкс.

2.2.4 Особливості стандарту Bluetooth 5.1

Можливості по позиціонуванню/локалізації виправлене з новою функцією визначення напрямку в Bluetooth 5.1, який був анонсований специальной группой по развитию Bluetooth (SIG), – галузевою групою, яка контролює Bluetooth. Система позиціонування (рис. 2.12) тепер може визначати напрямок, з якого надходить сигнал Bluetooth. Враховуючи відстань і напрямок, пристрої Bluetooth тепер зможуть визначити точне місце розташування пристрою аж до сантиметра.

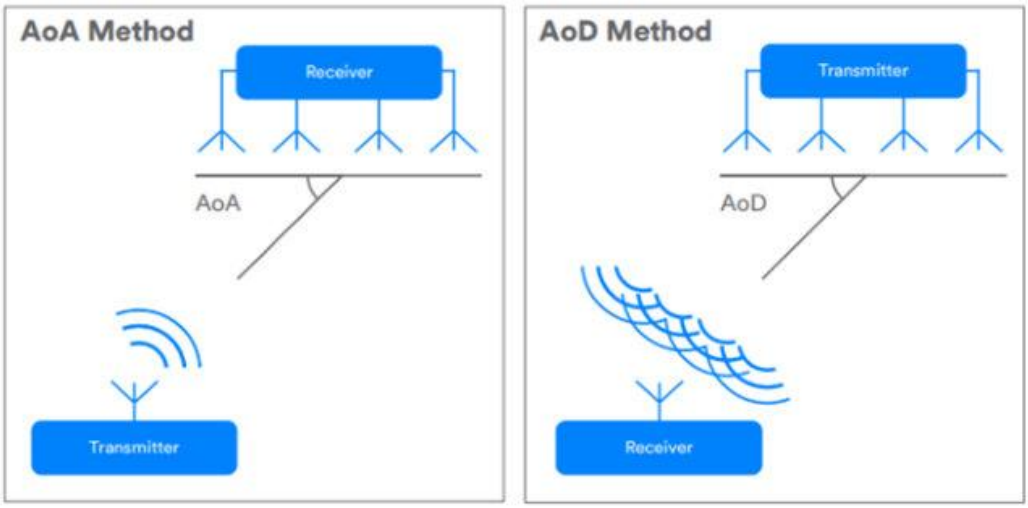


Рисунок 2.12 – Принцип дії кутоміра в Bluetooth 5.1

Bluetooth 5.1 пропонує два різні методи визначення напрямку: «Кут прибуття» (AoA) і «Кут вильоту» (AoF). Одне із двох пристроїв повинне мати масив з декількох антен, і дані, отримані від цих антен, можуть

використовуватися для визначення напрямку, з якого надходить сигнал Bluetooth [12].

Смартфон з Bluetooth 5.1, система позиціонування зможе точно визначити його місце розташування. Це може бути використане для поліпшення навігації в приміщенні, пошуку загублених ключів або включення встаткування Smarthome для більш точного визначення місця розташування.

3 РОЗРАХУНОК БЛОКІВ ВИЯВЛЯЧА BLUETOOTH ПРИСТРОЇВ

Для більш ефективного виявлення Bluetooth пристроїв необхідно забезпечити просторову й частотну вибірковість пошукового приладу. Просторова вибірковість забезпечить пеленгацію шуканого пристрою й крім того збільшить радіус пошуку. Частотна вибірковість забезпечить завадостійкість пристрою, знизить імовірність фіктивних тривог і тим самим також збільшить радіус пошуку.

3.1 Розрахунок й моделювання антени

Розрахунки й моделювання антени проводився в програмному комплексі IE3D. Дане програмний комплекс від компанії Mentor Graphics є повнохвильовим симулятором який складається з ряду продуктів:

Mgrid – редактор топології для створення різних структур, містить у собі засобу відображення й пост-процесорної обробки S-Параметрів, засобу відображення розподілу струму, відображення й пост-процесорна обробка полів близької зони.

Modua – це схемотехнічний редактор для відображення параметрів і аналізу вузлових схем.

Patternview – це модуль пост-процесорної обробки для відображення діаграми спрямованості й наступної її обробки.

У якості антени для пристрою, що розробляється була обрана патч-антенна. Вона складається з тонкої пластини, розташованої на малій відстані паралельно плоскому металевому екрану. Принцип дії патч-антени заснований на резонансі моди в обсязі під пластиною, збудження електричного поля в зазорах уздовж двох протилежних сторін пластини, що може розглядатися як соспрямоване протікання еквівалентного магнітного струму уздовж кожної із цих сторін, і збудження електромагнітної хвилі цими двома ділянками магнітного струму. Розміри екрана запропонованої антени становлять 110x88x2 мм, а пластини –

54x57x0.5 мм. У редакторі Mgrid програмного комплексу IE3D була відтворена геометрія антени, результат представлений на рис. 3.1.

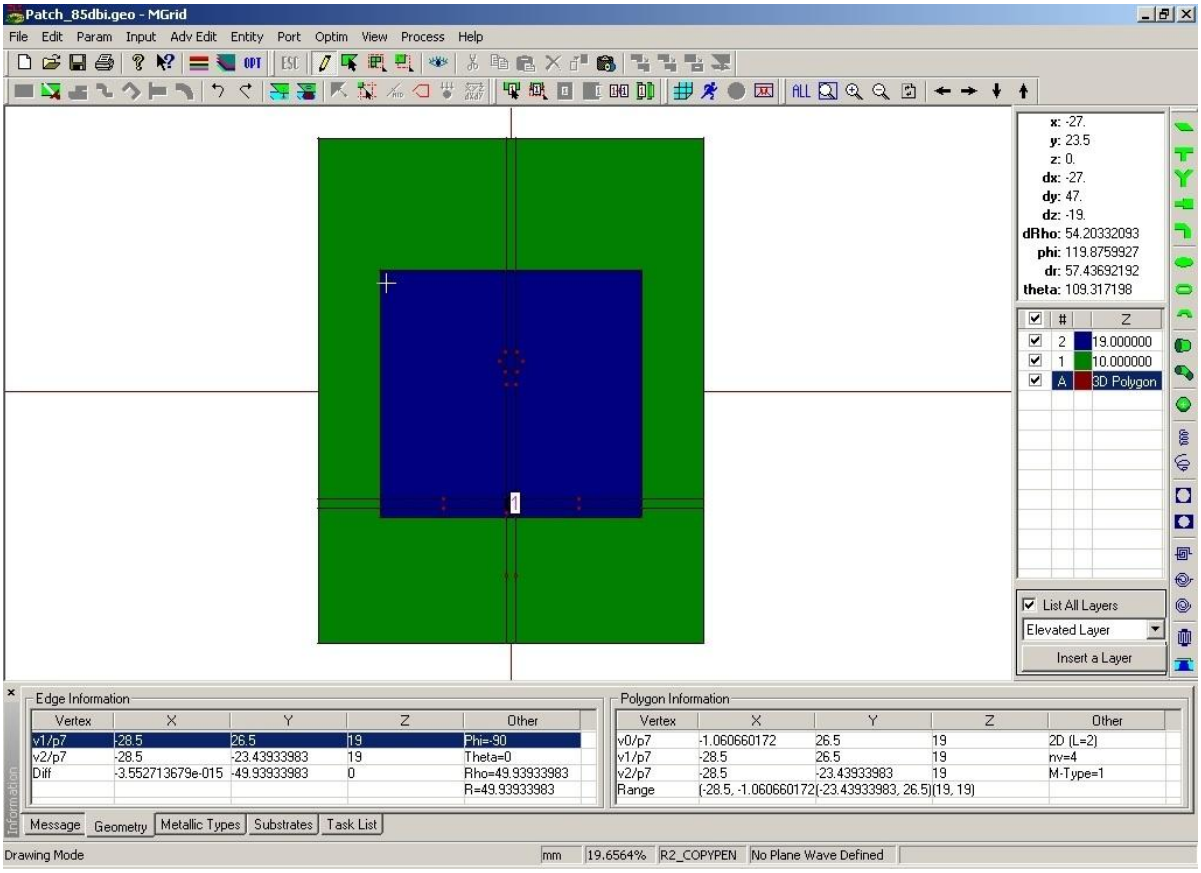


Рисунок 3.1 – Геометрія антени

Проведемо моделювання патч-антени в режимі випромінювання. Моделювання проводилося в діапазоні частот від 2400 МГц до 2500 МГц, з кроком в 10 МГц. Частотна залежність у вигляді зворотних втрат у дБ показана на рис. 3.2. Мінімальний коефіцієнт відбиття досягається на частоті 2440 МГц і рівний -32.3 дБ, у той час як на частоті 2483 МГц маємо [S11] = -17.2 дБ. За рівнем зворотних втрат -18,2 дБ смуга антени становить 75 МГц.

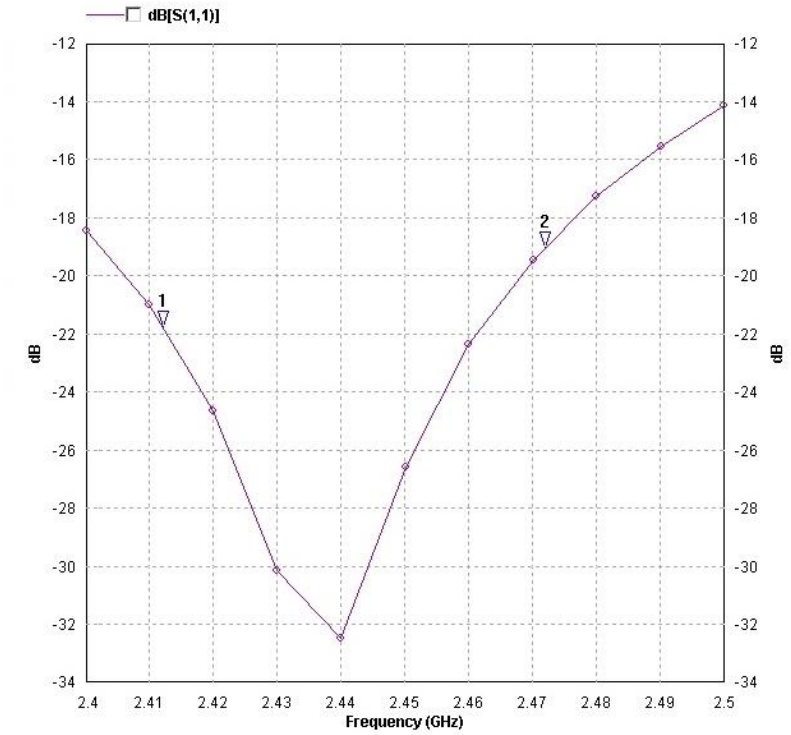


Рисунок 3.2 – Узгодження антени на околицях робочого діапазону

На рис. 3.3 представлена діаграма спрямованості даної антени.

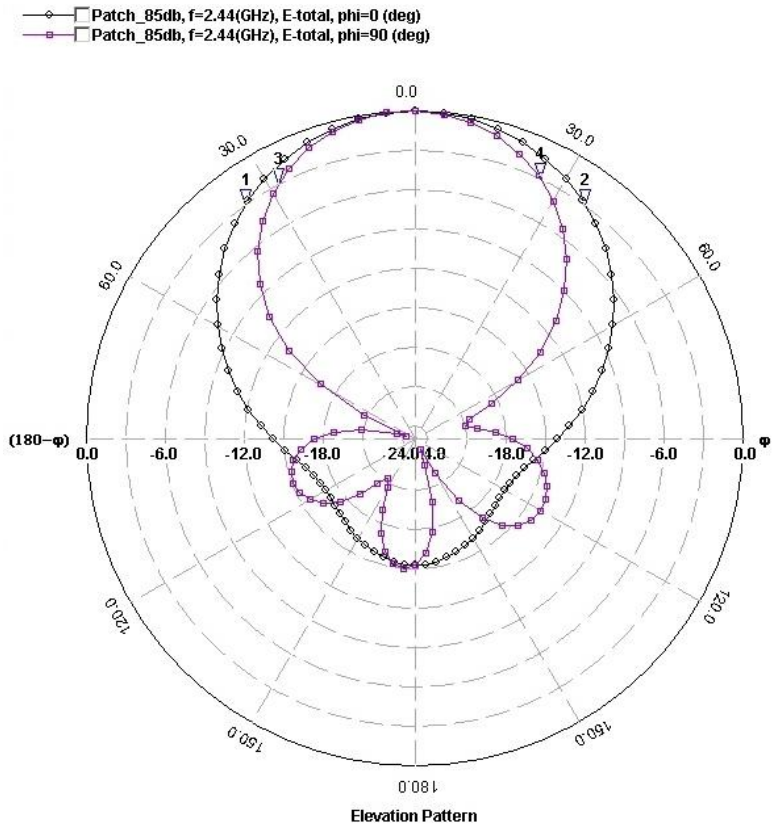


Рисунок 3.3 – Діаграма спрямованості антени

Моделювання проводилося на середній частоті Bluetooth діапазону – 2,44 ГГц у площинах φ=0° і φ=90°. Через наявність рефлектора ДН патч-антени має виражену спрямованість. Головна пелюстка перпендикулярна рефлектору, і його ширина становить близько 60, а також присутні слабко виражене задні й бічні пелюстки. На рис. 3.4 - 3.6 представлена ДН у тривимірній площині й продемонстровано залежність коефіцієнта підсилення антени від напрямку випромінювання. У такий спосіб від задніх пелюсток у напрямку променю він збільшується, при цьому максимальний коефіцієнт підсилення становить 9,04 дБ.

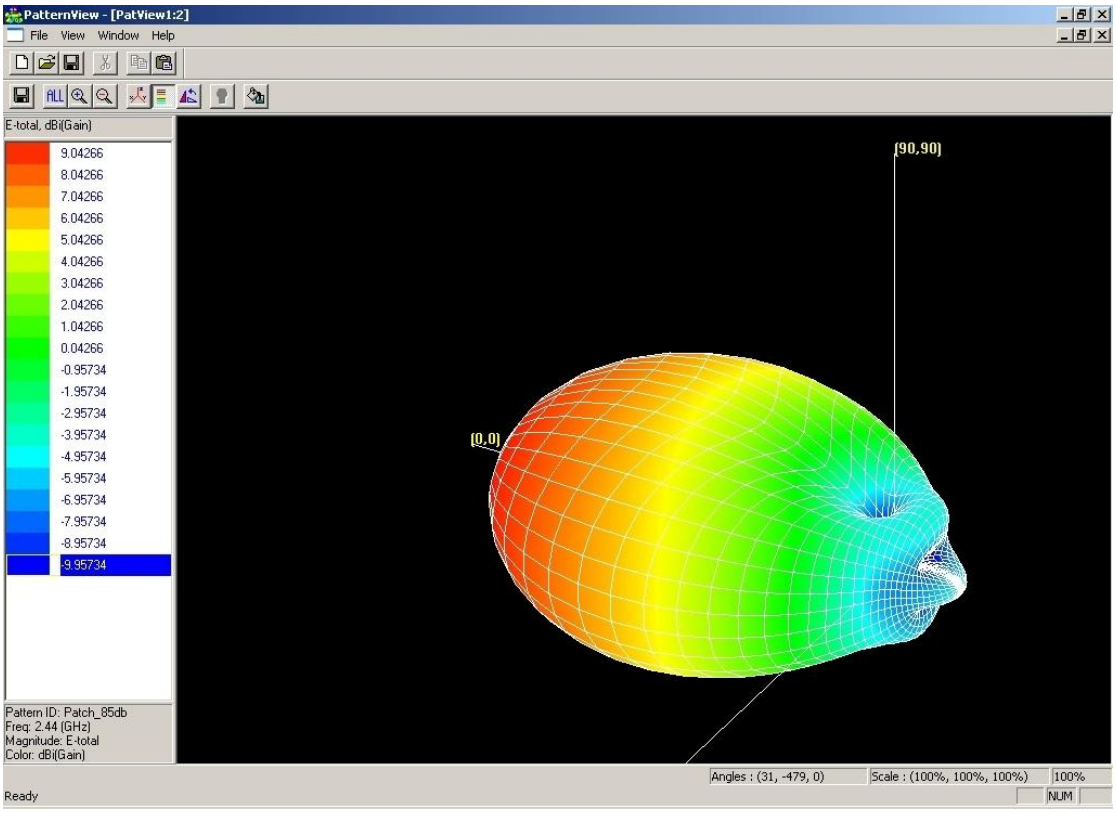


Рисунок 3.4 – Тривимірна діаграма спрямованості антени

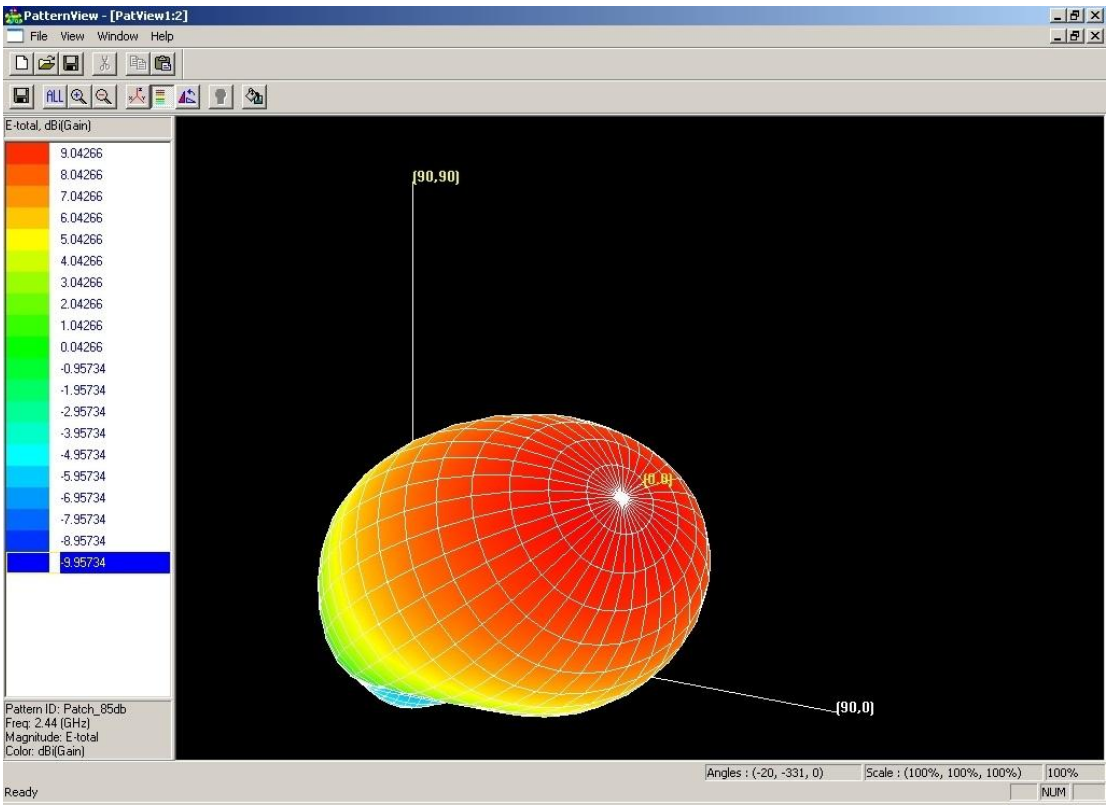


Рисунок 3.5 – Тривимірна діаграма спрямованості антени

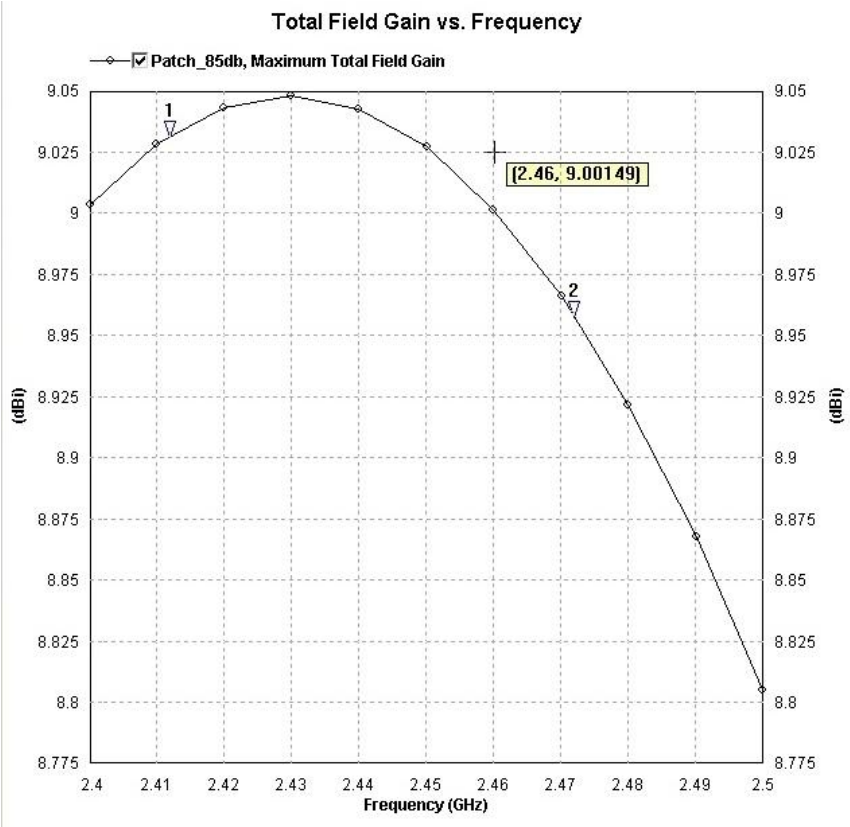


Рисунок 3.6 – Частотна залежність коефіцієнта підсилення антени

Ескіз антени приведено на рис. 3.7.

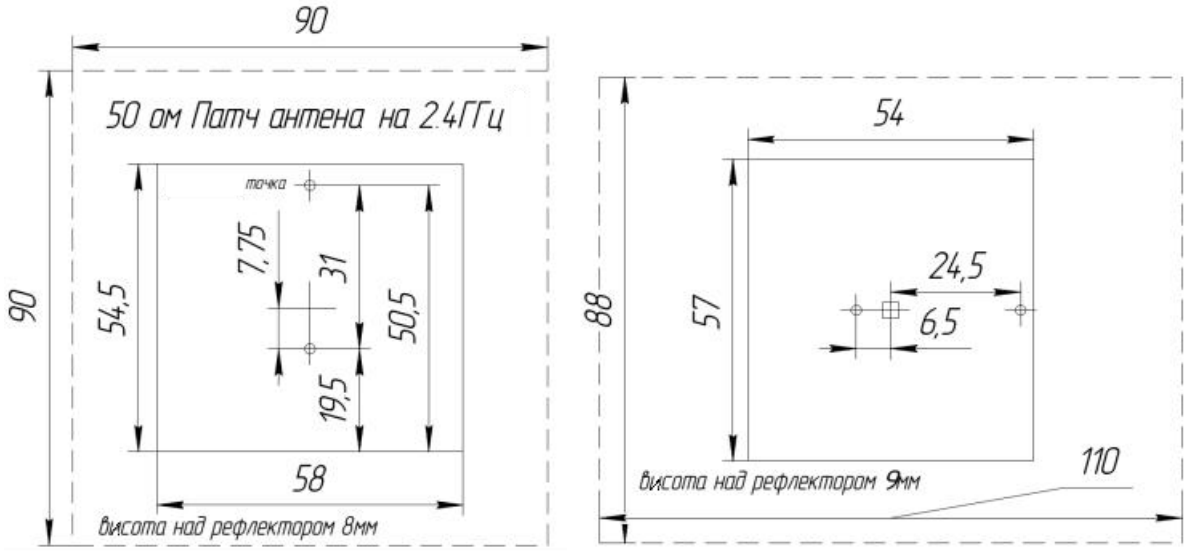


Рисунок 3.7 – Ескіз антени

3.2 Розрахунки антенного комутатора

Для реалізації перемикання режимів приймання й передачі в розроблювальному пристрої розрахуємо так званий комутатор 1:2 з одним послідовно включеним діодом у плечі приймального й передавального трактів (рис. 3.8) [13].

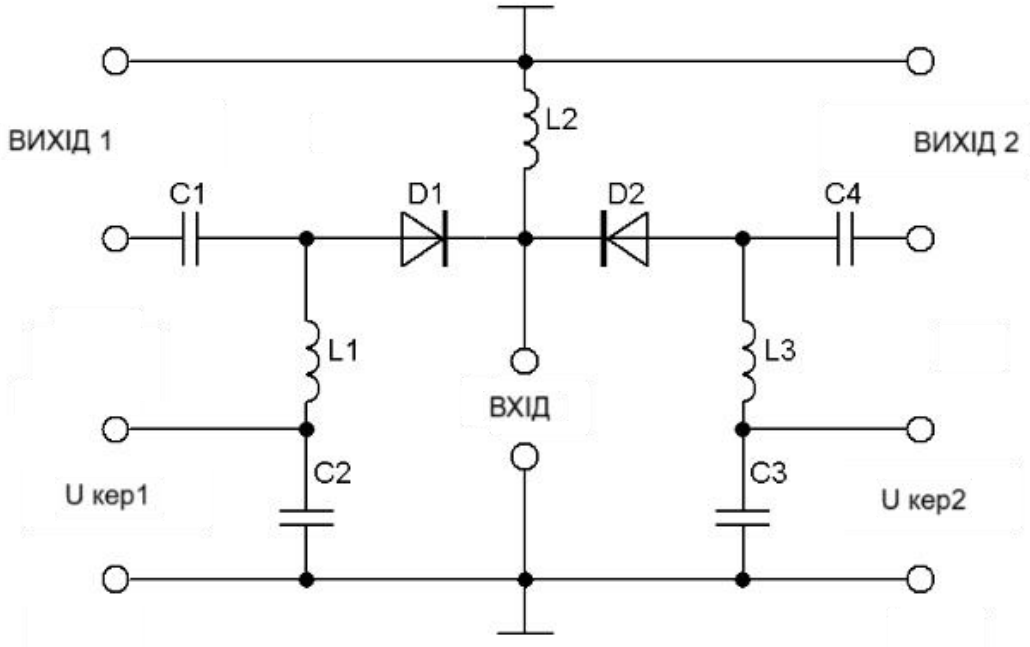


Рисунок 3.8 – Схема антенного перемикача

Відзначимо, що на помірно-високих частотах (до декількох ГГц) і застосуванні сучасних діодів з малою ємністю (0.1 – 0.2 пФ) для режиму пропущення можна зневажити ємнісної складової провідності закритого діода. Тоді діод може бути представлений у вигляді активних опорів R_- для закритого діода й R_+ для відкритого (див. рис. 3.9, де R_1 й R_2 опору діодів, відповідно VD1 і VD2). Для реалізації комутаторів виберемо діодну матрицю BAR63-05 з наступними параметрами:

- ємність і-шару $3 \approx 0.15$ пФ;
- опір відкритого діода R_+ =1.5 Ом;
- критична частота матриці $f_{KP} = 300$ ГГц;
- прямий струм $I_0 = 30$ мА;
- зворотний зсув $U_{ОБР} = 20$ В;
- максимальна потужність розсіювання матриці $P_{РАСМАХ} = 0.5$ Вт.

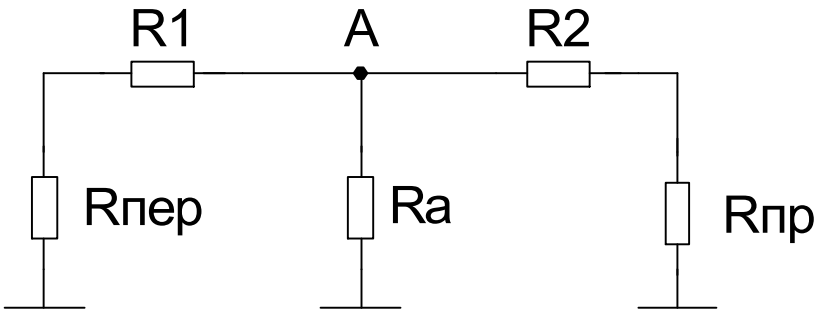


Рисунок 3.9 – Еквівалентна схема комутатора 1:2

Визначимо опір діода при негативному зсуві використовуючи параметри діода:

$$K = \frac{\sqrt{\ell_З} - 1}{\sqrt{\ell_П} - 1} = \left(\frac{f_{KP}}{f_0}\right)^2 = \left(\frac{300 \cdot 10^9}{2.44 \cdot 10^9}\right)^2 = 15116.9 \text{ Ом}; \quad (3.1)$$

$$g- = \frac{1}{K} = \frac{1}{15.117 \cdot 10^3}, \quad (3.2)$$

Розглянемо випадок, коли діод VD1 відкритий, а діод VD2 закритий. Визначимо струм у вузлі розгалуження ліній передачі:

$$I_A = \frac{\varepsilon}{R_+ + \frac{R_A \cdot R_-}{R_A + R_-}} = \frac{2.3}{1.5 + \frac{50 \cdot 15.117 \cdot 10^3}{50 + 15.117 \cdot 10^3}} = 0.045 \text{ А}, \quad (3.3)$$

де ε – напруга на клемах антени.

Напруга на вході:

$$U_A = I_A \cdot \frac{R_A \cdot R_-}{R_A + R_-} = 0.045 \cdot \frac{50 \cdot 15.117 \cdot 10^3}{50 + 15.117 \cdot 10^3} = 2.233 \text{ В}. \quad (3.4)$$

Потужність розсіювання на відкритому діоді:

$$P_{R+} = {I_A}^2 \cdot R_+ = 0.045^2 \cdot 1.5 = 3.011 \text{ мВт}. \quad (3.5)$$

Потужність в антені:

$$P_A = {I_A}^2 \cdot R_A = 0.045^2 \cdot 50 = 0.1 = 100 \text{ мВт}. \quad (3.6)$$

Струм зворотного зсуву:

$$I_{R-} = \frac{U_A}{R_-} = \frac{2.233}{15.117 \cdot 10^3} = 1.477 \cdot 10^{-4} \text{ А}. \quad (3.7)$$

Потужність розсіювання на закритому діоді:

$$P_{R-} = {I_{R-}}^2 \cdot R_- = \left(1.477 \cdot 10^{-4}\right)^2 \cdot 15.117 \cdot 10^3 = 3.298 \cdot 10^{-4} \text{ Вт}. \quad (3.8)$$

Потужність на вході приймача:

$$P_{ПР} = I_{R-}{}^2 \cdot R_{ПР} = \left(1.477 \cdot 10^{-4}\right)^2 \cdot 50 = 1.091 \cdot 10^{-6} \text{ Вт.} \quad (3.9)$$

Сумарна потужність:

$$P_{\Sigma} = P_{R+} + P_{R-} + P_A + P_{ПР} =$$

$$= 3.011 \cdot 10^{-3} + 3.298 \cdot 10^{-4} + 100 \cdot 10^{-3} + 1.091 \cdot 10^{-6} = 0.104 \text{ Вт.} \quad (3.10)$$

Визначимо загасання перемикача в стані “вимкнено“:

$$\ell_{ЗАП} = -10 \lg \frac{P_{ПР}}{P_{\Sigma}} = 10 \lg \frac{1.091 \cdot 10^{-6}}{0.104} = 49.781 \text{ дБ.} \quad (3.11)$$

Втрати перемикача в стані “увімкнено“:

$$\ell_{ПР} = -10 \lg \frac{P_A}{P_{\Sigma}} = -10 \lg \frac{0.1}{0.104} = 0.142 \text{ дБ.} \quad (3.12)$$

Для компенсації ємності діода до вузла розгалуження лінії передачі підключимо індуктивність з $x_C = -x_L$.

$$x = \frac{1}{\omega \cdot C} = \frac{1}{2 \cdot 3.14 \cdot 2.44 \cdot 10^9 \cdot 0.15 \cdot 10^{-12}} = 434.85 \text{ Ом.} \quad (3.13)$$

$$L2 = \frac{x}{\omega} = \frac{434.85}{2 \cdot 3.14 \cdot 2.44 \cdot 10^9} = 28.36 \text{ нГн.} \quad (3.14)$$

Визначимо номінали блокувальних індуктивностей і ємностей. Виберемо значення $x_{Lб} >> \rho_o = 50$ Ом, $x_{Lб} = 5$ кОм. Тоді

$$L1 = L3 = \frac{x_{Lб}}{\omega} = \frac{5 \cdot 10^3}{2 \cdot 3.14 \cdot 2.44 \cdot 10^9} = 0.326 \text{ мкГн.} \quad (3.15)$$

Значення $x_{Cб} << \rho_o = 50$ Ом. Виберемо $x_{Cб} = 5$ Ом, тоді

$$C2 = C3 = \frac{1}{\omega \cdot x_{Cб}} = \frac{1}{2 \cdot 3.14 \cdot 2.44 \cdot 10^9 \cdot 5} = 13.05 \text{ пФ.} \quad (3.16)$$

Ємності розділових конденсаторів $C1$ і $C4$ визначається з умови:

$$C1 = C4 = \frac{20\ldots30}{\omega \cdot \rho_o} = \frac{25}{2 \cdot 3.14 \cdot 2.44 \cdot 10^9 \cdot 50} = 32.61 \text{ пФ.} \quad (3.17)$$

3.3 Розрахунок вихідного смугового фільтра

У даній частині атестаційної роботи проектується вихідний мікрострічковий смуго-проникний фільтр передавального тракту, основним завданням якого є фільтрація гармонік і субгармонік переданого пристроєм сигналу, а також забезпечення вибірковості за сусіднім каналом в приймальному тракті. До фільтрів сигнальної частоти пред'являються вимоги по загасанню в смузі затримування. Заданий діапазон частот пропущення приймемо $f_{\min} \ldots f_{\max} = 1950 \ldots 2930$ МГц, смуга пропущення становить $2\Delta f_П = 980$ МГц.

Фільтр повинен забезпечувати запас на межах смуги пропущення порядку 1.1…1.5, тому оберемо:

$$2\Delta f_П = 1.1 \cdot 980 \approx 1080 \text{ МГц,} \quad (3.18)$$

Для фільтра із центральною частотою $f_0 = 2440$ МГц відносна смуга пропущення:

$$\frac{2\Delta f_{П}}{f_0} = \frac{1080}{2440} \cdot 100 \approx 44.3\ \%, \qquad (3.20)$$

Діапазон затримування фільтра ухвалюємо $2\Delta f_З$ = 1620 МГц (1630…3250 МГц), відносна смуга затримування:

$$\frac{2\Delta f_З}{f_0} = \frac{1620}{2440} \cdot 100 \approx 66.4\ \%\ . \qquad (3.21)$$

Смуговий фільтр повинен послабляти побічні продукти каналу передачі на величину не менш $A_П = 40$ дБ, а ослаблення сигналу в смузі пропущення, внесене фільтром, не повинне перевищувати значення $A_З = 0.2$ дБ. При цьому вважаємо, що хвильові опори ліній, що підводять $Z = 50$ Ом. Матеріал основи, на якій виконується фільтр – полікор (діелектрична проникність $\varepsilon_r = 9.8$, тангенс діелектричних втрат $tg\delta = 0.001$) товщиною 1 мм. Матеріал провідників – мідь (товщина $t = 0.2$ мм, питома провідність $\sigma_M = 5.72 \cdot 10^7$ См).

Для апроксимації частотних характеристик фільтрів звичайно застосовуються функції поліномів Чебишева й максимально-плоскі функції Баттерворта. Максимально-плоска АЧХ фільтра Баттерворта в смузі пропущення досягається за рахунок погіршення лінійності фазової характеристики. Її нелінійність приводить до фазових викривлень, тому що сигнали різних частот мають різний час затримки. На перехідній характеристиці фільтра при цьому з'являється викид і “дзенькіт” на вершині вихідного імпульсу, величина яких зростає при підвищенні порядку фільтра. Істотне поліпшення вибірковості вихідних кіл може бути досягнуте при використанні фільтрів Чєбишєва, що мають найбільш круті спади АЧХ за межами смуги прозорості. Тому для апроксимації частотної характеристики проектованого смуго-проникного фільтра застосуємо

функції поліномів Чебишева. Фільтри з такими характеристиками крім усього іншого реалізується також з меншим числом елементів, тому фільтри з максимально- плоскою характеристикою.

У нашому випадку доцільно також вибрати мікрострічкову зустрічно-стрижневу структуру фільтра. Зустрічно-стрижневі фільтри на лініях широко застосовуються завдяки компактності, високій технологічності виготовлення й малим втратам. Зустрічно-стрижневий фільтр складається з відрізків зв'язаних ліній, розімкнутих на одному кінці й короткозамкнених на іншому й розташовані так, що їх короткозамкнені й розімкнуті кінці чергуються (рис. 3.10).

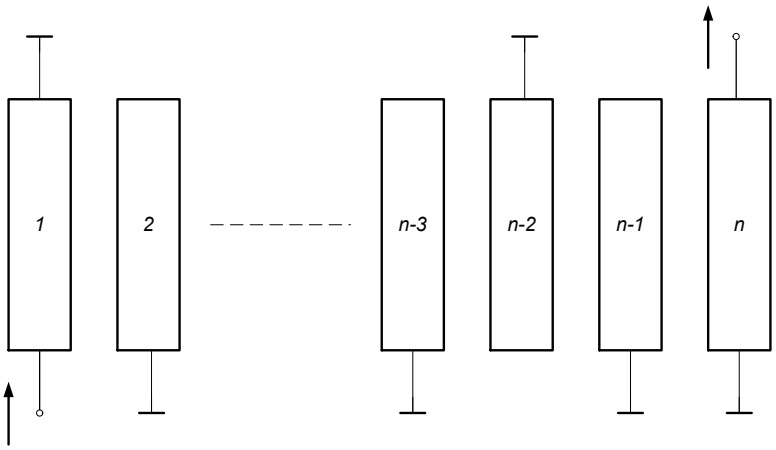


Рисунок 3.10 – Фільтр на зустрічних стрижнях з короткозамкненими вхідним і вихідним стрижнями

Розрахунки подібного смуго-проникного НВЧ фільтра заснований на зіставленні частотних характеристик проектованого фільтра й деякого фільтра-прототипу, наприклад, фільтр нижніх частот на елементах із зосередженими параметрами, параметри якого для різних смуг пропущення, а також значення $A_П$ й $A_З$ табулльовані й наведені в довідковій літературі [14].

Таким чином, згідно з обраною методикою розрахунків мікрострічкових фільтрів на зустрічних стрижнях [14] знаходимо смуги пропущення й затримки:

$$П_П = f_0 \cdot 0.01 \cdot \frac{\Delta f_П}{f_0} = 2440 \cdot 0.443 \approx 1080 \text{ МГц}, \quad (3.22)$$

$$П_З = f_0 \cdot 0.01 \cdot \frac{\Delta f_З}{f_0} = 2440 \cdot 0.664 \approx 1620 \text{ МГц}, \quad (3.23)$$

центральна частота визначається як середнє арифметичне частот затримування. Отже абсолютні значення частот затримки наступне:

$$f_{ЗН} = f_0 - \frac{П_З}{2} = 2440 - 810 = 1630 \text{ МГц}, \quad (3.24)$$

$$f_{ЗВ} = f_0 + \frac{П_З}{2} = 2440 + 810 = 3250 \text{ МГц}. \quad (3.25)$$

Добротність фільтра:

$$Q_0 = \frac{f_0}{П_П} = \frac{2440}{1080} \approx 2.26. \quad (3.26)$$

Нормована частота визначається як:

$$\xi(f) = Q_0 \left(\frac{f}{f_0} - \frac{f_0}{f} \right). \quad (3.27)$$

Тоді верхня й нижня нормовані частоти затримування:

$$\xi_{ЗН} = \xi(f_{ЗН}) = 2.26 \left(\frac{1630}{2440} - \frac{2440}{1630} \right) \approx -1.873, \quad (3.28)$$

$$\xi_{ЗВ} = \xi(f_{ЗВ}) = 2.26 \left(\frac{3250}{2440} - \frac{2440}{3250} \right) \approx 1.314, \quad (3.29)$$

тому що високе ослаблення складніше одержати при малих ξ , за нормовану частоту затримування оберемо менше зі значень $|\xi_{ЗН}|, \xi_{ЗВ}$:

$$\xi_З = \min(|\xi_{ЗН}|, \xi_{ЗВ}) = \min(|-1.873|, 1{,}314) = 1.314. \quad (3.30)$$

Величини, що характеризують перевищення ослаблення над одиницею в смузі пропущення:

$$a_П = 10^{0.1 \cdot A_п} - 1 = 100^{.02} - 1 = 0.047, \quad (3.31)$$

у смузі затримування:

$$a_З = 10^{0.1 \cdot A_з} - 1 = 104 - 1 \approx 104. \quad (3.32)$$

Електричні довжини стрижнів на перших граничних частотах смуг пропущення й загородження ($\gamma = 1$: номер смуги пропущення (див. рис. 3.11) [14]):

$$\theta_П = \frac{\pi(2\gamma - 1)}{1 + \frac{f_{П2}}{f_{П1}}} = \frac{3.14(2 \cdot 1 - 1)}{1 + \frac{2980}{1900}} \approx 1.223 \text{ рад}, \quad (3.33)$$

$$\theta_З = \frac{\pi(2\gamma - 1)}{1 + \frac{f_{З2}}{f_{З1}}} = \frac{3.14(2 \cdot 1 - 1)}{1 + \frac{3250}{1630}} \approx 1.049 \text{ рад}. \quad (3.34)$$

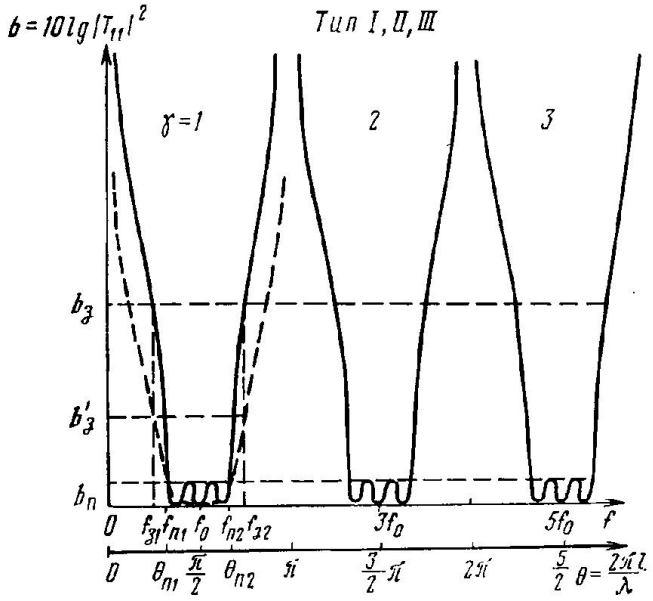


Рисунок 3.11 – Частотна характеристика фільтра на зустрічних стрижнях: «суцільна лінія» – Чебишевська апроксимація; «пунктирна лінія» – максимально плоска апроксимація

Кількість резонаторів прототипу фільтра Чебишева (порядок фільтра) визначається по формулі:

$$n \geq \frac{arch\sqrt{\frac{a_З}{a_П}}}{arch\frac{\cos(\theta_П)}{\cos(\theta_З)}} - m\left(\frac{arch\frac{ctg(\theta_З)}{ctg(\theta_П)}}{arch\frac{\cos(\theta_З)}{\cos(\theta_П)}} - 1\right), \qquad (3.35)$$

підставляючи в (3.35) вихідні вищеозначені значення, і задавшись кратністю $m = 1$ для короткозамкнених кінцевих стрижнів (рис. 3.10 – вхідний і вихідний стрижні з'єднані між собою), одержуємо $n \geq 6.03$. Правильність розрахунків підтверджується також рис. 3.12, на якому зображений графік для визначення числа резонансних стрижнів фільтра із Чебишевською характеристикою й робочого загасання ($A_П$, $A_З$) дБ: (0.2, 40), (0.01, 27), (0.00257, 21), (0.00066, 15). Суцільні лінії відповідають

випадку $m = 1$, пунктирні для $m = 3$ (випадок, коли вхідний і вихідний стрижні розімкнуті).

Однак враховуючи відомі недоліки мікрострічкових ліній, що приводять до випромінювання [14], згідно з рекомендаціями методики розрахунків необхідно збільшити число стрижнів фільтра в півтора-два рази. Ухвалюємо $n = 10$.

Далі, по таблицях [14], для відношення частот пропущення:

$$\frac{f_{П2}}{f_{П1}} = \frac{2980}{1900} \approx 1.57, \tag{3.36}$$

знаходимо незалежні параметри, які зведено в табл. 3.1. Конструктивний розрахунки фільтра припускає визначення розмірів фільтра за допомогою цих параметрів. Вони просто пов'язані із частковими погонними ємностями стрижнів через залежні параметри.

Таблиця 3.1 – Незалежні параметри для розрахунків зустрічно-стрижневого фільтра (КСХ ≤ 1.5, $A_3 \leq 0.2$ дБ)

$\alpha_1 = \alpha_{11}$	$\alpha_2 = \alpha_{10}$	$\alpha_3 = \alpha_9$	$\alpha_4 = \alpha_8$	$\alpha_5 = \alpha_7$	α_6
4.0716	16.886	28.220	30.756	31.666	31.902

З табл. 3.1 видне, що рівні провідності кінцевих стрижнів ($\alpha_1 = \alpha_{11}$) відрізняються від одиниці більш ніж у два рази, тобто досить великі). Тому при реалізації фільтра ширина кінцевих стрижнів виявиться неприйнятної через збільшення їх габаритів, а як наслідок і габаритів фільтра. Крім того, в області частот, де довжина хвилі порівнянна із шириною стрижнів, можливе виникнення інших типів хвиль. Уникнути цього можливо шляхом застосування фільтра зі стрижнями, що погодять.

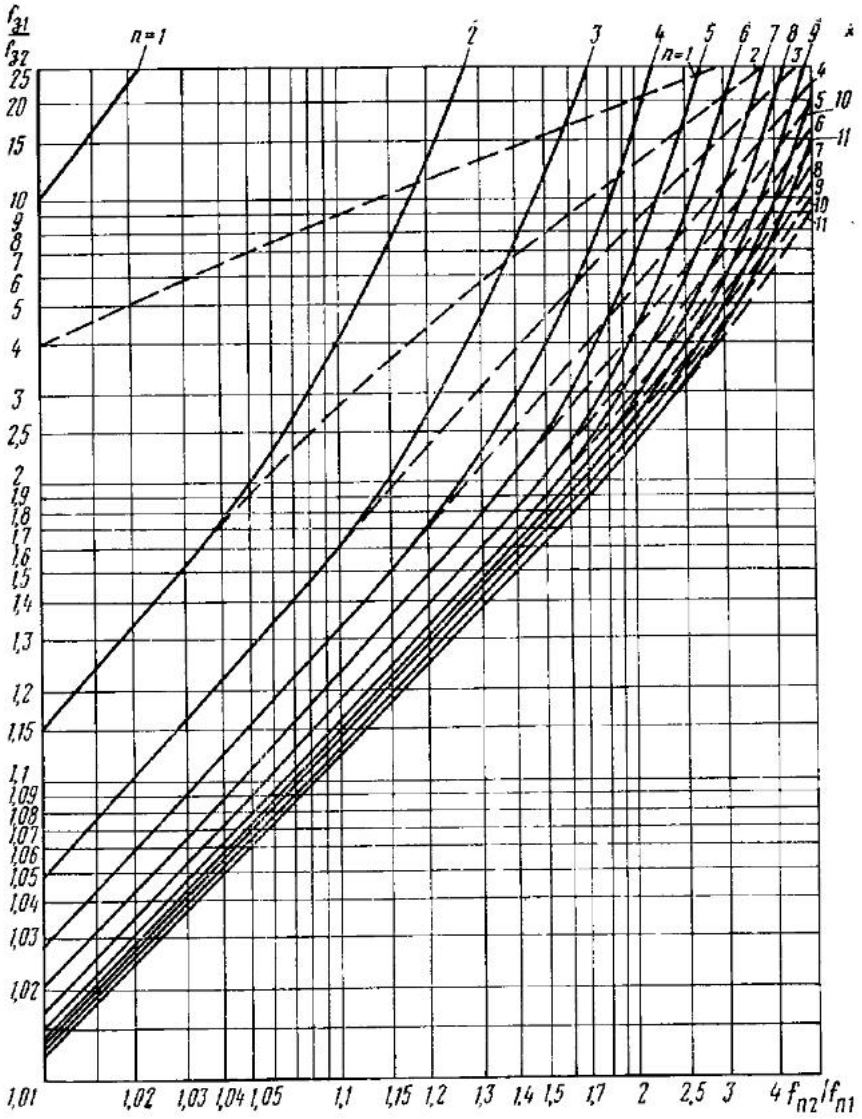


Рисунок 3.12 – Графік для визначення числа резонансних стрижнів фільтра

Значення незалежних параметрів для структури з, що погодять кінцевими стрижнями визначається у такий спосіб:

$$A_0 = 1; \tag{3.37}$$

$$A_1 = 1 + \alpha_1 = 1 + 4.0716 = 5.0716; \tag{3.38}$$

$$A_2 = \alpha_2\left(1 + \frac{1}{\alpha_1}\right) = 16.886\left(1 + \frac{1}{4.0716}\right) = 21.033; \tag{3.39}$$

$$A_3 = \alpha_3 = 28.220; \tag{3.40}$$

$$A_4 = \alpha_4 = 30.756; \tag{3.41}$$

$$A_5 = \alpha_5 = 31.666; \tag{3.42}$$

$$A_6 = \alpha_6 = 31.902. \tag{3.43}$$

Особливості перехід до розмірів мікрострічкового фільтра полягає в тому, що в розрахунках необхідно враховувати залежність ефективної відносної діелектричної проникності $\varepsilon_{эфф}$, використану для визначення розмірів зв'язаних провідників, необхідно уточнювати по графіках рис. 3.13 - 3.15 і для неї перерахувати розміри провідників. Це швидко збіжний процес, і після двох-трьох перерахувань значення ефективної відносної діелектричної проникності не змінюється.

Значення залежного параметра, що погодять кінцевих стрижнів визначається як:

$$w_0 = w_{11} = \frac{Z_0}{A_0} = \frac{50}{1} = 50 \text{ Ом}, \tag{3.44}$$

Для другого стрижня значення залежного параметра приймемо $w_1 = 40$ Ом, тоді

$$w_{0,1} = \sqrt{A_1 w_0 w_1} = \sqrt{5.0716 \cdot 50 \cdot 40} = 100.7 \text{ Ом}, \tag{3.45}$$

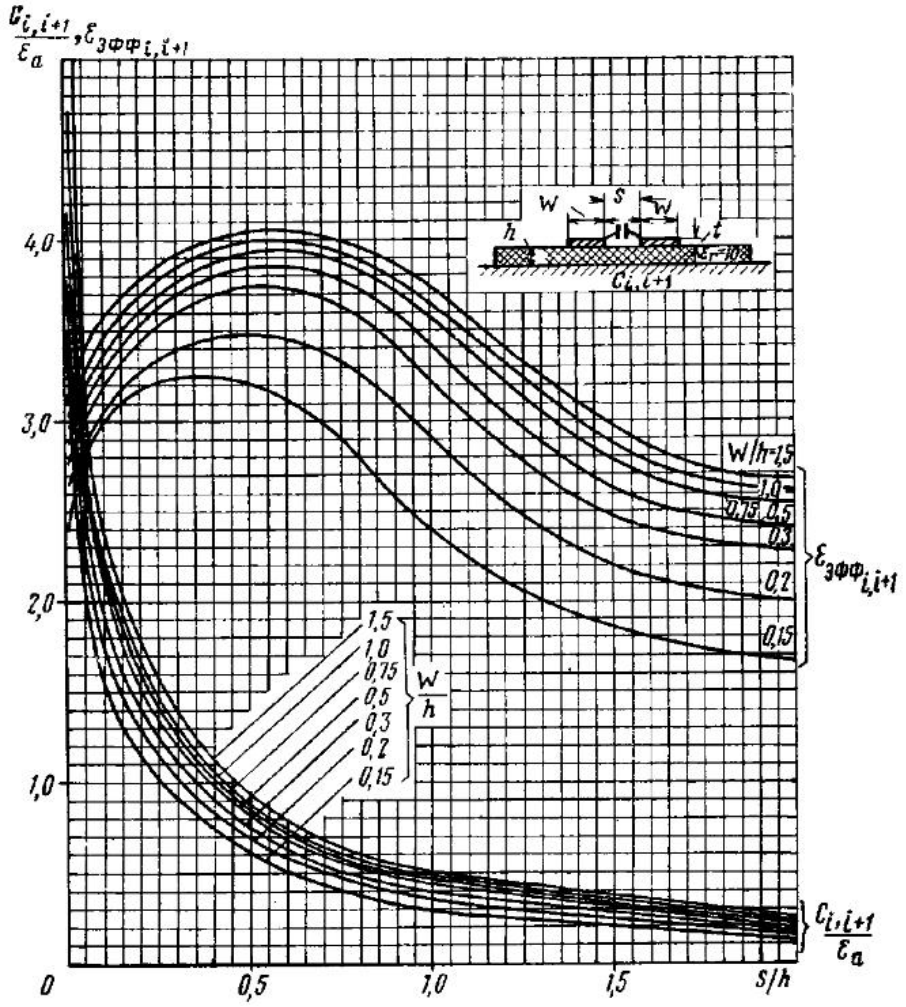


Рисунок 3.13 – Ємність зв'язки $\frac{C_{i,i+1}}{\varepsilon_a}$ й ефективний відносна діелектрична проникність мікростічкових зв'язаних ліній

Припускаємо, що $\varepsilon_{эфф\ 01}=5$ й $\varepsilon_{эфф\ 0}=7$ (ці значення орієнтовно узято із графіків на рис. 3.13 і рис. 3.14). Тоді ми можемо одержати погонну часткову ємність зв'язку між двома сусідніми стрижнями (віднесену до абсолютної діелектричної проникності середовища ε_a) використовуючи наступне вираз:

$$\frac{C_{i,i+1}}{\varepsilon_a}=\frac{120\pi}{\sqrt{\varepsilon_{эфф\ i,i+1}}\cdot w_{i,i+1}}, \tag{3.46}$$

а також можемо визначити часткову ємність крайнього провідника на заземлючий екран

$$\frac{C_{i,0}}{\varepsilon_a} = \frac{120\pi}{\sqrt{\varepsilon_{эфф\ i}}}\left(\frac{1}{w_i} - \frac{1}{w_{i,i+1}}\right). \qquad (3.47)$$

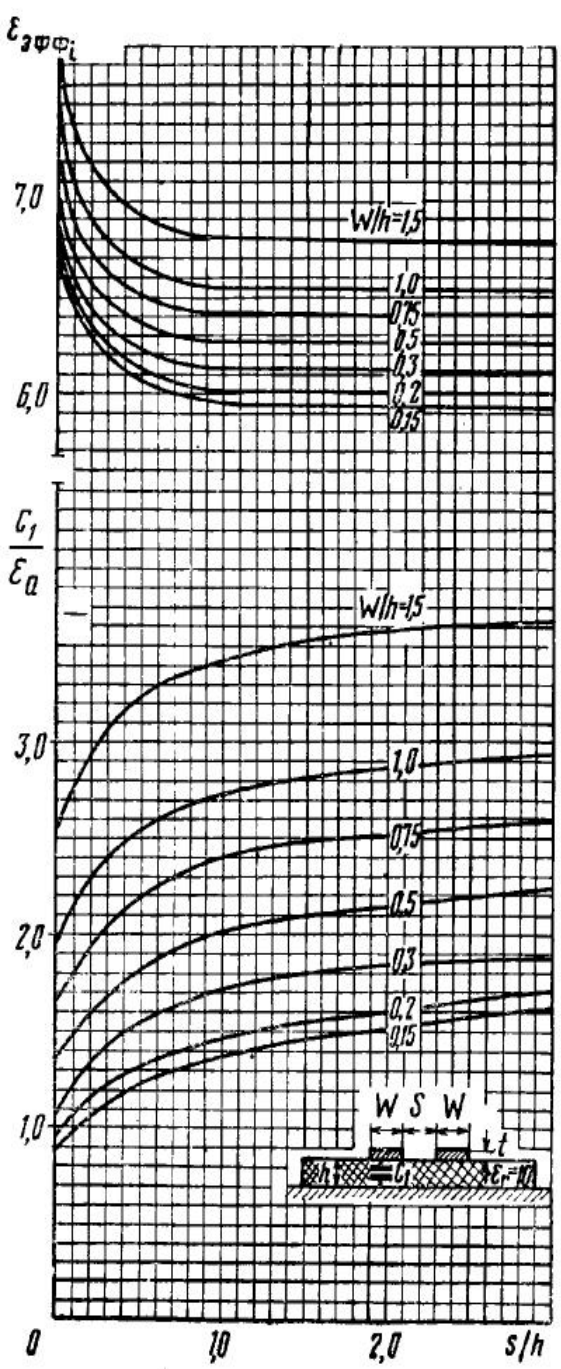


Рисунок 3.14 – Ємність стрижня з однобічним зв'язком і ефективна відносна діелектрична проникність

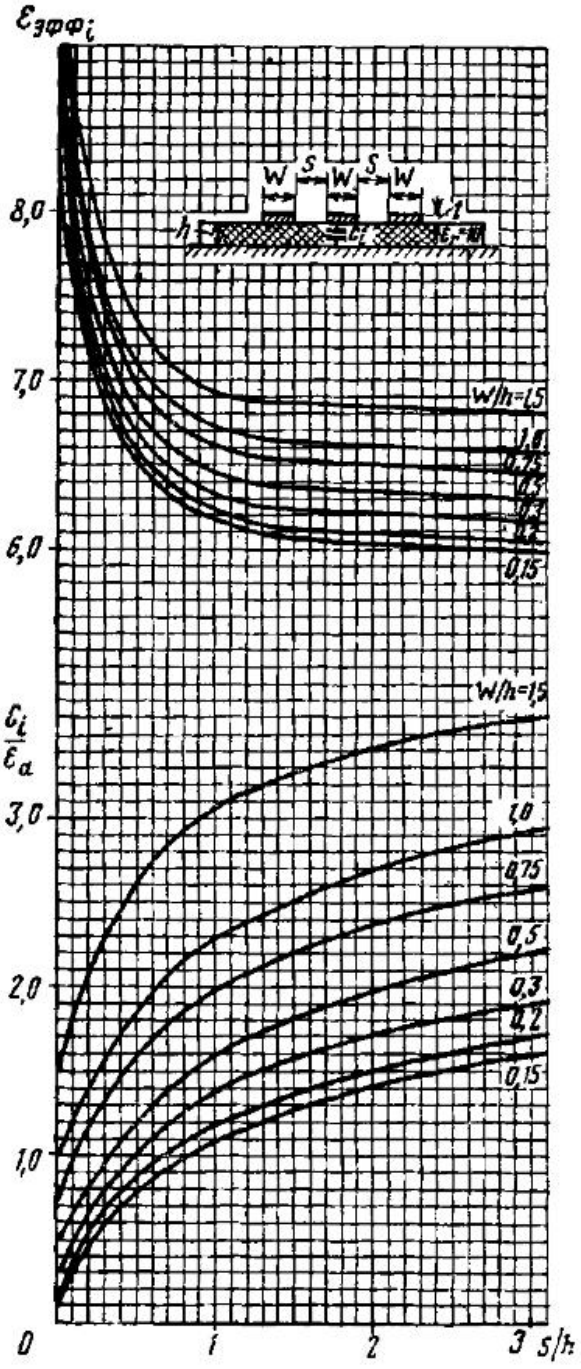


Рисунок 3.15 – Ємність стрижня із двостороннім зв'язком і ефективна відносна діелектрична проникність

Таким чином, підставляючи наявні дані в (3.49) і (3.50) для $i=0$ одержимо, що

$$\frac{C_{0,1}}{\varepsilon_a} = \frac{120\pi}{\sqrt{\varepsilon_{эфф\ 0,1}} \cdot w_{0,1}} = \frac{120\pi}{\sqrt{5} \cdot 100.7} = 1.675,$$

$$\frac{C_{0,0}}{\varepsilon_a} = \frac{120\pi}{\sqrt{\varepsilon_{эфф\ 0}}}\left(\frac{1}{w_0} - \frac{1}{w_{0,1}}\right) = \frac{120\pi}{\sqrt{7}}\left(\frac{1}{50} - \frac{1}{100.7}\right) = 1.425.$$

По графіках (рис. 3.13, рис. 3.14) знаходимо, що цим значенням часткових ємностей відповідають розміри зв'язаних провідників $\frac{s_{01}}{h} = 0.13$; $\frac{W_0}{h} = 0.4$ (див. рис. 3.16) і нові значення $\varepsilon_{эфф\ 01} = 3.32$ й $\varepsilon_{эфф\ 0} = 6.6$. Для знайдених значень $\varepsilon_{эфф}$ знову по (3.46), (3.47) обчислюємо $\frac{C_{0,1}}{\varepsilon_a} = 2.055$ й $\frac{C_{0,0}}{\varepsilon_a} = 1.465$, що відповідає зв'язаним провідникам з розмірами $\frac{s_{01}}{h} = 0.1$; $\frac{W_0}{h} = 0.425$ і значеннями $\varepsilon_{эфф\ 01} = 3.25$ й $\varepsilon_{эфф\ 0} = 6.5$. Після третього перерахування одержуємо остаточні результати:

$$\frac{C_{0,1}}{\varepsilon_a} = 2.08; \qquad \frac{C_{0,0}}{\varepsilon_a} = 1.475; \qquad \frac{s_{01}}{h} = 0.095;$$

$$\frac{W_0}{h} = 0.43; \qquad \varepsilon_{эфф\ 01} = 3.22; \varepsilon_{эфф\ 0} = 6.5,$$

де значення $\varepsilon_{эфф}$ практично збігаються з результатами другого перерахування. Аналогічно визначаємо розміри інших стрижнів, за винятком того, що замість графіків рис. 3.14 необхідні графіки рис. 3.15, які відповідають середнім стрижням фільтра.

Остаточні результати розрахунків наведені нижче. При цьому наведені результати для «половини» фільтра. Значення параметрів для

другої половини фільтра симетрично-ідентичні значенням наведених параметрів (фільтр – симетричний пристрій), наприклад $\frac{W_0}{h} = \frac{W_{11}}{h} = 0.43$.

$w_0 = 50$ Ом	$w_{0,1} = 100.7$ Ом	$\varepsilon_{эфф\ 0} = 6.5$	$\varepsilon_{эфф\ 01} = 3.22$
$w_1 = 40$ Ом	$w_{1,2} = 200$ Ом	$\varepsilon_{эфф\ 1} = 7$	$\varepsilon_{эфф\ 12} = 3.85$
$w_2 = 47.5$ Ом	$w_{2,3} = 250$ Ом	$\varepsilon_{эфф\ 2} = 6.9$	$\varepsilon_{эфф\ 23} = 3.95$
$w_3 = 46.6$ Ом	$w_{3,4} = 258$ Ом	$\varepsilon_{эфф\ 3} = 6.95$	$\varepsilon_{эфф\ 34} = 4$
$w_4 = 46$ Ом	$w_{4,5} = 261$ Ом	$\varepsilon_{эфф\ 4} = 6.95$	$\varepsilon_{эфф\ 45} = 4$
$w_5 = 46.6$ Ом	$w_{5,6} = 263$ Ом	$\varepsilon_{эфф\ 5} = 6.95$	$\varepsilon_{эфф\ 56} = 4$
$\frac{C_{0,0}}{\varepsilon_a} = 1.475$	$\frac{C_{0,1}}{\varepsilon_a} = 2.08$	$\frac{W_0}{h} = 0.43$	$\frac{s_{01}}{h} = 0.095$
$\frac{C_{1,0}}{\varepsilon_a} = 1.43$	$\frac{C_{1,2}}{\varepsilon_a} = 0.96$	$\frac{W_1}{h} = 0.67$	$\frac{s_{12}}{h} = 0.425$
$\frac{C_{2,0}}{\varepsilon_a} = 1.72$	$\frac{C_{2,3}}{\varepsilon_a} = 0.75$	$\frac{W_2}{h} = 0.8$	$\frac{s_{23}}{h} = 0.55$
$\frac{C_{3,0}}{\varepsilon_a} = 1.94$	$\frac{C_{3,4}}{\varepsilon_a} = 0.73$	$\frac{W_3}{h} = 0.96$	$\frac{s_{34}}{h} = 0.6$
$\frac{C_{4,0}}{\varepsilon_a} = 2$	$\frac{C_{4,5}}{\varepsilon_a} = 0.72$	$\frac{W_4}{h} = 1$	$\frac{s_{45}}{h} = 0.61$
$\frac{C_{5,0}}{\varepsilon_a} = 1.97$	$\frac{C_{5,6}}{\varepsilon_a} = 0.71$	$\frac{W_5}{h} = 1$	$\frac{s_{56}}{h} = 0.61$

Довжина стрижнів однакова й рівняється чверті довжини хвилі в мікрострічковій лінії:

$$l_1 ... l_9 = \frac{\lambda_0}{4\sqrt{\varepsilon_r}} = \frac{\frac{3 \cdot 10^8}{2440 \cdot 10^9}}{4\sqrt{9.8}} \approx 9.82 \text{ мм.} \qquad (3.48)$$

Ескіз спроектованого смуго-проникного фільтра й деякі з його характеристик представлено на рис. 3.16 – 3.19.

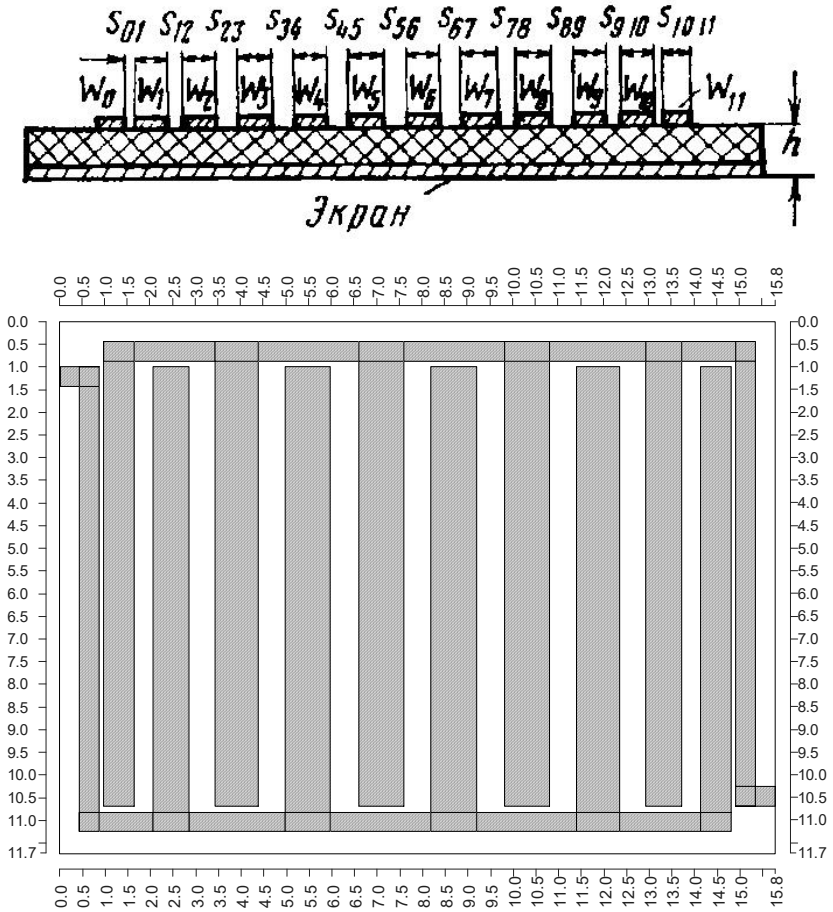


Рисунок 3.16 – Ескіз смуго-проникного фільтра на зустрічних стрижнях

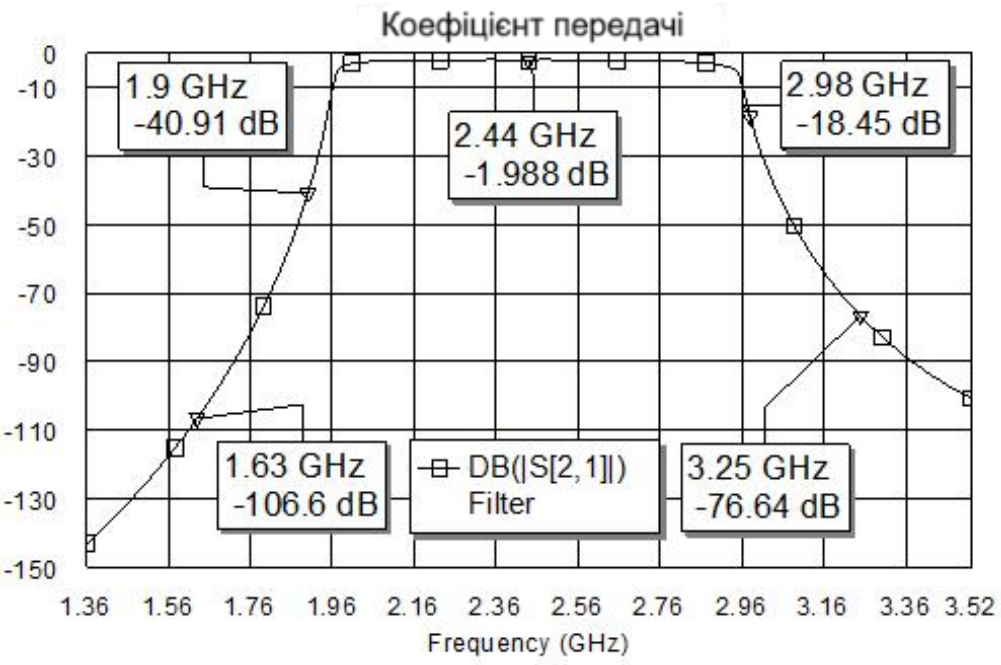


Рисунок 3.17 – Частотна характеристика коефіцієнта передачі фільтра

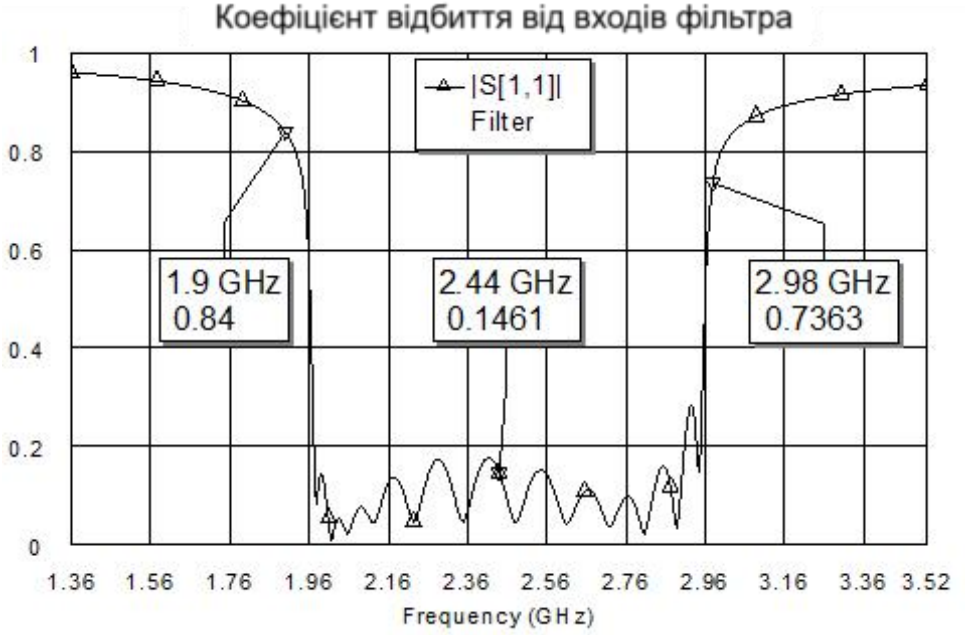


Рисунок 3.18 – Коефіцієнт відбиття від входу фільтра

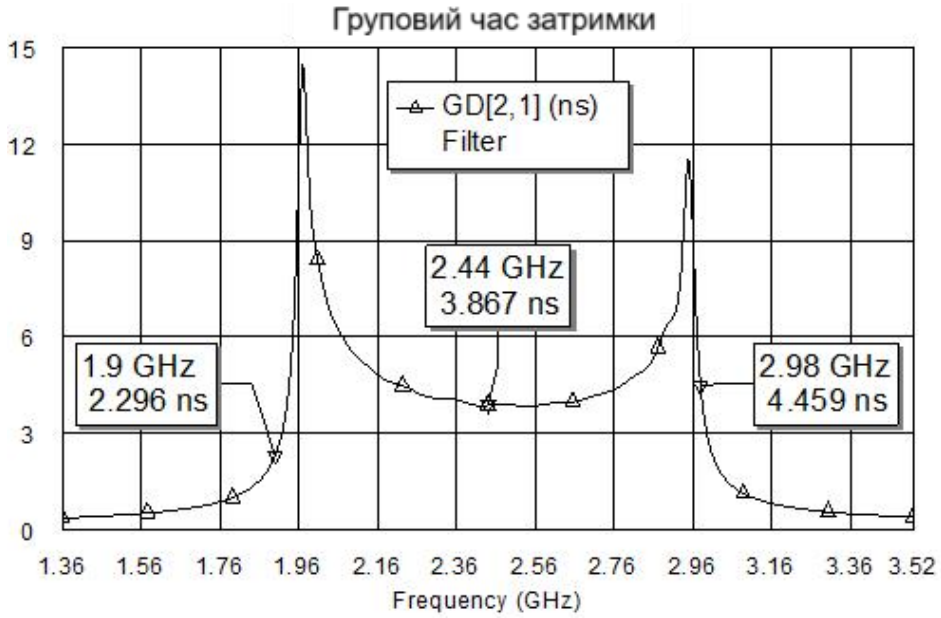


Рисунок 3.19 – Час затримки проходження сигналу через фільтр

4 НОРМАТИВНО-ТЕХНІЧНА ДОКУМЕНТАЦІЯ

4.1 Законодавче забезпечення охорони інформації

Закон України «Про інформацію»

Цей Закон закріплює право громадян України на інформацію, закладає [1] правові основи інформаційної діяльності.

Ґрунтуючись на Декларації про державний суверенітет України й Акті проголошення незалежності України, Закон затверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в області інформації.

Стаття 1. Визначення інформації

Поняття ”інформація” цей Закон тлумачить як документовані або привселюдно оголошені зведення про події і явища, що відбуваються в суспільстві, державі і навколишньому природному середовищі.

Стаття 2. Мета і задачі Закону

Закон установлює загальні правові основи одержання, використання, поширення і збереження інформації, закріплює право особи на інформацію у всіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації і забезпечує її охорону, захищає особу і суспільство від неправдивої інформації.

Стаття 5. Основні принципи інформаційних відносин

Основними принципами інформаційних відносин є:

- гарантованість права на інформацію;
- відкритість, доступність інформації і воля її обміну;
- об'єктивність, достовірність інформації;
- повнота і точність інформації;
- законність одержання, використання, поширення і збереження інформації.

Стаття 7. Суб'єкти інформаційних відносин

Суб'єктами інформаційних відносин є:

- громадяни України;

- юридичні особи;

- держава.

Суб'єктами інформаційних відносин відповідно до цього Закону можуть бути також інші держави, їхні громадяни і юридичні особи, міжнародні організації й особи без громадянства.

Стаття 14. Основні види інформаційної діяльності

Основними видами інформаційної діяльності є одержання, використання, поширення, і збереження інформації.

Одержання інформації – це знаходження, придбання, нагромадження відповідно чинному законодавству України документованої або привселюдно оголошуваної інформації громадянами, юридичними особами або державою.

Стаття 17. Області інформації

Області інформації – це сукупність документованих або привселюдно оголошених зведень про відносно самостійні сфери життя і діяльності суспільства і держави.

Основними областями інформації є: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна.

Стаття 30. Інформація з обмеженим доступом

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюється за їхнім бажанням відповідно передбаченими ними умовами.

Громадяни, юридичні особи, що володіють інформацією професійного, ділового, виробничого, банківського, комерційного й

іншого характеру, отриманої власними засобами, або такої, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного й іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи приналежність її до категорії конфіденційної, і встановлюють для неї систему (способи) захисту.

Виключення складає інформація комерційного і банківського характеру, а також інформація, правовий режим якої встановлений Верховною Радою України за представленням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків і т.п.), і інформація, збереження якої являє загрозу життю і здоров'ю людей.

До таємної інформації відноситься інформація, що містить відомості, що складають державну й іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, що складають державну таємницю, і доступ до неї громадян здійснюється згідно Закону про інформацію.

Порядок обороту таємної інформації і її захисту визначається відповідними державними органами за умови дотримання вимог, установлених цим Законом.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Стаття 45. Охорона права на інформацію

Право на інформацію охороняється Законом. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації.

Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених Законом.

Суб'єкт права на інформацію може вимагати усунення будь-яких порушень його права.

Забороняється вилучення друкованих видань, експонатів, інформаційних бланків, документів з архівних, бібліотечних, музейних фондів і знищення їх з ідеологічних або політичних розумінь.

Закон України «Про державну таємницю»

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

державна таємниця (далі також – секретна інформація) – вид таємної інформації, що охоплює відомості в сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України і які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з встановленням ступеня їхньої таємності шляхом обґрунтування і визначення можливої шкоди національній безпеці України; у випадку розголошення цих відомостей, включенням цієї інформації в Звід зведень, що складають державну таємницю, і з опублікуванням цього Зводу і змін до нього;

гриф таємності – реквізит матеріального носія секретної інформації, що засвідчує ступінь таємності даної інформації;

державний експерт із питань таємниць – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці в сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, зміна ступеня таємності цієї інформації і її розсекречення;

допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації;

доступ до державної таємниці – надання уповноважною, посадовою

особою дозволу громадянину на ознайомлення з конкретною, секретною інформацією і проведення діяльності, пов'язаної з державною таємницею або ознайомлення з конкретною секретною інформацією і проведення діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно його службовим повноваженням;

засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення і доступ до конкретної секретної інформації шляхом надання відповідного грифа таємності документам, виробам або іншим матеріальним носіям цієї інформації;

звід відомостей, що складають державну таємницю – акт, у якому зведені переліки зведень, що відповідно до рішень державних експертів з питань таємниць складають державну таємницю у визначених цим Законом сферах;

категорія режиму таємності – категорія, що характеризує важливість і обсяги відомостей, що складають державну таємницю, зосереджених в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

криптографічний захист секретної інформації – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою збереження (або відновлення) змісту інформації, підтвердження її дійсності, цілісності, авторства і т.п.;

матеріальні носії секретної інформації – матеріальні об'єкти, у тому числі фізичні поля, в яких відомості, що складають державну таємницю, відображені у виді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів і т. п.;

охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних і оперативно-розшукових заходів,

спрямованих на запобігання розголошення секретної інформації і втратам її матеріальних носіїв;

режим таємності – установлений відповідно до вимог цього Закону й інших виданих згідно нього нормативно-правових актів єдиний порядок забезпечення охорони державної тіни;

розсекречення матеріальних носіїв секретної інформації – зняття у встановленому законодавством порядку обмежень на поширення і доступ до конкретної секретної інформації шляхом скасування раніше наданого грифа таємності документам, виробам або іншим матеріальним носіям цієї інформації;

спеціальна експертиза щодо наявності умов для проведення діяльності, пов'язаної з державною таємницею – експертиза, що проводиться з метою визначення в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для проведення діяльності, пов'язаної з державною таємницею;

ступінь таємності («особливої важливості», «абсолютно секретно», «секретно») – категорія, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї і рівень її охорони державою;

технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності і недопущення блокування інформації.

4.2 Концепція технічного захисту інформації

Має таки розділи:

1. Загальні положення:

Концепція визначає основи державної політики в сфері захисту інформації інженерно-технічними заходами. ТЗІ є складовою частиною забезпечення національної безпеки України. Концепція може забезпечити

єдність принципів формування і проведення такої політики в сферах життєдіяльності особи, суспільства і держави (соціальної, політичної, економічної, військової, екологічної, науково-технічної, інформаційної і т.п.) і служити підставою для створення програм розвитку сфери ТЗІ.

2. Загрози безпеки інформації і стан його технічного захисту:

Відповідно до Концепції одна з основних можливих загроз національній безпеці України в інформаційній сфері – виток інформації, що складає державну й іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави. Напрямок розвитку ТЗІ обумовлюються необхідністю своєчасного проведення заходів, адекватних масштабам загроз для інформації, і будуються на основах правової демократичної держави відповідно правам суб'єктів і інформаційних відносин на доступ до інформації і її захисту.

3. Система ТЗІ:

Система ТЗІ – це сукупність суб'єктів, об'єднаних цілями і задачами з інженерно-технічними заходами, нормативно-правовою і матеріально-технічною базою. Основне правове забезпечення ТЗІ складають: Конституція України, Концепція національної безпеки України, Закони України: «Про інформацію», «Про захист інформації», «Про державну таємницю», «Про науково-технічну інформацію», та інші нормативно-правові акти і договори.

4. Основні напрямки державної політики в сфері ТЗІ:

Першочергові заходи щодо реалізації державної політики в сфері технічного захисту інформації, до яких відносять фінансування систем ТЗІ, координування дій і поділ сфер діяльності організаційних структур ТЗІ,, а також ієрархічну побудову цих структур, обов'язку захисту інженерно-технічними засобами інформації, що належить до державної таємниці або конфіденційної інформації.

4.3 Положення про технічний захист інформації

Положення визначає правові й організаційні основи технічного захисту важливої для держави, суспільства й особистості інформації, охорона якої забезпечується державою відповідно до законодавства.

ТЗІ, здійснюється щодо органів державної влади, органів місцевого самоврядування, органів керування Збройних Сил України й інших військових формувань, підприємств, організацій.

Державна політика ТЗІ, реалізується Департаментом спеціальних телекомунікаційних систем захисту інформації СБУ у взаємодії з органами, щодо яких здійснюється ТЗІ,.

Організація ТЗІ, в органах, щодо яких здійснюється технічний захист інформації, покладається на їхніх керівників.

Організаційно-технічні принципи, порядок здійснення заходів щодо ТЗІ,, порядок контролю в цій сфері, характеристики погроз для інформації, норми і вимоги до технічного захисту, порядок атестації й експертизи комплексів ТЗІ, визначаються нормативно-правовими актами, прийнятими у встановленому порядку відповідними органами.

Матеріально-технічна база системи ТЗІ, складається з технічних засобів загального призначення і спеціальних технічних засобів.

Технічні засоби загального призначення повинні мати документ, що підтверджує їхню відповідність вимогам нормативно-правових актів по ТЗІ,, отриманий у порядку, що встановлює Департамент спеціальних телекомунікаційних систем захисту інформації СБУ і Комітет України з питань спеціалізації, метрології і сертифікації.

Під час розробки і впровадження заходів щодо ТЗІ, використовуються засоби, дозволені Департаментом спеціальних телекомунікаційних систем захисту інформації СБУ для застосування і включені до відповідних переліків.

ВИСНОВКИ

У магістерській атестаційній роботі виконаний огляд технології Bluetooth, у результаті якого ухвалено рішення, що дана технологія може бути використана для організації зловмисником несанкціонованого каналу витоку інформації. Проведений аналіз сценаріїв використання Bluetooth пристроїв для витоку інформації.

Для пошуку потай установлених Bluetooth пристроїв можна використовувати більшість із традиційних методів пошуку радіозакладних пристроїв. Однак ці методи в більшості випадків (крім радіомоніторингу) не класифікують знайдений закладний пристрій як Bluetooth пристрій. Крім того, метод пошуку за допомогою детектора поля може виявитися неефективним і вимагає технічної доробки. Більш результативними можуть виявитися методи, які використовують особливості протоколу Bluetooth і описані в другому розділі роботи.

Для більш ефективного виявлення Bluetooth пристроїв необхідно забезпечити просторову й частотну вибірковість пошукового приладу. Просторова вибірковість забезпечить пеленгацію шуканого пристрою й крім того збільшить радіус пошуку. Частотна вибірковість забезпечить завадостійкість пристрою, знизить імовірність фіктивних тривог і тим самим також збільшить радіус пошуку.

У магістерській роботі проведений розрахунки патч антени з антенним комутатором на частоту 2.44 ГГц. Проведене моделювання антени в ПО IE3D. Мінімальний коефіцієнт відбиття досягається на частоті 2440 МГц і дорівнює - 32.3 дБ, у той час як на частоті 2483 МГц маємо [S11] = -17.2 дБ. За рівнем зворотних втрат - 17,2 дБ смуга антени становить 75 МГц. Коефіцієнт підсилення антени склав 9 дБ.

Для забезпечення додаткової частотної вибірковості пошукового пристрою в магістерській роботі виконаний розрахунки смугового фільтра на мікрострічковій зустрічно-стрижневій структурі. Проведене

моделювання фільтра в ПО AWR. У результаті моделювання отримані наступні параметри: діапазон частот пропущення 1.9 … 3 ГГц (із загасанням менш 3 дБ), діапазон частот затримки становить 1.76 …3.25 ГГц (із загасанням більш 70 дБ) МГц.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bluetooth: принципи будови та функціонування URL: [Електронний ресурс] Режим доступу: http://www.chipnews.ua/html.cgi/arhiv/01_07/stat-8.htm.

2. Бездротові модулі URL: [Електронний ресурс] Режим доступу: https://www.chipdip.ua/catalog-show/wireless-modules.

3. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації URL: [Електронний ресурс] Режим доступу: http://www.confident.org.ua/index.php/stati-po-teme/181-klassifikatsiya-metodov-i-sredstv-poiska-elektronnykh-ustrojstv-perekhvata-informatsii.html.

4. Accurate indoor positioning bluetooth beacons URL: [Електронний ресурс] Режим доступу: https://proximi.io/accurate-indoor-positioning-bluetooth-beacons.

5. API-first positioning platform for indoor and outdoor URL: [Електронний ресурс] Режим доступу: http://www.Proximi.io.

6. Показник рівня прийнятого сигналу URL: [Електронний ресурс] Режим доступу: https://ru.wikipedia.org/wiki/Показник рівня прийнятого сигналу.

7. Inferring distance from Bluetooth signal strength: a deep dive URL: [Електронний ресурс] Режим доступу: https://medium.com/personaldata-io/inferring-distance-from-bluetooth-signal-strength-a-deep-dive-fe7badc2bb6d.

8. B. Antic, J. O. N. Castaneda, D. Culibrk, A. Pizurica, V. Crnojevic and W. Philips, “Robust Detection and Tracking of Moving Objects in Traffic Video Surveillance”, Advanced Concepts for Intelligent Vision Systems, pages 494-505, 2009.

9. R. Bajaj, S.L. Ranaweera and D.P. Agrawal, “GPS: Location-Tracking Technology”, IEEE Vol.35, No.4, p. 92–94, 2002.

10. Визначення місця розташування за допомогою BLE-чипів Texas Instruments URL: [Електронний ресурс] Режим доступу: https://www.compel.ua/lib/97028.

11. An Indoor Tracking System Based on Bluetooth Technology URL: [Електронний ресурс] Режим доступу: https://arxiv.org/ftp/arxiv/papers/1209/1209.3053.pdf.

12. Стандарт зв’зку Bluetooth 5.1 URL: [Електронний ресурс] Режим доступу: https://webznam.ua/blog/standart_svjazi_bluetooth_51/2019-03-10-964.

13. Проектування НВЧ пристроїв комутації URL: [Електронний ресурс] Режим доступу: https://cyberleninka.ua/article/n/proektirovanie-svch-ustroystva-filtratsii-i-kommutatsii/viewer.

14. Леонченко В.П., Фельдштейн А.Л., Шепелянський Л.А. Розрахунок смужкових фільтрів на зустрічних стрижнях. [текст] Довідник, К.: "Зв’язок", 2011. - 312 с.