Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Розробка алгоритму роботи та системи оманливих рацій для боротьби з ворожими структурами та захисту військових об’єктів
(тема)

Виконав:

студент IV курсу, групи СПм-22-4

Шаманов Д.О.
(прізвище, ініціали)

Спеціальність 123 - Комп’ютерна інженерія

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування

Системне програмування
(повна назва освітньої програми)

Керівник: Ст. викл. Сорокін А.Р.
(посада, прізвище, ініціали)

Допускається до захисту

зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав.
кафедри _____
(підпис)

“ ___ ” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Шаманову Дмитру Олеговичу
(прізвище, ім’я, по батькові)

1. Тема роботи Розробка алгоритму роботи та системи оманливих рацій для боротьби з ворожими структурами та захисту військових об’єктів

затверджена наказом по університету від “ 1 ” квітня 2024 р. № 257 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 червня 2024 р.

3. Вхідні дані до роботи 1) Тема роботи; 2) Середовище розробки Visual Studio Code; 3) Технологія Wi-Fi

4. Перелік питань, що потрібно опрацювати у роботі

1) Аналіз предметної області;
2) Вибір і обґрунтування обладнання;
3) Вибір і обґрунтування програмних засобів;
4) Побудова системи позиціонування
5) Аналіз розміщення маяків в приміщенні
6) Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 15 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень	01.04.24-15.14.24	
2	Вибір технології розробки та	16.04.24-30.04.24	
	інструментальних засобів		
3	Розробка алгоритмічного забезпечення	01.05.24-15.05.24	
4	Розробка програмних модулів	16.05.24-25.05.24	
5	Відлагодження програмних модулів	26.05.24-28.05.24	
6	Оформлення матеріалів кваліфікаційної роботи	29.05.24-05.06.24	
7	Подання кваліфікаційної роботи керівникові та	06.06.24-07.06.24	
	її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	07.06.24-11.06.24	
	вання		

Дата видачі завдання 1 квітня 2024 р.

Студент _____
(підпис)

Керівник роботи _____ Ст. викл. Сорокін А.Р.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 107 с., 33 рис., 10 джерел.

СИСТЕМИ РЕБ, РАДІОЗВ’ЯЗОК, WI-FI, РАДІООБМІН, МОДУЛЬ, ФУНКЦІЯ

У сучасному світі, де електроніка пронизла всі сфери життя, важко уявити ведення бойових дій без використання радіоелектронних систем. Від наведення ракет до зв'язку між підрозділами, радіосигнали стали невід'ємною частиною військової справи. Однак, крім корисних функцій, радіосигнали можуть використовуватися й противником. Саме тут на сцену виходить радіоелектронна боротьба (РЕБ) - комплекс заходів, спрямованих на нейтралізацію ворожих радіоелектронних засобів (РЕЗ).

Завдяки РЕБ можна:

- Заглушити ворожі радіосигнали: Це може ускладнити або унеможливити зв'язок між підрозділами противника, координацію їхніх дій та наведення зброї.

- Виявити та знищити ворожі РЕЗ: Це може позбавити противника можливості використовувати радіолокаційні станції, системи розвідки та зв'язку.

- Дезінформувати противника: За допомогою хибних радіосигналів можна створювати імітацію активності військ, вводити ворога в оману щодо їхніх чисельності та розташування.

Саме тому усі країни докладають багато зусиль для того, щоб мати змогу обійти та перемогти усі можливі системи РЕБ.

ABSTRACT

Master’s thesis: 107 pages, 33 figures, 10 sources.

POSITIONING, TECHNOLOGY, PROTOCOL, COMPUTER, TABLET, MODULE, FUNCTION

In today's world, where electronics are everywhere, it's hard to imagine fighting a war without using radio systems. From guiding missiles to communicating between units, radio signals have become an essential part of warfare.

But just like any tool, radio signals can be used by both sides. That's where electronic warfare (EW) comes in. EW is a set of actions aimed at neutralizing enemy radio systems.

What EW can do:

- Jam enemy radio signals: This can make it difficult or impossible for enemy units to communicate, coordinate their actions, and target weapons.

- Detect and destroy enemy radio systems: This can deprive the enemy of the ability to use radar, intelligence, and communication systems.

- Misinform the enemy: Using fake radio signals, you can create the illusion of troop activity, misleading the enemy about their numbers and location.

That's why all countries put a lot of effort into being able to bypass and defeat all possible EW systems. It's a constant battle of developing new technologies and tactics to outsmart the enemy.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНь, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП 12
1 ТЕОРЕТИЧНІ ОСНОВИ РОЗУМІННЯ ПРИНЦИПІВ РОБОТИ ЧАСТОТНИХ СИГНАЛІВ ТА МЕТОДІВ ЇХ ВИЯВЛЕННЯ 13
1.1 Частотні діапазони 15
1.3 Використання частотних діапазонів для РЕБ 20
1.4 Канали зв’язку 22
1.4.1 Концепція каналів зв'язку 24
1.4.2 Типи каналів зв'язку 25
1.5 Огляд та класифікація радіостанцій 26
1.5.1 Призначення та класифікація радіостанцій 27
1.5.2 Основні характеристики радіостанцій 28
1.5.3 Типи радіосигналів 28
1.5.4 Сигнали радіостанцій та Wi-Fi 31
1.5.5 Властивості Wi-Fi сигналу 33
1.6 Методи розпізнавання сигналів 36
1.7 Вплив РЕБ на сигнали 36
1.8 Види боротьби з РЕБ 39
2 АНАЛІЗ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ДЛЯ ПРОЦЕСУ РАДІО ТА WIFI ОБМІНУ МІЖ ПРИСТРОЯМИ 41
2.1 Огляд бездротових технологій 41
2. 1. 1 Радіочастотні технології 41
2.1.2 Діапазони радіомодулів 49
2.1.3 Технологія Wi-Fi 50
3 ОГЛЯД І ВИБІР ПРИСТРОЇВ ДЛЯ РЕАЛІЗАЦІЇ 69
3.1 Вибір плати для розробки 69

3.1.1 Платформа Arduino 69
3.1.2 Платформа ESP32 70
3.1.2 Платформа STM32 70
3.2 Огляд дисплеїв для відображення інформації 71
3.2.1 OLED дисплей з I2C шиною 71
3.2.2 OLED дисплей без I2C шини 72
3.3 Вибір радіомодуля для роботи системи 72
3.3.1 Платформа FS1000A + MX-RM-5V 73
3.3.2 Платформа Si4432 73
3.4 Огляд бібліотек для радіомодулів 75
3.4.1 Бібліотека VirtualWire 75
3.4.2 Бібліотека RadioHead 75
3.4.3 Бібліотека RCSwitch 76
3.4.4 Бібліотека Gyver433 76
4 огляд та реалізація системи оманливих рацій 78
4.1 Загальний опис системи 78
4.2 Огляд функціональної принципової схеми 79
4.3 Огляд архітектурної схеми та режимів роботи 80
4.3.1 Огляд режимів та команд MASTER та SLAVE 82
4.3.2 Огляд режимів RADIO та WIFI 83
4.4 Вибір оптимальної відстані між пристроями для забезпечення максимальної якості і швидкості роботи 83
4.4.1 Розрахунок відстані для радіомодулів FS1000A та MX-RM-5V 84
4.4.2 Розрахунок відстані для Wi-Fi модулів ESP32 85
4.5 Імплементація системи 85
ВИСНОВКИ 91
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 92
ДОДАТОК А Графічний матеріал кваліфікаційної роботи 93
ДОДАТОК Б КОД ПРОЕКТУ 98

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

RFID - Radio Frequency IDentification (Радіочастотна ідентифікація)

FM - Frequency Modulation (Частотна Модуляція)

VHF - Very High Frequency (Ультракороткі Хвилі)

RSSI - Received Signal Strength Indicator (Індикація Рівня Прийнятого Сигналу)

AP - Access Point (Точка Доступу)

GNSS - Global Navigation Satellite System (Глобальна Навігаційна Супутникова Система)

SSID - Service Set Identifier (Ідентифікатор Набору Послуг)

MAC - Media Access Control (Управління Доступом до Посередників)

UUID - Universally Unique Identifier (Універсальний Унікальний Ідентифікатор)

WLAN - Wireless Local Area Network (Бездротова Локальна Мережа)

IP - Internet Protocol (Інтернет протокол)

TCP/IP - Transmission Control Protocol / Internet Protocol (Протокол Керування Даними / Інтернет Протокол)

РЕБ - Радіоелектронна боротьба

AM - Amplitude Modulation (Амплітудна модуляція)

DDS - Direct Digital Synthesis (Генератор аналогових сигналів)

ДХ - Довгі хвилі

СХ - Середні хвилі

КХ - Короткі хвилі

УКХ - Ультра короткі хвилі

НВЧ - Надвисокочастотні хвилі

ІЧ - Інфрачервоне випромінювання

УФ - Ультрафіолетове випромінювання

НЧ - Низькочастотний діапазон

СЧ - Середньочастотний діапазон

ВЧ - Високо частотний діапазон

УВЧ - Ультра високо частотний

ICM - Interim Control Module (Модуль тимчасового керування)

ISDN - Integrated Services Digital Network (Цифрова мережа з інтегрованими послугами)

GPS - Global Positioning System (Система глобального позиціонування)

ГЛОНАСС - Глобальна навігаційна супутникова система

VOX - Voice Operated Switch (Голосове керування)

DTMF - Dual-Tone Multi-Frequency (Система тональної сигналізації)

WI FI - Wireless Fidelity (Безпроводна точність)

CDMA - Code Division Multiple Access (Множинний доступ з кодовим розділенням каналів)

FFT - Fast Fourier Transform (Швидке перетворення Фур'є)

SWM - Single Wire Multi-Carrier (Одна мережа багато з'єднань)

РЕЗ - Радіоелектронні засоби

RFT - Radio Frequency Troubleshooting (Вирішення проблем з радіочастотою)

РЧ - Радіо частоти

ККД - Коефіцієнт корисної дії

ЄМС - Electromagnetic Compatibility (Електромагнітна сумісність)

АЧХ - Амплітудно-частотна характеристика

ФЧХ - Фазово-частотна характеристика

VHF - Very High Frequency (Дуже висока частота)

MF - Medium Frequency (Середня частота)

UHF – Ultra High Frequency (Надвисока частота)

OFDM - Orthogonal Frequency-Division Multiplexing (мультиплексування з ортогональним частотним розподілом)

DSSS - Direct Sequence Spread Spectrum (прямо-спектровий розподіл з

послідовністю)

IEEE - Institute of Electrical and Electronics Engineers (Стандарт інституту інженерів з електротехніки та електроніки)

VPA - Virtual Payment Address (Віртуальна адреса оплати)

AES - Advanced Encryption Standard (Розширенний стандарт шифрування)

IoT - Internet of Things (Інтернет речей)

WLAN - Wireless Local Area Network (Бездротова локальна мережа)

ISO - Міжнародна організація зі стандартизації

OSI - Мережева модель

OFDM - Orthogonal frequency-division multiplexing (Багатоканальний доступ з ортогональним розподілом частот)

MIMO - Multiple Input Multiple Output (Багато входів багато виходів)

WEP - Wired Equivalent Privacy (Протокол шифрування)

XOR - Exclusive Or (Виключне але)

WPA - Wi-Fi Protected Access (Захищенний доступ Wi-Fi)

EAP - Extensible Authentication Protocol (Розширюванний протокол автентифікації)

EAPOL - Extensible Authentication Protocol over LAN (розширюваний протокол автентифікації через локальну мережу)

TKIP - Temporal Key Integrity Protocol (Тимчасовий протокол цілісності ключа)

MD5 - Message Digest Algorithm 5 (Алгоритм дайджесту повідомлень 5)

TLS - Transport Layer Security (Захист транспортного рівня)

TTLS - Tunneled Transport Layer Security (Тунельний протокол Transport Layer Security)

PKI - Public Key Infrastructure (Інфраструктура відкритих ключів)

SSID - Service Set Identifier (Ідентифікатор набору служб)

PMK - Programmable Microcalculator (Програмний мікрокалькулятор)

RSA - Rivest–Shamir–Adleman (Захист даних надійним ключем)

DHE - Diffie-Hellman Ephemeral (Тимчасове з’єднання)

SAE - Simultaneous Authentication of Equals (Протокол автентифікації та узгодження ключа)

PAKE - Password-Authenticated Key Exchange (Аутентифікація паролем)

RSNE - Radio Station Network Engineering (Інженерія мережевих радіостанцій)

IDE - Integrated Development Environment (Програмне забезпечення розробки)

SOC - Security Operations Center (Центр операцій безпеки)

OLED - Organic Light Emitting Diode (Органічний світловипромінювальний діод)

SDA - Serial Data Signal (Сигнал послідовних даних)

SCL - Serial Clock Signal (Послідовний тактовий сигнал)

FSK - Frequency Shift Keying (Частотна маніпуляція)

MASTER - Головний пристрій

SLAVE - Залежний пристрій

RADIO - Режим роботи з радіомодулем

WIFI - Режим роботи з Wi-Fi

ВСТУП

Війна це завжди перегони. Перегони по технологіям, їх використанню та потужності. І от що дивно... Як тільки створюється якась новітня зброя, якої ще не було, то від неї вже одразу намагаються створити захист. Так було у минулому, коли захищали тіло від стріл та мечів щитами, місто захищали високими стінами. Так і зараз, захищають тіло бронею, місто системами ППО, ПРО.

У 21 сторіччі, засобів для знищення один одного в цьому світі дуже багато. Ця зброя допомагає вбивати, шпигувати та допомагати військовим. З появою радіо та радіохвиль, стало набагато легше виконувати комунікацію між людьми, керувати пристроями.

Але, як і казав, як тільки з’являється якась зброя, то усі одразу намагаються зробити спосіб її перемогти. І так само, з’явилися комплекси РЕБ (Радіоелектронна боротьба). Які можуть перехоплювати керування, яке відбувається через радіохвилі, перехоплювати та отримувати сигнали від супротивника, погіршувати роботу підрозділів.

Наш супротивник у цій війні також використовує РЕБ, усюди де тільки можна. Це можуть бути як фальш цілі для ППО, щоб ті запустили свої локатори для пошуку цілей для збиття, або придушення зв’язку на позиціях військових. Перехоплення важливих даних, які можуть бути в етері у військових, блокування будь якого способу зв’язку, включаючи мобільний та багато інших функцій.

І я захотів створити пристрій, точніше групу пристроїв, які будуть допомагати військовим, забираючи на себе увагу РЕБ, та приймати на себе можливі удари артилерії чи будь якої іншої зброї, по місцях скупчення моїх пристроїв. Але для створення такого пристрою, треба розглянути основи, такі як принципи роботи частотних сигналів, WI-FI, принципи роботи РЕБ та інше.

1 ТЕОРЕТИЧНІ ОСНОВИ РОЗУМІННЯ ПРИНЦИПІВ РОБОТИ ЧАСТОТНИХ СИГНАЛІВ ТА МЕТОДІВ ЇХ ВИЯВЛЕННЯ

Світ довкола нас пронизаний частотними сигналами: від радіо та телебачення до мобільного зв'язку, GPS, Wi-Fi та безлічі інших технологій. Ці сигнали, що мають певну частоту та амплітуду, є основою для багатьох сучасних технологій.

Розуміння принципів роботи частотних сигналів та методів їх виявлення є ключовим для багатьох галузей науки і техніки. Знання про них дає можливість не лише використовувати їх у різних пристроях, але й досліджувати різноманітні явища, а також розробляти нові технології.

Існує три основних види модуляції частотних сигналів:

- амплітудна модуляція (AM): в цьому випадку амплітуда носія змінюється відповідно до інформаційного сигналу;

- частотна модуляція (FM): тут змінюється частота носія, а амплітуда залишається постійною;

- фазова модуляція (PM): змінюється фаза носія, а амплітуда та частота залишаються постійними.

Кожен з цих типів модуляції має свої особливості та застосовується у різних сферах. Наприклад, AM використовується в радіомовленні, FM - в телебаченні та мобільному зв'язку, а PM - в супутниковому зв'язку.

Генерація частотних сигналів - це процес створення коливань з певною частотою та амплітудою. Існує два основних методи генерації:

Генератори гармонійних коливань: ці пристрої генерують сигнали синусоїдальної форми з фіксованою частотою. Їх робота ґрунтується на принципах електричних коливальних контурів, що складаються з індуктивності та ємності. Різні типи генераторів гармонійних коливань, такі як LC-генератори, RC-генератори та кварцові генератори, використовуються

в широкому спектрі застосувань.

Синтезатори частот: ці пристрої генерують сигнали з широким спектром частот, використовуючи різні методи, такі як фазова модуляція або DDS (технологія прямого синтезу частоти). Синтезатори частот засновані на принципах цифрової обробки сигналів і дозволяють генерувати сигнали з високою точністю та стабільністю.

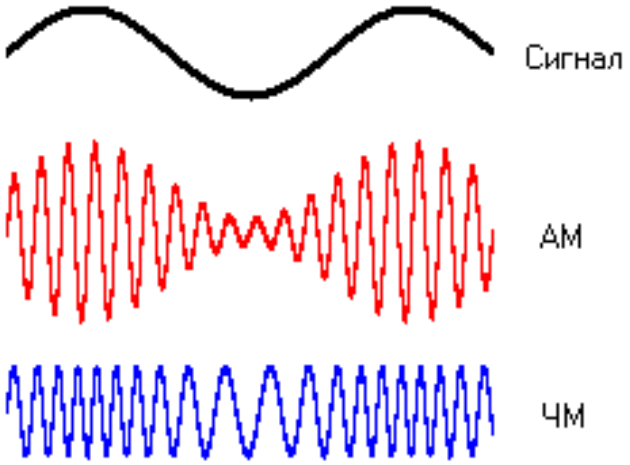

Рисунок 1.1 - Зображення амплітудної та частотної модуляції

Прийом частотних сигналів - це процес перетворення електромагнітних хвиль, що надходять від джерела, в електричні сигнали, які можуть бути оброблені далі. Для цього використовуються наступні компоненти:

Антенні системи: вони збирають електромагнітні хвилі та перетворюють їх в електричні сигнали. Різні типи антенних систем, такі як дипольні антени, параболічні антени та масивні антени, використовуються в залежності від діапазону частот та напрямку прийому.

Фільтри: вони виділяють сигнали потрібної частоти з шуму та інших небажаних сигналів. Різні типи фільтрів, такі як резонансні фільтри, активні фільтри та цифрові фільтри, використовуються для забезпечення чіткого прийому сигналу.

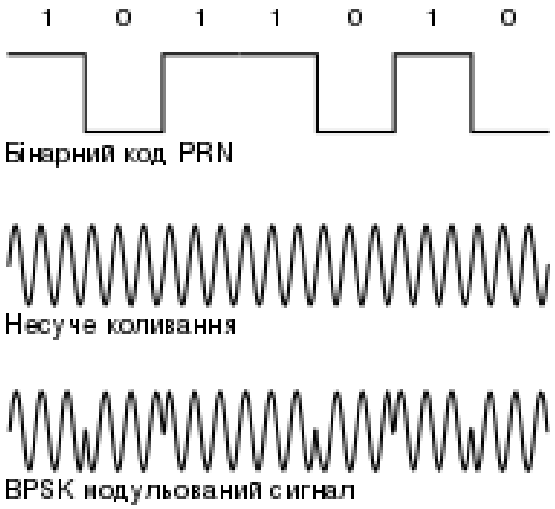

Рисунок 1.2 - Зображення фазової модуляції

Підсилювачі: вони збільшують амплітуду слабких сигналів, роблячи їх доступними для подальшої обробки. Різні типи підсилювачів, такі як транзисторні підсилювачі, мікрохвильові підсилювачі та оптичні підсилювачі, використовуються в залежності від діапазону частот та рівня сигналу.

Приймачі: вони перетворюють високочастотні сигнали, що надходять від антен та підсилювачів, в низькочастотні сигнали, які можуть бути оброблені далі. Різні типи приймачів, такі як супергетеродинні приймачі, програмно-визначені приймачі та приймачі прямого перетворення, використовуються в залежності від діапазону частот та складності сигналу.

Детектори: вони виділяють інформацію, що міститься в модульованому сигналі. Різні типи детекторів, такі як амплітудні детектори, фазові детектори та квадратурні детектори, використовуються в залежності від типу модуляції.

1.1 Частотні діапазони

Електромагнітний спектр - це широкий діапазон електромагнітних хвиль, що характеризуються своєю частотою та довжиною хвилі. Цей спектр

охоплює величезний діапазон, починаючи від низькочастотних хвиль, таких як радіохвилі, до високочастотного рентгенівського та гамма-випромінення. Для зручності роботи та вивчення електромагнітний спектр поділяють на окремі діапазони за частотою або довжиною хвилі.[1]

Основні діапазони частот:

- довгі хвилі (ДХ): частотний діапазон - 150 кГц - 300 кГц, довжина хвилі - 2000 м - 1000 м. Використовуються для передачі сигналів на великі відстані, але мають низьку якість звуку. Приклади застосування: радіомовлення на великі відстані, морська навігація;

- середні хвилі (СХ): частотний діапазон - 300 кГц - 1600 кГц, довжина хвилі - 1000 м - 190 м. Забезпечують краще покриття, ніж довгі хвилі, але сприйнятливі до атмосферних перешкод. Приклади застосування: радіомовлення середнього діапазону;

- короткі хвилі (КХ): частотний діазон - 3 МГц - 30 МГц, довжина хвилі - 100 м - 10 м. Мають здатність відбиватися від шарів іоносфери, що дозволяє здійснювати передачу на великі відстані. Приклади застосування: міжнародне мовлення, радіозв'язок на великі відстані;

- ультракороткі хвилі (УКХ): частотний діапазон - 30 МГц - 300 МГц, довжина хвилі - 10 м - 1 м. Забезпечують високоякісну передачу на менші відстані. Приклади застосування: FM-радіомовлення, аналоговий телевізійний сигнал, радіозв'язок;

- високочастотні (ВЧ) діапазони: частотний діапазон - 300 МГц - 300 ГГц, довжина хвилі - 1 м - 1 мм. Використовуються для різних цілей, таких як радіолокація, мобільний зв'язок, супутниковий зв'язок, Wi-Fi;

- надвисокочастотні (НВЧ) діапазони: частотний діапазон - 300 ГГц - 3000 ТГц, довжина хвилі - 1 мм - 0,1 мкм. Застосовуються в радарах, системах безпеки, медицині;

- інфрачервоне (ІЧ) випромінювання: частотний діапазон - 3000 ТГц - 430 ТГц, довжина хвилі - 0,1 мкм - 700 нм. Відчувається як тепло, використовується в пультах дистанційного керування, нічного бачення;

- видиме світло: частотний діапазон - 430 ТГц - 790 ТГц, довжина хвилі - 700 нм - 400 нм. Сприймається людським оком як різні кольори;

- ультрафіолетове (УФ) випромінювання: частотний діапазон - 790 ТГц - 30 ЕГц, довжина хвилі - 400 нм - 10 нм. Використовується для знезараження приміщень, засмаги;

- рентгенівське випромінювання: частотний діапазон - 30 ЕГц - 30 ЗЕ, довжина хвилі - 10 нм - 0,01 pm. Застосовується в медицині для діагностики;

- гамма-випромінювання: частотний діапазон - понад 30 ЗЕ.

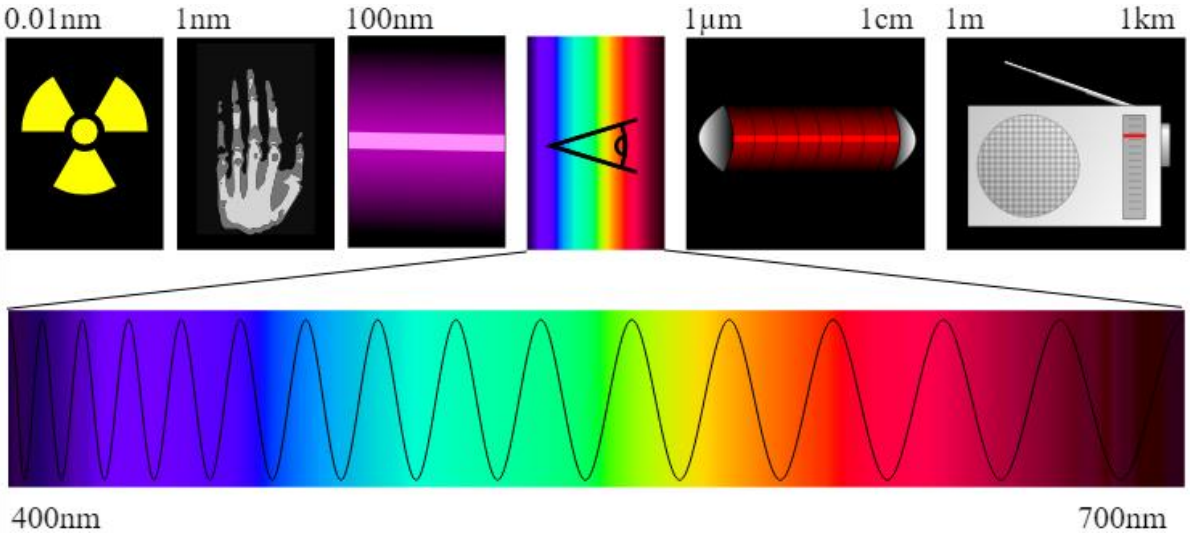

Рисунок 1.3 - Приклади частотних діапазонів

1.2 Особливості поширення радіохвиль в різних діапазонах

Поширення радіохвиль залежить від їх частоти, а точніше, від довжини хвилі. Різні діапазони радіохвиль мають різні особливості поширення, що впливає на їх практичне застосування.

Довгі (150 кГц - 300 кГц) та середні хвилі (300 кГц - 1600 кГц):

- добре огинають земну кулю, завдяки чому можливий зв'язок на великі відстані;

- сприйнятливі до атмосферних перешкод;

- використовуються для радіомовлення на великі відстані, морської навігації;

- менший радіус дії, ніж у ДХ, але краще покриття в межах певної території;

- сприйнятливі до атмосферних перешкод та промислових шумів;

- використовуються для радіомовлення середнього діапазону.

Короткі хвилі (3 МГц - 30 МГц):

- відбиваються від шарів іоносфери, що дозволяє здійснювати дальній зв'язок;

- якість сигналу залежить від стану іоносфери;

- використовуються для міжнародного мовлення, радіозв'язку на великі відстані.

Ультракороткі хвилі (30 МГц - 300 МГц):

- не огинають земну кулю, але забезпечують високоякісну передачу на менші відстані;

- стійкі до атмосферних перешкод;

- використовуються для FM-радіомовлення, аналогового телевізійного сигналу, радіозв'язку.

Високочастотні діапазони (300 МГц - 300 ГГц):

- широкий спектр застосувань, таких як радіолокація, мобільний зв'язок, супутниковий зв'язок, Wi-Fi;

- поширення залежить від конкретної частоти та умов середовища.

Надвисокочастотні діапазони (300 ГГц - 3000 ТГц):

- використовуються в радарах, системах безпеки, медицині;

- мають коротку довжину хвилі, що робить їх малопридатними для дальнього зв'язку.

Інші діапазони:

Інфрачервоне (ІЧ) випромінювання:

- відчувається як тепло;

- використовується в пультах дистанційного керування, нічного бачення.

Видиме світло:

- сприймається людським оком як різні кольори.

Ультрафіолетове (УФ) випромінювання:

- використовується для знезараження приміщень, засмаги.

Рентгенівське випромінювання:

- застосовується в медицині для діагностики.

Гамма-випромінювання:

- використовується в медицині та промисловості.

Додаткові фактори:

- рельєф місцевості: гори, ліси, будівлі можуть впливати на поширення радіохвиль;

- погодні умови: дощ, сніг, туман можуть погіршувати якість сигналу.

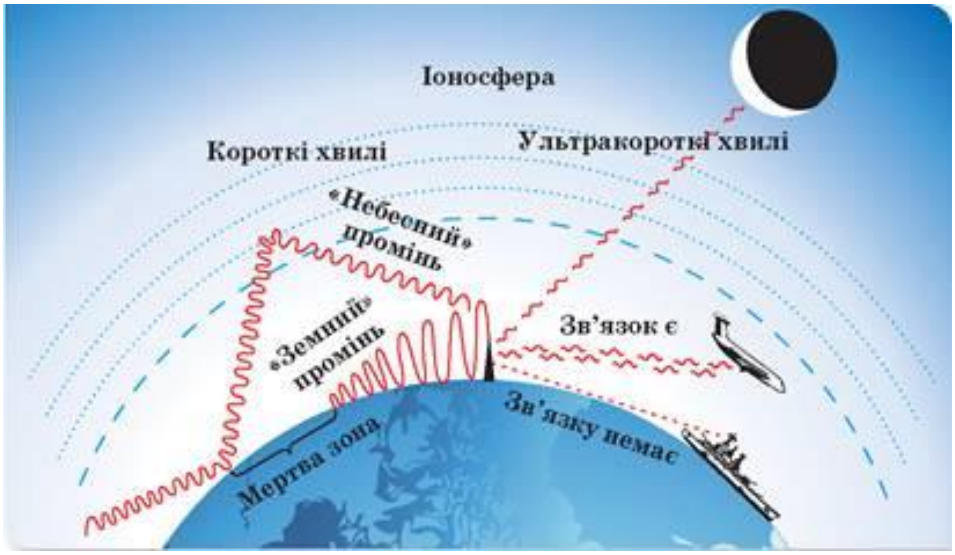

Рисунок 1.4 - Зображення діапазонів відносно планети

1.3 Використання частотних діапазонів для РЕБ

Радіоелектронна боротьба (РЕБ) - це комплекс заходів, спрямованих на порушення роботи радіоелектронних систем противника. Одним з ключових інструментів РЕБ є використання різних частотних діапазонів.

Рисунок 1.5 - Використання РЕБ для спущення дрону

Основні діапазони, що використовуються для РЕБ:

Низькочастотний (НЧ) діапазон - до 150 кГц. Використовується для постановки перешкод радіоелектронним системам, що працюють на наддовгих і довгих хвилях. Приклади: постановки перешкод системам навігації, радіомовлення.

Середньочастотний (СЧ) діапазон - 150 кГц - 3 МГц. Використовується для постановки перешкод радіоелектронним системам, що працюють на середніх хвилях. Приклади: постановки перешкод радіомовлення, авіаційному зв'язку.

Високочастотний (ВЧ) діапазон - 3 МГц - 30 МГц. Використовується для постановки перешкод радіоелектронним системам, що працюють на коротких хвилях. Приклади: постановки перешкод міжнародному мовленню,

дипломатичному зв'язку.

Ультрависокочастотний (УВЧ) діапазон - 30 МГц - 300 МГц. Використовується для постановки перешкод радіоелектронним системам, що працюють на УКХ. Приклади: постановки перешкод FM-радіомовленню, телебаченню, мобільному зв'язку.

Надвисокочастотний (НВЧ) діапазон - 300 МГц - 300 ГГц. Використовується для постановки перешкод радіоелектронним системам, що працюють на мікрохвильових частотах. Приклади: постановки перешкод радарам, системам наведення зброї.

Методи РЕБ:

Постановка перешкод: створення шумових або сигнальних перешкод, що забивають корисний сигнал.

Імітація сигналів: створення фальшивих сигналів, що вводять в оману радіоелектронні системи противника.

Пеленгація та виявлення: визначення місцезнаходження джерел радіовипромінювання противника.

Радіоелектронне придушення: виведення з ладу радіоелектронних систем противника.

Засоби РЕБ:

Станції постановки перешкод: генерують шумові або сигнальні перешкоди.

Системи імітації сигналів: генерують фальшиві сигнали, що імітують роботу радіоелектронних систем противника.

Пеленгатори: визначають місцезнаходження джерел радіовипромінювання.

Системи радіоелектронного придушення: генерують потужні імпульси, що виводять з ладу радіоелектронні системи противника.

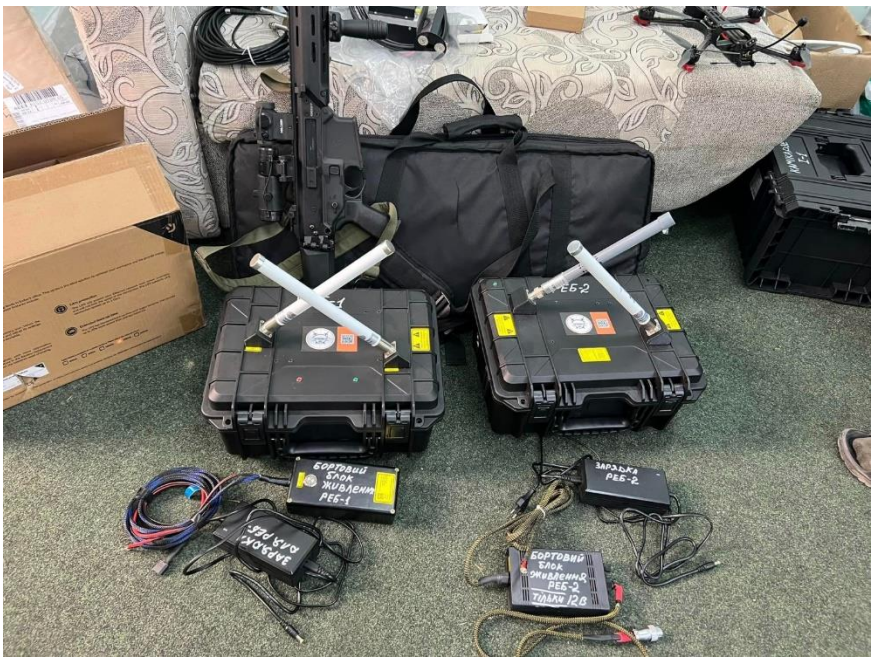

Рисунок 1.6 - Портативні засоби РЕБ для придушення дронів супротивника

1.4 Канали зв’язку

Канал зв'язку - це засіб передачі сигналів між пристроями, розташованими далеко один від одного в інформаційних деках. Сигнал (латинське signum-знак) - це інформація, представлена у вигляді певної фізичної величини з певним значенням або у вигляді зміни фізичної величини. При цифровій обробці інформації використовуються дискретні сигнали. Процес подання інформації у вигляді дискретних даних називається кодуванням. Відповідно до математичної сутності, кодування-це відображення будь-якого набору знаків a на інший набір знаків b, використовуючи встановлені правила. Цей код називається як правилом відображення, так і комбінацією різних кодів. Зворотне відображення (якщо воно існує) називається декодуванням. Комп'ютер використовує двійкове кодування букв будь-якого алфавіту. Кожному символу присвоюється база 1 відповідного розміру в 2 байта. Перетворення безперервного сигналу в дискретний сигнал здійснюється за допомогою аналого-цифрового перетворювача. Такі перетворення використовуються для створення з'єднань

з аналоговими комп'ютерами, наприклад, при обробці результатів вимірювань експериментальних досліджень, управлінні виробничими процесами. Інформація, що передається одиночним або послідовним сигналом, називається повідомленням. Система складається з 3 основних частин: передавача, приймача та лінії зв'язку. Передавач перетворює повідомлення в сигнал (модуляція), а приймач відновлює повідомлення з сигналу (Демодуляція). Лінія зв'язку-це фізичне середовище певної довжини, яке передає сигнал. Середовище в основному має штучне походження, наприклад, металевий дріт, хвилевід, скловолокно, але також є природним, наприклад, вакуум, повітря, вода.

Передача енергії завжди супроводжується розсіюванням частини енергії. Величина, пропорційна логарифму відношення потужності прийнятих і переданих сигналів, називається загасанням. Основою його роботи є поширення акустичних або електромагнітних коливань по лініях зв'язку у вигляді імпульсів (дискретних сигналів) або синусоїдальних гармонік (безперервних сигналів). Суперпозиція сигналу в залежності від часу в процесі первинного коливання полягає в зміні амплітуди, частоти і фази коливання, що називається амплітудною, частотною і фазовою модуляцією відповідно.

Модуляція в частотному діапазоні коливального процесу, в якому загасання сигналу приблизно однаково для будь-якої частоти, називається смугою пропускання смуги частот. У діапазоні частот, в якому загасання сигналу є приблизно однаковим для будь-якої частоти, називається смугою пропускання. Він визначається в грудні в діапазоні частот телефонів 300-3400 Гц, мовлення — 30 Гц — 15 кГц, телебачення — 50 Гц—5 МГц, оптоволокна — до ста МГц. В обчислювальній техніці ЦП використовується для передачі двійкової інформації між процесорними вузлами (ш декою, магістраллю), процесорами і зовнішніми пристроями (селективний ЦП), зв'язком комп'ютер-термінал (локальна мережа) і віддаленим зв'язком комп'ютер-комп'ютер (регіональна і глобальна для мережі). Пропускна

здатність або швидкість цифрового процесора визначається кількістю бітів інформації, що передаються за одиницю часу. Одиниця швидкості 1 біт / сек називається бодом. Внутрішня магістраль комп'ютера визначається його тактовою частотою на основі елементів і працює зі швидкістю десятки Мбіт / с.багатоканальні канали дозволяють процесорам підключатися до декількох зовнішніх пристроїв (дисплеїв, принтерів і т. д.).) Дозволяє підключатися.) в той же час.).

Продуктивність ЦП в локальній мережі залежить від його конструкції і коливається від декількох Кбіт / дек до 10 Мбіт/ с.у той же час зв'язок відрізняється виділеною лінією (постійно фіксованою) і каналом, який автоматично перемикає деякі лінії зв'язку при підключенні (наприклад, телефонний зв'язок).). Радіоканали все частіше використовуються в локальних мережах.

1.4.1 Концепція каналів зв'язку

Цифровий канал-це бітовий канал з цифровим (імпульсним) сигналом на вході і виході каналу. Безперервний сигнал подається на вхід аналогового каналу, і безперервний сигнал також виводиться з його виходу (рис. 1.7). Як відомо, сигнали характеризуються своєю формою подання.

Рисунок 1.7 – Цифрові й аналогові канали передачі

Цифрові канали-це ICM, ISDN, канали типу T1 / E1 та інші. Новий Spd

побудований на цифрових каналах і має багато переваг перед аналоговими каналами.

Аналогові канали є найбільш поширеними через їх тривалого історичного шляху розвитку і простоти реалізації. Типовим прикладом аналогового каналу є груповий канал, що складається з тонального частотного каналу та 12, 60 або більше тональних частотних каналів. Телефонна мережа з комутацією загального доступу, як правило, містить велику кількість комутаторів, розподільних пристроїв, групових модуляторів і демодуляторів. У такій мережі канал передачі (його фізичний маршрут і деякі параметри) змінюється при кожному наступному виклику.

При передачі даних пристрій повинен вводити Аналоговий канал, який перетворює цифрові дані з DTE в аналоговий сигнал, який буде передаватися по каналу. Приймач повинен містити пристрій, який перетворює отриманий безперервний сигнал в цифрові дані. Ці пристрої є модемами. Аналогічним чином, при передачі по цифровому каналу дані повинні бути перетворені в формат, прийнятий для цього конкретного каналу. Це перетворення можна здійснити за допомогою адаптера ISDN, канального адаптера E1 / T1, лінійного драйвера тощо.

1.4.2 Типи каналів зв'язку

Основні канали: Лінія зв'язку: телефонний кабель, волоконно-оптичний кабель. Електричний канал: канал зв'язку, що використовує електричні сигнали. Бездротові канали: Радіоканал: канал зв'язку, який використовує радіосигнали. Супутникові канали: канали зв'язку з використанням супутників. Оптичний канал: канал зв'язку, що використовує оптичний сигнал. Пропускна здатність каналу зв'язку-це максимальна швидкість, з якою інформація передається по каналу зв'язку без помилок. Він вимірюється в бітах в секунду або в символах в секунду.

Фактори, що впливають на якість передачі даних: шум може

спричинити помилки при передачі інформації та зменшити пропускну здатність. Перешкоди: перешкоди від інших сигналів також можуть зменшити пропускну здатність. Канал зв'язку має фізично обмежену пропускну здатність, яка визначається його характеристиками.

Метод кодування: спосіб кодування інформації може вплинути на пропускну здатність.

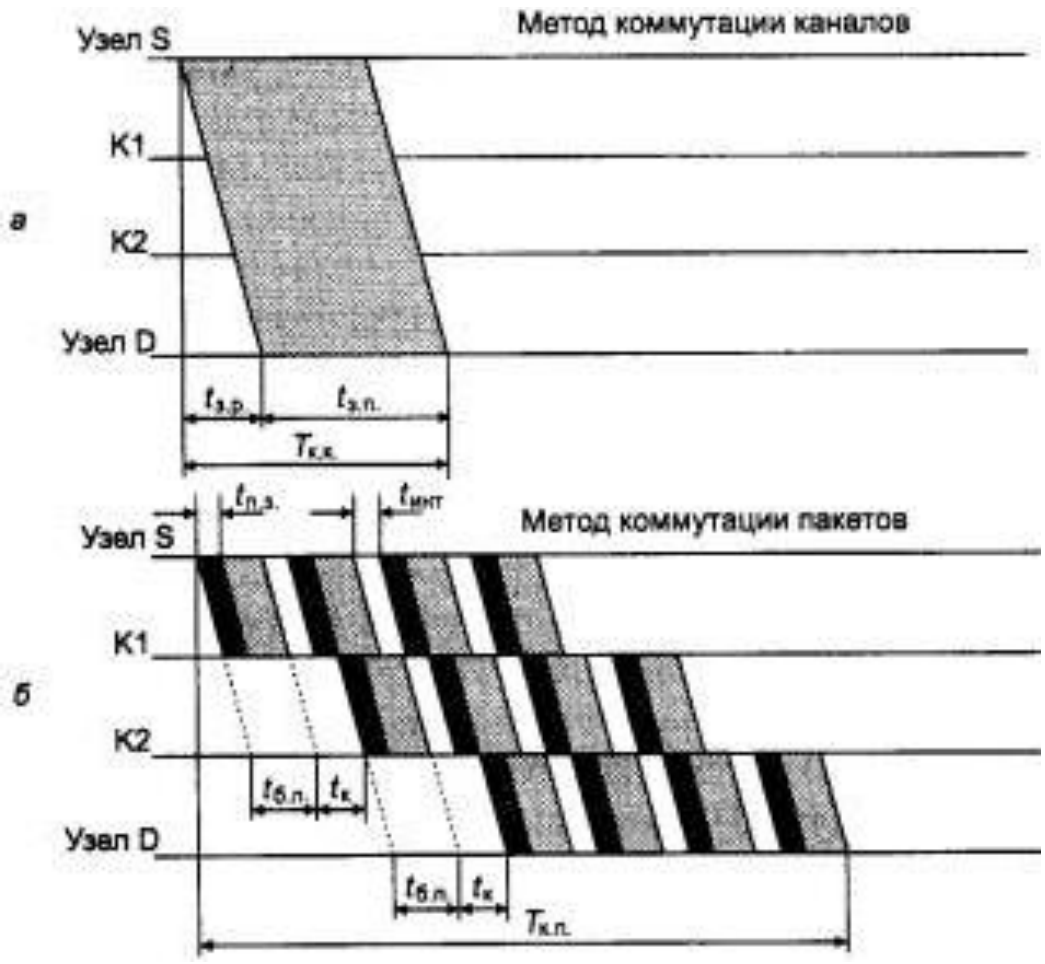

Рисунок 1.8 - Приклад пропускної здатності каналів

1.5 Огляд та класифікація радіостанцій

Радіостанція - це пристрій, який використовується для передачі та прийому радіохвиль. Зв'язок - мобільний зв'язок, радіозв'язок, диспетчерський зв'язок. Мовлення: радіомовлення, телебачення. Навігація -

GPS, ГЛОНАСС. Радіолокація - виявлення та визначення координат об'єктів.

1.5.1 Призначення та класифікація радіостанцій

Класифікація радіостанцій. За призначенням – базові - стаціонарні радіостанції, що використовуються для забезпечення зв'язку на великій відстані. Мобільні: портативні радіостанції, що використовуються для зв'язку на невеликій відстані. Переносні: радіостанції малого розміру, що використовуються для особистого зв'язку.

Рисунок 1.9 - Мобільна радіостанція

За типом сигналу - аналогові: радіостанції, що передають аналоговий сигнал. Цифрові: радіостанції, що передають цифровий сигнал. За частотним діапазоном - ДВ: довгохвильові радіостанції. СВ: середньохвильові радіостанції. КВ: короткохвильові радіостанції. УКВ: ультракороткохвильові радіостанції.

1.5.2 Основні характеристики радіостанцій

Потужність - визначає дальність зв'язку. Чим вища потужність, тим більша дальність зв'язку.

Важливо знати, що потужність радіостанції обмежена правилами та нормами, встановленими у вашій країні.

Чутливість - визначає мінімальну потужність сигналу, який може бути прийнятий. Чим вища чутливість, тим краще радіостанція може приймати слабкі сигнали.

Частотний діапазон - визначає частоти, на яких може працювати радіостанція.

Різні частотні діапазони мають різні характеристики, такі як дальність зв'язку, проникність через перешкоди, шумозахищеність.

Модуляція визначає метод кодування інформації в радіосигнал. Існує багато різних типів модуляції, кожен з яких має свої переваги та недоліки.

Дальність зв'язку визначає максимальну відстань, на якій можливий зв'язок. Дальність зв'язку залежить від потужності радіостанції, чутливості приймача, частотного діапазону, умов поширення радіохвиль.

Функціональні можливості - шифрування сигналу: забезпечує конфіденційність зв'язку. Шумозаглушення покращує якість зв'язку в умовах шуму. GPS дозволяє визначити координати радіостанції. Дисплей відображає інформацію про параметри роботи радіостанції. Інші - VOX, DTMF, Roger Beep, тощо.

1.5.3 Типи радіосигналів

На підставі цієї класифікації можна виділити наступні 4 типи сигналів:

- аналоговий або безперервний - безперервний у часі і набір значень;
- дискретизація-дискретна за часом і безперервна по набору значень;
- квантування-набір значень, які є безперервними і дискретними в часі;

- цифровий-дискретний одночасно в діапазоні часу і значень.

Отже, будь-яке первинне повідомлення може бути перетворено в будь-який з 4 перерахованих вище типів сигналів. Наприклад, первинне повідомлення у вигляді безперервного аудіосигналу може бути перетворено:

- аналоговий електричний сигнал перетворюється на Sa (t), і його миттєве значення пропорційне інтенсивності звуку (рисунок 1.10 а);

- дискретизований сигнал sD (t) являє собою коротку послідовність імпульсів, амплітуда яких пропорційна інтенсивності звуку в дискретні моменти часу;

- у квантованому сигналі s c(t) являє собою послідовність швидких змін з прийнятним постійним значенням, що відповідає миттєвому значенню аудіосигналу з допуском;

- цифровий сигнал sc(t), що представляє собою послідовність коротких імпульсів, отримує прийнятне постійне значення, амплітуда якого відповідає миттєвому значенню аудіосигналу з певним допуском.

Основне повідомлення може бути перетворено в один з 4 можливих типів сигналів: Аналоговий, дискретизуючий, квантуючий і цифровий.

Найбільш поширеними є аналогові і цифрові сигнали. Оскільки методи здійснення операцій з передачі, обробки, зберігання і відтворення інформації, представленої аналоговими і цифровими сигналами, принципово різні, в інформаційній електроніці існує цілий ряд аналогових і цифрових електронних засобів, які стосуються методів технічного застосування, принципів конфігурації і проектування пристроїв і систем, що виконують різні функції. аналогові та цифрові операції. Ви можете виділити 2 аспекти електроніки.Кожен з них. Цифровий сигнал.

Аналогова та цифрова електроніка - це 2 сфери інформаційної електроніки.

Залежно від тривалості проміжку часу, протягом якого присутній сигнал, розрізняють безперервний (тривалий) сигнал і імпульсний сигнал.

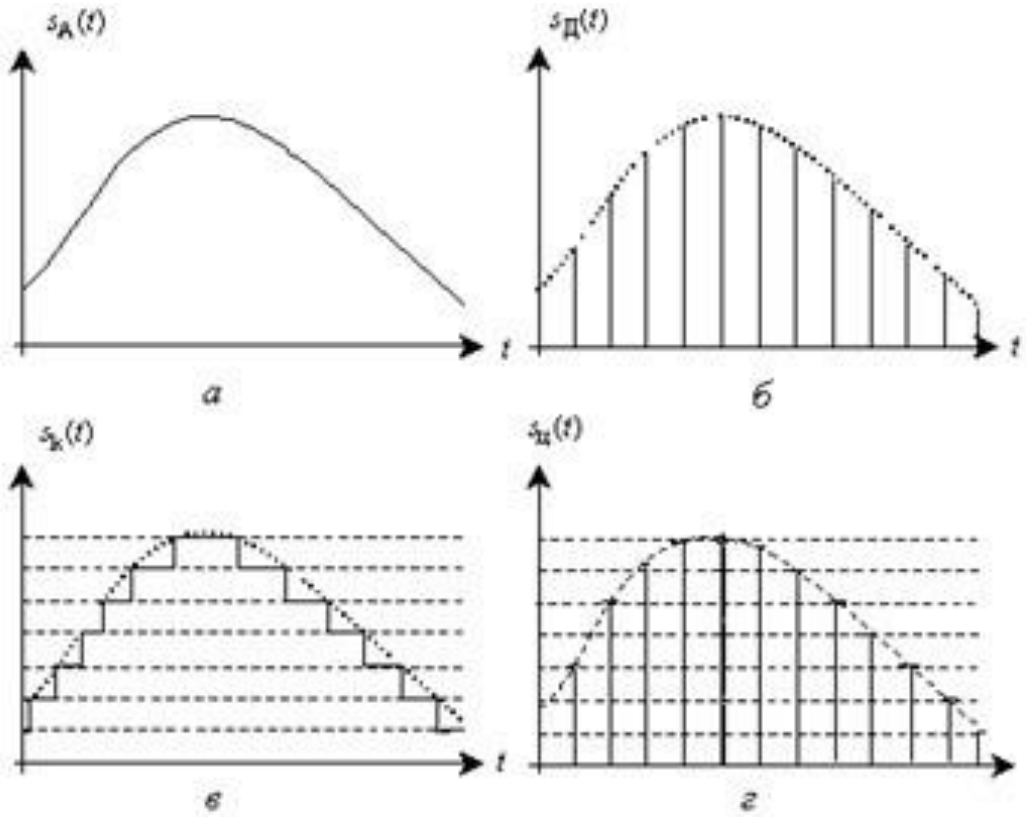

Рисунок 1.10 - аналоговий (а), дискретизований (б), квантований (в) та цифровий (г) сигнали, які відповідають одному й тому ж первинному повідомленню

Безперервні сигнали теоретично існують протягом нескінченного періоду часу. Фактичний сигнал має початок і кінець і не може вважатися безперервним. Однак в більшості випадків досить довгостроковий сигнал вважається безперервним.

Імпульсні сигнали (поодинокі імпульси) існують лише протягом короткого періоду часу, і в усі інші моменти часу їх значення дорівнюють нулю.

Всі реальні фізичні сигнали є дійсними функціями часу, але в залежності від потреб аналітичного методу найчастіше використовуються наступні методи математичної ідентифікації:

- визначення сигналу як функції часу-визначення часу;

- визначення сигналу як функції частоти-визначення частоти (спектра);

- визначення сигналу в операторній формі - визначення оператора.

У більшості випадків, щоб спростити аналіз проходження сигналу через електронне коло, можна визначити сигнал як набір елементарних (найпростіших) сигналів, обраних певним чином: гармонійні коливання, поодинокі скачки (функція Хевісайда), дельта-імпульси (функція Дірака). Гармонічні коливання використовуються для визначення частоти (спектра) сигналу, а одиночні стрибкоподібні та дельта-імпульси використовуються для визначення часу, також відомого як динамічна ідентифікація.

Способи математичного опису реальних сигналів:

- часовий;
- частотний;
- операторний.

1.5.4 Сигнали радіостанцій та Wi-Fi

Радіостанції та Wi-Fi використовує радіохвилі для передачі інформації, але роблять це по-різному.

Радіостанції передають сигнали на великі відстані. Використовують широкий спектр частот. Можуть передавати звук, даний, або і те, й інше. Сигнали можуть бути амплітудно-модульовані (AM), частотно-модульовані (FM), або фазово-модульовані (PM).

AM та FM - це аналогові сигнали, які можуть бути сприйнятливі до шуму та перешкод. PM - це цифровий сигнал, який більш стійкий до шуму та перешкод.

Радіо-це загальна назва методу радіопередачі та отримання інформації з використанням електромагнітних хвиль у радіочастотному діапазоні. Інформація використовується в системах бездротового зв'язку, радіомовленні, телебаченні, радіокеруванні, активних радарах тощо. У пасивних радарах, системах пеленгації і подібних системах береться тільки інформація. Слово радіо також скорочується до радіомовлення, засобу

масової інформації, призначеного для широкої аудиторії, та домашнього радіо.

Радіозв'язок використовує сигнали в радіочастотному діапазоні, тобто частоти, які набагато вище, ніж у акустичних сигналів. Таким чином, для реалізації передачі акустичний сигнал накладається на високочастотну базу, модулюється при прийомі, демодулюється і відтворює вихідний сигнал. [2]

Наприклад, при передачі аудіоінформації голос оператора генерує акустичну звукову вібрацію, яка перетворюється в відповідну електричну вібрацію звукової частоти в мікрофоні — це модульований сигнал, що надходить в передавальний пристрій. Виникають гармоніки, які називаються носячими вібраціями (призначеними для "перенесення" інформації в просторі), частота яких значно перевищує частоту модульованого сигналу. Один або кілька параметрів носяться коливань (амплітуда, частота, фаза) змінюються у відповідь на зміни модульованого сигналу. Модульована носна вібрація поширюється в космос передавальною антеною у вигляді електромагнітних хвиль. Разом з багатьма іншими радіохвилями від інших передавальних пристроїв і джерел перешкод вони досягають приймальної антени радіоприймача: природної (в основному блискавки) і штучної. Приймач вибирає (вибирає), підсилює і демодулює (виявляє) вібрацію переданої модульованої несучої. В результаті виходить електрична вібрація звукової частоти, яка відтворює голос оператора в динаміці.

Wi-Fi - це знайомий метод бездротового зв'язку, заснований на електромагнітному випромінюванні. Сигнали Wi-Fi класифікуються як радіохвилі відповідно і мають однакові характеристики, характеристики та поведінку. Радіохвилі дотримуються майже тих самих законів фізики, що і світло: вони поширюються в космосі з однаковою швидкістю (близько 300 000 кілометрів на секунду) і можуть зазнавати дифракції, поглинання, загасання, розсіювання тощо.

Отже, основними характеристиками радіохвиль, основними характеристиками сигналів Wi-Fi є їх довжина і частота (грудень частот).

Останній параметр відноситься до частоти змінного струму, необхідної для генерації хвилі бажаної довжини, яка використовується для класифікації радіохвиль. Іншим визначенням частоти є кількість хвиль, що проходять через певну точку простору за 1 секунду.

Вони посилають сигнали з невеликої відстані. Використовують вузький частотний спектр. Надсилають лише дані. Сигнал завжди цифровий. Wi-Fi дозволяє використовувати кілька пристроїв, що використовують технологію розподіленого множинного доступу за кодом (CDMA)

1.5.5 Властивості Wi-Fi сигналу

Основною умовою створення бездротової мережі на відстані більше 100 метрів є пряма видимість між точками установки обладнання. Простіше кажучи, якщо ви стоїте біля 1 точки доступу Wi-Fi, 2. лінія прямої видимості, спрямована в точку, спрямована на стіни, ліси, багатоповерхові будівлі, насипи і т.д. він не повинен нахилятися.

Такі об'єкти відображають і поглинають сигнал Wi-Fi, що становить лише левову частку, якщо не всі з них.

Те ж саме відбувається в кімнатах, де сигнали від маршрутизаторів Wi-Fi або точок доступу проходять через стіни в інші кімнати / на інші поверхи. Кожна стіна або стеля отримує певну кількість сигналу від сигналу.

Наприклад, на невеликій відстані від маршрутизатора в кімнаті до ноутбука радіосигнал може проходити через стіну і досягати пункту призначення. Але на великій відстані в кілька кілометрів таке скорочення робить значний вплив на якість і дальність зв'язку Wi-Fi.[3]

Швидкість спотворення сигналу Wi-Fi при проходженні перешкод залежить від декількох факторів:

Таблиця 1.1 - Порівняння сигналу Wi-Fi та радіосигналу

Характеристика	Радіостанції	Wi-Fi
Дальність	Велика	Коротка
Спектр частот	Широкий	Вузький
Тип інформації	Звук, дані	Дані
Модуляція	AM, FM, PM	Цифрова
Стійкість до шуму	AM/FM: низька	Цифрова: висока
Множинний доступ	Немає	CDMA

Довжина хвилі. Теоретично, чим довша довжина хвилі (і чим нижча частота Wi-Fi), тим більшим буде проникнення сигналу. Таким чином, Wi-Fi в діапазоні 2,4 ГГц матиме більш високу швидкість проникнення, ніж в діапазоні 5 ГГц. У реальних ситуаціях застосування цього правила дуже тісно пов'язане з перешкодами структури та конфігурації, через які проходить сигнал.

Такі об'єкти відображають і поглинають сигнал Wi-Fi, що становить лише левову частку, якщо не всі з них.

Те ж саме відбувається в кімнатах, де сигнали від маршрутизаторів Wi-Fi або точок доступу проходять через стіни в інші кімнати / на інші поверхи. Кожна стіна або стеля отримує певну кількість сигналу від сигналу.

Наприклад, на невеликій відстані від маршрутизатора в кімнаті до ноутбука радіосигнал може проходити через стіну і досягати пункту призначення. Але на великій відстані в кілька кілометрів таке скорочення

робить значний вплив на якість і дальність зв'язку Wi-Fi.

Таблиця 1.2 - Порівняння сигналу WI-FI відносно перешкоди

Перешкода	Додаткові втрати при проходженні (dB)	Відсоток ефективної відстані*, %
Відкритий простір	0	100
Нетоноване вікно (відсутнє металізоване покриття)	3	70
Вікно з металізованим покриттям (тонуванням)	5-8	50
Дерев'яна стіна	10	30
Стіна 15,2 см (міжкімнатна)	15-20	15
Стіна 30,5 см (несуча)	20-25	10
Бетонна підлога або стеля	15-25	10-15
Цілісне залізобетонне перекриття	20-25	10

Швидкість спотворення сигналу Wi-Fi при проходженні перешкод залежить від декількох факторів:

Довжина хвилі. Теоретично, чим довша довжина хвилі (і чим нижча частота Wi-Fi), тим більшим буде проникнення сигналу. Таким чином, Wi-Fi в діапазоні 2,4 ГГц матиме більш високу швидкість проникнення, ніж в діапазоні 5 ГГц. У реальних ситуаціях застосування цього правила дуже тісно пов'язане з перешкодами структури та конфігурації, через які проходить сигнал. [4]

1.6 Методи розпізнавання сигналів

Існує багато методів розпізнавання радіосигналів, які можна поділити на дві основні категорії:

- методи, засновані на параметрах сигналу: частота, амплітуда, фаза, потужність та смуга пропускання;

- методи, засновані на структурі сигналу: модуляція, формат сигналу кодування.

Вибір методу розпізнавання радіосигналів залежить від: типу сигналу, наявності шуму, точності розпізнавання.

Деякі з найпоширеніших методів розпізнавання радіосигналів: алгоритм швидкого перетворення Фур'є (FFT), метод опорних векторів (SVM) та нейронні мережі.

1.7 Вплив РЕБ на сигнали

Радіоелектронна боротьба-це сукупність дій, координованих цілями, місцями і часом: розташування радіоелектронних засобів (РЕЗ), система управління силами і озброєнням противника, знищення всіма доступними засобами ураження, а також захист власних РЕЗ і систем управління від дій противника (протирадіоелектронна реакція).

Електронна війна визначається як реакція в складних умовах електромагнітного середовища, в результаті якої всі радіочастотні елементи розглядаються як елементи електронної війни. Електромагнітні ефекти охоплюють різні аспекти середовища радіоелектронної боротьби, від радіолокаційних систем і генераторів перешкод до систем військового зв'язку.

Метою радіоелектронної боротьби є порушення управління силами противника, зниження ефективності їх розвідки, використання військової

техніки та забезпечення стабільності їх власних систем.

Рисунок 1.11 - Українські системи РЕБ

Зазвичай перед застосуванням засобів радіоелектронної боротьби потрібна ретельна розвідка: ідентифікація РЕЗ з випромінюванням противника, визначення координат, аналіз характеристик випромінюваного сигналу. Збір таких даних ведеться на постійній основі, в тому числі в мирний час. У той же час бувають випадки, коли одна сторона намагається використовувати засоби радіоелектронної боротьби проти іншої сторони для застосування певних методів на майбутнє.

Придушення: електронна боротьба може бути використана для придушення радіосигналів, що робить їх нечитабельними. Це може бути досягнуто шляхом генерації сигналу, який блокує шум або бажаний сигнал.

Перешкоди: радіоелектронна боротьба може використовуватися для перешкод радіосигналів, що робить управління менш руйнівним. Цього можна досягти, генеруючи сигнал, подібний до бажаного сигналу, але з невеликою різницею.

Рисунок 1.12 - Візуалізація впливу систем РЕБ на аеродром

Обман: електронна війна може бути використана для того, щоб обдурити радіоприймачі, думаючи, що вони отримують сигнал від іншого джерела. Це може бути досягнуто шляхом генерації помилкового сигналу.

Електронна війна може використовуватися для крадіжки, перехоплення та використання радіосигналів без дозволу.

Вплив радіоелектронної боротьби на радіосигнали може мати серйозні наслідки:

Втрата зв'язку: електронна війна може призвести до втрати зв'язку між військовими підрозділами, урядовими установами та цивільними особами. декомунізація.

Відмова системи: це може призвести до збоїв в роботі систем, заснованих на радіосигналах, таких як системи радіоелектронної боротьби, GPS, навігації та управління повітряним рухом.

Витік інформації: електронна війна може бути використана для перехоплення конфіденційної інформації, що передається через радіосигнали.

1.8 Види боротьби з РЕБ

Заходи захисту:

- шифрування: коли ви шифруєте передані дані, вони стають нечитабельними для системи;

- стрибкоподібна перебудова частоти: зміна частоти сигналу ускладнює визначення його напрямку.

Спрямована антена - коли сигнал фокусується в певному напрямку, він фокусується в певному напрямку, що ускладнює перехоплення сигналу. Щит - захист електронних пристроїв від зовнішніх сигналів. Дисципліна радіоелектронної боротьби: дотримання правил, що стосуються радіообладнання.

Активні контрдії:

- система виявлення і транспортування: джерело радіоелектронної боротьби і визначення місця розташування;

- система глушіння: генерація або придушення шуму радіоелектронної боротьби;

- оманливі системи: генерує помилкові сигнали, щоб ввести систему в оману.

2 АНАЛІЗ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ДЛЯ ПРОЦЕСУ РАДІО ТА WIFI ОБМІНУ МІЖ ПРИСТРОЯМИ

2.1 Огляд бездротових технологій

У цьому розділі буде оглянуто бездротові технології, досліджуючи їхні принципи роботи, переваги, недоліки та сфери застосування.

2. 1. 1 Радіочастотні технології

Радіочастотні технології (RFT) - це широкий спектр методів, які використовують електромагнітні хвилі в грудні в діапазоні від 3 кГц до 300 ГГц для надсилання та отримання інформації. Ці хвилі, відомі як радіочастотні (РЧ) хвилі, є частиною електромагнітного спектра, який знаходиться між інфрачервоним і мікрохвильовим випромінюванням.

Електромагнітні хвилі: радіочастотні хвилі складаються з коливань електричного і магнітного полів, які поширюються перпендикулярно один одному в просторі. Вони характеризуються частотою (вимірюється в герцах, Гц), довжиною хвилі (вимірюється в метрах, м) і амплітудою (вимірюється в вольтах, В).

Випромінювання та прийом: радіочастотні хвилі генеруються коливаннями струму або навантаження антени. Ці коливання створюють електричне поле, яке створює магнітне поле, і навпаки. Ці Взаємодіючі поля створюють електромагнітні хвилі, які можуть поширюватися в просторі. Радіохвилі підхоплюються антенами, які перетворюють енергію електромагнітних хвиль в електричні сигнали.

Передача інформації: сама радіочастотна хвиля не передає інформацію. Радіочастотні хвилі необхідно модулювати для передачі даних, таких як голос або текст. Модуляція - це процес, за допомогою якого радіочастотні

хвилі (амплітуда, частота, фаза тощо) перетворюються в) - це процес зміни певних властивостей.) залежно від переданих даних.

Типи модуляції: існує багато типів модуляції, кожен з яких має свої переваги та недоліки. Дека AMI-це тип фазової модуляції, який включає фазову модуляцію (FM), фазову модуляцію (FM), амплітудну модуляцію (AM) та фазову модуляцію (FM).

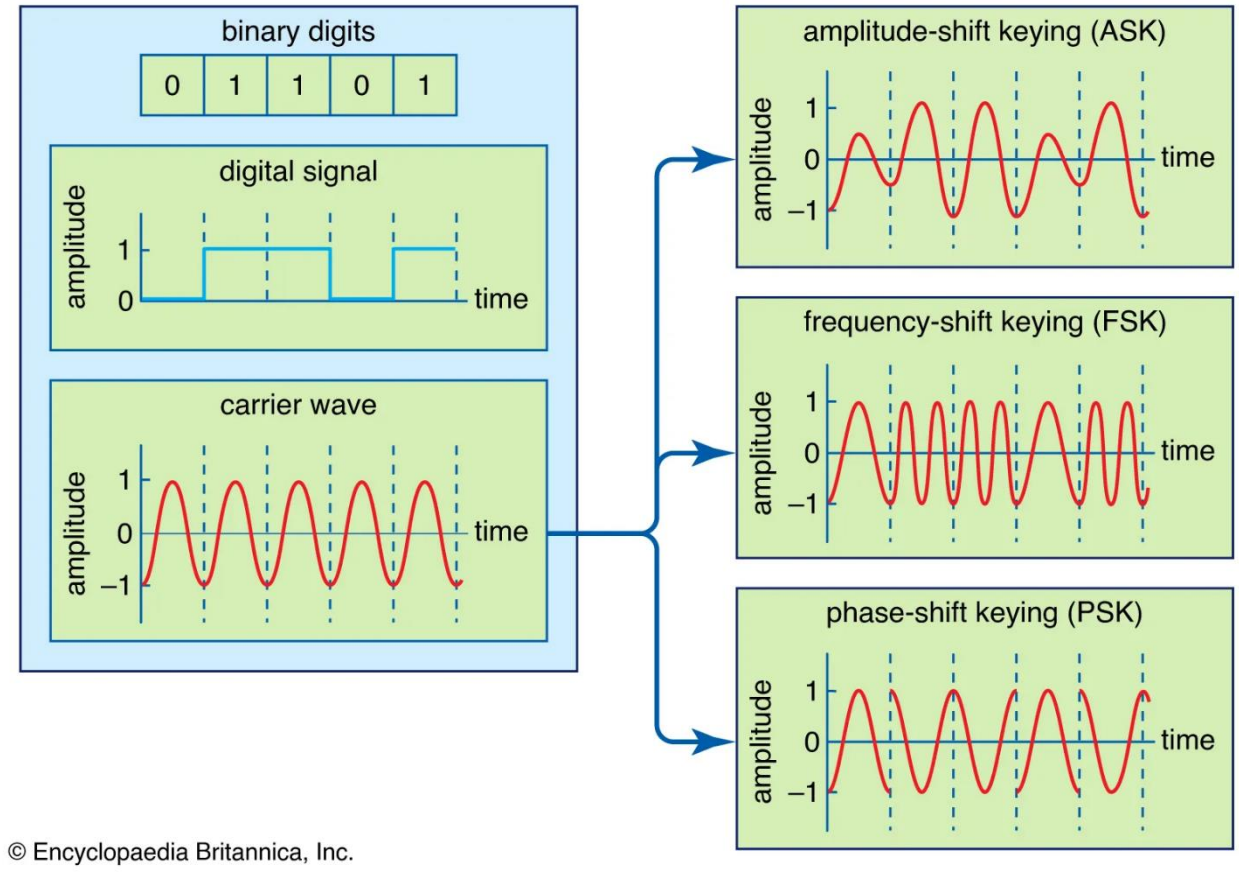

Рисунок 2.1 - Приклад модуляції

Бездротовий передавальний пристрій складається з самого передавача та передавальної антени. Передавальна антена призначена для перетворення високочастотного струму в енергію електромагнітного випромінювання, а приймальна антена призначена для перетворення прийнятого електромагнітного випромінювання в енергію високочастотного струму. Характер процесів, що відбуваються в передавальної і приймальної антенах,

визначає їх оборотність.Тобто одна і та ж антена може використовуватися як для передачі, так і для прийому.

Передавач класифікується в залежності від призначення, грудня хвилі, випромінюваної потужності, типу кондиціонування сигналу, типу випромінювання і умов експлуатації.

Призначення передавача залежить від системи, в якій використовується передавач. Залежно від призначення, передавач може передавати аудіо, телевізор, місцезнаходження, телеметрію, навігацію тощо.

Радіо передає в кілометровому, гектометровому, декаметровому, метровому та дециметровому діапазонах хвиль.

Перші три діапазони традиційно використовують амплітудну модуляцію з кроком сітки на робочій частоті 10 кГц, а останні два діапазони використовують широкосмугову частотну модуляцію з кроком сітки на робочій частоті 250 кГц.

Найпоширенішими трансляціями є метрові хвилі в діапазонах 65,8-74,0 МГц (4,56-4,05 м) і 87,5-108,0 МГц (3,43-2,78 м) з використанням методів частотної модуляції.[5]

Трансляція російського телебачення здійснюється в метрових, дециметрових і сантиметрових хвилях.

Для телевізійної передачі призначені п'ять піддіапазонів метрового і дециметрового діапазонів: I (48,5-66 МГц), II (76-100 МГц), III (174-230 МГц), IV (470-622 МГц) , V (622).

-958 МГц) з понад 70 каналами.

Для кабельного телебачення додано канали SK1SK8 і SK11SK18, що охоплюють діапазони 110-174 МГц і 230-294 МГц.

Активно розвиваються системи бездротового зв'язку, які використовують мікрохвильові радіохвилі.

Здатність цих хвиль проникати в іоносферу використовується для зв'язку з системами супутникового телебачення та космічними апаратами.

Для всіх систем супутникового радіозв’язку Міжнародний комітет

реєстрації частот (μRh) призначив такі діапазони частот у діапазоні ГГц: 5 (1 930-2 700); 5 725-7 075); Залежно від середньої випромінюваної потужності переданого радіосигналу передавач може бути дуже низької потужності (менше 3 Вт), малої потужності (3-10 Вт), середньої потужності (10 500 Вт) або високої потужності (від 0,5 до 10 Вт).

10 кВт), диференційовані на надпотужність.

Велика потужність (більше 10 кВт).

Залежно від типу модуляції сигналу передавачі (і приймачі) поділяються на пристрої з амплітудною (симетричною та односмуговою), частотною, фазовою, імпульсною, квадратурною, черезсигнальною та іншими видами модуляції.

Залежно від виду випромінювання розрізняють передавачі, що працюють в безперервному режимі і в імпульсному режимі.

У першому випадку при відправленні повідомлення сигнал надсилається безперервно, а в другому – безперервно.

У цьому випадку передача відбувається у вигляді радіоімпульсів.

Передавачі доступні стаціонарного типу, типу польоту (космічні, корабельні, авіаційні, автомобільні) і портативного типу (портативні) залежно від умов використання.

грудень Основні параметри передавача включають ефективність, частотний діапазон, робочу частотну сітку, фіксовану смугу частот випромінювання, стабільність частоти коливань несучої, бічні та позасмугові випромінювання, коефіцієнти нелінійних спотворень, електромагнітну сумісність тощо.

$$\eta = \frac{P_a}{P_0} \tag{1}$$

Ра - середня потужність коливань в антені; Ро - потужність, споживана пристроєм від всіх джерел живлення. ККД сучасних передавачів досягає 30-40%, причому він зростає зі збільшенням випромінюваної потужності.

Передавачі працюють на фіксованих частотах в діапазоні частот несучих коливань де N - число частот всередині цього діапазону (рис. 2.2).

Крок сітки робочих частот в заданому діапазоні визначають як

$$\Delta f = \frac{(f_N - f_1)}{(N-1)},\ N \geq 2 \qquad (2)$$

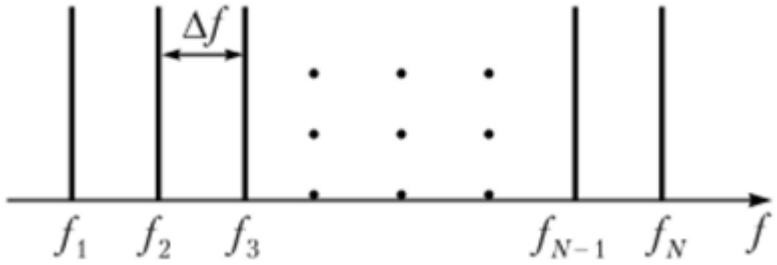

Рисунок 2.2 - Сітка робочих частот передавача

Для будь - якого типу модуляції - амплітудної, частотної, фазової або імпульсної-спектр сигналу є лінійним (рис. 1). Рис. 2.3, а) або тверде тіло (рис. 2.3, а) або тверде тіло (рис. 2.3, б) займають певну смугу частот: зверху / знизу.

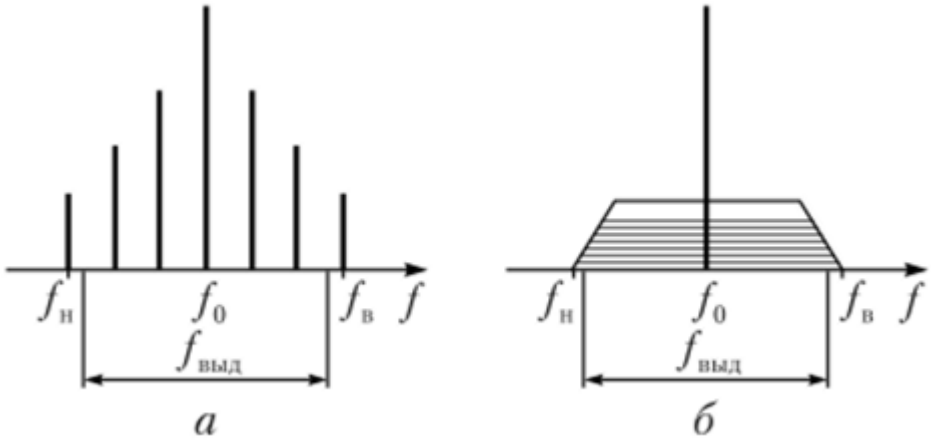

Рисунок 2.3 - Виділена смуга частот випромінювання з видами спектрів: а - лінійчатим; б - суцільним

Цьому спектру присвоюється певна смуга частот. Водночас слід поважати нерівність.

Нестабільність частоти коливань. Існує абсолютна і відносна нестабільність частоти коливань, а також довгострокова і короткострокова нестабільність. вівторок. Абсолют - це різниця між поточним значенням частоти коливань і номінальним значенням. Зокрема, номінальне значення частоти дорівнює 125 МГц, і насправді радіопередавач генерує сигнал з частотою 124,995 МГц. Таким чином, абсолютна частотна нестабільність є:

$$\Delta f = f_n - f = 125\,\text{МГц} - 124{,}995\,\text{МГц} = 0{,}005\,\text{МГц} = 5\text{кГц} \quad (3)$$

Відносна нестабільність частоти визначається коефіцієнтом нестабільності , рівним відношенню абсолютної нестабільності частоти до її номінального значення. Тоді відносна нестабільність дорівнює:

$$\Delta_f = \frac{0{,}005}{125} = 0,\,00004 = 40 \cdot 10^{-6} = 0,\,004\% \quad (4)$$

У передавачі відносна частота не повинна перевищувати нестабільність. Відповідно до міжнародних стандартів відхилення від номінальної частоти підключеного передавача на гектометровій хвилі не повинно перевищувати 0,005, а відхилення частоти в цьому грудні для широкомовних передавачів не повинно перевищувати 10 Гц.

Побічні ефекти від донорів. В ідеалі передавач будь-якої системи зв'язку повинен випромінювати тільки корисні сигнали на частотах, а його спектр повинен вписуватися в спеціальну смугу частот (рис. 2.4, а). Однак нелінійність процесів в передавачі призводить до виникнення побічних ефектів (включаючи перешкоди) в робочій смузі (рис. 2.4, б). Побічні ефекти поблизу робочої смуги називаються позасмуговими. Крім позасмугових передавачів, передавачі можуть випромінювати гармоніки.

Передавача кожної системи зв'язку відводиться певна смуга частот, в якій допускається радіовипромінювання. Однак будь-який передавач крім

корисного сигналу випромінює і побічні коливання, які по відношенню до іншої системи є перешкодами. Розглянемо діаграми на рис. 2.4, б. Нехай номінальна частота передавача однієї системи дорівнює 0. Але крім неї антена випромінює і радіосигнал, нехай і малої потужності. На цю частоту може бути налаштований приймач сусідній системи зв'язку. По відношенню до неї сигнал буде перешкодою.

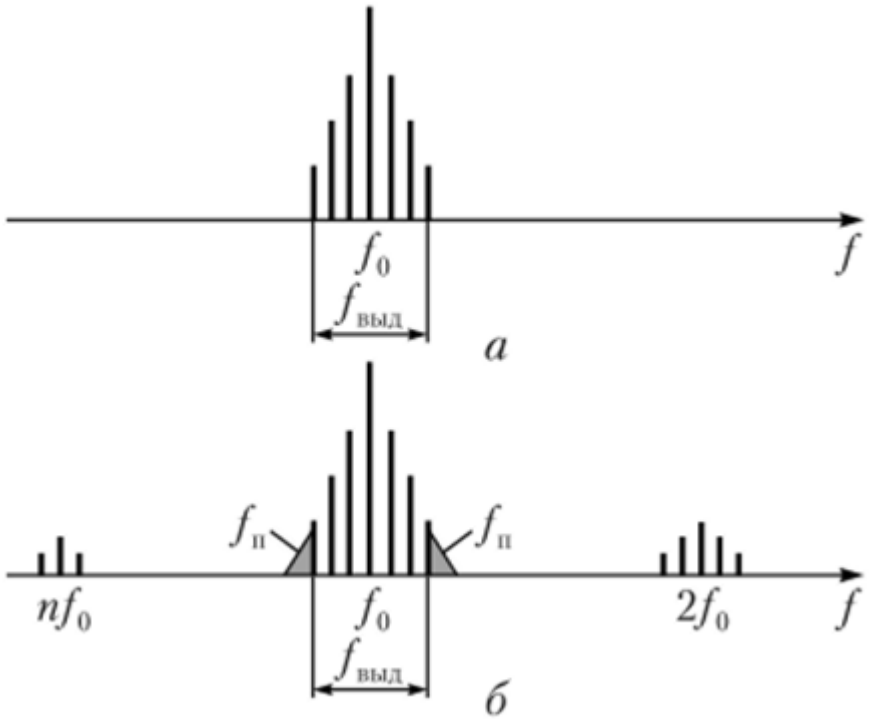

Рисунок 2.4 - Випромінювання передавача: а - без побічних складових; б - з наявністю побічних складових

Крім того, можливо випромінювання паразитних коливань, причиною виникнення яких є самозбудження в потужних підсилюючих каскадах радіопередавача. Оскільки повністю виключити побічні випромінювання не можна, то встановлюють норму на їх значення або в абсолютних, або у відносних одиницях до потужності корисного випромінювання. Зазвичай рівень потужності позасмугових випромінювань повинен бути не менше 60 дБ від потужності корисного сигналу. На деяких частотах норма може становити 100 дБ і більше.

Електромагнітна сумісність. У світі працюють величезна кількість

передавачів, що створюють навколо Землі електромагнітне иоле. При одночасній роботі безлічі систем перешкоди прийому неминучі. Інтенсивність перешкод визначається числом діючих випромінювачів, їх потужністю, розташуванням в просторі, формою діаграми спрямованості антен і т. д. Здатність систем зв'язку одночасно функціонувати в реальних умовах з необхідною якістю при впливі на них ненавмисних електромагнітних перешкод і не створювати неприпустимих таких же перешкод іншим радіосистемам називають електромагнітною сумісністю (EMC).

Параметри переданого повідомлення. Повідомленням може бути мовна, факсимільний, телевізійна, телеметрическая і інша різноманітна інформація, в тому числі і прочитується з комп'ютера.

Нелінійні процеси в передавачі викликають появу нелінійних спотворень (вищих гармонік та IMI) сигналів. Побічні випромінювання потрапляють в частотний діапазон інших систем і створюють їм перешкоди в роботі. Крім нелінійних, в передавачі виникають і лінійні спотворення, пов'язані з проходженням сигналів через фільтри з недосконалими АЧХ і нестрого лінійними ФЧХ.

Конструкції, габаритні розміри і маса передавачів в основному визначаються середньої випромінюваної потужністю.

Структурна схема сучасного передавача містить: джерело кодованого повідомлення, яке потрібно передати, задає генератор частоти, що створює високостабільного гармонійнеколивання, синтезатор сітки несучих частот, модулятор, підсилювач потужності, вихідні ланцюг і антену.

VHF (Very High Frequency) - це діапазон радіочастот, що лежить у межах від 30 МГц до 300 МГц. Він знаходиться між діапазонами MF (Medium Frequency) та UHF (Ultra High Frequency) і використовується для широкого спектру застосувань, таких як:

- радіомовлення: AM та FM-радіостанції транслюють свої сигнали в діапазоні VHF;

- радіозв'язок: VHF використовується для радіозв'язку між людьми, такими як поліцейські, пожежні, таксі, авіадиспетчери та радіоаматори;

- авіаційний зв'язок: Пілоти та диспетчери спілкуються один з одним за допомогою VHF-радіо;

- морський зв'язок: Капітани суден та берегові служби спілкуються один з одним за допомогою VHF-радіо;

- радіоаматорство: Радіоаматори використовують VHF для зв'язку один з одним на різні відстані.

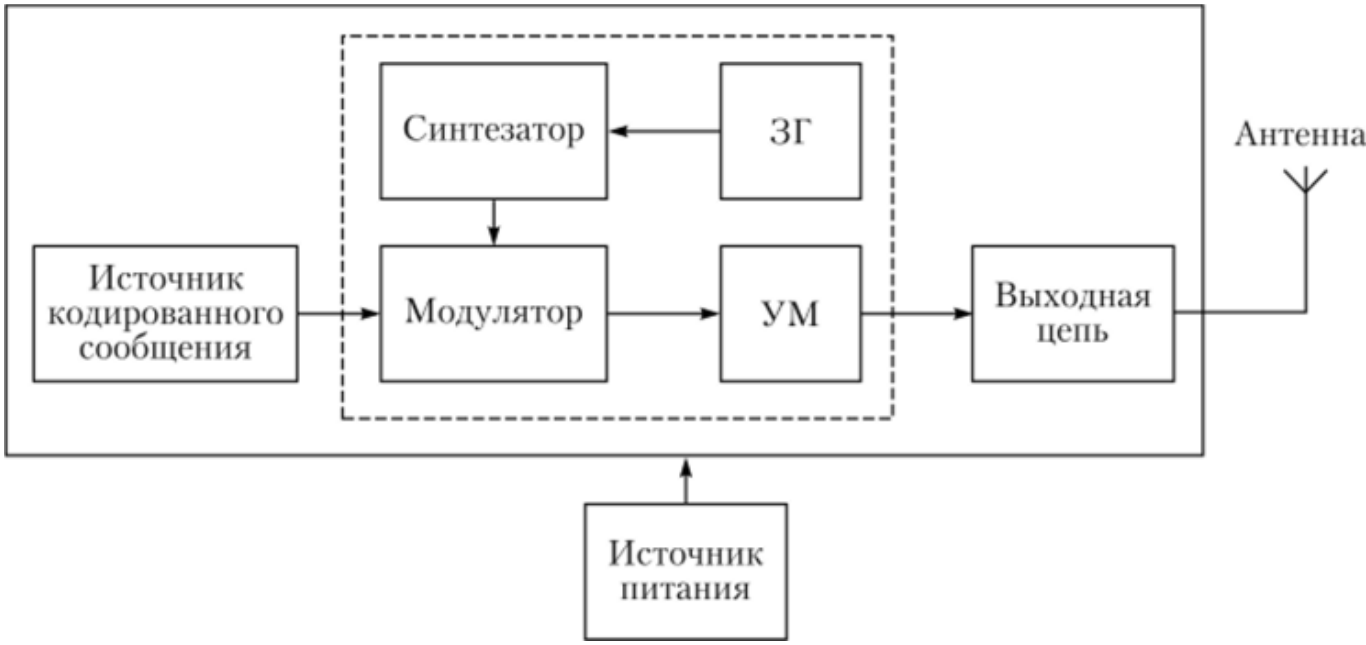

Рисунок 2.5 - Узагальнена структурна схема сучасного передавача

2.1.2 Діапазони радіомодулів

Переваги VHF:

- дальність: VHF-сигнали можуть поширюватися на великі відстані, особливо в порівнянні з діапазонами MF та HF;

- надійність: VHF-сигнали стійкі до шуму та перешкод;

- простота: Технологія VHF відносно проста та недорога.

Недоліки VHF:

- ширина каналу: VHF-сигнали займають більше місця в радіочастотному спектрі, ніж сигнали UHF;

- розмір антени: VHF-антени зазвичай більші, ніж UHF-антени.

Піддіапазони VHF. Діапазон VHF ділиться на кілька піддіапазонів, кожен з яких має свої особливості:

- VHF-I (30 МГц - 50 МГц): Використовується для радіоаматорства, радіозв'язку та деяких типів радіомовлення;

- VHF-II (50 МГц - 75 МГц): Використовується для телебачення, радіомовлення та радіозв'язку;

- VHF-III (75 МГц - 108 МГц): Використовується для авіаційного зв'язку, морського зв'язку та радіоаматорства;

- VHF-IV (108 МГц - 136 МГц): Використовується для авіаційного зв'язку, радіоаматорства та деяких типів радіомовлення;

- VHF-V (136 МГц - 174 МГц): Використовується для радіоаматорства, радіозв'язку та деяких типів радіомовлення;

- VHF-VI (174 МГц - 216 МГц): Використовується для радіоаматорства, радіозв'язку та деяких типів радіомовлення;

- VHF-VII (216 МГц - 230 МГц): Використовується для радіоаматорства, радіозв'язку та деяких типів радіомовлення;

- VHF-VIII (230 МГц - 300 МГц): Використовується для радіоаматорства, радіозв'язку та деяких типів радіомовлення.

2.1.3 Технологія Wi-Fi

Wi-Fi - це бездротова технологія локальної мережі (LAN), яка використовує радіочастотні (РЧ) хвилі для передачі даних між комп'ютерами, мобільними пристроями та іншими пристроями. Вона стала однією з найпоширеніших технологій бездротового зв'язку в світі, завдяки своїй простоті використання, широкому діапазону дії та високій швидкості передачі даних.

Фізичні принципи: РЧ хвилі: Wi-Fi використовує РЧ хвилі в діапазоні 2,4 ГГц або 5 ГГц. Ці хвилі складаються з коливань електричного та магнітного полів, які поширюються в просторі. Довжина хвилі РЧ хвиль Wi-Fi становить близько 12 см (2,4 ГГц) або 6 см (5 ГГц). [6]

Антени: Антени використовуються для передачі та прийому РЧ хвиль. Існують різні типи антен, кожна з яких має свої характеристики, такі як спрямованість, посилення та діапазон дії.

Модуляція: РЧ хвилі самі по собі не несуть інформації. Щоб передати дані, РЧ хвилю потрібно модулювати. Wi-Fi використовує різні методи модуляції, такі як OFDM (Orthogonal Frequency Division Multiplexing) та DSSS (Direct Sequence Spread Spectrum).

Протоколи: IEEE 802.11: Wi-Fi базується на сімействі протоколів IEEE 802.11, які визначають стандарти для бездротових локальних мереж. Існує кілька версій протоколу 802.11, кожна з яких має свої характеристики та можливості.

Стандарти Wi-Fi: Wi-Fi Alliance публікує стандарти Wi-Fi, які гарантують сумісність між пристроями від різних виробників. Найпоширеніші стандарти Wi-Fi включають 802.11b, 802.11g, 802.11n, 802.11ac та 802.11ax.

Інфраструктура Wi-Fi. Точки доступу (AP): AP - це пристрої, які дозволяють пристроям підключатися до мережі Wi-Fi. AP підключаються до кабельної мережі або до іншого AP за допомогою кабелю Ethernet.

Мережеві пристрої: Мережеві пристрої, такі як маршрутизатори та комутатори, можуть використовуватися для створення та розширення мереж Wi-Fi.

Клієнтські пристрої: Клієнтські пристрої, такі як ноутбуки, смартфони та планшети, підключаються до мережі Wi-Fi за допомогою адаптерів Wi-Fi.

Безпека Wi-Fi. Методи аутентифікації: Wi-Fi використовує різні методи аутентифікації, такі як WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) та WPA2 (Wi-Fi Protected Access II), щоб запобігти

несанкціонованому доступу до мережі.

Шифрування: Wi-Fi використовує шифрування, таке як AES (Advanced Encryption Standard), щоб захистити дані, які передаються по мережі. [7]

VPN (Virtual Private Network): VPN можна використовувати для створення безпечного тунелю між клієнтським пристроєм та AP, що забезпечує додатковий рівень безпеки.

Переваги та недоліки Wi-Fi технологій. Переваги Wi-Fi - простота використання: Wi-Fi простий у налаштуванні та використанні. Більшість пристроїв мають вбудовані адаптери Wi-Fi, і не потрібно прокладати кабелі для підключення до мережі. Гнучкість Wi-Fi дозволяє користувачам підключатися до мережі з будь-якого місця в межах зони дії AP. Це робить Wi-Fi ідеальним для мобільних користувачів та для використання в динамічних середовищах. Широкий діапазон дії: Wi-Fi має широкий діапазон дії, що дозволяє підключати пристрої на значній відстані від AP. Висока швидкість: Wi-Fi пропонує високу швидкість передачі даних, що робить його придатним для таких завдань, як потокове відео, онлайн-ігри та завантаження великих файлів.

Доступність Wi-Fi широко доступний у багатьох місцях, включаючи будинки, офіси, кав'ярні, бібліотеки, аеропорти та інші публічні місця. Низька вартість: Wi-Fi відносно недорогий порівняно з іншими технологіями бездротового зв'язку.

Недоліки Wi-Fi. Безпека Wi-Fi може бути вразливим до атак хакерів, якщо не вжито належних заходів безпеки. Перешкоди: Wi-Fi сигнали можуть бути схильні до перешкод від стін, меблів та інших об'єктів. Обмежена пропускна здатність: У мережах Wi-Fi з великою кількістю користувачів пропускна здатність може бути обмеженою, що може призвести до зниження швидкості та перебоїв у роботі.

Вплив на здоров'я: Деякі люди стурбовані можливим впливом радіочастотних хвиль Wi-Fi на здоров'я. Однак, наукові дослідження не показали остаточної шкоди від Wi-Fi при нормальному рівні впливу.

Залежність від електроенергії: Wi-Fi пристрої потребують електроенергії для роботи, що може бути проблемою в місцях з перебоями в електропостачанні.

Застосування Wi-Fi. Домашнє використання: Wi-Fi широко використовується в домашніх умовах для підключення комп'ютерів, смартфонів, планшетів, ігрових консолей та інших пристроїв до Інтернету. Бізнес-використання: Wi-Fi використовується в офісах, магазинах, ресторанах та інших підприємствах для підключення пристроїв до мережі та Інтернету. Громадські Wi-Fi: Wi-Fi доступний у багатьох публічних місцях, таких як кав'ярні, бібліотеки, аеропорти та залізничні вокзали. Інтернет речей (IoT): Wi-Fi використовується для підключення пристроїв IoT, таких як розумні термостати, камери спостереження та освітлення, до Інтернету.

Рисунок 2.6 - Приклад з’єднання пристроїв через Wi-Fi

Майбутнє Wi-Fi. Wi-Fi 6 (802.11ax): Wi-Fi 6 - це новітнє покоління Wi-Fi, яке пропонує значні покращення в швидкості, пропускній здатності та ефективності. Wi-Fi 6E: Wi-Fi 6E розширює діапазон Wi-Fi на новий діапазон 6 ГГц, який пропонує ще більшу пропускну здатність і менше перешкод. Wi-

Fi Mesh: Wi-Fi Mesh - це нова технологія, яка використовує кілька AP для створення єдиної безшовної мережі. Wi-Fi SON (Self-Organizing Networks): Wi-Fi SON - це технологія, яка автоматично налаштовує та оптимізує мережу Wi-Fi.

У 1990 році IEEE802 створив групу для дослідження стандартів бездротових мереж Wi-Fi. Їх основне завдання-встановити загальний стандарт для мереж, що працюють в грудні в діапазоні частот 1-2 ГГц, зі швидкістю з'єднання 2,4 Мбіт/с.розробка стандарту була завершена в 1997 році, і була затверджена первісна специфікація 802.11.

Цей стандарт вважається першим стандартом для обладнання WLAN. Однак початкова швидкість передачі інформації на той час не відповідала побажанням користувачів. Таким чином, щоб догодити всім користувачам і популяризувати технологію, розробники встановили новий стандарт. А восени 1999 року були затверджені удосконалення існуючих стандартів.

На сьогодні існує велика кількість стандартів групи IEEE 802.11. Розглянемо найбільш розповсюдженні і найбільш вживані:

- базовий 802.11;
- IEEE 802.11a (Wi-Fi 2);
- IEEE 802.11b (Wi-Fi 1);
- IEEE 802.11g (Wi-Fi 3);
- IEEE 802.11n (Wireless-N чи Wi-Fi 4);
- IEEE 802.11ac (гігабітний WiFi або WiFi 5);
- IEEE 802.11ax (WiFi 6 або високоефективна WLAN).

Всі стандарти IEEE 802.11 працюють на нижніх двох рівнях моделі ISO/OSI, фізичному та канальному, тому будь-який мережевий додаток, мережева операційна система, або протокол (наприклад, TCP/IP), будуть так само добре працювати в мережі 802.11, як і в мережі Ethernet.[7]

У середині літа 1997 року було оголошено стандарт IEEE802.11.Це було названо "специфікацією фізичного рівня та рівня контролю доступу для каналів передачі бездротової локальної мережі". У цьому протоколі

викладені різні принципи мережевої архітектури, форматів пакетів, методів захисту даних і аутентифікації, а також доступу пристроїв до каналів зв'язку.

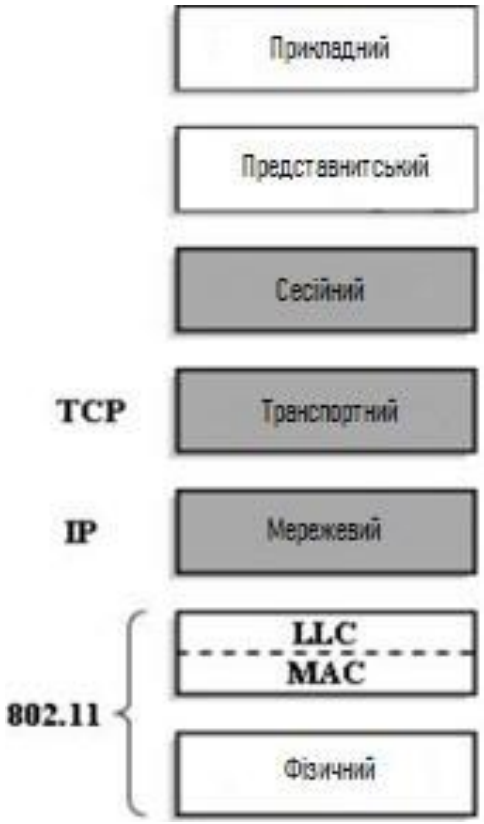

Рисунок 2.7 - Рівні моделі ISO/OSI і їх відповідність стандарту 802.11

На ранніх етапах свого існування стандарт 802.11 використовував обладнання з частотою 2,4 ГГц і максимальною швидкістю 2 Мбіт/с. Стандарт 802.11 є "основою" майбутніх стандартів.

2.1.4 Технологія 802.11a (Wi-Fi 2)

Стандарт IEEE 802.11a був введений в 1999 році. Передбачається, що він використовує частоту 5 ГГц замість діапазону 2,4 ГГц. Як правило, більш високі частоти поєднуються з більш високими швидкостями, але в меншому прискоренні. Щоб забезпечити прискорення, спочатку необхідно використовувати технологія OFDM (ортогональне мультиплексування

частотного поділу), метод цифрової модуляції, що використовується для кодування даних на декількох частотах, який теоретично може збільшити максимальну швидкість до 54 Мбіт / с.

Недоліками даного стандарту є високе енергоспоживання і невеликий асортимент обладнання. 802.11 a працює в діапазоні 5 ГГц, що робить продукт дорожчим. Ось чому він в основному використовувався в бізнес-мережах.

2.1.5 Технологія 802.11b (Wi-Fi 1)

У 802.11 b використовується спектр прямого послідовного розповсюдження (DSSS), схема модуляції, яка використовується для зменшення втрат сигналу в діапазоні 2,4 ГГц і здатна розвивати швидкість до 11 Мбіт / с. 2,4-ГГц смуга відмінно справляється з подоланням перешкод і забезпечує більший охоплення Wi-Fi. На жаль, дані передаються набагато повільніше, особливо якщо мережеві перешкоди виникають через незвичайні пристрої, що працюють на тій же частоті, такі як дитячі Монітори, мікрохвильові печі, бездротові телефони, високошвидкісні побутові прилади та пристрої Bluetooth. Зберігання пристроїв 802.11 b подалі від таких пристроїв може зменшити перешкоди.

Wi-Fi використовував лише діапазон частот у 2.4 ГГц, тому продукт був набагато дешевшим, ніж 802,11 a, і був більш популярним у домашніх мережах.

2.1.6 Технологія 802.11g (Wi-Fi 3)

Стандарт IEEE802.11g є вдосконаленням стандарту IEEE802. 11b.швидкість передачі інформації збільшилася до 54 Мбіт/сек завдяки використанню більш ефективної технології модуляції сигналів.

У той час багато з них все ще мали точки доступу та комп'ютери, що

використовували попередній стандарт, тому зворотна сумісність була необхідністю. Сумісний з продуктами 802.11 g, 802.11 B. однак продукти Wi-Fi можуть підключатися лише до одного робочого стандарту. Комп'ютер 802.11 b, підключений до точки доступу 802.11 g, може працювати тільки на швидкостях, дозволених стандартом B. з іншого боку, пристрої, підключені до точки доступу Ag-Ab, працюють тільки на тій швидкості, яку забезпечує точка доступу.

2.1.7 Технологія 802.11n (Wi-Fi 4)

Wireless N був розроблений у 2009 році для підвищення швидкості, надійності та дальності бездротової передачі. Це був перший стандарт, який використовував технологію Multi-Input Multi-output (MIMO). Продукти MIMO тепер використовують масив антен для отримання більшої кількості даних з одного пристрою, що дозволяє швидше передавати дані. Крім того, він був першим, хто дозволив використання радіочастот 2,4 ГГц і 5 ГГц 2 жовтня. Стандарт 802.11 n, що використовує обидві частоти, сумісний з пристроями 802.11 a / b / G. основними поліпшеннями є:

- створення багатоканальних входів і виходів (MIMO);
- збільшення пропускної здатності з 20 МГц до 40 МГц.

Завдяки всім розширеним функціям Wi-Fi 4 підтримує швидкість передачі даних до 600 Мбіт / сек і теоретичній відстані до 70 метрів. Він був значно підвищений порівняно з попереднім стандартом.

П’яте покоління Wi-Fi було створено в 2013 році. Він призначений для роботи в діапазоні 2,4 ГГц, щоб зменшити перешкоди в діапазоні 5 ГГц. Технологія Wi-Fi802.11ac використовує дві смуги частот для бездротового зв'язку. Щоб зробити це можливим, деякі постачальники включили технологію Wireless-N, щоб їх продукти змінного струму були сумісні з діапазоном 2,4 ГГц. Швидкість передачі даних залежить від використовуваної частоти, смуга частот 5 ГГц може досягати швидкості

смуги пропускання до 1300 Мбіт / сек, а смуга частот 2,4 ГГц може досягати швидкості смуги пропускання до 450 Мбіт / с.

WiFi802.11ac - це перший стандарт, який використовується багатьма користувачами низхідної лінії ЗВ'ЯЗКУ MIMO. Технологія Wireless - N MIMO зробила ще один крок до подальшого поліпшення передачі даних. DL MU-MIMO дозволяє бездротовим маршрутизаторам передавати інформацію на кілька пристроїв одночасно, збільшуючи пропускну здатність і зменшуючи затримку. Завдяки технології Wireless N 802.11 ac - це 802.11 a / b / g / N. Сумісність з такими доповненнями на основі стандартів - IEEE802.11ad і IEEE802.11AH - також розроблялася протягом декількох років.

Розроблений для забезпечення високої пропускної здатності даних для багатогігабітних бездротових систем, 802.11 ad є частиною серії 802.11.2012. На відміну від попереднього стандарту, він не використовував діапазон 2,4 ГГц або 5 ГГц і працював у діапазоні 60 ГГц. Чим вище частота, тим менше відстань. В ідеальних умовах пристрій 802.11 ad має розташовуватися на відстані близько 9 метрів від точки доступу.

Прийнятий стандарт 2017/5 802.11 ah призначений для використання неліцензійного грудня частот менше 1 ГГц. Його метою було зменшити споживання енергії та створити розширену мережу WLAN в діапазоні 2,4 / 5 ГГц. Грудень грудня 2015 року Wi-Fi HaLow працює в діапазоні 900 МГц, тому теоретичний діапазон становить 543 м (1781,5 футів) в приміщенні, а швидкість передачі даних становить до 347 Мбіт / с. через низький попит на енергію для 802,11 Ач, занадто багато енергії

Існує багато технологій безпеки, кожна з яких є найважливішими компонентами стратегії захисту даних: автентифікація, цілісність даних та ефективна перевірка.Автентифікація визначається як автентифікація користувача або кінцевого пристрою та його місцезнаходження з подальшою авторизацією користувача та кінцевого пристрою. Він включає такі сфери, як цілісність даних, Безпека мережевої інфраструктури, безпека периметра та

конфіденційність даних. Проактивні перевірки можуть допомогти вам по-справжньому дотримуватися встановлених політик безпеки та відстежувати будь-які відхилення або спроби несанкціонованого доступу.

У той же час, коли був введений базовий стандарт IEEE802.11, IEEE також схвалив механізм захисту дротової еквівалентної конфіденційності (WEP). Дротова еквівалентна конфіденційність (WEP) - це стандартна технологія 802.11, що забезпечує безпеку передачі інформації. Шифрування даних було здійснено за допомогою алгоритму RC4 з ключами, що мають статичні компоненти від 40 до 104 жовтня та додатковий 24-бітний вектор ініціалізації. Таким чином, в цілому було виконано шифрування даних за допомогою ключів розміром 64-128 біт. WEP не мав на меті повністю захистити інформацію від зловмисників, він просто робив її нечитабельною. Основним завданням цієї технології було шифрування потоку даних, що передаються в бездротовій мережі.

Для підвищення захисту використовується вектор ініціалізації (IV), призначений для рандомізації додаткових частин ключа, а також шифрів для різних пакетів даних. Цей вектор дорівнює 24 Бітам. В результаті виходить загальне шифрування з бітовою глибиною від 64 (40 + 24) до 128 (104 + 24) біт.

Процес шифрування WEP виконується в 2 етапи. По-перше, алгоритм циклічної перевірки надмірності (CRC-32), який додається до кінця незашифрованого повідомлення і використовується приймаючою стороною для перевірки його цілісності. На другому етапі шифрування виконується безпосередньо;

Ключ шифрування WEP-це загальний приватний ключ, який повинні розпізнавати пристрої по обидва боки бездротового каналу передачі даних. Цей секретний 40-бітний ключ разом із випадковим 24-бітним IV є вхідною послідовністю для генератора псевдовипадкових чисел на основі криптографії.

Цей процес виконується, щоб уникнути методів злому, заснованих на

статистичних властивостях відкритого тексту. IV використовується для забезпечення унікального потоку ключів для кожного повідомлення.

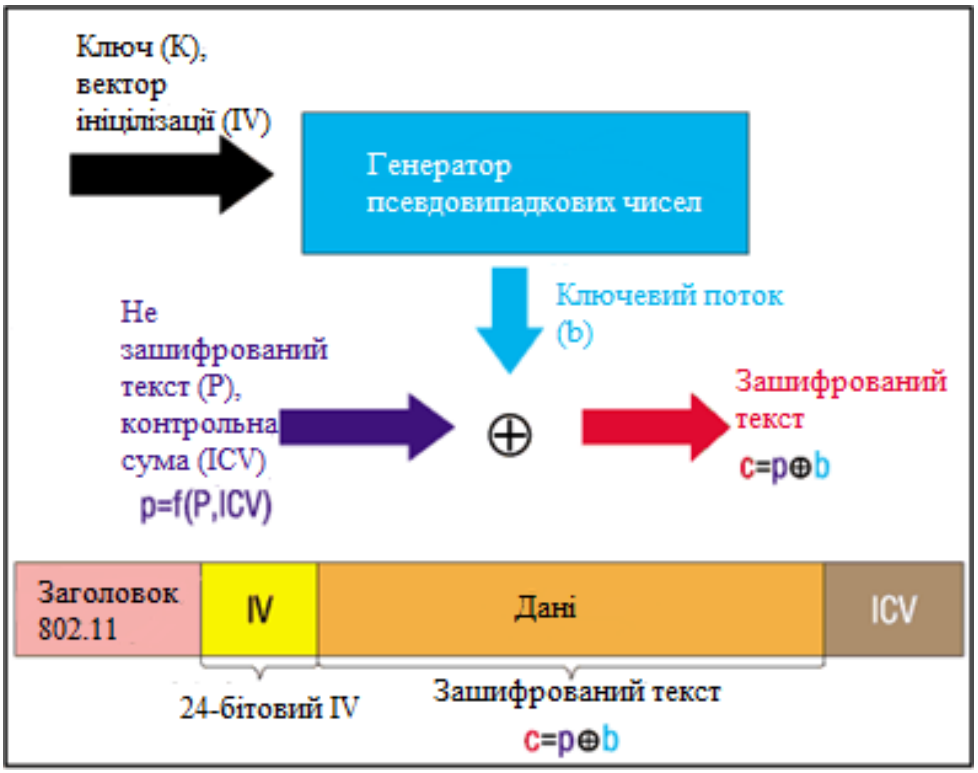

Рисунок 2.8 - Схема роботи шифрування по протоколу WEP

Зашифровані повідомлення створюються в результаті виконання операції XOR над незашифрованим повідомленням за допомогою ICV та потоку ключів. Коли інформація береться з іншого боку, виконується зворотна операція (p = c + b)[2]. Приймач обчислює значення b, застосовуючи код Вернама до вхідної послідовності клавіш K (знайте заздалегідь) та IV. Для кожного наступного пакета процес повторюється з новообраним значенням IV. Однією з відомих особливостей алгоритму RC4 є те, що якщо ви використовуєте одне і те ж значення ключа та вектор ініціалізації, ви завжди отримаєте одне і те ж значення b, тому застосування операції XOR з однаковим значенням b до 2 текстів, зашифрованих за допомогою RC4, є не що інше, як операція XOR до початкових текстів.

Таким чином, ви можете отримати незашифрований текст, який є

результатом операції XOR між двома іншими вихідними текстами. Процедура їх видалення не складна. Наявність оригінального тексту дозволяє обчислити ключ, і в майбутньому ви зможете прочитати всі повідомлення цієї бездротової мережі. Після простого аналізу легко обчислити, коли B повторюється. Клавіша K фіксована, а кількість опцій дорівнює 224 = 16 777 216, тому при достатньому навантаженні на точку доступу середній розмір пакета бездротової мережі становить 1500 байт (12 000 біт), середня швидкість передачі даних становить 5 Мбіт / сек (до 11 Мбіт / сек), а швидкість точки доступу збільшується. вставати кожну секунду. Він буде відправляти 416 повідомлень на годину, або 1 1 497 600 повідомлень, якщо бути точним.Тобто повторення відбувається через 11 годин, а повторення відбувається через 11 годин.12 хвилин (224/1 497 600 = 11,2 години). Ця проблема називається"векторним зіткненням". Існує багато способів прискорити цей процес. Крім того, атака "відомий відкритий текст" може бути використана, якщо повідомлення з відомим контентом відправляється 1 жовтня користувачам мережі і зашифрований трафік прослуховується. У цьому випадку ви можете обчислити ключ, якщо у вас є 4 з 3 компонентів (незашифрований текст, вектор ініціалізації, зашифрований текст).

WPA означає Бездротовий безпечний доступ. Стандарт WPA був введений Альянсом Wi-Fi. Стандарт WPA представив tkip як введення wep для забезпечення більшої безпеки. WPA також запровадила аутентифікацію користувачів високого рівня для пристроїв 802.11. Описано два методи аутентифікації користувачів

Рукостискання верхнього рівня 802.1 x EAP / EAPOL для автентифікації користувача;

Обидва вищезазначені механізми автентифікації включають автентифікацію користувача, а також генерують набір ключів шифрування, які можна використовувати для захисту ваших даних. Механізм атрибуції та аутентифікації WLAN можна розділити на наступні 3 етапи. Станції та точки доступу WLAN підключаються одна до одної та визначають, чи

використовується механізм аутентифікації з відкритим ключем / 802.1 X. Якщо обраний механізм аутентифікації використовує відкритий ключ, то в кінці етапу він створює "головний ключ". Він використовується в чотиристоронньому рукостисканні EAPOL, отриманому за допомогою тимчасового ключа для шифрування даних. В кінці етапу інформаційні елементи WPA і RSN. Стандарт Wi-Fi / 802.11 ввів 2 нових елемента інформації, щоб забезпечити новий метод шифрування WPA - елемент інформації WPA (безпечний бездротовий доступ) та Cat (надійна мережа безпеки).

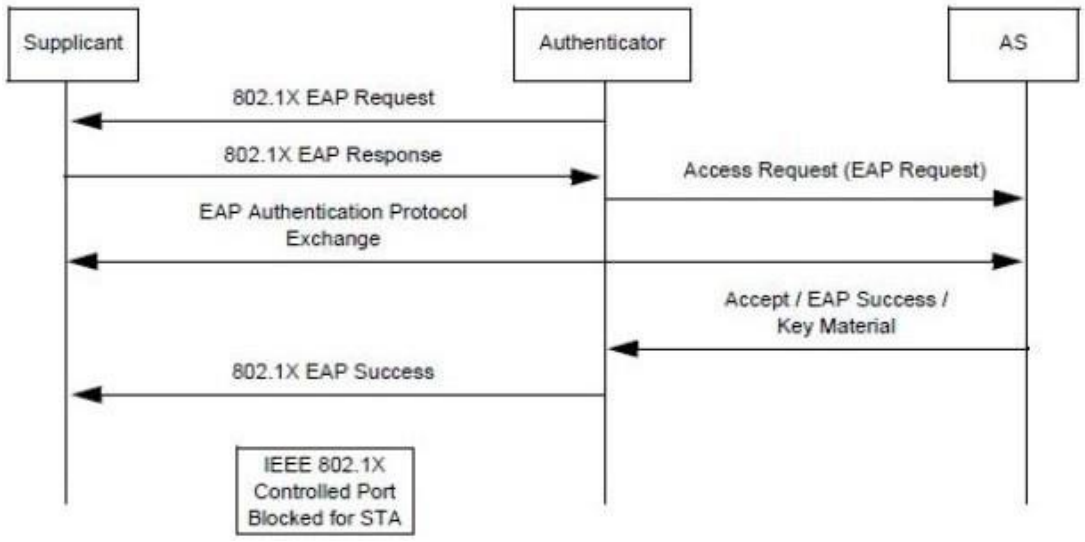

Рисунок 2.9 - Автентифікація EAP, яка забезпечує парний головний ключ для рукостискання EAPOL

Станції, що містять інформаційні елементи WPA / Cat у запиті на асоціацію, повинні виконати безпечне рукостискання 802.11 і / 802.1 X.

Ідентифікатор елемента WPA має значення 0x221. WPA відповідає ідентифікатору елемента Постачальника. Таким чином, при отриманні ідентифікатора для конкретного постачальника-OUI необхідно перевірити точку доступу / станцію, щоб побачити, чи є елемент інформації WPA. Якщо WPA-не є AP Station, він може вирішити змінити аналіз елемента інформації.

TKIP-це набір паролів за замовчуванням для wpa. WEP-40 і WEP-104 доступні лише в мережі транзитних станцій (TSN) у вигляді групових пакетів шифрування.

Рисунок 2.10 - Інформаційний елемент WPA

Інформаційний елемент RSN походить від групи IEEE802.11i. RSN означає надійну мережу безпеки і вимагає шифрування AES при використанні надійної мережі безпеки.

Паролі TKIP можуть використовуватися як широкосмугові / широкомовні паролі, подібні до паролів WEP-40 / wep104, але якщо метод автентифікації становить 802.1 x, WEP-40 / WEP-104 / TKIP також може використовуватися як групові паролі. Елементи інформації показані нижче. Розмір IE RSN обмежений максимум 255 байтами.

Стандарт WPA2 складається з 2 компонентів: шифрування і аутентифікації, необхідних для безпечної бездротової локальної мережі. Хоча елемент шифрування WPA2 передбачає використання розширеного стандарту шифрування (AES), протокол цілісності тимчасового ключа (Tkip). Він зворотньосумісний з існуючим WAP-обладнанням. Елемент аутентифікації WPA2 має 2 режими: особистий і діловий. В особистому режимі вам не потрібно використовувати раніше наданий PSK-ключ і вимагати від користувача індивідуальної аутентифікації.

Корпоративний режим вимагає індивідуальної автентифікації користувача на основі стандарту автентифікації IEEE802.1x, але

використовує розширений протокол EAP (розширюваний протокол автентифікації).

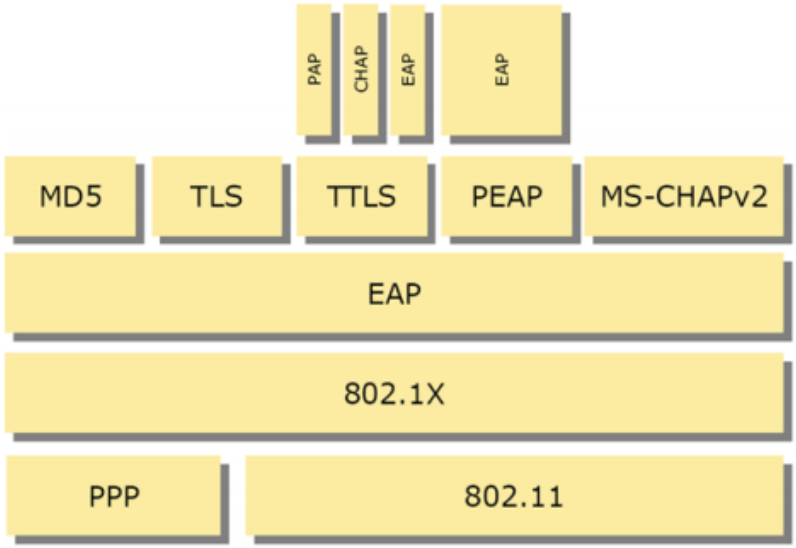

Рисунок 2.11 - Список протоколів

EAP-MD5 використовує алгоритм MD5 для обчислення хеш-значення пароля та зіставлення його з хеш-значенням, надісланим на сервер і збереженим на стороні сервера. Протокол EAP-FAST дозволяє входити за допомогою імені користувача та пароля та входити в PEAP-gtc за допомогою спеціального маркера. Протокол PEAP-Mschapv2 та EAP-TLS використовують клієнтські сертифікати для здійснення авторизації.

Максимальний захист мереж Wi-Fi забезпечується тільки сертифікатами WPA2-Enterprise і Digital Security в поєднанні з протоколами EAP-TLS або EAP-TTLS. Сертифікати - це файли, попередньо створені на серверах RADIUS та клієнтських пристроях. Протокол EAP-TTL / TTLS є частиною стандарту 802.1 X і використовує інфраструктуру відкритих ключів (PKI) 63 для обміну даними між клієнтом і Radius.дек. Протокол EAP-TTL / TTLS є частиною стандарту 802.1 X і використовує інфраструктуру відкритих ключів (PKI) 63 для обміну даними між клієнтом і Radius. PKI використовує приватний ключ (відомий Користувачеві) та відкритий ключ

(зберігається у сертифікаті та доступний для всіх) для автентифікації. Ці комбінації клавіш забезпечують надійну аутентифікацію.

WPA2 створює безпечний контекст зв'язку за 4 кроки. На першому етапі точка доступу та клієнт узгоджують політику безпеки (методи автентифікації, протоколи одноадресного трафіку, багатоадресні протоколи та методи попередньої автентифікації) для використання, що підтримується точкою доступу та клієнтом. На другому етапі (застосовується лише до корпоративного режиму).

Однією з найважливіших змін, внесених до стандарту WPA2, є відокремлення автентифікації користувача від цілісності та конфіденційності повідомлень, що забезпечує більш масштабовану та надійну архітектуру безпеки, придатну для порівнянних домашніх або корпоративних мереж.1

У персональному режимі WPA2 декомунізація, для якої не потрібен сервер автентифікації, виконується між клієнтом і точкою доступу, а 256-розрядний PSK створюється з відкритого тексту шляху (8-63 символи). PSK разом з ідентифікатором набору послуг та довжиною SSID складають математичну основу для головного ключа з подвійним брудом (PMK), що використовується у пізнішому виробництві ключів.

Аутентифікація в режимі WPA2Enterprise заснована на стандарті аутентифікації IEEE802.1x. основними компонентами є заявник (клієнт), що підключається до мережі, аутентифікатор, що забезпечує контроль доступу (AR діє як аутентифікатор), і аутентифікатор, що приймає рішення про авторизацію, що розділяє кожен віртуальний порт на 2 логічні порти для обслуговування декомунізації і аутентифікації і створює об'єкт доступу до порту (APPAE). PAE перевірки автентичності завжди включений, але служба PAE включена тільки після успішної перевірки автентичності сервером RADIUS. Аутентифікатор перетворює повідомлення EAPOL у повідомлення RADIUS, а потім пересилає їх на сервер RADIUS. Сервер автентифікації повинен бути сумісним з типом EAP заявника і повинен отримувати та обробляти запити на автентифікацію. Після завершення процесу

автентифікації заявник та сертифікатор матимуть секретний mk (головний ключ), як показано на рисунку-2.11.

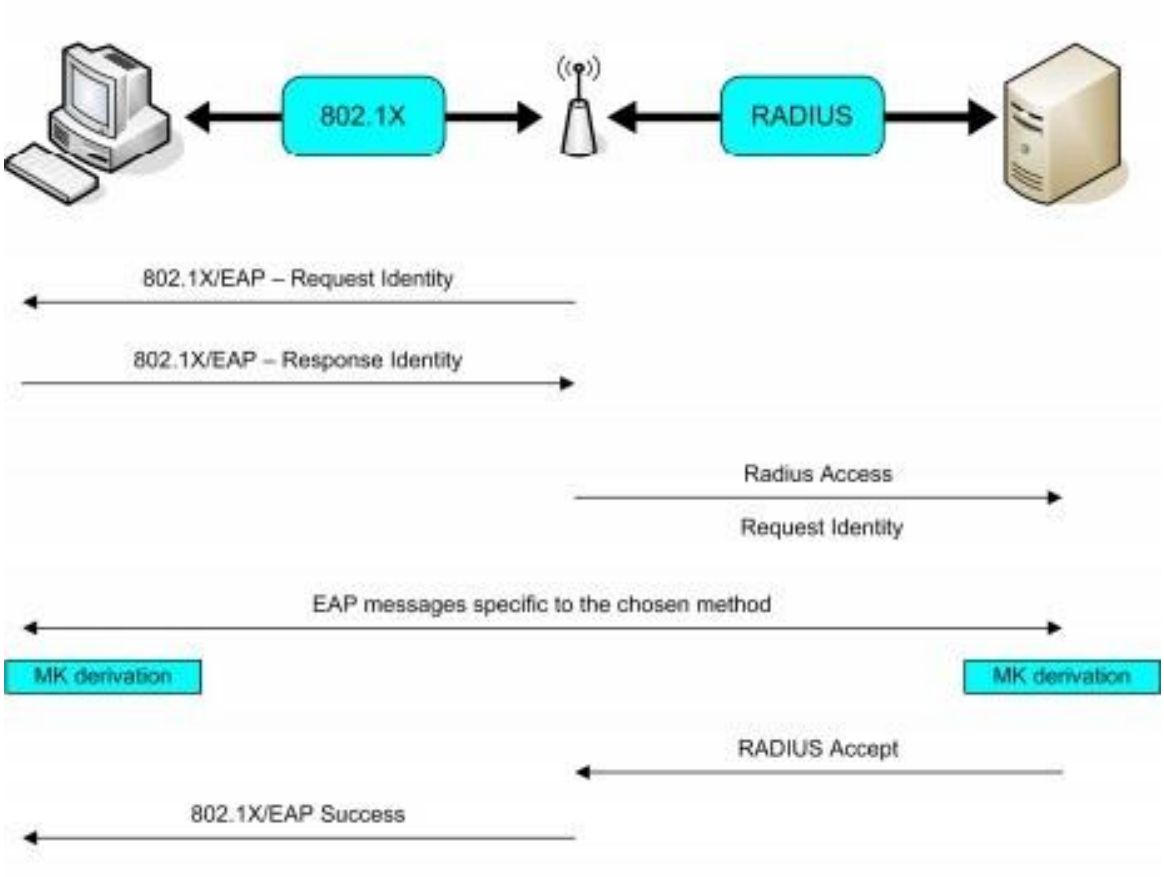

Рисунок 2.12 - 802.1X аутентифікація

WPA3, випущений на початку літа 2018 року,-це найновіша схема безпеки, розроблена для підвищення безпеки існуючих мереж Wi-Fi та вирішення проблем, з якими стикалися попередні версії. WPA3 автентифікує клієнта в точці доступу методом паралельної однорангової автентифікації на основі пароля (SAE). Після перегляду стандарту RFC7764 у 2015 році:

Був розроблений протокол, що забезпечує обіцяний захист. Цей захист досягається за допомогою шифрування з дискретними логарифмічними та еліптичними кривими за допомогою рукостискання бабки. В результаті рукостискання виходить PMK, який використовується в стандартному 2-смуговому рукостисканні, використовуваному в схемі WPA4.

Сертифікат WPA3 був створений з урахуванням двох типів мереж. Перша-це домашня мережа, де користувач автентифікується за допомогою загальнодоступного пароля. Більш складні методи аутентифікації (сертифікати, смарт-картки тощо)- це Корпоративна мережа, яка дозволяє використовувати її.

Для розрізнення обох типів використовується термін WPA3-SAE для домашніх мереж та термін WPA3-Enterprise для корпоративних мереж. WPA3-Enterprise використовує існуюче рукостискання, але вимагає, щоб пароль, який використовується під час автентифікації, забезпечував принаймні 192 біт безпеки. Це означає, що паролі повинні використовувати принаймні 384-бітну криву для паролів з еліптичною кривою та принаймні 3072-бітний модуль при використанні RSA або DHE.B даний час автентифікація WPA3 не згадує вимоги до тривалості для сеансових ключів або хеш-функцій, що використовуються після автентифікації. Однак після перевірки автентичності також можна використовувати рівень безпеки не менше 192 біт.

Режим WPA3-SAE більш цікавий для домашньої мережі. Він передбачає підтримку одночасної автентифікації існуючих рукостискань Equals (SAE). Це рукостискання - це обмін ключами з автентифікацією паролем (PAKE), що означає, що автентифікація здійснюється на основі пароля. Рукостискання SAE забезпечує конфіденційність і стійкість до атак автономного словника. Результатом рукостискання SAE WPA3 є двійковий головний ключ (PMK), який потім використовується для виконання 4-позиційного рукостискання для отримання "двійкового" ключа ("PTK").

Точка доступу зберігає підтримувані пакети шифрування або алгоритми аутентифікації та шифрування в елементі захищеної мережевої безпеки (RSNE). Rsne не входить до числа авторизованих маяків, які регулярно надсилаються для заохочення існування мережі. Клієнт також використовує rsne у своєму запиті на асоціацію, щоб повідомити точку доступу про використаний зашифрований набір.

Спочатку SAE узгоджує головний ключ рукостискання (PMK), потім отримує чотиристоронній сеансовий ключ рукостискання (PTK). Рукостискання SAE було створено для підтримки сітчастої мережі, щоб обидві сторони могли запускатися паралельно (отже, діагональні стрілки).

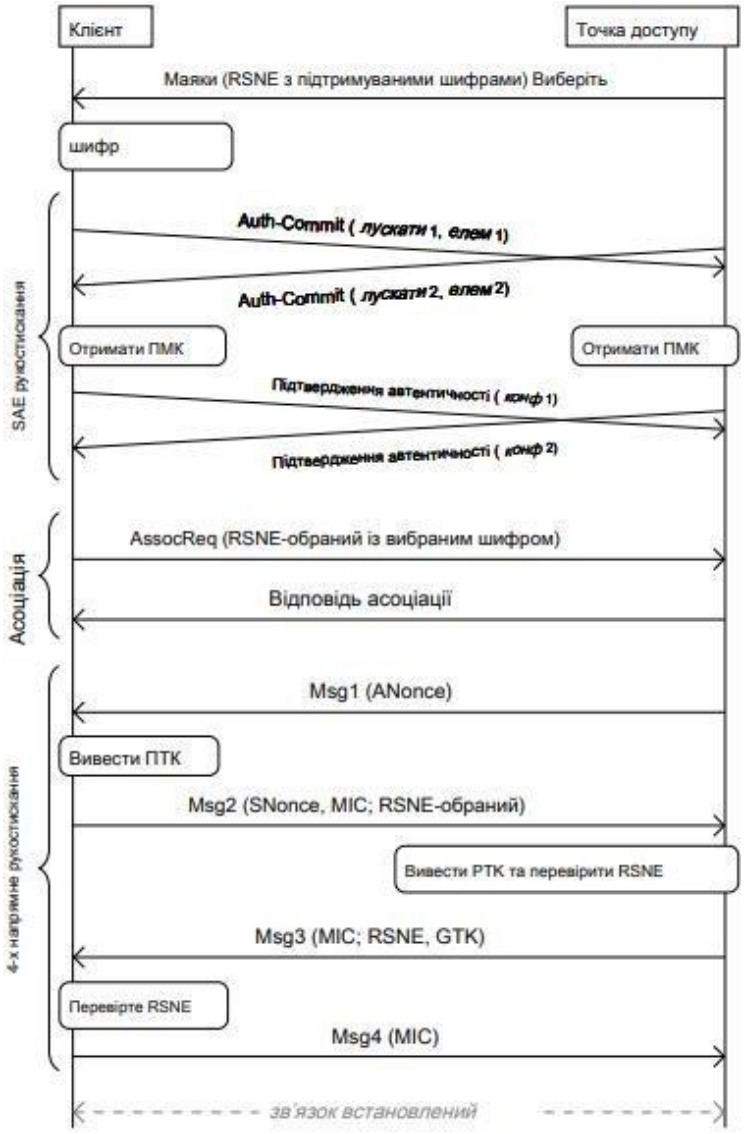

Рисунок 2.13 - Підключення до AP за допомогою WPA3

Сертифікація WPA3 передбачає підтримку рукостискання SAE. Це рукостискання вперше було введене Харкінсом у 2008 році, і було додане до стандарту 802.11 у 2011 році.

3 ОГЛЯД І ВИБІР ПРИСТРОЇВ ДЛЯ РЕАЛІЗАЦІЇ

3.1 Вибір плати для розробки

Для вибору плати розробки в було декілька варіантів: Arduino, ESP32, STM32. Всі ці плати мають свої недоліки та переваги, тож треба розглянути кожну з них для вибору оптимальної плати для розробки. [8]

3.1.1 Платформа Arduino

Arduino – це платформа відкритого типу для прототипування електроніки, що складається з апаратної частини (плати) та програмного забезпечення. Її створила команда італійських інженерів у 2005 році з метою спростити процес створення інтерактивних об'єктів для художників та дизайнерів, не маючи глибоких знань в електроніці та програмуванні. Апаратна частина Arduino складається з мікроконтролера Atmel AVR, елементів обв'язки, роз'ємів для підключення датчиків та виконавчих пристроїв, а також джерела живлення. Програмне забезпечення Arduino включає середовище розробки (IDE) на основі Processing/Wiring, яке використовує спрощену мову програмування, подібну до C/C++.

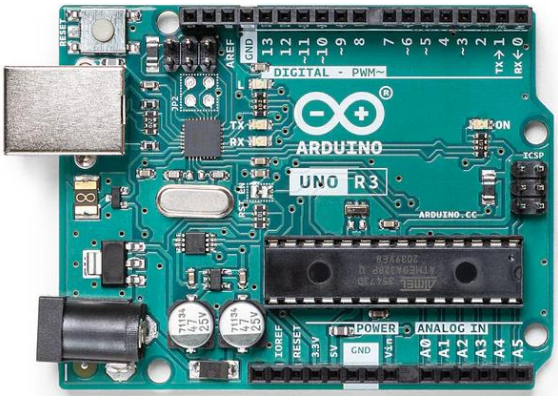

Рисунок 3.1 - Плата для розробки Arduino UNO

3.1.2 Платформа ESP32

ESP32 – це мікроконтролер типу "система на кристалі" (SoC) з вбудованими модулями Wi-Fi та Bluetooth, розроблений компанією Espressif Systems. Він є наступником популярного мікроконтролера ESP8266 і пропонує значні переваги в продуктивності, функціональності та енергоефективності.

До переваг цієї плати можна віднести невелику ціну, високу продуктивність, низьке енергоспоживання та багатофункціональність.

Рисунок 3.2 - Плата для розробки ESP32

3.1.2 Платформа STM32

STM32 – це сімейство 32-бітних мікроконтроллерів, розроблених компанією STMicroelectronics. Їх використовують у широкому спектрі електронних пристроїв, від побутової техніки до автомобілів та промислових систем.

До переваг цього мікроконтроллера можна віднести широкий вибір, бо в цьому сімействі є багато різних модифікацій мікроконтроллера, високу продуктивність, низьке енергоспоживання, простота використання та доступність.

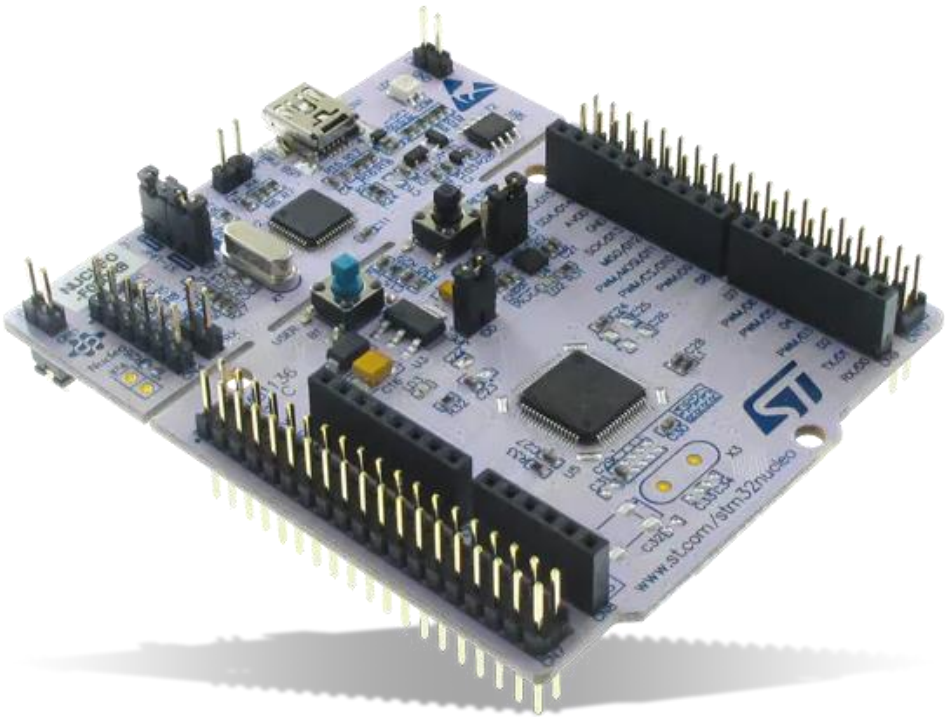

Рисунок 3.3 - Плата для розробки STM32

3.2 Огляд дисплеїв для відображення інформації

Для виконання роботи було потрібно мати візуальну інформацію для вибору режиму роботи, та спостереження за процесом виконання алгоритмів. Вибір пав на OLED дисплеї, і з варіантів було 2, це OLED дисплей з підтримкою I2C шини, чи без нього.

3.2.1 OLED дисплей з I2C шиною

OLED дисплеї з підтримкою I2C шини стають все більш популярними завдяки своїй простоті використання та компактності. I2C - це двопровідна шина зв'язку, яка дозволяє підключати до мікроконтролера кілька пристроїв за допомогою лише двох проводів (SDA та SCL).

З переваг цього дисплею можна виокремити простоту використання, компактність, низьке енергоспоживання, широкий спектр розмірів та якісне

зображення.

I2C шина допомогає спростити роботу з таким дисплеєм, підвищуючи швидкість підключення до нього.

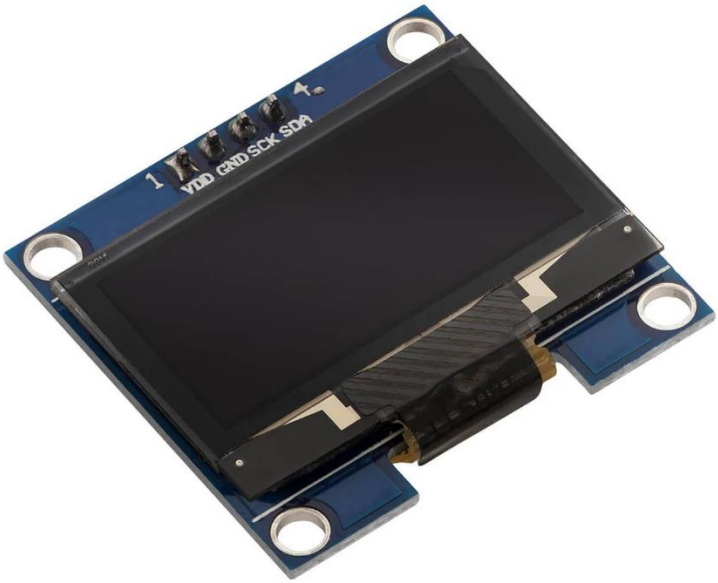

Рисунок 3.4 - Дисплей OLED з I2C шиною

3.2.2 OLED дисплей без I2C шини

OLED дисплеї без I2C шини, як правило, підключаються до мікроконтролера за допомогою паралельного інтерфейсу, який може потребувати більше проводів (зазвичай від 8 до 18) порівняно з двома проводами I2C.

Враховуючи, що цей проект є прототипом для майбутнього пристроя, було вирішено обрати дисплей без I2C шини, щоб краще зрозуміти його роботу.

3.3 Вибір радіомодуля для роботи системи

Українські військові працюють з радіомодулями в діапазоні від 134 МГц до 170 МГц. Але в силу того, що такі частоти використовуються

військовими, доступу до таких радіомодулів у цивільних немає. Тому було вирішено взяти максимально зближений радіомодуль з частотою 433 МГц. [9]

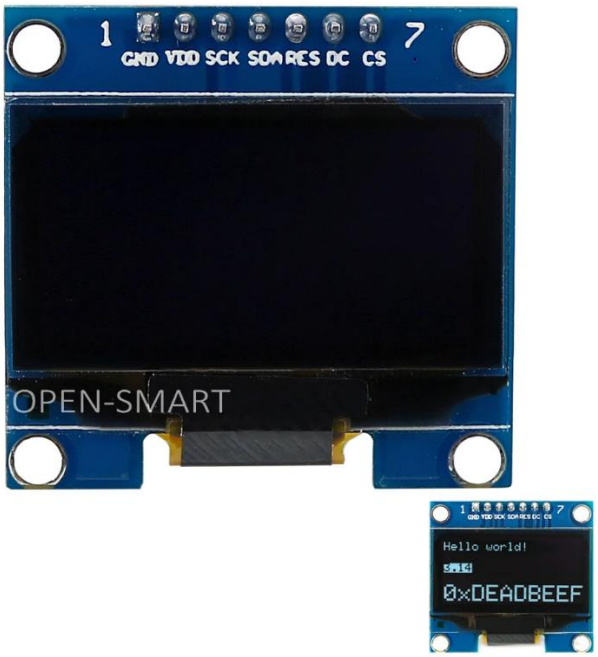

Рисунок 3.5 - OLED дисплей без I2C шини

3.3.1 Платформа FS1000A + MX-RM-5V

FS1000A та MX-RM-5V - це комплект радіомодулів, що працює на частоті 433,92 МГц. FS1000A - це передавач, який використовується для надсилання даних, а MX-RM-5V - це приймач, який використовується для їх отримання.

Ці радіомодулі прості при роботі, компактні та дешеві.

3.3.2 Платформа Si4432

Si4432 - це високопродуктивний радіочастотний трансивер, який може використовуватися як передавач, так і приймач. Він працює в діапазоні

частот 433-473 МГц, що робить його придатним для широкого спектру застосувань.

Рисунок 3.6 - FS1000A та MX-RM-5V

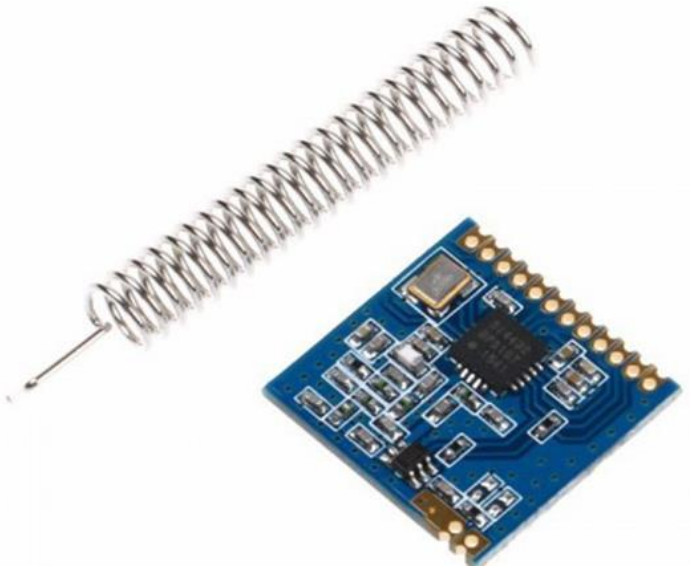

Рисунок 3.7 - FS1000A та MX-RM-5V

Він може використовуватися для бездротового керування, зчитування даних з датчиків, систем безпеки, автоматизацій будівель тощо.

З переваг можна вказати широкий діапазон, високу потужність, чутливий приймач, низьке споживання енергії та можливість працювати як передавач та приймач.

Для виконання роботи було обрано радіомодулі FS1000A + MX-RM-5V.

3.4 Огляд бібліотек для радіомодулів

3.4.1 Бібліотека VirtualWire

VirtualWire - це популярна бібліотека з відкритим кодом для Arduino, яка спрощує роботу з радіомодулями на частоті 433 МГц, такими як CC1101, Si4432 та RA-02. Вона надає простий інтерфейс для надсилання та прийому даних бездротовим способом. [10]

Переваги бібліотеки:

- надає простий інтерфейс з функціями для надсилання та прийому даних;
- підтримує різні типи модуляції, такі як ASK, OOK і FSK, а також різні швидкості передачі даних;
- використовує алгоритми корекції помилок для забезпечення надійної передачі даних у зашумованих середовищах;
- має велике та активне співтовариство користувачів, що робить його легким для отримання допомоги та обміну досвідом.

Але ця бібліотека вже застаріла, тож її було відкинуто.

3.4.2 Бібліотека RadioHead

RadioHead - це об'єктно-орієнтована бібліотека з відкритим кодом для Arduino, яка спрощує роботу з різними радіомодулями на частоті 433 МГц, такими як CC1101, Si4432, RA-02 та SYN115.

Переваги бібліотеки:

- підтримує широкий спектр радіомодулів та функцій, що робить її універсальною для різних проектів;

- використовує об'єктно-орієнтований підхід, що робить її код зрозумілим, легким у використанні та розширюваним;

- має детальну документацію, яка полегшує її вивчення та використання;

- має активну спільноту користувачів, що робить його легким для отримання допомоги та обміну досвідом.

3.4.3 Бібліотека RCSwitch

RCSwitch - це популярна бібліотека з відкритим кодом для Arduino, яка спрощує роботу з радіомодулями на частоті 433 МГц, такими як RFlink, Powercode, Jaycar, Elenco та Kemo.

Вона надає простий інтерфейс для надсилання та прийому кодируваних даних, таких як коди пультів дистанційного керування та сигнали датчиків.

3.4.4 Бібліотека Gyver433

Gyver433 - це легка та швидка бібліотека для Arduino, яка спрощує роботу з радіомодулями 433 МГц, такими як Si4432, CC1101, RA-02 та FS1000A. Вона відрізняється від інших бібліотек тим, що не використовує переривання та таймери, що робить її гнучкою та економною для ресурсів.

Можливості бібліотеки:

- надає простий інтерфейс з функціями для надсилання та прийому даних, що робить її зручною для початківців;

- використовує прямий доступ до пам'яті та оптимізовані алгоритми, що робить її однією з найшвидших бібліотек для радіомодулів 433 МГц;

- ця бібліотека не використовує переривання та таймери, що робить її

сумісною з різними типами плат Arduino та іншими бібліотеками;

- економно використовує ресурси плати для розробки, що робить її придатною для портативних проектів.

Я вирішив зупинитися на бібліотеці Gyver433, як найбільш оптимальний варіант для конкретного проекту.

4 ОГЛЯД ТА РЕАЛІЗАЦІЯ СИСТЕМИ ОМАНЛИВИХ РАЦІЙ

4.1 Загальний опис системи

Сама по собі, система оманливих рацій - це радіопередавачі, які використовуються для імітації сигналів законних радіостанцій з метою введення в оману або обману інших користувачів радіочастотного спектру. Тобто, в нас є пристрої, що виробляють радіо / Wi-Fi сигнали, які мають бути захоплені системами РЕБ супротивника. Самі по собі, оманливі рації поділяються на три типи:

- системи імітацій. Такі оманливі рації перехоплюють або записують сигнали цільових радіостанцій, а потім повторюють їх з іншого місця або з іншою метою;

- системи генерації. Такий тип оманливих рацій генерує фейкові радіосигнали, які не є копіями законних передавачів;

- системи імітації зазвичай більш складні та дорогі, але вони можуть бути більш реалістичними та складнишими для виявлення ніж системи генерації. Системи генерації більш дешеві та простіші, але через це їх легше викрити.

Сама ідея таких рацій не нова, і є декілька дуже відомих прикладів, де використовувався такий самий принцип, як у оманливих раціях:

- висадка в Нормандії. Де Німеччина використовувала оманливі рації, для імітації британських радіопередач, щоб ввести в оману союзників;

- в'єтнамська війна. Північнов'єтнамці використовували оманливі рації для перешкоджання американським радіопередачам та для створення фейкових новин;

- війна в Іраку. Ірак використовував оманливі рації для імітації американських радіопередач, щоб ввести в оману іракських дезертирів.

Ідея полягала в тому, щоб створити універсальний пристрій, який міг

би працювати як використовуючи Wi-Fi, так і радіообмін, в залежності від вибору режиму для роботи.

4.2 Огляд функціональної принципової схеми

Задля якісної реалізації, було розроблено функціонально-принципову схему пристроя. Ця схема показує загальне представлення проекту, враховуючи всі його електричні компоненти.

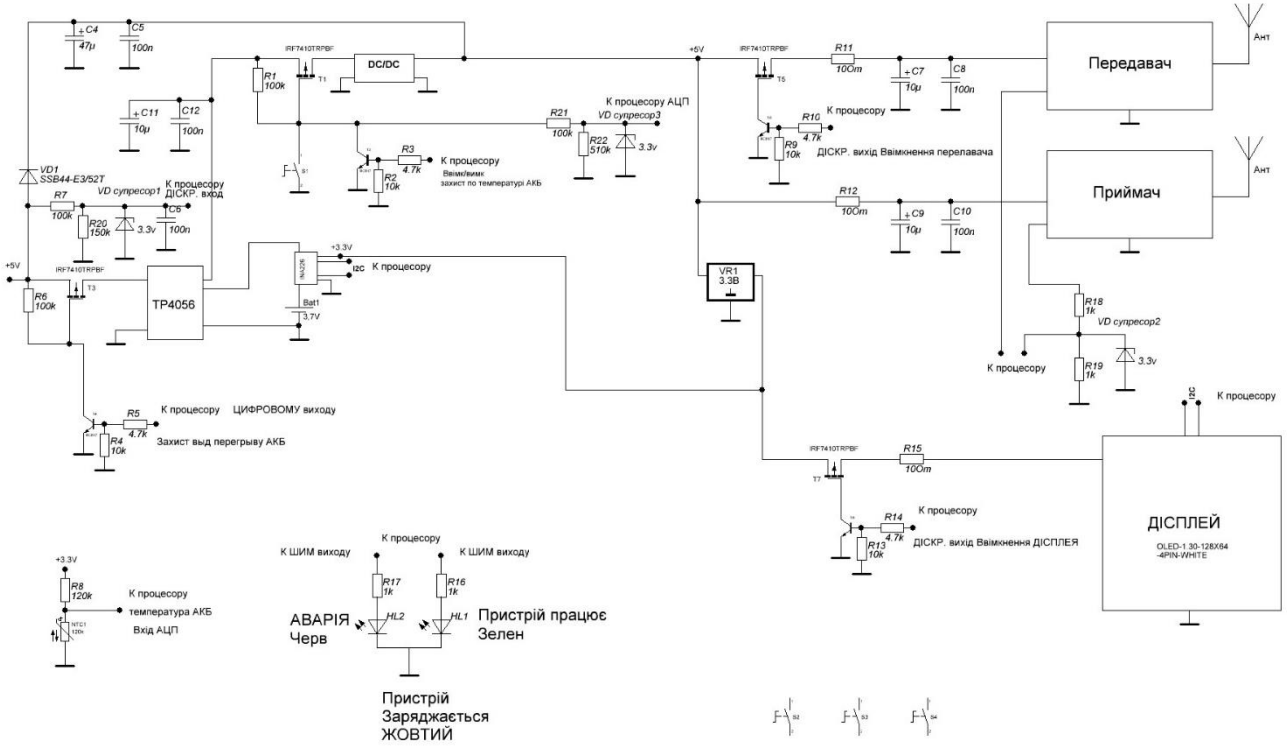

Рисунок 4.1 - Функціонально-принципова схема

На цій схемі показано всі компоненти, які буде в собі включати фінальний продукт. Сама схема складається з:

- центрального процессора;
- передавача;
- приймача;
- дисплея;

- клавіатури;
- зарядного пристрою;
- li-ioh аккумулятор для живлення ємністю мінімум 2500 mAh;
- інші дрібні периферійні компоненти.

Завдяки невеликій кількості електричних компонентів, було досягнуто простоти збірки, невеликих розмірів та відносної дешевизни продукту. Це дає переваги у масовому випуску таких продуктів.

4.3 Огляд архітектурної схеми та режимів роботи

Сама архітектура проекту не дуже вибаглива до заліза, і в об’єднанні з доволі потужним ESP32 ми отримуємо високу швидкість роботі з мінімальним навантаженням на пристрій. Нижче описана архітектура проекту, з поясненням основних його частин, і також блок схема архітектури.

Робота починається з запуску проекту, і програма шукає в своїй пам’яті, чи є збережені режими. У випадку, якщо вони є, програма пропускає момент з ручним вибором режимів, і одразу починає налаштовувати пристрій під обрані режими. В іншому випадку, користувач має обрати потрібні йому режими. Режими поділяються на MASTER/SLAVE та RADIO/WIFI.

Після запуску з обраним режимом, програма починає нескінченний цикл роботи. Ця робота полягає в пошуку повідомлень, обробки запитів та надсилання відповідей. У випадку, якщо SLAVE пристрій втрачає зв’язок з MASTER пристроєм, і цей зв’язок не поновлюється протягом якогось часу, SLAVE пристрій може стати MASTER пристроєм, та виконувати всі його алгоритми. Завдяки цьому, система може працювати незалежно від втручання людини допоки не сяде аккумулятор або усі пристрої не будуть знищені.

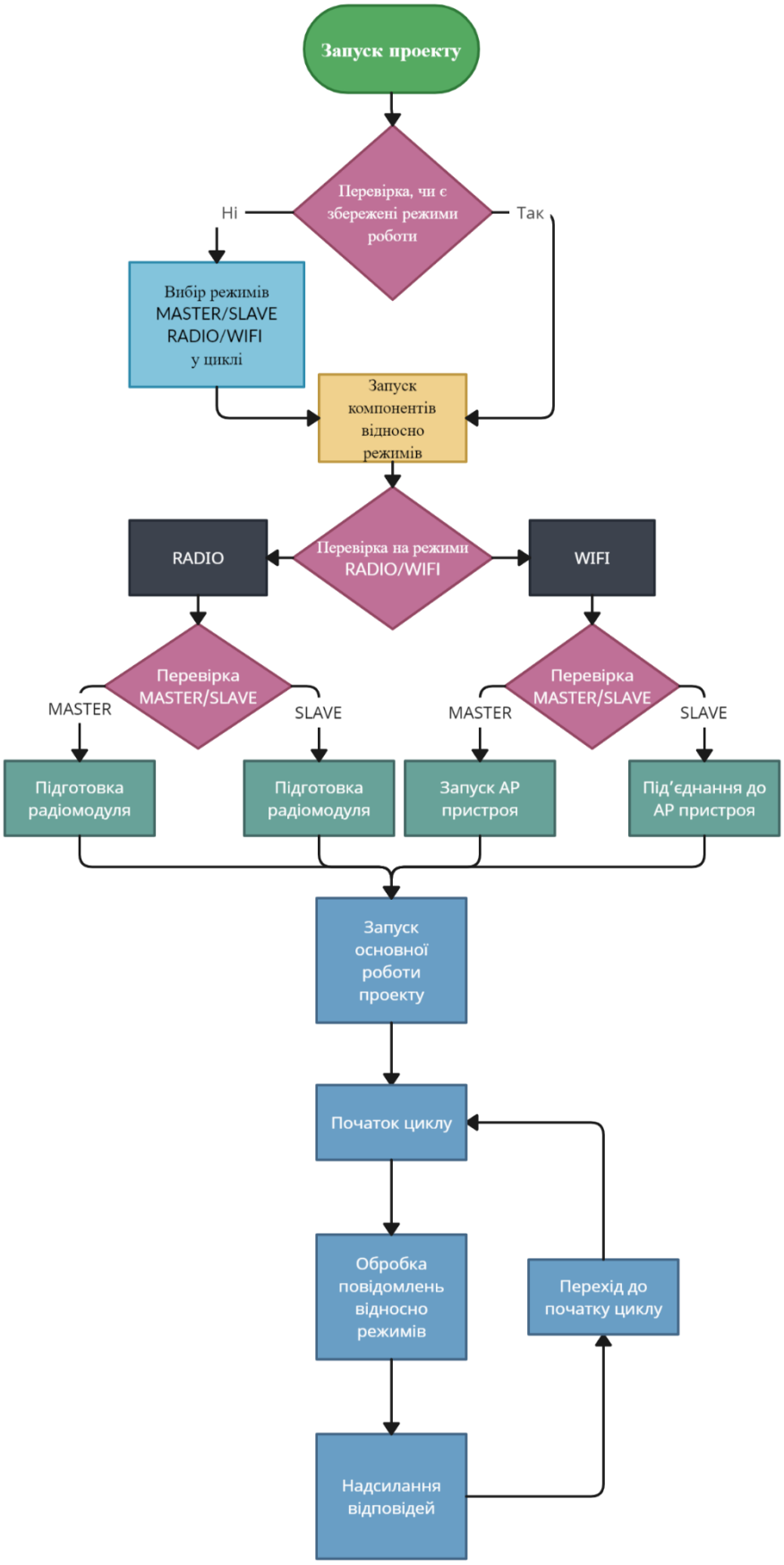

Рисунок 4.2 – Схема роботи системи

4.3.1 Огляд режимів та команд MASTER та SLAVE

Враховуючи, що у кожному підрозділі є командир, а у Wi-Fi з’єднанні є роутер, було розділено логіку режимів на MASTER та SLAVE.

4.3.1.1 Команди та режим MASTER

Режим MASTER є головним пристроєм, до якого приєднуються інші SLAVE пристрої. Під час з’єднання, SLAVE пристрої передають свої унікальні ID, які MASTER зберігає до свого масиву. Порядок елеменетів у масиві айді визначає, який з SLAVE елементів стане MASTERом у випадку знищення або вимкнення поточного MASTER пристроя.

Також, у нього є можливість обробляти команди від SLAVE пристроїв, які просять якийсь набор даних для імітації спілкування.

Тож, команди які може обробляти MASTER режим це:

- IP - команда для додавання нового айпі пристроя до масиву з'єднаних пристроїв;

- GT - команда для відправки масиву під’єднаних пристроїв SLAVE пристрою;

- DT – випадковий набір даних, який відправляється SLAVE пристрою для імітації спілкування.

4.3.1.2 Команди та режим SLAVE

SLAVE режим є режимом, при якому пристрій шукає MASTER пристрій для з’єднання. В цьому випадку SLAVE пристрій робить запити до MASTER, щоб отримати потрібні йому дані. У випадку, якщо IP SLAVE пристроя є першим в масиві IP пристроїв MASTER, то такий SLAVE пристрій стає MASTER пристроєм, зберігая налаштування режимів.

До команд, які може обробляти SLAVE режим відносяться:

- IG: Команда для отримання масиву IP від MASTER пристрою.

4.3.2 Огляд режимів RADIO та WIFI

4.3.2.1 Команди та режим RADIO

Цей режим має в собі роботу з радіомодулем. Так як у радіомодулів немає явного вибору головного та залежного модулів, це було зроблено програмно. В пристрої є як відправник радіосигналів так і отримувач, тож при роботі він може як відправляти так і отримувати повідомлення відносно режиму MASTER або SLAVE.

Режим постійно сканує радіопростір, шукаючи повідомлення, і коли його знаходить, то обробляє та відправляє в етер відповідь.

4.3.2.2 Команди та режим Wi-Fi

Цей режим працює з Wi-Fi модулем пристроя. У випадку вибору режиму MASTER, створюється точка доступу (AP), яка випадковим чином обирає назву для точки доступу з масиву збережених назв. Після цього, пристрій очікує з’єднання з іншими пристроями, та обробляє команди, які отримує від них.

Якщо обрали режим SLAVE, то пристрій починає перебирати масив збережених Wi-Fi назв, на кожну з яких дається 100 спроб під’єднатися. Після успішного з’єднання надсилається IP адреса пристроя, що і починається звичайний обмін повідомленнями по запитам від SLAVE пристроя.

4.4 Вибір оптимальної відстані між пристроями для забезпечення максимальної якості і швидкості роботи

Враховуючи, що якість сигналу у радіо та Wi-Fi модулів залежить від відстані між пристроями, наявності перешкод та інших факторів, є потреба в

розрахунку оптимальної відстані між пристроями для максимального ефекту.

4.4.1 Розрахунок відстані для радіомодулів FS1000A та MX-RM-5V

Як ми бачимо на графіку, пристрої з різним живленням, видають доволі схожу чутливість відносно відстані. Але, видно що при живленні у 5V, маємо найкраще співвідношення чутливості відносно відстані. Відомо, що для більшості радіомодулів оптимальним буде значення dBm у межі до -90, у рідких випадках до -100. Але я обрав варіант зі значенням у межах до -90. По графіку видно, що таке значення чутливості є в межах відстані до 300м, що підходить під середню відстань розрахунку військових на позиціях.

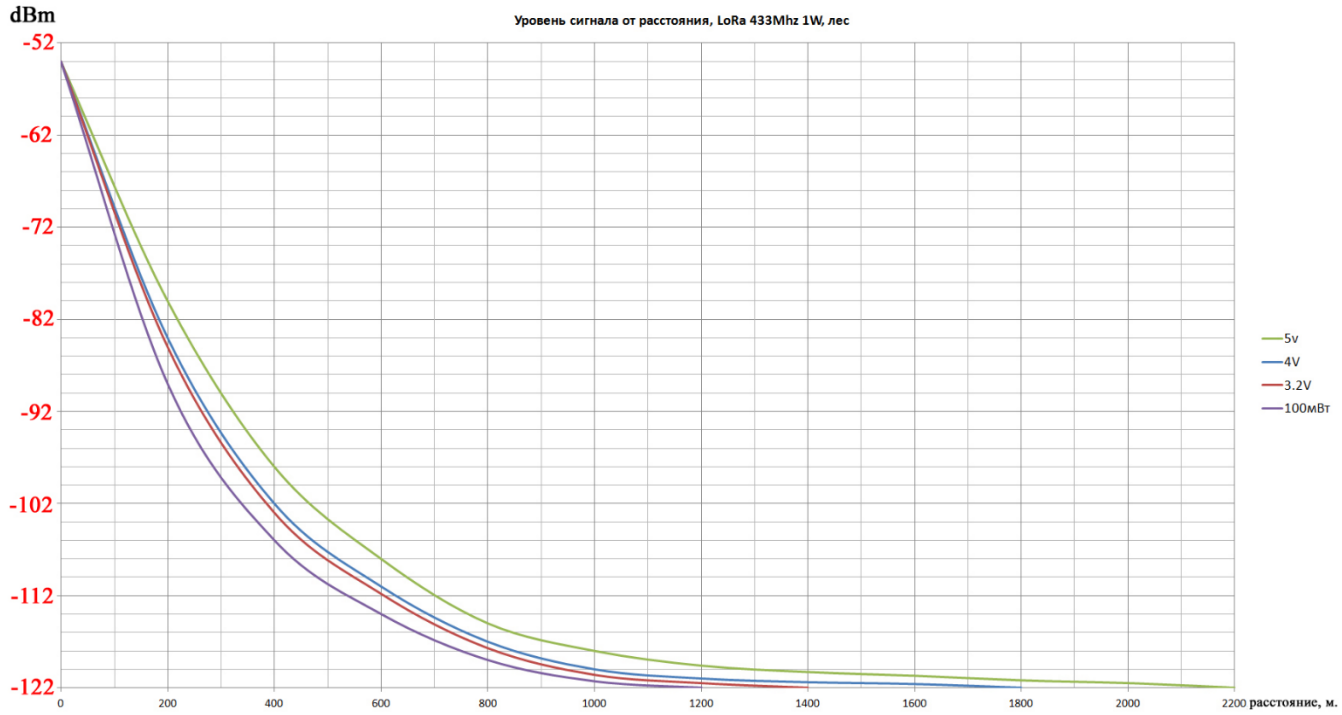

Рисунок 4.3 - Порівняння рівня чутливості сигналу радіомодуля відносно відстані

4.4.2 Розрахунок відстані для Wi-Fi модулів ESP32

Відносно цього графіку видно, що максимальна дальність з’єднання Wi-Fi модулів є 84 метри зі стандартним передавачем, тож ця відстань також нам підходить. Тож маючи оці дані, можна сказати, що якщо пристрої будуть працювати лише як Wi-Fi, то їх треба класти в межах до 84м (80, бо є похибка по відстані та людський фактор). А для радіомодулів, відстань збільшується для 300м, що дає більше простору для дій.

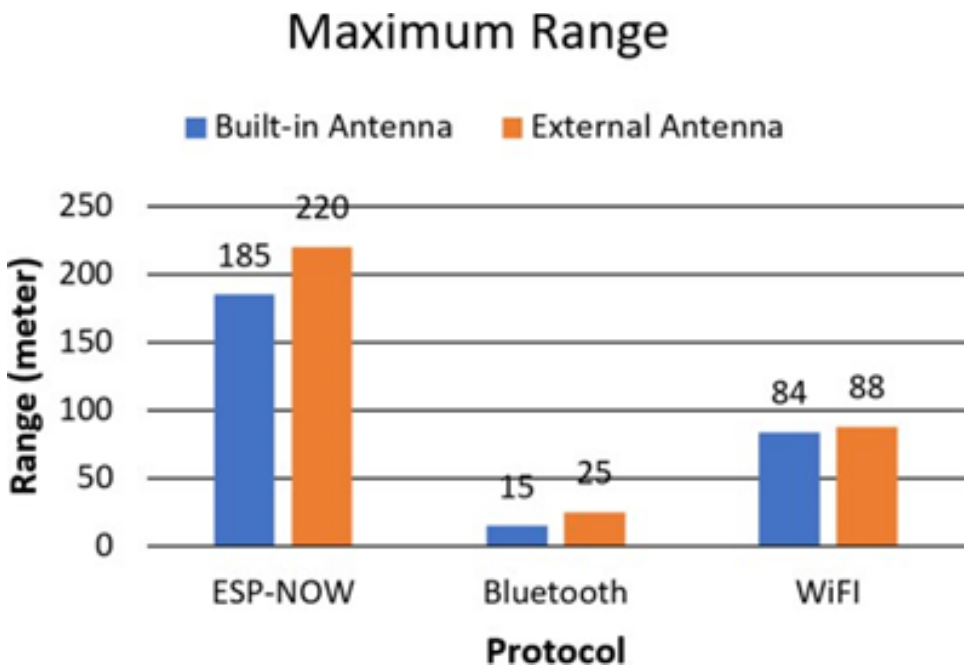

Рисунок 4.4 - Графік дальності сигналів Wi-Fi, Bluetooth, ESP-NOW у ESP32

4.5 Імплементація системи

Наведений нижче код є частиною проекту, яка відповідає за вибір режимів роботи. Він перевіряє, чи є збережені налаштування для режимів роботи, та у випадку, якщо ні, запускається нескінченний цикл, який чекає вибору спочатку MASTER або SLAVE, а потім RADIO або WIFI.

Лістинг 4. 1 - Реалізація меню вибору проекта

```
if (masterSlaveAction.isEmpty() && radioWifiAction.isEmpty())
  {
    String masterSlaveMenu[2] = {"MASTER", "SLAVE"};
    String radioWifiMenu[2] = {"RADIO", "WIFI"};
    String currentMenu[2];
    String defaultAction = "DEFAULT";
    int currentPos = 0;
    isActionSetted = false;

    while (!isActionSetted)
    {
      if (currentPos == 0)
      {
        currentMenu[0] = masterSlaveMenu[0];
        currentMenu[1] = masterSlaveMenu[1];
      }
      else
      {
        currentMenu[0] = radioWifiMenu[0];
        currentMenu[1] = radioWifiMenu[1];
      }

      TextDisplay(currentMenu[cursor]);

      uint16_t val = analogRead(KEYBOARD_OUT);

      String value = getAction(val);

      if (value.equals(defaultAction))
      {
        delay(150);
        continue;
      }

      defaultAction = value;

      if (value.equals("OK"))
      {
        if (currentPos == 0)
        {
          masterSlaveAction = currentMenu[cursor];
          currentPos++;
          cursor = 0;
          delay(150);
        }
        else
        {
          radioWifiAction = currentMenu[cursor];
          isActionSetted = true;
        }
      }
      else if (value.equals("LEFT"))
      {
        cursor -= 1;
      }
      else if (value.equals("RIGHT"))
      {
        cursor += 1;
      }

      if (cursor > 1)
      {
```

```
      cursor = 0;
    }
    else if (cursor < 0)
    {
      cursor = 1;
    }

    delay(150);
  }
}
```

Наступний алгоритм вже опрацьовує обрані режими, і робить дії відносно їх. У випадку, якщо пристрій працює у стані роутера, то береться випадкове число для назви роутера, та ставиться стандартний пароль. У випадку, якщо пристрій у стані підключення до роутера, то він через цикл намагаєтсья під’єднатися до будь якого роутера, який є в базі назв. Якщо під’єднання не успішне, то пристрій перезавантажуєтсья.

Лістинг 4.2 - Реалізація налаштування проекту відносто вибраних режимів

```
if (radioWifiAction.equals("WIFI"))
 {
   if (masterSlaveAction.equals("MASTER"))
   {
     uint8_t rand = random(0, 7);
     WiFi.mode(WIFI_AP);
     TextDisplay(ssid[rand]);
     WiFi.softAP(ssid[rand], password);

     server.begin();
   }
   else if (masterSlaveAction.equals("SLAVE"))
   {
     WiFi.mode(WIFI_STA);
     WiFi.onEvent(WiFiEvent);
     bool isConnected = false;

     for (int i = 0; i < 7; i++)
     {
       TextDisplay("Connect to");
       TextDisplay(ssid[i]);
       delay(100);

       int counter = 0;
       WiFi.begin(ssid[i], password);

       while (counter < 100)
       {
         if (WiFi.status() == WL_CONNECTED)
         {
           isConnected = true;
           break;
         }
```

```
        delay(100);
        counter++;
      }

      if (isConnected)
      {
        break;
      }
    }

    if (isConnected)
    {
      WiFiClient client;

      if (client.connect("192.168.4.1", 80))
      {
        TextDisplay("SEND LOCAL IP");
        currLocalIP = WiFi.localIP().toString();
        String localIP = "IP:" + currLocalIP + ";";

        TextDisplay(localIP);

        client.print(localIP);

        delay(100);
        client.stop();
      }
    }
  }
  else
  {
    esp_restart();
  }
}
else if (radioWifiAction.equals("RADIO"))
{
  if (masterSlaveAction.equals("MASTER"))
  {
    attachInterrupt(0, isr, CHANGE);
  } else if (masterSlaveAction.equals("SLAVE")) {
attachInterrupt(0, isr, CHANGE);
      uint64_t chipId = ESP.getEfuseMac();

      String id = "IP:" + String(chipId, HEX);

      tx.sendData(id);
  }
}
else
{
  esp_restart();
}
```

Далі йде циклічна програма яка займається прослуховуванням, обробкою та надсиланням команд. Ця программа отримує повідомлення, розбиває його на ключ-значення, та надсилає відповідь.

Лістинг 4.3 - Реалізація циклічної роботи програми

```
void loop()
{
  if (radioWifiAction.equals("WIFI"))
  {
    if (masterSlaveAction.equals("MASTER"))
    {
      uint8_t nums = WiFi.softAPgetStationNum();

      TextDisplay(to_string(nums).c_str());

      WiFiClient client = server.available();

      if (client)
      {
        TextDisplay("accepted");

        String res = client.readStringUntil(';');

        if (!res.isEmpty())
        {
          String key = getKey(res);
          String value = getValue(res);

          String processRes = processMasterCommand(key, value);

          client.flush();

          client.println(processRes);
        }

        client.stop();
      }
    }
    else if (masterSlaveAction.equals("SLAVE"))
    {
      WiFiClient client;
      if (client.connect("192.168.4.1", 80))
      {
        if (queryCount == 10)
        {
          client.flush();

          client.print("GT;");
          queryCount = 0;
        }
        else
        {
          client.flush();

          client.print("DT;");
        }

        String res = client.readStringUntil(';');

        if (!res.isEmpty())
        {
          String key = getKey(res);
          String value = getValue(res);

          String processRes = processSlaveCommand(key, value);
          client.flush();
```

```
          client.println(processRes);
        }
        else
        {
          TextDisplay("EMPTY");
        }

        client.stop();
      }
      queryCount++;

      delay(random(500, 2000));
    }
  }
  else if (radioWifiAction.equals("RADIO"))
  {
    if (radioWifiAction.equals("MASTER"))
    {
      if (queryCount == 10)
      {
        tx.sendData("GT;");
        queryCount = 0;
      }
      if (rx.gotData())
      {
        String res;
        rx.readData(res);

        String key = getKey(res);
        String value = getValue(res);

        String processRes = processMasterCommand(key, value);

        tx.sendData(processRes);
      }
    }
    else if (radioWifiAction.equals("SLAVE"))
    {
      if (queryCount == 10)
      {
        tx.sendData("GT;");
        queryCount = 0;
      }
      else
      {
        tx.sendData("DT;");
      }

      if (rx.gotData())
      {
        String res;
        rx.readData(res);

        String key = getKey(res);
        String value = getValue(res);

        String processRes = processSlaveCommand(key, value);

        tx.sendData(processRes);
      }
    }
    queryCount++;
  }
}
```

ВИСНОВКИ

В сучасному світі, у стані війни, проблема протидії системам РЕБ є надзвичайно актуальною та важливою. І задля виправлення цієї проблеми, найбільші світові виробники, компанії, військові інститути працюють над способами подолання цих систем. В даній магістерській роботі ми провели розробку та локальне тестування пристроїв, які можуть вводити ворожі системи РЕБ в оману, чим захистять військових та різні військові та цивільні об’єкти, викликаючи вогонь на себе.

Як згадувалося вище, цей пристрій може працювати як з радіомодулями, так і з Wi-Fi пристроями. Пристрій має невеликі розміри, маленьку ціну, швидке налаштування роботи та автономність. Це все дає велику перевагу для запуску цього пристрою у швидке виготовлення.

Крім того, кожен з пристроїв має доволі великий радіус дії, що дозволяє розмістити його на великій відстані один від одного, та від військових, що є плюсом для їх безпеки. І нарешті, будуть створені такі системи, які зможуть убезпечити військових та об’єкти від ударів. У подальших дослідженнях доцільно доповнити пристрій кращими та потужнішими радіомодулями, антенами, системами безпровідної зарядки та можливо системами самознищення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гурський Т.Г. «Лінії радіозв’язку та антенні пристрої», с. 171-179.

2. John Wiley «Wi-Fi», с. 215

3. Сундар Ганді Санкаран, Сусіндер Раджан Гуласекаран «Wi-Fi 5 protocol and network", с. 177

4. Засорнов О. С. «Програмування мікроконтролерних та робототехнічних систем», с. 23

5. Ліззі Прадер, Пітер Ходді "IoT Development for ESP32 and ESP8266", с. 66

6. Elecia White "Making Embedded Systems: Design Patterns for Great Software 2nd Edition", с. 97-112

7. Ерл Бойсен, Гаррі Кайбетт "Complete Electronics Self-Teaching Guide with Projects", с. 175

8. Брюс А. Фетте, Ден Бенскі “RF and Wireless Technologies: Know It All”, с. 134

9. Джефф Варролл, Роджер Белчер “Data Over Radio Data and Digital Processing Techniques in Mobile and Cellular Radio”, с. 211

10. Ерл Бойсен, Гаррі Кайбетт “Complete Electronics Self-Teaching Guide with Projects”, с. 312