

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Факультет інформаційних технологій
(факультет)

Кафедра системного аналізу та управління
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

Здобувача вищої освіти Городецької Юлії Миколаївни
академічної групи 124-21-1
спеціальності 124 Системний аналіз
за освітньо-професійною програмою Системний аналіз

на тему: *«Оптимізація ведення радіоелектронної розвідки тактичного рівня в сучасних бойових умовах з використанням методів системного аналізу»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	<i>к.т.н., доц. Алексеев О.М.</i>			
розділів:				
Інформаційно- аналітичний	<i>к.т.н., доц. Алексеев О.М.</i>			
Спеціальний розділ	<i>к.т.н., доц. Алексеев О.М.</i>			
Рецензент	<i>д.т.н., проф. Швачич Г.Г.</i>			
Нормоконтролер	<i>к.ф.-м.н., доц. Хом'як Т.В.</i>			

Дніпро
2025

ЗАТВЕРДЖЕНО:

завідувач кафедри

Системного аналізу та управління

(повна назва)

к.т.н., доц. Желдак Т.А.

(прізвище, ініціали)

« ____ » _____ 20 ____ року

ЗАВДАННЯ

на кваліфікаційну роботу

ступеня бакалавра

здобувачу вищої освіти Городецькій Ю. М. академічної групи 124- 21-1

спеціальності: 124 Системний аналіз

за освітньо-професійною програмою Системний аналіз

на тему «Оптимізація ведення радіоелектронної розвідки тактичного рівня в сучасних бойових умовах з використанням методів системного аналізу»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 17.05.2025 р. №163-с

Розділ	Зміст	Терміни виконання
1. Інформаційно-аналітичний розділ	<i>Проаналізувати структуру об'єкта дослідження. Визначити предметну область дослідження та проблему, що розв'язується. Обґрунтувати методи виконання поставлених завдань</i>	10.01.2025 – 01.03.2025
2. Спеціальний розділ	<i>Розв'язати поставлені задачі: розглянути алгоритми та розробити систему автоматизації ведення радіоелектронної розвідки</i>	01.03.2025 – 10.06.2025

Завдання видано _____

(підпис)

доц. Алексєєв О.М.

(прізвище, ініціали)

Дата видачі: 06.12.2024 р.

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____

(підпис студента)

Городецька Ю. М.

(прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 52с., 4 табл., 14 рисунків, 14 джерел.

Об'єктом дослідження є порівняльна характеристика корисної ефективності SDR приймачів та вибір найбільш вдалих моделей для побудови комплексів автоматизованого чи напівавтоматизованого радіомоніторингу пультів керування БПЛА ударного типу.

Предметом дослідження є SDR приймачі, їх технічні характеристики, вартість та ефективність в застосуванні.

Метою даної кваліфікаційної роботи є аналіз проблем в процесах ведення радіоелектронної розвідки в сучасних бойових умовах а також надання пропозицій з застосування засобів, алгоритмів та ПЗ для їх вирішення.

Основними методами дослідження є: аналіз наявної літератури та наукових робіт, що передували розробці фізичних чіпів модуляції та демодуляції радіосигналу, порівняльна оцінка пропонованих засобів на основі описаних розробниками їх технічних характеристик.

В межах інформаційно-аналітичного розділу розглянута теоретична база Лінійного Програмування, технології SDR, аналогово-цифрової обробки радіосигналів, LoRa модуляції та заснованого на ній протоколу керування БПЛА під назвою ExpressLRS.

Спеціальний розділ включає в себе порівняльний аналіз SDR приймачів для цілей радіорозвідки, огляд та порівняння алгоритмів детекції корисного сигналу в умовах великої кількості шумів та способи демодуляції LoRa пакетів.

Результати цієї роботи можуть бути використані для вибору оптимального підходу та засобів для розробки автоматизованих систем радіоелектронної розвідки, що мають значно ширший за сучасні засоби діапазон робочих частот,

розробки нового програмного забезпечення, що відповідає часу та викликам, які ставляться перед засобами РЕР в сучасних конфліктах.

Структура роботи включає вступ, теоретичні аспекти , огляд літератури, методологію дослідження, аналіз існуючих алгоритмів з цифрової обробки модуляції LoRa, порівняльну характеристику SDR приймачів для задач ведення радіоелектронної розвідки, висновки та список використаних джерел.

ЗМІСТ

ВСТУП

1. ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ РОЗДІЛ

1.1 PEP в контексті виявлення БПЛА

1.2 SDR технологія, як можливий спосіб вирішення проблеми

1.3 Модуляція і демодуляція, теорема Найквіста

1.4 Найбільш розповсюджені моделі SDR приймачів і їх основні характеристики

1.5 Огляд шуканого сигналу, модуляція LoRa, протокол ELRS, ППРЧ

1.6 IQ модуляція в контексті SDR, ШПФ

1.7 Пошук через кореляцію з еталонним символом

1.8 Пошук через детекцію лінійної зміни частоти

1.9 Пошук за допомогою нейронної мережі

1.10 Оптимізація, рівні шуму, швидкість сканування

1.11 Порівняльний аналіз алгоритмів

1.12 Теоретичні відомості з Лінійного Програмування та постановка задачі

2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Вирішення задачі ЛП, представлення результатів

2.2 Аналіз отриманих даних

2.3 Проведення порівняльного аналізу пристроїв

ВИСНОВКИ

ВСТУП

Всю історію людства одним з найбільш простих способів пришвидшити науково-технічний прогрес, ріст економік та темпів виробництва була війна. Вона дозволяє звільнити велику кількість ресурсів з менш важливих напрямків та задач і направити їх, в тому числі, і на розвиток ВПК. Протистояння кількох високо розвинених країн, так чи інакше, мало б призвести до розробки новіших і складніших, більш високотехнологічних видів озброєння, що і сталось під час низки конфліктів, які виникли за останні роки по всьому світу.

Одним з таких видів новоствореної зброї, що показав вражаючі результати на полі бою, стало застосування БПЛА ударного та розвідувального типів. І, оскільки більшість з них радіокеровані, як основний спосіб протидії, посилену увагу отримала також розробка засобів радіоелектронної боротьби та радіоелектронної розвідки.

Найбільш доступним і масовим методом дослідження радіоефіру є використання програмованих радіоприймачів(SDR), які дозволяють не тільки зафіксувати наявність сигналу, але і дістати інформацію, що передавалась, провівши демодуляцію.

Метою цієї роботи є спроба за допомогою методів системного аналізу спроектувати апаратну та програмну частини комплексу радіомоніторингу, який міг би автоматизовано функціонувати на тактичному рівні в зоні бойових дій та надавати необхідну інформацію віддаленому оператору про наявність в радіоефірі різних типів модульованого сигналу, проводити аналіз отриманих з ефіру даних та, в цілому, допомагати в прийнятті рішень про

Для досягнення цієї мети нам необхідно:

1. Провести огляд та аналіз засобів і способів перехоплень радіосигналу пульта керування

2. Описати основні характеристики найбільш відомих моделей SDR приймачів, дослідити їх тактико-технічні характеристики та документацію
3. Описати та вирішити задачу з оцінки корисності кожного конкретного приймача відносно його вартості
4. Провести аналіз отриманих даних, спрогнозувати можливі варіанти застосування приймачів для ведення радіоелектронної розвідки.
5. Навести приклади ПЗ та алгоритмів, які дозволять застосувати обраний приймач для задач радіоелектронної розвідки по виявленню пультів керування ворожих БПЛА.
6. Порівняти запропоновані способи в контексті ведення бойових дій та застосування в тактичних умовах.

Актуальність теми

Внаслідок швидкого технічного розвідку ударних дронів та значного збільшення кількості їх застосувань в останні роки, гостро стоїть питання вироблення протидії загрозі, що збільшується з кожним днем. Розробляються нові засоби радіоелектронного подавлення, досліджуються способи постановки більш ефективних перешкод. Проте, будь-яке подавлення неможливе без виявлення.

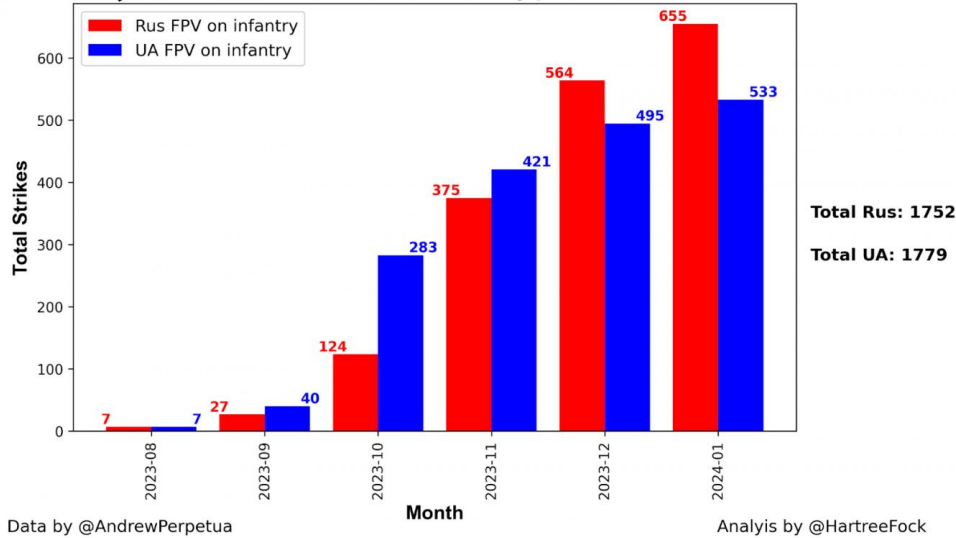


Рисунок 1: статистика застосування фпв дронів в Російсько-Українській війні за 2023-2024 роки

Для того, щоб подавити БПЛА необхідно абсолютно точно зрозуміти частоту, на якій він отримує команди та максимум параметрів налаштувань його пульта керування. Таким чином, РЕБ не може ефективно працювати без РЕР, який, на відміну засобів подавлення, розвивається значно повільніше, ніж мав би.

Ця робота має на меті частково виправити ситуацію, що склалась. Кінцевим результатом, до якого варто прагнути, має стати гнучке, легко налаштовуване програмне забезпечення, в комплексі з доступним, багатофункціональним апаратним комплексом. Пристрій має бути достатньо простим для швидкого розгортання та налаштування, але при цьому давати максимум корисної інформації, без необхідності постійної присутності людини поруч та високої кваліфікації оператора.

Такий комплекс міг би стати максимально важливим доповненням до технічно складних, але високоефективних засобів радіоелектронного подавлення, що розробляються, тестуються та поставляються в останні роки.

1. ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ РОЗДІЛ

1.1 РЕБ в контексті виявлення БПЛА

За останні кілька років розвиток технологій керування БПЛА сягнув своїх висот, і, не зважаючи на це, все ще активно продовжується. Початкові частоти керування були виключно заводського виробництва, завчасно відомі і не мали практично ніякої різноманітності. З подавленням каналів такого зв'язку чудово справлялись в тому числі раніше розроблені і вироблені засоби РЕБ, які проектувались під зовсім інші цілі та задачі.

Проте, з часом з'явилися недорогі методи і технології зміни частот пультів керування БПЛА таким чином, щоб максимально розширити діапазон можливих частот. Це призвело до збільшення можливої смуги частот керування практично в 4 рази. Почали з'являтися нові типи прошивок та способи організації зв'язку в цілому, які дозволяють уникати дії застарілих на даний момент засобів подавлення.

Внаслідок стрімкого розвитку засобів ураження, звичайно, слідує не менш стрімкий розвиток засобів захисту різних видів. І через збільшення кількості можливих варіантів використаних частот керування, складність керування засобами подавлення та виявлення значно виросла, проте складність виявлення пультів зросла в значно більшій мірі. В ручному режимі перебір всіх імовірних частот керування займає катастрофічно багато часу, що повністю зводить нанівець спроби з'ясувати на яких саме частотах керується конкретний дрон, і за час його польоту більше не є можливим дослідити характеристики пульта, який ним керує.

Автоматизований перебір, окрім значного збільшення швидкості сканування, дає можливість для демодуляції сигналу та діставання різної корисної інформації з отриманих даних. Така інформація є критично

важливою для правильного підбору типів перешкод для кожного конкретного дрону.

До розробки засобів автоматизованого перебору робочих частот керування БПЛА є кілька підходів, основний з яких передбачає використання плат приймачів, таких самих, які приймають команди на дроні. Це значно спрощує конструкцію, але має досить важливий недолік: плата може прийняти лише той сигнал, для приймання якого її було створено, і має фізичні обмеження приймача.

Якщо ж з'являються дрони, що керуються на будь-яких нових частотах чи за допомогою нових плат керування, необхідне фізичне оновлення обладнання для їх моніторингу. До того ж, відсутність пристроїв для ведення радіоелектронної розвідки на частотах, що раніше не були помічені в користуванні, дозволяє противнику використовувати ці частоти досить довгий час, поки не буде виявлено їх застосування за допомогою більш складних технічних, чи тактичних пристроїв або заходів. Інколи ці процеси від появи нової загрози до виявлення можуть займати тижні, чи навіть місяці, надаючи ворогу суттєву перевагу в повітрі, і зрештою, на землі, призводячи до втрат позицій чи погіршення логістики, в тому числі на цілих напрямках.

1.2 SDR технологія, як можливий спосіб вирішення проблеми

Software Defined Radio (SDR) — це революційний підхід до побудови радіосистем, в якому більшість функцій традиційного аналогового приймача переноситься у цифрову обробку. SDR надає змогу змінювати параметри прийому програмно, без втручання в апаратну частину, що відкриває широкі можливості для дослідження, моніторингу та реалізації складних протоколів зв'язку.

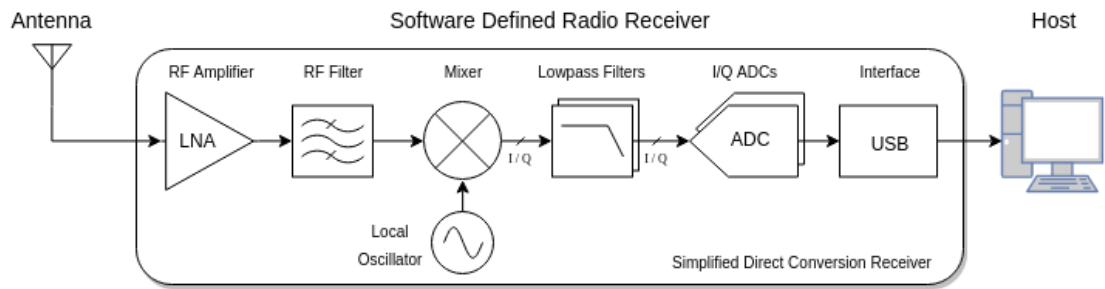


Рисунок 1.1- схема роботи SDR приймача поетапно

SDR складається з мінімального апаратного комплексу, який включає антену, підсилювач, фільтр, перетворювач частоти, генератор локальної частоти (LO) та аналогово-цифровий перетворювач (АЦП). Решта обробки виконується у цифровому вигляді на комп'ютері або мікроконтролері. Це дозволяє гнучко змінювати алгоритми фільтрації, демодуляції, декодування та аналізу сигналів.

Ці компоненти дозволяють програмно замінити собою фізичні елементи, які додавались на приймальному шляху раніше, у вигляді фільтрів, аттенюаторів, підсилювачів, тощо. Архітектура SDR приймачів значно зменшує матеріальну базу необхідних елементів для початку роботи.

Сигнал з ефіру потрапляє на антену, підсилюється і фільтрується, щоб уникнути завад. Потім він зміщується у проміжну частоту або базову смугу за допомогою змішувача та локального генератора. Отриманий сигнал дискретизується АЦП і передається на цифрову обробку. У цифровому вигляді він представлений у вигляді IQ-зразків (In-phase та Quadrature), які дозволяють аналізувати фазу, частоту та амплітуду сигналу.

Зміна параметрів у SDR відбувається шляхом передачі команд на пристрій. Наприклад, при зміні центральної частоти змінюється частота локального генератора (LO), що визначає, яку частину спектру буде приймати система. Також змінюється частота дискретизації (sample rate), підсилення (gain), смуга пропускання (filter width) тощо. Таким чином, SDR може миттєво переключатися між різними діапазонами без зміни апаратної конфігурації.

SDR активно використовується в радіоаматорстві, системах спостереження, наукових дослідженнях, сигнальній розвідці, телекомунікаціях, аналізі протоколів IoT (напр. LoRa, Zigbee, BLE), а також у військових системах та безпілотах. Відкриті платформи на зразок RTL-SDR, HackRF, BladeRF зробили технологію доступною для широкого кола користувачів.

1.3 Модуляція і демодуляція, теорема Найквіста

Модуляцією, в контексті радіозв'язку, називається процес зміни у часі одного або декількох параметрів високочастотного несучого сигналу залежно від заданого інформаційного сигналу.

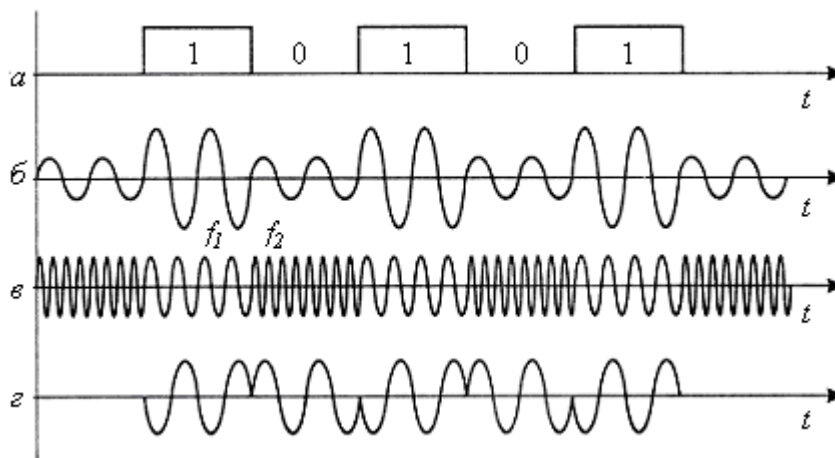


Рисунок 1.2 – основні способи модуляції сигналу: амплітудний, частотний, фазовий

Цей процес застосовується для ефективної передачі інформації на великі дистанції за допомогою радіохвиль, в які ця інформація фактично «запаковується».

З іншого боку, на стороні приймача відбувається зворотній процес, демодуляції, виділення з високочастотних модульованих коливань низькочастотного корисного сигналу.

Модуляція і демодуляція неперервного сигналу, за теоремою Найквіста, для можливості технічної обробки сигналу як на передавачі, так і на приймачі, має відбуватись з певним рівнем дискретності(кількості точок на секунду), який повинен бути мінімум в два рази більшим за максимальну частоту основного сигналу. Отже, для приймання пакета інформації, шириною в 500МГц нам необхідно читати його з частотою дискретизації в 1 ГТ/с (точок на секунду), а якщо ми хочемо просканувати одразу на ширину двох таких пакетів, то необхідна кількість точок(далі - SR) збільшиться до 2 мільярдів точок на секунду.

1.4 Найбільш розповсюджені моделі SDR приймачів і їх основні характеристики

Розглянемо найбільш відомі, але при цьому доступні назагал, моделі програмованого радіо. Окрім їх технічних характеристик нас цікавитиме ціна та додаткові особливості кожного пристрою:

1) RTL-SDR

Бюджетний SDR-приймач, створений на базі цифрових ТВ-тюнерів з мікросхемою RTL2832U. Його популярність обумовлена низькою вартістю, широким частотним діапазоном і підтримкою відкритого програмного забезпечення. RTL-SDR надає змогу вивчати радіозв'язок, аналізувати ефір та створювати власні приймальні системи. Не розглядається як основний пристрій для радіомоніторингу пультів керування через свій обмежений діапазон, а також максимальну ширину смуги, проте може біти частиною більшої системи з декількох приймачів.

Максимальна ширина смуги: 2.4МГц

Діапазон частот сканування: 500кГц – 1.76ГГц

Максимальна частота дискретизації: 2.56 МТ/с

2) HackRF One

Повноцінний дводіапазонний SDR-трансивер (приймач і передавач) з відкритим вихідним кодом та відкритою апаратною архітектурою.

Пристрій був розроблений Майклом Османом і спільнотою Great Scott Gadgets як багатофункціональний інструмент для дослідження радіочастотного спектру. Найбільш розповсюджений пристрій з списку, має найбільшу ком'юніті і найпростіше підключення до комп'ютера. Закриває весь необхідний діапазон.

Максимальна ширина смуги: 20МГц

Діапазон частот сканування: 1МГц – 6ГГц

Максимальна частота дискретизації: 20 МТ/с

3) BladeRF micro

Повнофункціональний SDR-трансивер (приймач і передавач), розроблений компанією Nuand. Він підтримує широкосмугову обробку сигналів, високу частоту дискретизації та гнучке програмне налаштування, що робить його придатним як для промислових застосувань, так і для дослідницьких цілей у сфері цифрового зв'язку. Має високу швидкість сканування, може одночасно працювати з кількома антенами на прийом та передачу. Закриває собою весь необхідний діапазон.

Максимальна ширина смуги: 122.88МГц

Діапазон частот сканування: 47МГц – 6ГГц

Максимальна частота дискретизації: 61.44 МТ/с

4) Aaronia SPECTRAN V6

Один з найсучасніших портативних спектроаналізаторів з функціональністю SDR, створений компанією Aaronia AG (Німеччина). Пристрій призначений для моніторингу, аналізу та виявлення радіочастотних сигналів у режимі реального часу. Завдяки підтримці широкої смуги, високій роздільності та унікальній архітектурі, SPECTRAN V6 Plus підходить як для наукових досліджень, так і для військового чи промислового застосування. Величезна швидкість сканування та обробки сигналів. Закриває собою весь необхідний діапазон частот.

Максимальна ширина смуги: 80МГц

Діапазон частот сканування: 10МГц – 8ГГц

Максимальна частота дискретизації: 2 ГТ/с

Для зручності внесемо всі необхідні зібрані дані в таблицю:

Таблиця 1.2

Основні характеристики SDR приймачів

№	Назва моделі	SR(точок на с)	BW	Ціна
1	RTL-SDR	2.56 МТ/с	2.4МГц	1594 грн
2	HackRF One	20 МТ/с	20МГц	14278 грн

3	BladeRF micro	61.44 МТ/с	122.88МГц	22680 грн
4	Aaronia SPECTRAN V6	2 ГТ/с	80МГц	167904 грн

1.5 Огляд шуканого сигналу, модуляція LoRa, протокол ELRS, ППРЧ

Для того, щоб сформулювати будь-який алгоритм пошуку корисного сигналу необхідно спочатку визначити який саме сигнал ми шукаємо, і в подальшому відштовхуватись в своїх дослідженнях від його характеристик та способів застосування.

Для керування БПЛА як мультироторного типу, так і розвідувальних літакового типу, зазвичай застосовується тип модуляції, який має комерційну назву LoRa(від англ. “Long Range” – далека дистанція). Він використовує такий принцип модуляції корисного сигналу, як CSS – Chirp Spread Spectrum. Суть цього типу модуляції полягає у використанні імпульсів сигналу, частота якого змінюється за лінійним законом.

Саме цей тип модуляції використовується в першу чергу тому, що має високу стійкість до будь-яких радіоелектронних перешкод, дозволяє передавати сигнал на далекі дистанції при малій потужності передавача та невеликому споживанні електроенергії. Цей тип модуляції сигналу єдиний, що може бути знайдений та демодульований при силі сигналу нижче рівня загального шуму.

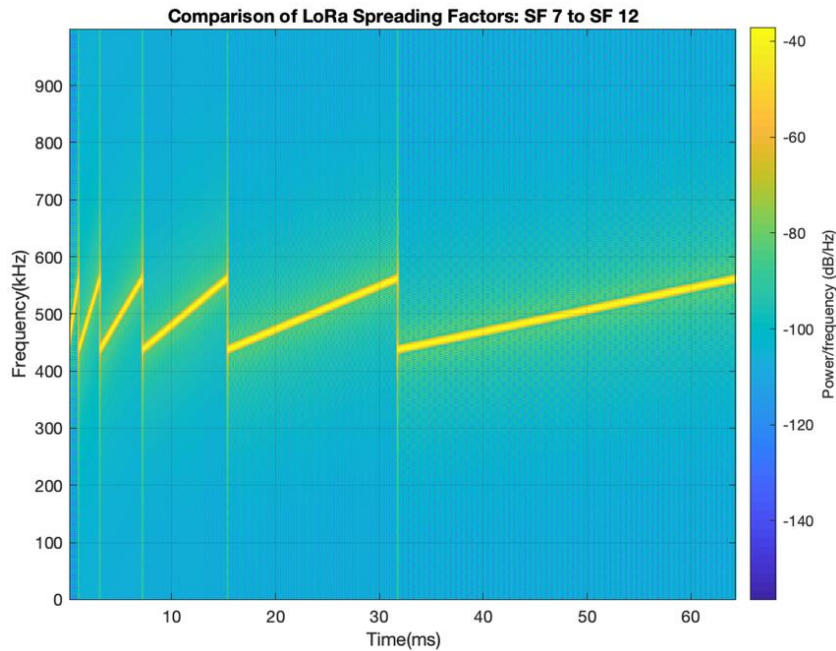


Рисунок 1.3 – порівняння ширини та нахилу символів LoRa для різних варіацій налаштувань

На малюнку вище зображені базові символи модуляції LoRa, так звані «чірпи»(Chirp англ.). Як можна помітити, вони мають різну довжину та швидкість зміни несучої частоти, що візуально на спектрограмі виглядає як похила лінія, кут нахилу якої може варіюватись. Модуляція сигналу відбувається за допомогою кодування корисної інформації в символи різної довжини, з перериванням в різних місцях.

Одним з ключових параметрів в модуляції LoRa є поняття «спрединг фактору» (Spreading Factor англ.), він може варіюватись від SF7 до SF12. Цей параметр визначає скільки символів є в алфавіті при передачі(кількість символів, які може розрізнити приймач і передавач), якою буде довжина кожного символу та скільки часу буде передаватись один пакет інформації. Фактично, від цього параметру залежить швидкість передачі даних, а, в контексті керування БПЛА, ще й маневреність та затримка в часі між отриманням команди і її виконанням.

Швидкість передачі даних для різних варіантів налаштувань LoRa

SF	Розмір символу (кількість символів в алфавіті)	Час передачі одного пакета	Бітрейт
7	128	56 мс	5469 біт/с
8	256	103 мс	3125 біт/с
9	512	205 мс	1758 біт/с
10	1024	371 мс	977 біт/с
11	2048	741 мс	537 біт/с
12	4096	1483 мс	293 біт/с

Загалом, чим більше SF – тим довша робоча дистанція – тим менша швидкість передачі даних – тим стійкіший зв'язок до засобів подавлення, і навпаки. Менший SF дозволяє швидше передавати дані, проте є менш стійким до радіоелектронних перешкод.

Передавач і приймач завчасно програмуються однаково розуміти значення чірпів, і демодуляція, як така, алгоритмічно проводиться за допомогою порівняння отриманого символу з базою символів на приймачі. Для цього отриманий чірп множиться на чірп зі зворотнім нахилом, таким чином в місці їх перетину утворюється імпульс, що і є по суті значенням переданого символу.

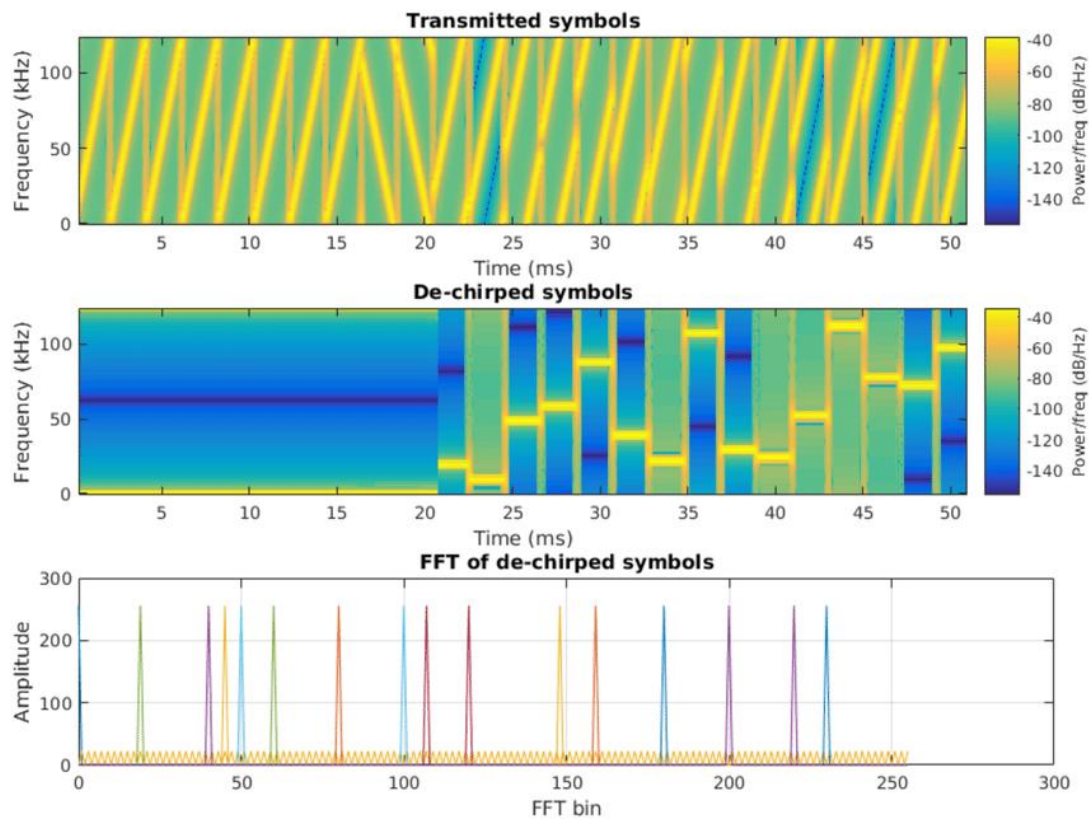


Рисунок 1.4 – демодуляція LoRa

Пакет інформації завжди складається з наступних елементів:

- 1) Преамбула: декілька базових символів повної довжини підряд, вони означають початок пакету, оскільки мало ймовірно, що така послідовність попадеться під час передачі саме корисних даних
- 2) Хедер пакету: в цьому місці знаходиться загальна інформація про пакет та підпис хедеру
- 3) Основна частина пакету, де знаходиться вся корисна інформація, в нашому випадку містить команди дрону
- 4) Підпис, для ідентифікації основної частини пакету, за допомогою цього підпису дрон розуміє, що команда відправлена саме йому

Побітова розбивка елементів пакету виглядає наступним чином:

Побітовий опис структури пакету LoRa

Початковий біт	Назва елементу
0	Розмір основної частини(1 байт)
8	Код рейт, розмір матриці (3 біта)
11	Чи присутній підпис(1 біт)
12	Підпис хедера - верхній шматочок(4 біта)
16	Підпис хедера – нижній шматочок(4 біта)
20	Основна частина(від 0 до 255 байт)
20+8*(розмір ОЧ)	Підпис основної частини(2 байти), може бути відсутній

Отже, з наявної інформації про структуру та склад пакету, можна зробити кілька висновків:

- Преамбулу пакету можна використовувати як варіант ідентифікації наявності LoRa модуляції в ефірі, якщо відома завчасно ширина символу, або SF
- По повтору одного і того ж самого повного символу можна зрозуміти де знаходиться початок пакету
- Якщо при спробі демодуляції декілька пакетів мають однаковий елемент підпису – імовірно їх відправив один і той самий передавач

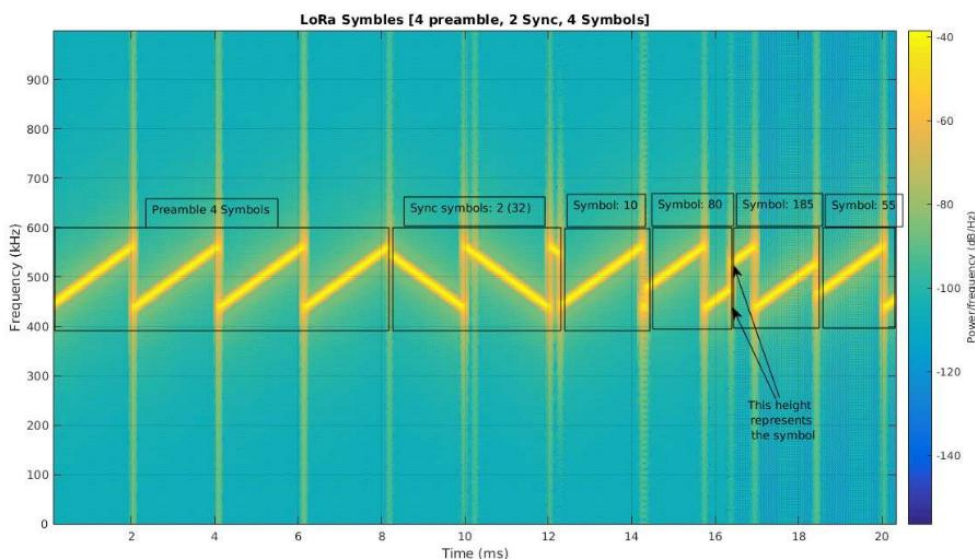


Рисунок 1.5 – структура пакету інформації LoRa

В майбутньому це може дати змогу виділяти статистику для кожного окремого виявленого пульта керування, проводити аналітику застосовуваних частот керування конкретним розрахунком, аналізувати години активності точок вильоту, тощо. А також, при достатньому часі на сканування, зрозуміти всю ширину ППРЧ.

В той час, як LoRa – це спосіб модуляції сигналу, найбільш розповсюдженим саме протоколом керування є ELRS(ExpressLRS). Він має відкритий код і був розроблений спільнотою ентузіастів для керування радіокерованими моделями різних типів, від крил і дронів мультироторного типу, до катерів чи наземних роботизованих платформ.

Це відкритий протокол радіозв'язку з надзвичайно низькою затримкою, великою дальністю і високою надійністю, що використовується для керування безпілотними літальними апаратами (FPV-дронами). Його поява викликала справжню революцію у сфері дронів, завдяки гнучкості, потужності та відкритості платформи. Основна ідея — реалізація максимальної продуктивності та адаптивності на LoRa-сумісному апаратному забезпеченні.

На основі протоколу ExpressLRS було створено низку кастомних протоколів керування БПЛА, що мають свої змінені алгоритми генерації підпису пакетів, структурі пакету та кодуванні команд. Проте, вони все одно використовують LoRa для організації радіозв'язку, тому алгоритми пошуку та детекції будуть дійсними і для цих перероблених протоколів теж.

Протокол ELRS використовує таку технологію, як ППРЧ. Це технологія розширення ширини спектра частот, що широко застосовується у військовому та цивільному зв'язку для підвищення надійності й захищеності передачі даних. У сучасних протоколах керування безпілотними апаратами є критичною складовою, яка дозволяє зменшити вплив перешкод і знижує ймовірність перехоплення сигналу.

ППРЧ була розроблена у середині ХХ століття (1940-і роки), зокрема для військового зв'язку, де потрібно було уникати перешкод і подавлення сигналу, забезпечити прихованість передачі та реалізувати можливість передачі декількох сигналів на одному каналі.

Суть ППРЧ полягає в тому, що передавач використовує набір частотних каналів, псевдовипадковим чином обираючи наступний канал раз на певний період часу. При цьому, наступний канал обирається згідно з псевдовипадковою послідовністю, однаковою для передавача і приймача. В разі перешкод на окремих каналах сигнал не втрачається, оскільки інші канали в цей же момент можуть бути вільними. Така схема роботи підвищує стійкість до завад, допомагає запобігти виявленню та створює можливість працювати паралельно кільком передавачам.

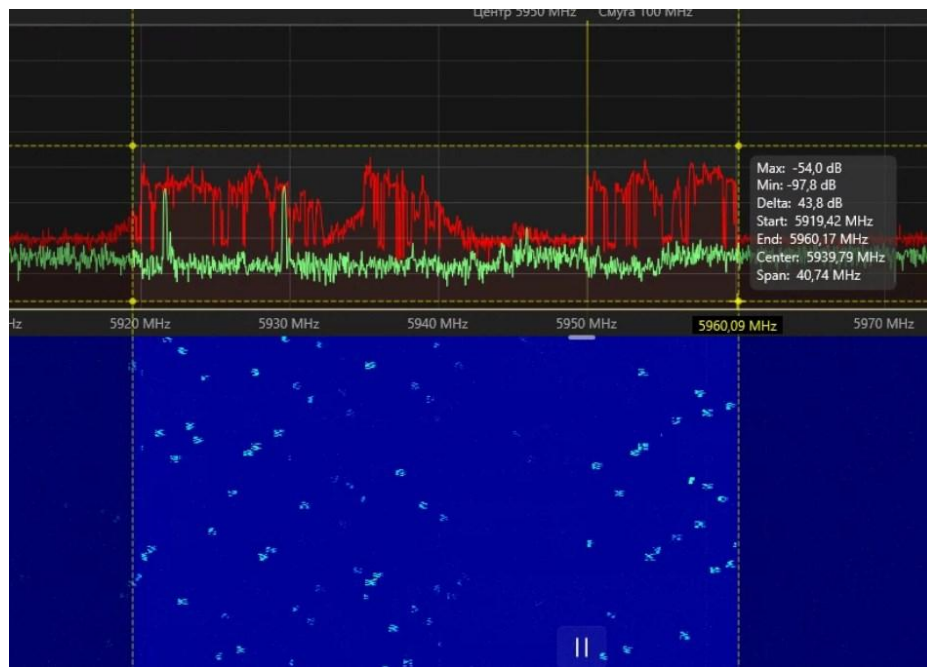


Рисунок 1.6 – ППРЧ пульта керування БПЛА на спектрограмі

При розробці для управління радіокерованими моделями, використовувалась в першу чергу для організації змагань з пілотування. Під час таких заходів в повітрі можуть знаходитись кілька десятків дронів на невеликій території, при цьому вони не мають заважати одне одному в радіоефірі. ExpressLRS реалізує ППРЧ через алгоритм частотного хопінгу, що залежить від Device UID і Seed(параметри пульта та інформацію, що вноситься в прошивку пульта та дрона в якості налаштувань для їх майбутнього радіозв'язку):

- Створюється хопінг-таблиця з частотами всіх можливих каналів для передачі сигналу
- Передавач та приймач перемикаються синхронно по цій таблиці
- Частота хопінгу може становити десятки чи сотні стрибків на секунду

В бойових умовах використання ППРЧ має вагомий вплив на здатність подавити БПЛА, оскільки дозволяє зберегти керування дроном навіть в ситуації,

коли з кількох сотень пакетів за секунду дрон прийме хоча б один. Для ефективного подавлення необхідно перекрити смугою перешкоди повну ширину ППРЧ. Ширина цієї смуги може становити більше 200МГц, що становить значну проблему навіть для досить сучасних засобів подавлення.

1.6 IQ модуляція в контексті SDR

IQ-модуляція є основою сучасної цифрової обробки сигналів і використовується у більшості радіотехнологій, включно з Wi-Fi, LTE, LoRa, GPS, DVB-T. Вона дозволяє ефективно передавати складну інформацію через зміну амплітуди та фази несучої хвилі, розкладаючи сигнал на дві ортогональні компоненти: I (in-phase) та Q (quadrature).

Ідея IQ-модуляції базується на представленні сигналу у вигляді комплексного числа:

$$x(t) = I(t) + jQ(t)$$

де $I(t)$ — складова, співфазна з несучою, а $Q(t)$ — складова, зсунута на 90° . Такий підхід дозволяє одночасно керувати фазою і амплітудою сигналу. Це важливо для реалізації складних модуляцій (наприклад, QAM, PSK), де кожен символ може мати як амплітудне, так і фазове представлення.

На передавальному боці сигнал модуляції множиться на косинус і синус відповідно, утворюючи I та Q компоненти. Ці компоненти комбінуються для утворення реального сигналу.

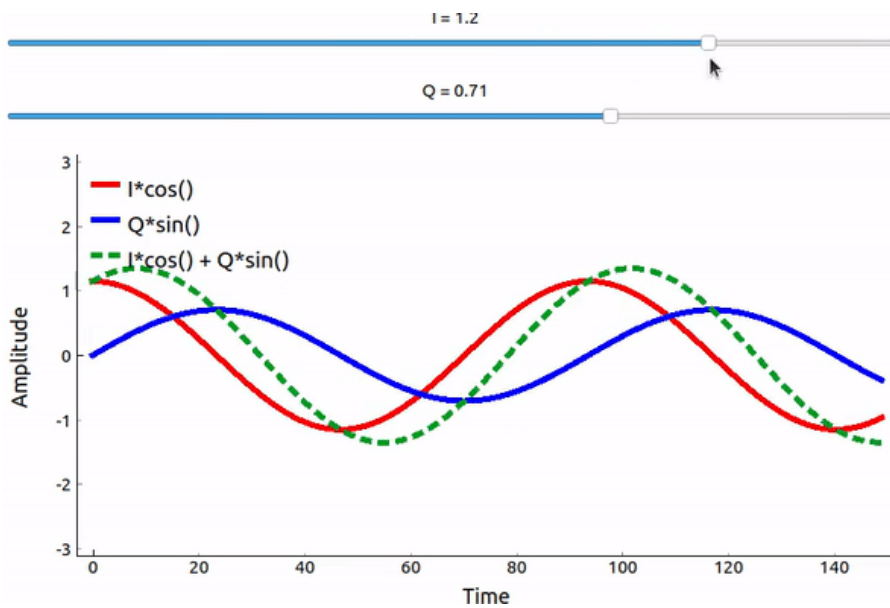


Рисунок 1.7 – I та Q частини опису цілісного сигналу

Після цього сигнал передається в ефір через антену. Завдяки ортогональності синуса і косинуса, I та Q не заважають один одному і можуть бути розділені на приймальному боці.

У SDR або будь-якому цифровому приймачі, сигнал зміщується в базову смугу (baseband), після чого виділяються I та Q компоненти за допомогою зміщення з синусом і косинусом, фільтрації та дискретизації (АЦП). Це дозволяє отримати повну інформацію про амплітуду та фазу сигналу в кожен момент часу.

В той час, як IQ описує загальну ситуацію в радіоефірі, повністю змішану хвилю, що складається з усього переданого в ефір в цей час, досить часто необхідно отримати інформацію про наявність енергії конкретної частоти. Цей перехід від домену хвиль в часі до домену частот зазвичай виконується за допомогою дискретної версії Швидкого Перетворення Фур'є.

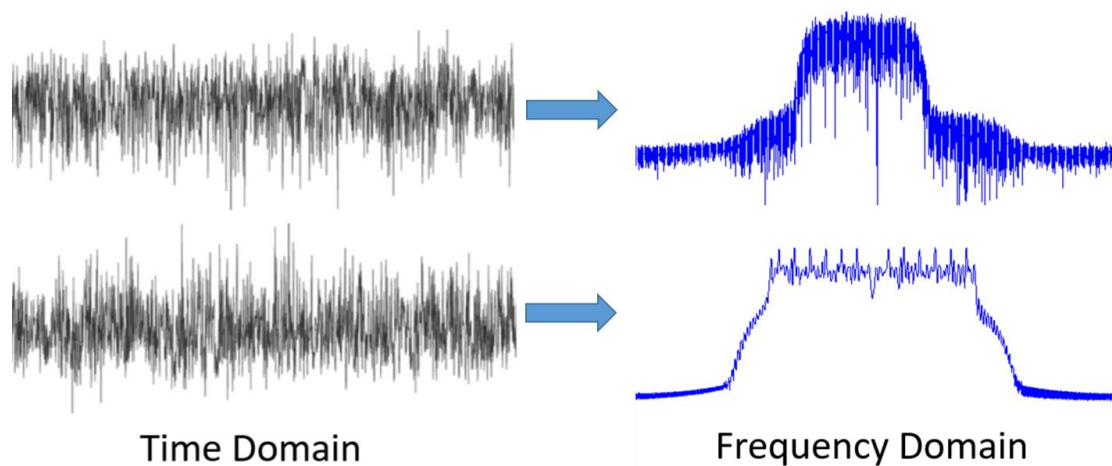


Рисунок 1.8 – перехід від опису хвилі в часі до аналізу частот складових хвилі

Перетворення Фур'є дозволяє замість суміші енергій хвиль різної частоти перейти до бачення сили сигналу хвиль кожної конкретної частоти окремо. Для цілей виявлення коливань, що змінюють свою частоту в часі за лінійним законом вкрай важливо мати можливість працювати саме з частотами.

Отже, це весь необхідний теоретичний базис для огляду та аналізу алгоритмів, які можуть дозволити знайти необхідний сигнал пультів керування БПЛА серед загального шуму та інших корисних сигналів, що присутні на будь-якій ділянці фронту.

1.7 Пошук через кореляцію з еталонним символом

Цей спосіб має назву Узгоджений Фільтр і є оптимальним методом виявлення відомих сигналів у присутності шуму. Використовується для пошуку по зображенню елементів, та, до прикладу, в медицині для автоматизованого аналізу кардіограм. У контексті LoRa це означає створення еталонного апчірп-сигналу (висхідного символу) та обчислення кореляції цього еталону з потоком IQ-даних.

Формально, узгоджене фільтрування розраховується по аналогії з множенням на зворотній символ під час демодуляції. Знайдений відрізок спектру множиться на базовий символ такої ж направленості(апчірп). Раніше було розглянуто структуру пакету інформації LoRa, а саме преамбулу, яка складається з послідовності повних по довжині чірпів. Тобто фактично ми знаємо як виглядає початок кожного пакету.

Математично описати процес множення сигналів за допомогою згортки для функцій дискретних величин можна наступним чином:

$$y(n) = \sum_N^{m=0} x(m) \cdot h(n-m)$$

Де h – послідовність Фур'є для функції шаблону шуканого символу, а x – дискретна послідовність, яка є результатом швидкого перетворення Фур'є отриманих з приймача IQ даних.

При наявності серед потоку схожого символу, таке множення підсилить його і створить додатковий потужний пік сигналу, який легко буде виявити по значному перевищенні над рівнем шуму.

Особливістю застосування згортки для пошуку корисного сигналу по шаблону є здатність цього способу знаходити кореляції навіть при високому рівні шуму. В таких умовах оператор візуально не зміг би виявити присутність модуляції LoRa в ефірі, переглядаючи спектрограму.

Таким чином загальна ідея алгоритму пошуку може виглядати наступним чином:

- Генеруємо послідовність Фур'є для кожного з базових символів всіх спредінг факторів, від SF7 до SF12
- Зчитуємо за допомогою SDR частину спектру, найменшу кратну по розміру всім розмірам згенерованих базових чірпів

- Виконуємо Швидке Перетворення Фур'є для отриманих з приймача даних
- Для кожного SF, проходимо по результатам ШПФ, та множимо їх на базовий згенерований символ
- При відсутності очевидного піку після множення, зсуваємось на точку по спектру і виконуємо операцію множення ще раз, так поки не закінчиться зчитана ділянка спектру, тоді зчитуємо наступну ділянку і проводимо всі операції множення знову
- При виявленні після множення зчитуємо конкретну

Плюси:

- Висока чутливість до конкретного шаблону LoRa
- Можливість точного визначення часу початку пакета, що значно допоможе при демодуляції
- Статистично оптимальний метод в умовах шуму

Мінуси:

- Необхідність знання параметрів (BW, SF)
- Необхідність перескановувати ефір під кожен SF, що значно збільшує складність розрахунків та час на обробку
- Високе обчислювальне навантаження при скануванні широкого спектру

1.8 Пошук через детекцію лінійної зміни частоти

Мета методу виявити у IQ-потоці такі ділянки, де частота змінюється лінійно в часі, що і є ознакою присутності чірпів, тобто LoRa-символів.

Для цього:

- Розбиваємо всю IQ смугу на невеликі вікна по 256 або 128 точок дискретизації
- Для переходу в частотний домен застосовуємо Швидке Перетворення Фур'є до кожного вікна
- Знаходимо в кожному вікні точку з найсильнішим рівнем сигналу(амплітудою), таким чином формується послідовність з найяскравіших точок вікон
- Перевіряємо чи знайдені точки знаходяться на одній лінії
- Фільтруємо знайдені ділянки з точок, щоб уникнути помилок апроксимації та відфільтрувати короткі сплески

Отримані ділянки, що лишилися, можна вважати такими, що мають високу імовірність бути шуканим корисним сигналом.

Плюси методу:

- Простий алгоритм
- Не вимагає знання точних параметрів сканування смуги чи параметрів LoRa, що використовувались при передачі сигналу

З мінусів методу можна зазначити:

- Ігнорування ділянок, де рівень шуму близький або більший за силу сигналу від передавача
- Можливі хибні спрацювання на інші види модуляцій

1.9 Пошук за допомогою нейронної мережі

Застосування методів машинного навчання для виявлення LoRa-сигналів є перспективним напрямком. Існує два основних підходи до застосування нейронних мереж у виявленні сигналів, це виявлення по спектрограмі, коли

нейронна мережа шукає на ній чірки, і по сирих IQ даних з SDR при пошуку паттерну зміни параметрів змішаної хвилі.

Для виявлення по спектрограмі використовуються згорткові нейронні мережі (CNN), які навчаються розпізнавати спектральні ознаки, характерні для LoRa. Для цього створюється набір спектрограм, на яких присутні або відсутні LoRa-сигнали, інші типи модуляцій. Ці зображення використовуються як вхідні дані для тренування класифікатора. В подальшому можливий перехід до результатів обробки IQ за допомогою ШПФ, на основі якого і будується спектрограма.

Імовірно більш точним та більш доцільним є спосіб роботи з даними напряму одразу ж в IQ форматі. Застосування нейронних мереж може дозволити виявляти сигнали навіть глибоко заховані під рівнем загального шуму, вони здатні вивчати приховані закономірності, які складно аналітично змоделювати. При такому застосуванні, для пошуку паттернів ще в сирих даних, значно простіше потім провести демодуляцію корисного сигналу для отримання з нього всієї можливою інформації.

Загальний принцип роботи згорткових нейронних мереж частково схожий на принцип роботи узгоджених фільтрів. Відбувається «сканування» вікна на предмет схожості чи кореляції з еталонним «фільтром», з тією різницею, що нейронна мережа сама визначає які фільтри є ефективними, а які ні.

Варто зазначити, що для тренувань необхідно зібрати максимально різноманітний набір даних, з різним рівнем сигналу, шуму, підсиленням, використовуючи як згенеровані сигнали, так і зібрані в польових умовах. Необхідно додавати до датасету дані з додатковими фазовими зсувами, SF, можливо інші види модуляцій щоб виключити хибнопозитивні детекції. Загальний алгоритм роботи з CNN для детекції сигналів виглядає наступним чином:

- Розділяємо потік сигналів на вікна по, наприклад, 128 чи 256 точок
- Кожне вікно подаємо на аналіз до CNN
- Нейронна мережа виявляє ознаки наявності необхідної модуляції, її основні параметри
- На вихід подається інформація про наявність сигналу/тип модуляції/SF тощо

Переваги:

- Висока адаптивність і масштабованість
- Автоматичне навчання ознакам без ручної інженерії
- Можливість багатокласової класифікації (різні SF LoRa/FSK/шум)

Недоліки:

- Потреба у великому датасеті з розміченими даними
- Високі вимоги до обчислювальних ресурсів (особливо для навчання)
- Погана інтерпретованість рішень ("чорний ящик")

Застосування таких підходів актуальне в умовах великого обсягу SDR-даних, а також для автоматизованих систем моніторингу, які мають працювати без участі оператора.

1.10 Оптимізація, рівні шуму, підсилення

Аналіз радіоефіру в бойових умовах супроводжується низкою певних можливих проблем.

До них можна віднести:

- високий загальний рівень шуму

- наявність засобів радіоелектронного подавлення поблизу, графік роботи яких невідомий
- деякі з засобів РЕБ в тому числі формують свою перешкоду з символів модульованого сигналу, до прикладу, LoRa чи QPSK, що забиватиме ефір потужним і, головне, шуканим сигналом
- корисний сигнал може бути згенерований дружніми силами, проте визнаний помилково ворожим, що супроводжуватиметься викривленням статистики та можливим подавленням дружніх БПЛА

В загальному випадку, необхідно провести цілий ряд в тому числі емпіричних випробувань для визначення прийняттого рівня зовнішнього шуму, налаштуванні підсилення сигналу, фільтрації зайвих сигналів та загальної адаптації параметрів сканування до максимальної ефективності в середовищі, яке постійно змінюється.

1.11 Демодуляція LoRa

Не зважаючи на те, що основною задачею, яка досліджується в цій роботі, є саме пошук корисного сигналу пультів БПЛА, варто згадати також процес демодуляції. Саме для проведення цього процесу ми виставили обмеження ширини смуги сканування при виборі приймача.

Для того, щоб мати можливість розібрати пакет інформації LoRa необхідно звернутись до рівнянь, якими описуються символи-чірпи, та змодельовати роботу фізичної плати приймача. Процес демодуляції також вимагає знання параметрів LoRa, які використовувались при модуляції, в першу чергу SF, BW та структуру пакету як такого.

Проведення демодуляції можливе як у вигляді продовження обробки сигналу, після знаходження початку пакету будь-яким зі способів, описаних

вище, або як самостійний окремий процес за допомогою існуючого програмного забезпечення.

Проведемо огляд вже існуючих програмних рішень:

GNU Radio + gr-lora

GNU Radio – це безкоштовне відкрите програмне забезпечення для роботи з радіосигналами, обробки, отримання та передачі за допомогою SDR. ПЗ дозволяє за допомогою візуального програмування або невеликої кількості коду формувати флов, по якому буде «подорожувати» та оброблятися сигнал з приймача.

Для роботи з LoRa в середовищі GNU Radio існують розроблені, в відкритим кодом, блоки модуляції, демодуляції та загальної обробки чірпів. Флов для демодуляції в повному вигляді виглядає наступним чином:

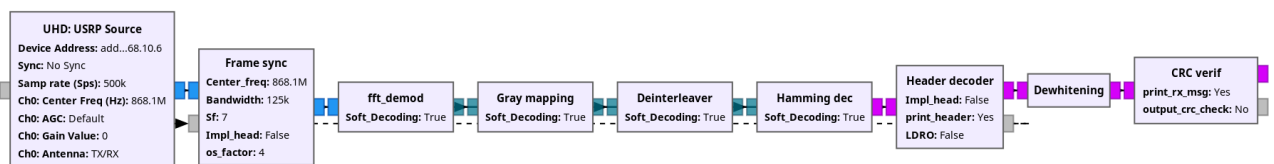


Рисунок 1.9 – флоуграф з кроків демодуляції LoRa сигналу в ПЗ GNU Radio

В цьому випадку перший блок відповідає за прийом сигналу через SDR приймач, `frame_sync` – вирівнює «вікно» сканування по отриманому символу преамбули. Наступні чотири блоки відповідають саме за демодуляцію та діставання корисних даних, і останній перевіряє правильність і цілісність пакету, за допомогою перевірки підпису, якщо підпис наявний.

До мінусів цього методу можна віднести необхідність застосовувати зовнішнє ПЗ, яке неможливо зв'язати з, до прикладу, детекцією нейронною мережею. Тобто, необхідна активна присутність оператора, який буде вносити отримані з висновків роботи нейронної мережі дані в параметри роботи флову,

та, після демодуляції, вручну вноситиме отримані байти пакету в розроблювану систему для аналізу.

Іншим можливим підходом може бути використання бібліотек для інтеграції в ПЗ, що дасть можливість проводити демодуляцію автоматично, одразу після виконання детекції. В такому випадку можливо одразу використати отримані дані про центральну частоту, SF, імовірні фазові та частотні зсуви для спрощення алгоритму демодуляції.

Розглянемо покроково алгоритм проведення демодуляції LoRa:

1) Синхронізація

Необхідно визначити чи правильно обране «вікно», в якому знаходиться символ, через використання фізичних чіпів та плат передавачів, можливі невеликі зсуви по частотам, які не дозволять правильно визначити значення «чіпів»

2) Виконання ШПФ

Для того, щоб визначити на якій саме частоті стався розрив символу, необхідно перейти до аналізу саме частот та місця зсуву

3) Множення на зворотній символ

В залежності від обраного для передачі SF, алфавіт LoRa містить $2^{SF} - 1$ символів, що може значно збільшити кількість необхідних обчислень для порівняння з кожним можливим символом.

Множення на зворотній символ дозволяє одразу отримати необхідний результат, оскільки точно вказує на місце розриву чірпа.

1.12 Порівняльна характеристика запропонованих алгоритмів та способи їх застосування

Розглянуті алгоритми мають як свої певні недоліки, так і переваги, тож імовірно виходити необхідно з їх складності, точності аналізу радіоефіру та

необхідної обчислювальної потужності для обробки. Спробуємо підсумувати висновки щодо алгоритмів виявлення корисного сигналу.

Таблиця 3.1

Порівняння алгоритмів детекції корисного сигналу

Назва	Складність реалізації	Точність	Вимоги до «заліза»
Узгоджений фільтр	Просто	Середня	Середні
Пошук лінійної зміни частоти	Просто	Низька	Низькі
ШП для аналізу IQ	Складно	Висока	Високі

Розробка ПЗ на основі будь-якого з вказаних алгоритмів передбачає певне тестування на датасеті, тому задачу по збору та генерації тестових даних варто виконувати в першу чергу.

В подальшому, можлива комбінація пристроїв різних типів з різним програмним забезпеченням для покращеного покриття та аналізу на різній глибині відносно ЛБЗ. До прикладу, пристрій на основі HackRF One та одноплатного комп'ютера, рівня RaspberryPi міг би виконувати попереднє сканування та детекцію, знаходячись ближче до лінії фронту та передаючи інформацію про знахідки на тилівіший командно-спостережний пункт підрозділів РЕБ чи РЕР. В той же час, пристрій на основі BladeRF micro, підключений до потужного ноутбука, але в більш спокійних тилівих умовах, за допомогою згорткової нейронної мережі проводить дорозвідку, повноцінне сканування та допомагає операторам РЕБ прийняти швидке рішення про необхідність та параметри подавлення.

Також можна розглянути варіант, при якому на одному пристрої комбінуються декілька варіантів сканування. До прикладу, на одному достатньо потужному варіанті пристрою, з ноутбуком та SPECTRAN V6 проводиться спочатку швидкий пошук за допомогою алгоритму узгодженого фільтру чи пошуку лінійної зміни частоти, але при наявності ознак сигналу з шуканим типом модуляції, одразу починається обробка сигналу за допомогою нейронної мережі для підвищення точності сканування.

Самі по собі алгоритми аналізу радіоефіру варто застосовувати з розумінням типу модуляції та роботи протоколу керування БПЛА. Наприклад, під час швидкого сканування узгодженим фільтром було знайдено початок пакета інформації з модуляцією LoRa. Ми знаємо, що пульти керування застосовують ППРЧ, тобто скоріше за все наступний пакет від цього пульта буде на іншій частоті, проте з високою долею імовірності, протягом пари секунд ППРЧ знову повернеться до цього ж хопу. Отже, якщо не вийшло з якихось причин провести демодуляцію цього пакету, можна почекати наступного. Або, якщо в даний момент часу нас цікавить в першу чергу детекція, без демодуляції, варто продовжувати сканування навколо частоти знайденого пакету на ширину середньостатистичного пульта, щоб збільшити імовірність визначити його таблицю хопів ППРЧ і з'ясувати повну ширину спектру цього пульта. Це критично необхідна інформація для ефективного подавлення будь-якого радіокерованого БПЛА.

2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Постановка задачі порівняння SDR приймачів

Лінійне програмування – метод оптимізації, який допомагає знайти найкраще (мінімальне або максимально можливе) значення лінійної цільової

функції за умов лінійних обмежень. Методи вирішення задач з ЛП часто лежать в основі багатьох рішень в інженерії та науці.

В контексті цієї роботи, нас здебільшого цікавить такий розділ ЛП, як задачі оптимальної витрати ресурсів. Вони застосовуються в умовах, коли необхідно максимізувати вихід(чи мінімізувати витрати) в умовах обмежених ресурсів.

Припустимо, що наша ціль – зібрати комплекс радіомоніторингу, який автоматично скануватиме ефір і збиратиме всю корисну інформацію. SDR приймач буде підключений до комп'ютера, що має достатню потужність для обробки та аналізу смуги будь-якої ширини.

В такому випадку, швидкість роботи комплексу напряму залежатиме в першу чергу від швидкості сканування приймачем, а отже від ширини смуги, яку цей приймач може просканувати за один прохід таким чином, щоб модульований радіосигнал, який він передасть далі на комп'ютер, можна було демодулювати і зчитати всю корисну інформацію.

Це накладає певні умови на можливість використання ресурсу приймача.

Позначимо табличні дані про максимально фізично можливі частоту дискретизації та ширину смуги читання приймача як SR_{max} та BW_{max} відповідно, а максимальну ефективну смугу та необхідну для неї частоту дискретизації через BW та SR також відповідно.

По-перше, пристрій не зможе зчитати смугу більшу, ніж фізично здатен просканувати:

$$(1) BW \leq BW_{max}$$

По-друге, приймач не зможе зчитувати з більшим SR , ніж фізично здатен:

$$(2) \quad SR \leq SR_{max}$$

По-третє, за теоремою Найквіста, максимальна корисного сигналу смуги читання має бути хоча б в два рази меншою за частоту дискретизації сканування, а для модуляцій, що використовуються при передачі пакетів керування з пульта до БПЛА, ширина смуги корисного сигналу співпадає з його частотою, отже:

$$(3) \quad BW \leq \frac{1}{2} SR$$

При цьому, для ефективності роботи комплексу нас цікавить в першу чергу максимально велика смуга роботи приймача, тобто:

$$(4) \quad BW \rightarrow max$$

(1)-(4) є канонічним виглядом задач Лінійного Програмування з ефективного розподілу ресурсів:

$$\begin{cases} SR \leq SR_{max} \\ BW \leq BW_{max} \\ BW \leq \frac{1}{2}SR \end{cases}$$

$$BW \rightarrow \max$$

В цьому випадку система рівнянь відіграє роль системи обмежень використання наявних ресурсів приймача, в той час як (4) – цільова функція, до максимізації значення якої ми прагнемо.

2.2 Вирішення задачі ЛП, представлення результатів

Розв'яжемо задачу окремо для кожного з приймачів, щоб дізнатись його ефективну смугу сканування:

1) RTL-SDR

Для розв'язання задачі вибору найоптимальнішого приймача, підставимо значення з таблиці в систему рівнянь і отримаємо задачу ЛП:

$$\begin{cases} SR \leq 2.56 \\ BW \leq 2.4 \\ BW \leq \frac{1}{2}SR \end{cases}$$

$$BW \rightarrow \max$$

Оскільки система рівнянь має всього дві змінних, найбільш простим і швидким способом вирішення цієї задачі ЛП є графічний спосіб. Побудуємо графік можливих значень змінних:

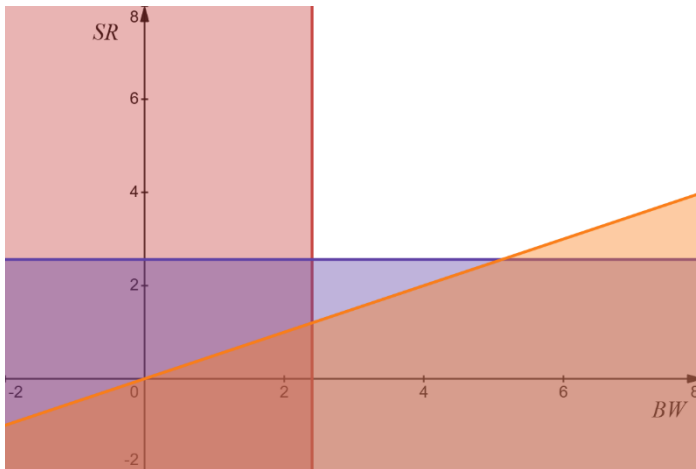


Рисунок 2.2 – графічний розв'язок задачі ЛП для RTL-SDR

Як можна помітити, точка, що є рішенням задачі знаходиться на перетині графіків першої і другої нерівностей системи. Вирішимо систему з цими рівняннями і отримаємо максимальну ефективну ширину смуги сканування для пристрою RTL-SDR рівну 1.28 МГц при частоті дискретизації 2.48 МТ/с. Тобто, «ресурс» частоти дискретизації задіюється повністю, в той час як максимальна ширина смуги сканування може бути практично в два рази більшою.

$$BW = 1.28 \text{ МГц}$$

2) HackRF One

Підставимо значення характеристик приймача з таблиці в систему нерівностей, і отримаємо задачу:

$$\begin{cases} SR \leq 20 \\ BW \leq 20 \\ BW \leq \frac{1}{2}SR \end{cases}$$

$BW \rightarrow \max$

Графічний розв'язок задачі:

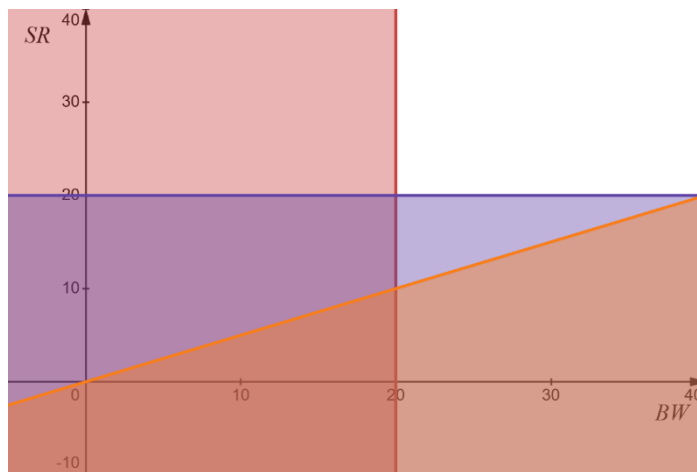


Рисунок 2.3 – графічний розв'язок задачі ЛП для HackRF One

На основі графічного розв'язку задачі ЛП, значення максимальної ефективної смуги для приймача HackRF One складає:

$$BW = 10 \text{ МГц при частоті дискретизації } SR = 20 \text{ МТ/с}$$

Для цього пристрою, так само як і з попереднім, основним обмежуючим фактором є частота дискретизації.

3) BladeRF micro

Внесемо дані характеристик з таблиці в систему нерівностей, і отримаємо:

$$\begin{cases} SR \leq 61.44 \\ BW \leq 122.88 \\ BW \leq \frac{1}{2}SR \end{cases}$$

$BW \rightarrow \max$

Графічний розв'язок в даному випадку виглядає наступним чином:

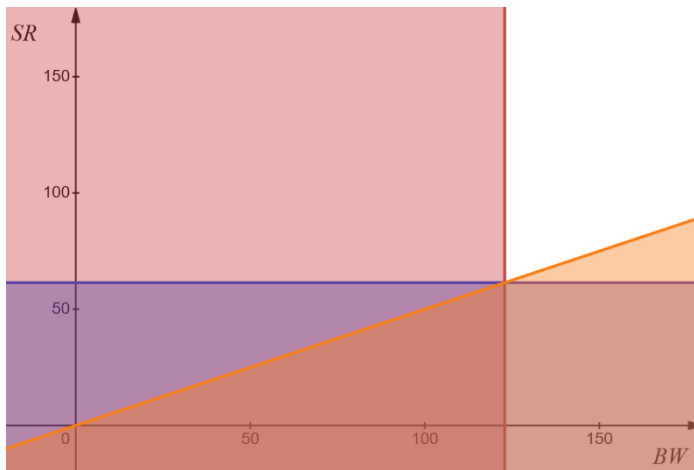


Рисунок 2.4 – графічний розв'язок задачі ЛП для BladeRF micro

Точка розв'язку задачі знаходить на перетині всіх трьох графіків нерівностей одночасно. Виберемо, для простоти розв'язання, другу і третю нерівність системи, розв'яжемо і отримаємо:

$$BW = 30.72 \text{ МГц при частоті дискретизації } SR = 61.44 \text{ МТ/с}$$

4) Aaronia SPECTRAN V6

Внесемо дані цього приймача в систему нерівностей і отримаємо задачу ЛП:

$$\begin{cases} SR \leq 2000 \\ BW \leq 80 \\ BW \leq \frac{1}{2}SR \end{cases}$$

$BW \rightarrow \max$

Графічний розв'язок отриманої задачі виглядатиме наступним чином:

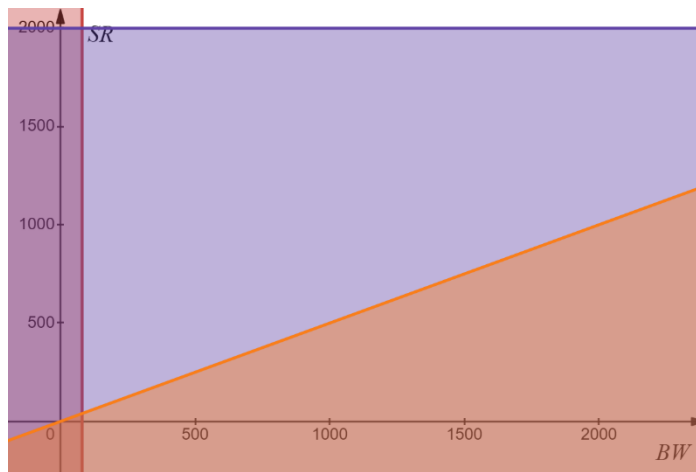


Рисунок 2.5 – графічний розв'язок задачі ЛП для SPECTRAN V6

Точка перетину графіків другої та третьої нерівності системи є розв'язком задачі для цього приймача. Побудуємо систему рівнянь на основі обраних нерівностей, розв'яжемо її і отримаємо розв'язок:

$$BW = 80 \text{ МГц при частоті дискретизації } SR = 160 \text{ МТ/с}$$

Це єдиний пристрій зі списку, що в якості основного обмежуючого «ресурсу» має максимальну ширину смуги сканування.

Внесемо отримані дані в нову таблицю, додатково порахувавши вартість 1 МГц ефективною смуги сканування, розділивши вартість пристрою на отримане значення ширини смуги:

Результати дослідження ширини ефективної смуги сканування

№	Назва моделі	Максимальна ефективна ширина смуги сканування	Вартість 1МГц смуги сканування
1	RTL-SDR	1.28МГц	1245.31 грн
2	HackRF One	10МГц	1427.8 грн
3	BladeRF micro	30.72МГц	738.28 грн
4	Aaronia SPECTRAN V6	80МГц	2098.8 грн

Варто зазначити, що виробник дозволяє придбати версію з можливістю розширення до 120МГц в момент часу, але пристрій в такому випадку стає ще більш дороговартісним, хоча при цьому ціна за 1МГц стає навіть більшою: 2209.85 грн/МГц. Тому варіант з розширеною смугою в цьому дослідженні не враховувався, але можна припустити, що, з точки зору розробки, він був би більш прийнятним.

2.3 Аналіз отриманих даних

Згідно з даними результатів розрахунків та аналізу технічних характеристик найбільш розповсюджених SDR приймачів, для автоматичного сканування всього можливого наразі діапазону частот керування ударних та розвідувальних БПЛА, найкраще, з точки зору співвідношення вартості до можливої ширини смуги сканування, підходить пристрій BladeRF micro.

Звичайно, такий аналіз не враховує різні особливості конкретних пристроїв, які, імовірно, теж можуть зіграти роль при виборі засобів для закупівлі чи при проектуванні більш складних комплексів, наприклад,

можливості SPECTRAN V6 з постобробки отриманих сигналів, чи подвоєний тракт прийому сигналу засобу BladeRF micro. Проте, в загальному випадку, ми змогли оцінити наскільки ефективно будуть витрачені кошти при купівлі кожного конкретного засобу.

Кожен з цих засобів також можливо застосовувати для аналізу радіоефіру в режимі ручного перебору. В такому випадку необхідна частота дискретизації може бути зменшена як мінімум вдвічі, тобто робоча ефективна смуга кожного з засобів виросте в два і більше рази. І навіть для ручного режиму роботи і перегляду активності БПЛА в радіоефірі все ще найкраще підходить пристрій BladeRF micro, оскільки має найбільше співвідношення можливої ширини смуги до частоти дискретизації. Він дозволить оператору бачити одночасно значно ширшу смугу при достатній для аналізу роздільній здатності.

В своєму дослідженні ми спирались на припущення про те, що отримані з радіоефіру дані будуть оброблятися на аналізуватися на достатньо потужному комп'ютері, щоб знехтувати часом, необхідним на постобробку. Насправді ж, обчислювальна потужність в даному випадку вкрай важлива, оскільки мова йде про мільйони обчислень операцій множення чисел з крапкою на секунду. З іншого боку, при застосуванні малопотужних комп'ютерів, чи навіть окремих мікропроцесорів, для проведення демодуляції, можна припустити, що найкращим вибором були б менш дорогі приймачі, не зважаючи на їх обмежені можливості. Таким чином отриманий пристрій, маючи значно меншу загальну вартість, може бути застосований в більш ризикованих тактичних умовах, або, наприклад, такі пристрої, через спрощення збірки, могли б випускатись набагато більшою серією. Це в свою чергу дозволяє збільшити кількість пристроїв на ЛБЗ для більш детального моніторингу, ефективнішого розбиття загальної смуги діапазону частот на декілька піддіапазонів при паралельному скануванні і т.д.

З іншого боку, використання більш потужного комп'ютера та приймача в парі для обробки сигналів, імовірно дозволило б отримати більше корисної інформації з радіоефіру та дозволило б більш точно проводити аналіз. До прикладу, методи детекції радіосигналу за допомогою нейронних мереж показали досить високу ефективність та низький рівень кількості помилкових спрацювань, проте такий спосіб вимагає значну кількість ресурсів для обробки.

ВИСНОВКИ

В рамках цієї роботи ми визначили основні характеристики SDR приймачів, які необхідні для автоматизованого виявлення пультів керування ударних та розвідувальних БПЛА в сучасних бойових умовах. Ми визначили найбільш розповсюджені моделі пристроїв та розрахували максимальну ширину смуги їх роботи в режимі, який дозволить перехоплювати дані, що передаються, і проводити їх аналіз.

Окрім робочої ефективності пристроїв, ми також порівняли їх вартість, та змогли дати фінансову оцінку закупівлі кожного з них. Проаналізували способи їх застосування в контексті ведення радіоелектронної розвідки в автоматичному та ручному режимі роботи.

За результатами проведеного дослідження, найбільш прийнятним для використання виявився пристрій BladeRF micro. Його технічні характеристики дозволяють сканувати радіоефір смугами по 30МГц за один прохід в автоматичному режимі, та 60+МГц в режимі ручної роботи оператора. Засіб має достатню швидкодію, і при цьому не вирізняється занадто високою вартістю. А його показник співвідношення загальної вартості пристрою до максимальної ефективної ширини смуги сканування виявився приблизно в два рази кращим за найближчого конкурента повноцінного HackRF One.

Було запропоновано кілька варіантів алгоритмів, що дозволяють автоматизувати обробку радіосигналу, який має прийматись за допомогою SDR. Кожен з цих алгоритмів може бути визнаний як найбільш прийнятний за певних умов, при різних обставинах та при використанні для обробки сигналу більш або менш потужних комп'ютерів. При необхідності, ці алгоритми, для більшої точності, можна комбінувати між собою.

Рекомендації щодо подальших наукових розвідок та практичної діяльності

- Розробка алгоритмів автоматизованого пошуку корисного сигналу в радіоєфірі, в тому числі пошуку специфічних модуляцій, наприклад LoRa та QPSK
- Аналіз алгоритмів роботи фізичних чіпів та плат приймачів і передавачів, що застосовуються в радіокеруванні різними типами авіамоделей
- Дослідження відкритого коду протоколів керування БПЛА на предмет пошуку логічних «дірок» та можливостей для втручань в канал зв'язку між дроном та пультом керування
- Проведення тестувань в декількох різних варіантах умов, як на згенерованих сигналах, так і в бойовому середовищі

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кваліфікаційна робота бакалавра [Електронний ресурс] : методичні рекомендації для здобувачів ступеня бакалавра освітньо-професійної програми «Системний аналіз» зі спеціальності 124 Системний аналіз / уклад.: Т. А. Желдак, Т. В. Хом'як, А. В. Малієнко ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2025. – 32 с. url: <https://ir.nmu.org.ua/handle/123456789/170863>
2. MIT Radar Course: Linear Chirp Detection
3. Хом'як, Т. В., Шевченко, Ю. О., & Гаранжа, Д. М. ПРОГРАМУВАННЯ ТА АЛГОРИТМІЧНІ МОВИ. <https://ir.nmu.org.ua/handle/123456789/173373>
4. Мінеєв, О. С., & Шевченко, Ю. О. (2026). Аналіз програмного забезпечення: методичні рекомендації до виконання практичних робіт для здобувачів ступеня бакалавра галузі знань 12 (F) Інформаційні технології. <https://ir.nmu.org.ua/handle/123456789/173326>
5. <https://greatscottgadgets.com/hackrf> – HackRF One documentation
6. <https://nuand.com> – BladeRF micro documentation
7. <https://aaronia.com> – SPECTRAN V6 datasheets
8. Коряшкіна, Л. С., Алексєєв, О. М., & Гаранжа, Д. М. (2025). Навчальна практика з обчислень: методичні рекомендації для здобувачів ступеня бакалавра освітньо-професійної програми «Системний аналіз» спеціальності 124 Системний аналіз. <https://ir.nmu.org.ua/handle/123456789/1731>
9. Коряшкіна, Л. С., Станіна, О. Д., & Шевченко, Ю. О. (2024). Практикум з диференційних рівнянь. <https://ir.nmu.org.ua/handle/123456789/167658>
10. Хом'як, Т. В., Шевченко, Ю. О., & Гаранжа, Д. М. (2026). Програмування та алгоритмічні мови: методичні рекомендації до виконання лабораторних робіт для здобувачів ступеня бакалавра ОПП «Системний аналіз» зі спеціальності 124 Системний аналіз Ч 1. <https://ir.nmu.org.ua/handle/123456789/173373>

Додаток А. Відомість матеріалів кваліфікаційної роботи

№ з/п	Позначення	Найменування	Кількість аркушів	Примітки						
1										
2		Документація								
3										
4	САУ.КР.25.13.ДА.ПЗ.	Пояснювальна записка	№1	Формат А4						
5										
6		Демонстраційний матеріал	№2	Презентація на CD-R						
7										
8		Копія роботи	1	Диск CD-R						
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
					САУ.КР.25.13.ДА.ПЗ.					
Змін.	Аркуш	№ докум.	Підпис	Дата						
Розроб.	Городецька Ю.М.				Матеріали кваліфікаційної роботи	Літ.	Аркуш	Аркушів		
К. розд.	Алексєєв О.М.									
Керівн.	Алексєєв О.М.					НТУ «ДП», 12; 124-21-1				
Н.контр.	Хом'як Т.В.									
Зав. каф.	Желдак Т.А.									