Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження застосування платформи HACK-RF для задач автоматизованого радіомоніторингу
(тема)

Виконав:
студент 2 курсу, групи ІМІм-21-1
Попаденко М. О.
(прізвище, ініціали)

Спеціальність 172 – Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна
Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник д. тех. н., проф. Безрук В. М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Безрук В. М.
(підпис) (прізвище, ініціали)

2022 р.

Не містить відомостей, заборонених до відкритого публікування.

Студент __Попаденко М. О.____ /_____ /

Керівник_____Безрук В. М.___/_____ /

Харківський національний університет радіоелектроніки

Факультет _____Інфокомунікацій_____

Кафедра _____Інформаційно-мережної інженерії_____

Рівень вищої освіти _____другий (магістерський)_____

Спеціальність _____172- Телекомунікації та радіотехніка_____
(код і повна назва)

Тип програми _____освітньо-професійна_____

Освітня програма_____Інформаційно-мережна інженерія_____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові_____Попаденко Марії Олександрівні_____
(прізвище, ім'я, по батькові)

1. Тема роботи _Дослідження застосування платформи HACK-RF для задач автоматизованого радіомоніторингу_____
_____
затверджена наказом університету від _21_ __жовтня____2022 р. № __1376Ст__
2. Термін подання студентом роботи до екзаменаційної комісії _23_ __грудня__ 2022 р.
3. Вихідні дані до роботи _провести аналіз автоматизованого радіомоніторингу та_____ тенденцій його розвитку, дослідити особливості програмно-апаратної платформи HACK-RF,_ виділити обрану платформу серед інших SDR-пристроїв та її відмінності від_____ китайської версії, розглянути опціональні пристрої для роботи з обраною платформою,__ дослідити застосування HACK-RF для задач радіомоніторингу, розглянути можливості__ даної платформи для задач радіобезпеки_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі _аналіз особливостей та розвитку__ автоматизованого радіомоніторингу, дослідження особливостей програмно-___ апаратної платформи HACK-RF, дослідження застосування HACK-RF для задач автоматизованого_ радіомоніторингу_____
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____ _____Слайди у форматі Power Point (актуальність та тема роботи, поняття радіо -____ моніторингу, область застосування його систем, технічні засоби та тенденції розвитку____ радіомоніторингу, технологія SDR, платформа HACK-RF, її оптимальність та технічні____ характеристики, відмінність оригінального пристрою від китайської версії, опціональні___ пристрої для роботи платформи, застосування HACK-RF для прийому радіомовлення, ____ декодування цифрових сигналів, використання HACK-RF для знаходження координат літака та радіосигналів, що випромінює БпЛа, HACK-RF для задач РЕБ, висновки)_____ _____ _____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням	24.10.2022	
2	Підбір літератури за темою роботи	24.10.2022-27.05.2022	
3	Аналіз автоматизованого радіомоніторингу	28.10.2022- 11.11.2022	
4	Дослідження апаратно-програмної платформи HackRF	12.11.2022- 26.11.2022	
5	Дослідження застосування HACK-RF для задач автоматизованого радіомоніторингу	27.11.2022-13.12.2022	
6	Висновки	14.12.2022	
7	Оформлення пояснювальної записки	15.12.2022 – 16.12.2022	
8	Оформлення презентації та підготовка до захисту	17.12.2022-22.12.2022	

Дата видачі завдання _24__ ___жовтня____2022 р.

Студент _____
(підпис)

Керівник роботи _____ ___проф. Безрук В. М._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 77 с., 39 рис., 2 табл., 18 джерел, 1 додаток.

Об’єкт роботи – автоматизований радіомоніторинг.

Мета роботи – дослідження застосування платформи HACK-RF для задач автоматизованого радіомоніторингу.

Проаналізовано особливості та тенденції розвитку автоматизованого радіомоніторингу, виявлено необхідність використовувати більш сучасні пристрої для його задач. Розглянуто платформу HACK-RF, її опціональні пристрої та переваги над китайською версією. Досліджено застосування даної платформи для задач радіомоніторингу, а саме знаходження координат літаків, прийому радіомовлення та декодування цифрових сигналів та визначення сигналів БпЛА. Описано можливості HACK-RF для РЕБ.

Радіомоніторинг, HACK-RF, ADS-B, ,БпЛА, безпека.

THE ABSTRACT

Explanatory note: 77 pages, 39 figures, 2 tables, 18 sources, 1 appendix.

The object of work is automated radio monitoring.

The purpose of the work is to research the application of the HACKRF platform for the tasks of automated radio monitoring.

The peculiarities and trends of the development of automated radio monitoring are analyzed, the need to use more modern devices for its tasks is revealed. The HACK-RF platform, its optional devices and advantages over the Chinese version are considered. The application of this platform for radio monitoring tasks, namely finding the coordinates of aircraft, receiving radio broadcasts and decoding digital signals, and determining UAV signals, was investigated. Describes the capabilities of HACK-RF for radio-electronic warfare.

Radio monitoring, HACK-RF, ADS-B, UAV, security.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АЦП – аналого-цифровий перетворювач;

БД – база даних;

БпЛА – безпілотний літальний апарат;

ВП – випромінювальні пристрої;

ДРВ – джерело радіовипромінювання;

ККД – коефіцієнт корисної дії;

НЧ – низькі частоти;

ПК – персональний комп’ютер;

ПЛІС – програмна логічна інтегральна схема;

ПЧ – проміжна частота;

РЕЗ – радіоелектронний засіб;

РЕБ – радіоелектронна безпека;

РЕР – радіоелектронна розвідка;

РМ – радіомоніторинг;

РЧР – радіочастотний ресурс;

РПП – радіоприймальний пристрій;

ФАПЧ – фазове автопідлаштування частоти;

ФНЧ – фільтр низьких частот;

ЦАП – цифро-аналоговий перетворювач;

AM – амплітудна модуляція;

DSD – декодер цифрових перемовин;

FM – частотна модуляція;

SDR – програмно-визначаюча радіосистема;

ZIF – нульове підсилення.

ВСТУП

Термін, що з'явився у галузі радіозв'язку відносно нещодавно – "радіомоніторинг", розкриває діяльність з контролю та вивченню радіообстановки.

Основними пристроями радіомоніторингу на даний момент є багатоканальні скануючі приймачі, що дозволяють здійснювати автоматичний пошук тих, хто перебуває в ефірі радіосигналів, а також здійснювати постійний контроль заздалегідь заданих частот. У точці прийому є сторонні електромагнітні поля, природного та штучного походження створювані джерелами радіоперешкод. Корисний сигнал спотворюється за рахунок перешкод і тому відбуваються помилки у прийомі повідомлення. Враховуючи, що реальні умови прийому сигналів змінюються в часі, режими його роботи та структура приймача повинна бути оптимізована, з метою отримання мінімальної величини помилки в точці прийому повідомлень.

Забезпечення безпеки під час переговорів у радіосистемі стає на перше місце, коли передана інформація має конфіденційний характер або є інформацією обмеженого доступу, що особливо актуально для державних установ та великих комерційних підприємств. Однак саме той факт, що інформація представляє інтерес, може спонукати потенційного порушника до протиправних дій.

З розвитком нових технологій, радіоефір, що використовується, «забруднюється» непотрібними перешкодами, які дуже сильно впливають на якість переданої інформації. Найчастіше при організації зв'язку між абонентами чутність повідомлень, що передаються, залишається на низькому рівні. Для підвищення якості зв'язку необхідний якісний радіомоніторинг, але його

використання ускладнюється, наприклад через те що вітчизняні та зарубіжні аналізатори спектру мають високу вартість та не розраховані для роботи в польових умовах.

Виходячи з цього, у дипломному проекті пропонується використання приймального пристрою за технологією SDR для оперативного моніторингу радіомережі. Концепція SDR проклала шлях для когнітивних радіоприймачів, динамічно змінюючи модуляцію та зайняті частоти. Всі необхідні функції в даній концепції змінюються лише на програмному рівні, тому її пріоритетністю є зниження вартості та розширення функціоналу.

Платформа HACK-RF має ряд переваг щодо іншої апаратури вимірювання та аналізу, вона є досить недорогою та має величезні можливості, доказом цього є участь у багатьох конференціях, таких як DEF CON, BlackHat и BSides та інших.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ТА РОЗВИТКУ АВТОМАТИЗОВАНОГО РАДІОМОНІТОРИНГУ

Радіочастотний моніторинг є найефективнішим інструментом отримання об'єктивної інформації стосовно стану електромагнітної обстановки та використання радіочастотного ресурсу (РЧР) в державі для забезпечення підвищення ефективності регулювання у сфері користування РЧР, упровадження новітніх радіотехнологій, систем і стандартів та нових послуг зв'язку [1].

1.1 Поняття та особливості автоматизованого радіомоніторингу

Радіомоніторинг – діяльність з вивчення та контролю радіообстановки, виявлення та пошук законних та незаконних радіопередавачів та джерел інших радіовипромінювань. Безперервність отримання даних, актуальність і достовірність даних, що добуваються, є важливою перевагою радіомоніторингу. Безперервність досягається сталістю роботи засобів моніторингу, актуальність – своєчасністю отримання необхідних для прийняття рішень даних, достовірність – документальним характером інформації, що надходить.

Характером функціонування радіомоніторинг поділяється на активний (виявляє та розпізнає непрацюючі джерела радіовипромінювання) та пасивний (розпізнає та ідентифікує функціонуючі джерела радіовипромінювання) [2].

Багатоканальні скануючі приймачі в даний час використовують як основні засоби радіомоніторингу, що дозволяють здійснювати автоматично, як пошук радіосигналів, що знаходяться в ефірі, так і постійний контроль заздалегідь заданих частот зв'язку. Крім сканерів у процесі ведення радіомоніторингу застосовується також інша необхідна апаратура: портативні частотоміри, аналізатори радіоспектру, широкосмугові антени, смугові та

режекторні фільтри, малошумливі антенні підсилювачі, пристрої шумоочищення мови, високочастотні кабелі з малими втратами та інше.

Пошукові способи радіомоніторингу засновані на перебудові приймача в заданій смузі частот, дозволяють виявити і виміряти несучу частоту з високою точністю. Розрізняють три способи пошуку:

1. повільний пошук;
2. швидкий пошук;
3. пошук із середньою швидкістю.

При повільному пошуку час перебудови приймача на ширину його смуги пропускання більше за період повторення сигналу. Повільний пошук добре підходить для виявлення постійно працюючих радіоелектронних засобів, точність визначення частоти дуже висока. Серйозними недоліками повільного пошуку є великий час виявлення сигналу і мала ймовірність розвідки короткочасних радіоелектронних засобів, що працюють. Для подолання цієї вади необхідно збільшувати ширину смуги пропускання приймача, що призводить до зниження чутливості.

При пошуку із середньою швидкістю, виявлення короткочасних сигналів не гарантується протягом одного періоду перебудови, інші ж параметри виявляються досить гарними для цілей радіомоніторингу.

При швидкому пошуку час перебудови приймача у всьому діапазоні дуже малий, а швидкості перебудови дуже великий. При цьому способі пошуку висока ймовірність виявлення короткочасно працюючих радіоелектронних засобів за один період перебудови приймача, проте роздільна здатність і точність визначення частоти в порівнянні з повільним пошуком нижче, що пов'язано з інерційністю резонансних ланцюгів приймача [3].

Безпошукові способи засновані на одночасному прийомі сигналів широкого діапазона робочих частот без перебудови гетеродинів чи фільтрів. Час розвідки частоти діючих радіоелектронних засобів може бути дуже малим, оскільки всі складові спектру виявляються одночасно і практично миттєво.

Типи безпошукових методів:

1. інтерференційні методи;

2. використання одноканальних приймачів;

3. використання багатоканальних приймачів.

Інтерференційний спосіб заснований на певній залежності зсуву фази від довжини лінії та частоти. Сигнал з виходу антени розгалужується на дві фідерні лінії різної довжини. Після проходження цих ліній відбувається тимчасове усунення сигналів. Отримані сигнали нормуються за рівнем та віднімаються. Перевагою інтерференційного способу є простота реалізації апаратури, недоліком – зниження точності під час розширення діапазону розвідки та низька чутливість.

Отримання своєчасного та якісного результату радіомоніторингу, як і в подібних сферах діяльності, залежать не лише від наявності дорогої апаратури, але і правильного розташування та монтажу антен і кабелів, і від методів та прийомів роботи [4]

Область застосування систем радіомоніторингу має бути обмежена виходячи з бюджетних обмежень та з урахуванням певних вимог та завдань. Вона має здійснювати:

– контроль та вимірювання за радіоелектронними засобами, призначеними для передачі (випромінювання) електромагнітних хвиль різних діапазонів, з метою забезпечення електромагнітної сумісності різних засобів зв'язку, виконання санітарних і законодавчих обмежень;

– отримання інформації про працюючі передавачі у певній місцевості (або в межах об'єкта), визначення їх типу, основних характеристик, кількості та демодуляція/декодування переданої інформації з метою їх виявлення чи контролю;

– виявлення, спостереження, перехоплення та обробка даних, отриманих за допомогою засобів радіомоніторингу, як засіб оперативного отримання

інформації з метою виконання інформаційної безпеки (радіорозвідка - різновид радіомоніторингу).

Відповідно до положень Регламенту радіозв’язку на службу контролю використання спектра покладаються такі завдання [5]:

1) контроль радіовипромінювань на відповідність умовам присвоєння радіочастот;

2) нагляд за використанням смуг частот і вимірювання зайнятості частотних каналів;

3) вивчення випадків появи та впливу радіозавад;

4) розпізнавання та усунення несанкціонованих радіовипромінювань.

Основною метою проведення регулярного радіоконтролю випромінювань на національному рівні є запобігання появі радіозавад. Механізм реалізації цього завдання базується на регулярному контролі технічних параметрів радіовипромінювань та, для певних радіослужб, змісту радіопередач (наприклад, контроль аматорського радіозв'язку може проводитися також із метою перевірки використання позивних сигналів та відсутності передавання сигналів мовлення).

Згідно зі ст. 19 Закону України "Про радіочастотний ресурс України" [6] радіомоніторинг в Україні здійснюється з метою:

– захисту присвоєнь радіочастот;

– визначення наявного для використання РЧР України;

– визначення ефективності використання розподілених смуг частот;

– розроблення науково обґрунтованих рекомендацій для прийняття відповідних рішень щодо підвищення ефективності використання та задоволення потреб користувачів РЧР України.

Таким чином, радіомоніторинг, як спостереження за реальним станом використання РЧР, передбачає вирішення таких завдань:

– оцінювання реального стану електромагнітної обстановки;

– отримання даних для оцінки ефективності використання РЧР;

– участь у міжнародних програмах із радіомоніторингу;

– виявлення порушень у сфері використання РЧР і користування РЧР;

– вимірювання параметрів радіовипромінювання РЕЗ і ВП.

Моніторинг радіочастотного спектра реалізується шляхом використання таких методів:

1) пошук і виявлення радіовипромінювання в заданому діапазоні (смузі) частот (на заданій частоті);

2) спостереження за радіовипромінюваннями в певному діапазоні (смузі) частот (на заданій частоті);

3) селекція радіовипромінювань;

4) інструментальне оцінювання (вимірювання) параметрів радіовипромінювання;

5) пеленгування ДРВ;

6) визначення місцезнаходження ДРВ;

7) ідентифікація радіовипромінювання та ДРВ.

1.2 Технічні засоби радіомоніторингу

Головним засобом для радіомоніторингу є радіоприймальний пристрій, призначений для роботи у певному діапазоні частот. Залежно від завдання це може бути радіоприймач або аналізатор спектру. Найважливішим елементом радіоприймального пристрою є антена, яка вибирається в залежності від діапазону частот, задачі та умов застосування РПП. Устаткування для радіомоніторингу може бути розрахованим як на певний діапазон частот і тип сигналів, так і бути широкосмуговим, універсальним. РПП може бути обладнано різними демодуляторами, пристроями візуального відображення та реєстрації радіосигналів, можливістю запису, різними засобами технічного аналізу. Зазвичай РПП спеціально призначене для радіомоніторингу має спеціальні функції для пошуку радіосигналів, такі як пошук у заданому

діапазоні або сканування осередків пам'яті, відображення спектра в реальному часі або його записи; автоматична реєстрація сигналів на виході демодулятора [7]. РПП часто є частиною комплексу, призначеного для радіомоніторингу та знаходиться під керуванням комп'ютера, який керує РПП, забезпечує інтерфейс і реєструє дані. Комплекс для радіомоніторингу може мати дистанційне керування, наприклад з метою пеленгації радіосигналів або віддаленого спостереження за електромагнітною обстановкою та інформаційною безпекою. РПП бувають автономними, із власними органами управління.

Приймачі та аналізатори спектру є незамінними інструментами всіх служб радіомоніторингу. Основні відмінності полягають у тому, що приймачі, як правило, забезпечують попередню селекцію в тракт радіочастоти і призначені для демодуляції, в той час як аналізатори спектру призначені для відображення спектральних характеристик радіочастотного сигналу Вимірювання щодо аналогових радіослужб, у тому числі, наприклад, вимірювання відхилення частоти та сумарної потужності сигналу ЧС-радіомовлення повинні виконуватися в приймачі. Вимірювання напруженості поля також виконуються з використанням приймачів. Вимірювання таких параметрів, як частота та ширина смуги можуть здійснюватися і з використанням аналізатора спектра. Аналізатори можуть використовуватися також для вимірювання сигналів із цифровою модуляцією або виявлення невідомих джерел перешкод. Сучасні приймачі можуть мати деякі характеристики, які зазвичай потрібні від аналізаторів спектра. І навпаки, аналізатори спектру, працюючі в режимі нульового інтервалу часу можуть виконувати деякі функції приймачів. У той же час, виконання аналізу з використанням швидкого перетворення Фур'є (ШПФ) і в приймачі, і в аналізаторі спектру стало прийнятним у ціновому відношенні, і йому слід віддавати перевагу. Зовсім не обов'язково, що цей метод виявиться дорожчим, ніж традиційний аналіз з використанням частоти, що коливається.

За характером застосування можна поділити РПП на:

1. портативні;

2. носимі/мобільні;

3. стаціонарні.

Одноканальні приймачі широкосмугові: їхня смуга пропускання дорівнює діапазону розвідуваних частот. Найпростіший широкосмуговий приймач прямого посилення складається з антени, демодулятора, відео підсилювача та індикатора. Точність визначення частоти та чутливість низькі. Одноканальні приймачі застосовуються лише для встановлення самого факту випромінення.

Багатоканальні приймачі забезпечують високу точність визначення частоти. Це пов’язано з тим, що робочий діапазон частот розділяється системою фільтрів на ряд піддіапазонів. Смуги прозорості фільтрів примикають один до одного. Багатоканальні приймачі застосовуються для визначення частоти та типу радіоелектронного засобу, число каналів у яких сягає кількох десятків.

Оскільки з поширенням цифрових засобів зв'язку завдання радіомоніторингу значно ускладнилися. На охоронюваних територіях та державних об'єктах та в безпосередній близькості від них, як правило, знаходяться різні легальні громадські та персональні засоби зв'язку. Стільникові стандарти: GSM-900/1800, CDMA-2000, UMTS, LTE, засоби передачі даних: WiMAX та Wi-Fi, персональні мережі TETRA, DMR, бездротові телефони DECT, бездротові відеокамери DVB-T та інші. Радіозакладки можуть використовувати стандартні види модуляції і не відрізнятися від легальних за спектральними та тимчасовими характеристиками.

Приймач за технологією SDR може забезпечити вищу ефективність, ніж під час використання традиційних аналогових методів, тому що при цифровій обробці сигналів їхня фільтрація близька до ідеальної. Крім того, за допомогою програмних алгоритмів можуть бути реалізовані такі функції, які дуже складно одержати при аналоговій обробці [8].

Для порівняння пристрою SDR та традиційного приймача динамічного діапазону обрано структуру приймача із прямим перетворенням. Вибір обґрунтований тим, що реалізація приймача прямого перетворення простіше і перспективніше з погляду розвитку схемотехнічної реалізації.

Традиційним приймачем є аналізатор спектру С4-25 – високочутливий прилад із широким діапазоном вимірювань у компактному корпусі. Активно використовується в лабораторних дослідженнях, майстернях з ремонту мобільної, телекомунікаційної та радіоапаратури, польових умовах, і скрізь він зберігає високу точність, що дозволяє максимально коректно аналізувати частоту, амплітуду та рівні сигналів різної природи. За рахунок легкості та оптимальних габаритів його легко транспортувати на місце експлуатації, а надійний корпус виключає пошкодження внутрішніх компонентів через механічні та інші зовнішні впливи.

Даний прилад використовується для дослідження в широкому діапазоні частот спектрів періодичних сигналів з можливістю слухового контролю. Аналізатори спектру С4-25 призначені для дослідження та контролю сигналів різних пристроїв. Прилади можуть використовуватися спільно з антенами для аналізу завантаження радіодіапазонів та вимірювання параметрів випромінювань радіопередающих та випромінюючих пристроїв. Зовнішній вигляд аналізатора зображено на рисунку 1.1.

Рисунок 1.1 – Зовнішній вигляд С4-25

Параметри С4-25 наступні:

– діапазон частот: 0,02МГц – 50 МГц;

– смуга обзору:50МГц;

– динамічний діапазон: 60дБ;

– вхідний опір: 50Ом;

– потужність: 100Вт;

– маса: 35кг;

– габарити: 485×256×490мм.

Аналізатори спектру С4-25 мають смугу обзору 50МГц. Смуга пропускання приладів на рівні 3дБ становить 3кГц – 70кГц; 300кГц. Для аналізаторів спектра С4-25 чутливість приладів становить 5мкВ.

Прикладом приймача з технологією SDR може слугувати Malahit DSP. Портативний, майже кишеньковий, автономний радіоприймач широкого охоплення DSP із використанням програмного забезпечення SDR (програмне забезпечення). Включає власний кольоровий 3,5-дюймовий сенсорний РК-екран, внутрішню літій-іонну батарею зі схемою заряджання та виготовлений у міцному легкому металевому корпусі. Також містить досить великий вбудований динамік на справжній панелі. Найголовніше, що він був розроблений для продажу за розумною ціною.

Рисунок 1.2 – Зовнішній вигляд Malahit DSP

Параметри даного пристрою наступні:

– діапазон частот: від 50 кГц до 2,0 ГГц ;

– вибір полоси пропускання, що регулюється від 50 Гц до 15 кГц ;

– всі види аналогової модуляції: AM, LSB, NFM, WFM (додавання режимів CW, DSB і синхронного виявлення з прошивкою 1.10b);

– потужні функції: змінна ширина фільтра, адаптивний приглушувач шуму, пороговий приглушувач шуму, для шумозаглушення, AGC, еквалайзер вбудований декодер азбуки Морзе;

– чудовий синхронний детектор бічної смуги з можливістю вибору;

– застосований потужний stm32H743VIT6 з тактовою частотою 480 МГц;

– споживання: 300мА при прослуховуванні в навушниках;

– 50 каналів пам'яті з легким доступом, які зберігають: частоту, режим, пропускну здатність та інші параметри;

– прийом на вбудований телескоп або зовнішню антену призначений для покращення КХ прийому на антену телескопа;

– підключіться до комп’ютера через USB, який може передавати CAT, IQ та аудіо;

– діапазон 160 кГц, з можливістю масштабування;

– завдяки характеристикам мікросхеми msi001, що використовується, динамічний діапазон блокування становить близько 85 дБ.

Для кращого розуміння відмінностей приладів розглянемо таблицю 1.

Таблиця 1 Порівняльна характеристика Malahit DSP та С4-25

Назва пристроїв / Характеристика	Malahit DSP	С4-25
Діапазон частот	50 кГц – 2,0 ГГц	0,02МГц – 50 МГц
Смуга пропускання	245 МГц	300кГц

Маса	0, 05 кг	35кг
Ціна	≈ 6 000 грн.	≈ 18 200 грн.

Порівнюючи параметри обох пристроїв можна зробити висновки, що Malahit DSP є набагато більш оптимальним. Даний пристрій має набагато більше функцій, має більший діапазон частот, є набагато легшим за вагою та нескладним у використанні, його ціна набагато менша. До того даний приймач можна покращити за допомогою використання антен, що збільшить його параметри.

1.3 Тенденції розвитку радіомоніторингу

В даний час до основних тенденцій розвитку радіомоніторингу можна віднести наступні завдання:

1. Адаптація структури та завдань радіомоніторингу до рівня розвитку засобів зв'язку. Сучасні технології зв'язку мають набагато більшу гнучкість у використанні спектру, ніж система регулювання в частині можливостей забезпечення його ефективного використання, розподілу та перерозподілу частот і смуг частот. Використання вузькоспрямованих антенних систем, кодового та тимчасового поділу каналів, ефективних методів модуляції, низького рівня потужності випромінювання дозволяють цим технологіям ефективніше використовувати радіочастотний спектр за рахунок просторового, частотного, тимчасового, поляризаційного рознесення систем. В даний час автоматизовані системи радіомоніторингу функціонують у багатьох країнах світу. Виходячи з цього, основним напрямом подальшого розвитку системи радіомоніторингу, з одного боку, є створення структури системи, здатної забезпечити вирішення задачі отримання повної поточної та інтегральної інформації про реальну електромагнітну обстановку в будь-якому регіоні. З

іншого боку, забезпечення комплексного радіомоніторингу є надто дорогим заходом [9].

2. Автоматизація системи радіомоніторингу. Автоматизація даної системи може бути системною та апаратною. Незважаючи на те, що провідні виробники обладнання радіомоніторингу та розробники програмного забезпечення пропонують готові системні рішення у сфері автоматизації регулювання використанням РЧР, слід зазначити, що лише одиниці країн можуть похвалитися наявністю таких систем, що функціонують. Основою забезпечення функціонування всієї системи регулювання використання РЧР загалом і кожної з підсистем, що входять до її складу, є наявність єдиної БД обліку радіоелектронних засобів (обліку частотокористувачів). Джерелами інформації для формування та супроводу єдиної БД є: система частотного планування та система радіомоніторингу. Структура автоматизованої системи радіомоніторингу передбачає наявність центру управління та регіональних підсистем радіомоніторингу. У свою чергу кожна регіональна підсистема складається з пункту управління та станцій радіоконтролю, що замикаються на нього. Таким чином, станції, що не обслуговуються, розглядаються переважно як джерела інформації про стан електромагнітної обстановки, що вирішують завдання радіоконтролю за завданнями з пунктів управління і передають туди результати.

3. Розширення функціональних та технічних можливостей радіомоніторингу. В даний час розширення функціональних можливостей радіомоніторингу здійснюється в таких основних напрямках: забезпечення радіоконтролю в діапазонах частот вище 3 ГГц; забезпечення радіоконтролю нових технологій та систем зв'язку в діапазонах частот до 3 ГГц; забезпечення контролю послуг мереж зв'язку.

Проаналізувавши завдання тенденції розвитку радіомоніторингу, можна сказати, що системи SDR є оптимальними для вирішення даних задач, адже вони є в різних цінових діапазонах, і навіть зовсім недорогий пристрій може

мати гарні параметри та широкий діапазон технічних можливостей, мають можливість удосконалюватися завдяки антенам і іншим підсилювачам.

2 ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ПРОГРАМНО-АПАРАТНОЇ ПЛАТФОРМИ HACK-RF

SDR (Software Defined Radio) - це програмно обумовлена радіосистема, де софт перетворює радіосигнал в цифровий вигляд, що надає найширші можливості для аналізу сигналу. Один з найбільш часто використованих та впізнаваємих SDR трансиверів – HACK-RF One. Даний пристрій не можна назвати повноцінною радіостанцією, адже його потужність невелика, близько 20мВт, ККД штатної антени менше 1%. Проте є різні опціональні пристрої та функції, які можна підключити, маючи оригінал девайсу, аби значно покращити його можливості та зробити унікальним.

2.1 Поняття технології SDR

Програмно-обумовлена радіосистема (SDR) - радіопередавач і / або радіоприймач, який використовує технологію, що дозволяє за допомогою програмного забезпечення встановлювати або змінювати робочі радіочастотні параметри, включаючи, зокрема, діапазон частот, тип модуляції або вихідну потужність, за винятком зміни робочих параметрів, використовуваних в ході звичайної попередньо визначеної роботи з попередніми установками радіопристрою, згідно з тією чи іншою специфікації або системи [10].

SDR виконує більшу частину цифрової обробки сигналів на звичайному персональному комп'ютері (ПК) або на програмованій логічній інтегральній схемі (ПЛІС). Метою такої схеми є радіоприймач або радіопередавач довільних радіосистем, змінюваний шляхом програмної переконфігурації (звідси походить альтернативне найменування таких систем - програмно конфігуровані) [11].

SDR надає наступні можливості: змінити тип модуляції, легке протипування, обрати розмір семплірування та смугу пропускання, програмне управління радіочастотами.

Ідея даної концепції базується на передачі широкосмугового сигналу з радіоприймача в ПК та демодуляції сигналу.

В SDR-обладнанні форма модульованого радіосигналу задається в ПЗ. Формується цифровий сигнал, який потім за допомогою широкосмугового ЦАП перетворюється в аналоговий на проміжній частоті (ПЧ). Далі сигнал ПЧ за допомогою перетворення вгору перетворюється у високочастотний сигнал. У приймач все відбувається в зворотному порядку. Широсмуговий АЦП перетворює в цифровий вид безліч вузькосмугових сигналів, що потрапляють до вхідного тракту. У відповідності зі вбудованим ПЗ приймач залучає, перетворює вниз і демодулює сигнали кожного каналу, тобто технологія SDR дозволяє змінювати експлуатаційні параметри радіообладнання на рівні ПЗ.

Схема сучасного SDR-приймача зображена на рисунку 2.1.

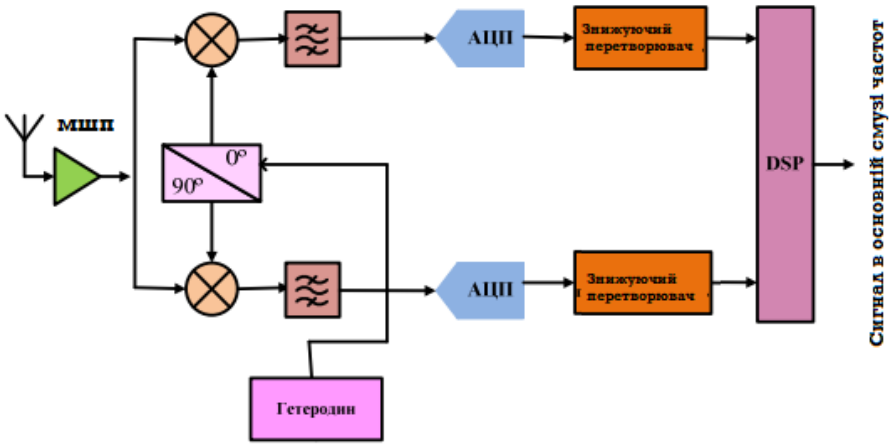


Рисунок 2.1 – Сучасна схема SDR-приймача

Вхідний сигнал посилюється малошумним підсилювачем і ділиться на компоненти I і Q шляхом змішування з гетеродина із синтезу частот у ФАПЧ (для отримання квадратурної компоненти він зміщується на 90 º). Частота

гетеродина підлаштовується під частоту сигналу, щоб різниця вихідних сигналів змішувачів була рівна нулю без модуляції. Для модульованого сигналу вона дорівнює сигналу основної смуги або вихідному модульованому сигналу. Ця архітектура отримала назву пряме перетворення чи перетворення з нульовою проміжною частотою. Після фільтрації сигналів основної смуги у ФНЧ оцифровуються в парі АЦП. Далі в цифровому перетворювачі частота сигналу знижується до робочого діапазону сигнального процесу.

На ринку існує велика різноманітність пристроїв SDR, кожен зі своїми функціями та ціною. Серед найпопулярніших варіантів, які підтримують GNU Radio можна зустріти наступні: AirSpy SDR Receiver, BladeRF,Ettus USRP, або SDR Play RS, HackRF.

2.2 Використання технології SDR для радіомоніторингу. Її основна відмінність від традиційних систем

Концепція SDR полягає в тому, що параметри приймача визначаються за допомогою програмного забезпечення, а не програмної конфігурації. Саме тому, їх можна використовувати для розробки кількох компонентів (підсилювачів, фільтрів, демодуляторів/модуляторів та інших), а також цілих систем (осцилографів, передавачів, приймачів, детекторів та інших модулів). В межах SDR параметри можна динамічно змінювати, що надає гнучкість при реалізації системи радіозв'язку [12].

Концепція SDR проклала шлях для когнітивних радіоприймачів, знаходячи вільні місця та працювати відповідно, динамічно змінюючи модуляцію та зайняті частоти. Це дозволяє ефективніше та економічніше використовувати спектр. Таким чином, моніторинг спектру є попередньою основною функцією для включення когнітивного радіо.

Окрім когнітивного радіо, електромагнітний спектр є дуже важливим і вирішальним надбанням не лише для зв’язку, але й для внутрішньої безпеки та

оборони, у сфері електронної війни, де слід ідентифікувати канали зв’язку супротивника, контролювати та, якщо можливо, демодулювати.

Основна відмінність між традиційними радіосистемами та SDR-системами те, що в перших всі функції реалізуються на апаратному рівні, отже, будь-які зміни в разі потреби можуть бути здійснені тільки за рахунок зміни параметрів фізичних компонентів, що входять у пристрій. Це також призводить до обмеженості системи за необхідності реалізації кількох стандартних протоколів зв'язку та, крім того, значно збільшує вартість виробу. У SDR-системах всі необхідні зміни здійснюються лише на програмному рівні, що дозволяє значно знизити вартість виробу та розширити його функціональні можливості.

2.3 Оптимальність платформи HACK-RF серед інших SDR пристроїв

SDR-пристроїв , що можна просто купити в магазині, дуже багато: Funcube Dongle, RTL-SDR, USRP, OsmoSDR, BladeRF, HackRF, AirSpy, пристрої LimeSDR USB Type-A і інші. В таблиці 1 зібрані деякі SDR з їх характеристиками.

Таблиця 2 – Пристрої SDR та їх характеристики

Пристрій / Характеристика	AirSpy	BladeRF	USRP	SDR Play RSP	HACK-RF
Частотний діапазон	24 МГц – 1,8 ГГц	300 МГц – 3,8 ГГц	50 МГц – 2,2 ГГц	0,1 МГц – 2 ГГц	0,1 МГц – 6 ГГц
Пропускна здатність	10 МГц	28 МГц	16 МГц	8 МГц	20 МГц
ТХ	Відсутній	Повний дуплекс	Повний дуплекс	Відсутній	Напівдуплекс

Продовження таблиці 2.

Хост інтерфейс	USB	USB 3.0 SuperSpeed	USB 3.0	USB 2.0	USB 2.0
Ціна	200$	420$	675 $	150 $	300 $

Аналізуючи таблицю 2 слід зазначити, що кожен виробник може мати різні моделі, тому показана лише найпростіша версія пристрою. Як видно з наведеної вище таблиці, HACK-RF є дешевою платформою, поступаючись лише AirSpy і SDR Play RSP. Однак він має можливість передачі, а також має найбільший частотний діапазон серед усіх платформ. Інші рішення, такі як RTL-SDR на основі ключа, що використовується в Берклі, також не мають можливості передачі. Також HackRF виділяє те, що вона є єдиною повністю відкритою платформою. Саме тому HACK-RF було обрано як платформу для дослідження.

2.4 Технічні характеристики HACK-RF

HackRF — це апаратний проект із відкритим вихідним кодом, який дозволяє створювати периферійні пристрої SDR. Це апаратне забезпечення працює в діапазоні від 30 МГц до 6 ГГц, широкому частотному діапазоні, який дозволяє користувачам вивчати сигнали, що належать до високочастотного (HF), дуже високочастотного (VHF) і надвисокочастотного (UHF) діапазонів. Крім того, використання перетворювачів, дозволяє вивчати навіть діапазон середніх частот (MF). Отже, HackRF можна використовувати для віртуальної реалізації різних технологій, таких як: AM/FM-радіо, Bluetooth, ZigBee або WiFi [13].

Рисунок 2.2 – Зовнішній вигляд HackRf One

Характеристики HackRf One:

– робочий діапазон від 1 МГц до 6 ГГц;

– напівдуплексний трансивер (приймач);;

– частота дискретизації до 20 мільйонів семплів на секунду (20 МГц);

– 8 біт квадратурне семплювання (8 біт на синфазну частину та 8 біт на квадратурну частину);

– працює з програмами GNU Radio, SDR# та іншими;

– програмно-керований смуговий фільтр на прийом та передачу;

– програмно-контрольоване живлення антенного порту (до 50 мА при 3,3 В);

– SMA-мама антенний конектор;

– SMA-мама тактовий вхід та вихід для синхронізації;

– зручні кнопки для програмування.

HackRF здатний передавати і приймати радіосигнали. Він працює в напівдуплексному або повному дуплексному режимі, якщо два пристрої HackRF використовуються разом. Цей компонент зв’язується з головним комп’ютером через USB. Протокол 2.0, також живлення від USB. Іншими цікавими властивостями цього апаратного забезпечення є його низька вартість (близько 300 доларів США) і відкритий код. Це означає, що всі конструкції

апаратного забезпечення та вихідний код програмного забезпечення доступні за ліцензією з відкритим кодом.

До SDR HACK-RF One можна додати PortaPack H1 (рис.2.3) після чого ПК стає не потрібним. Даний пристрій підключається до HACK-RF і додає сенсорний дисплей, елементи навігації, еталон годин 2.5ppm, годинник реального часу, роз'єм для навушників, слот для карти micro SD і спеціальний алюмінієвий корпус [14]. Підключивши USB-павербанк з`являється можливість досліджувати радіочастотний спектр в будь-якому місці. Прошивка PortaPack працює на швидких процесорах ARM в HackRF. Прошивок існує 2: офіційна та модифікована.

Рисунок 2.3 – Зовнішній вигляд PortaPack

HackRF One SDR, на рис. 2.4 показана блок-схема його приймальної гілки. Вхідний РЧ-сигнал від антени (роз'єм SMA) може бути посилений широкосмуговим LNA (підсилювач з низьким рівнем шуму, коефіцієнт посилення 14 дБ, MGA-81563), який перемикається користувачем, де сигнал може проходити через активний пристрій. Його можна відфільтрувати за допомогою HPF (фільтр високих частот) або LPF (фільтр низьких частот), залежно від частотного діапазону, вибраного користувачем. Його квадратурний змішувач забезпечує два компоненти, так звані синфазний (I) і квадратурний (Q). Сигнал гетеродина (LO), впливаючи на нелінійну складову, переводить

високочастотну вхідну смугу в діапазон ПЧ. Стабілізований змішувач PLL (фазова автопідстроювана частота) з VCO (генератор, керований напругою), чіпсет RFFC5072, перетворює енергію вхідної частоти в ПЧ між 2,3 ГГц і 2,7 ГГц, пізніше оцифрований 8-розрядним АЦП (аналого-цифровий перетворювач). HackRF One, зокрема, має АЦП, діапазон якого охоплює до 22 МГц одночасно, MAX 5864. Максимальний SDR встановлено на 20 МГц, потік якого потім надсилається на 32-розрядний процесор ARM Cortex, LPC43XX, пізніше перенесено на USB-канал. Пристрої RTL, з іншого боку, мають ПЧ в діапазоні 3,57 МГц або 4,57 МГц (випадок тюнера R802) або навіть з нульовим ПЧ (неіснуючий тюнер E4000). Вибір низької ПЧ забезпечує кращу вибірковість, тоді як вищі ПЧ призводять до нижчих відгуків зображення змішувача, тому існує компроміс між вибірковістю та відгуком зображення.

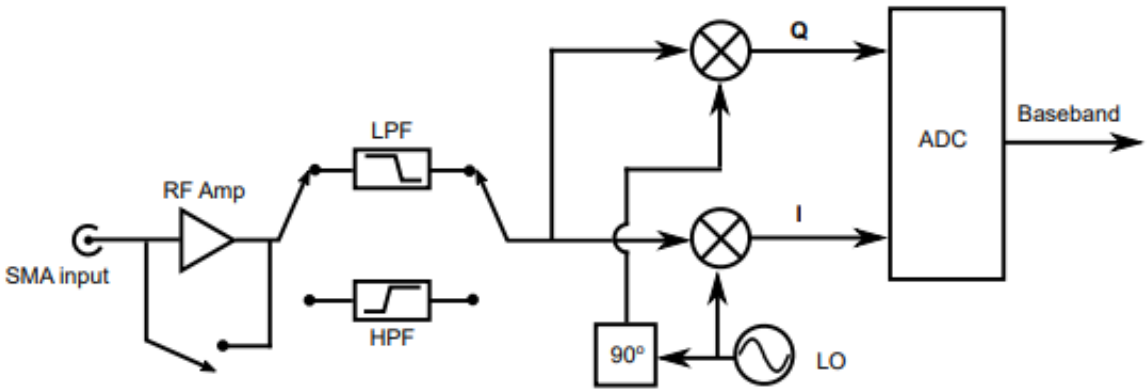


Рисунок 2.4 – Блок-схема сторони прийому HackRF One

2.5 Відмінність оригінального HACK-RF від китайської версії

HackRF One від Great Scott Gadgets (китайський клон)— це програмно визначена радіоперіферія, здатна передавати або приймати радіосигнали від 1 МГц до 6 ГГц.

Рисунок 2.5 – Китайський клон HACK-RF

В комплекті китайського HACK-RF :

– HackRF One з останньою прошивкою PortaPack Mayhem 1.5.4

– PortaPack H2+ з аккумулятором

– Телескопічна антена 40MHz-6GHz

– USB кабель

. Китайський micro-USB шнур взагалі не завадостійкий.

Переваги над оригіналом - комплектні антенни, а недоліки - менша чутливість

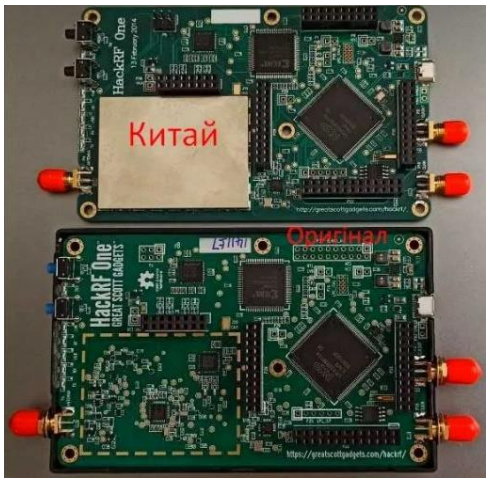


Рисунок 2.6 – Відмінність китайського клона від оригінала

Відмінністю плати китайської версії від оригінала (рис. 2.6) є розпаяний захист від перешкод, але відсутній радіатор.

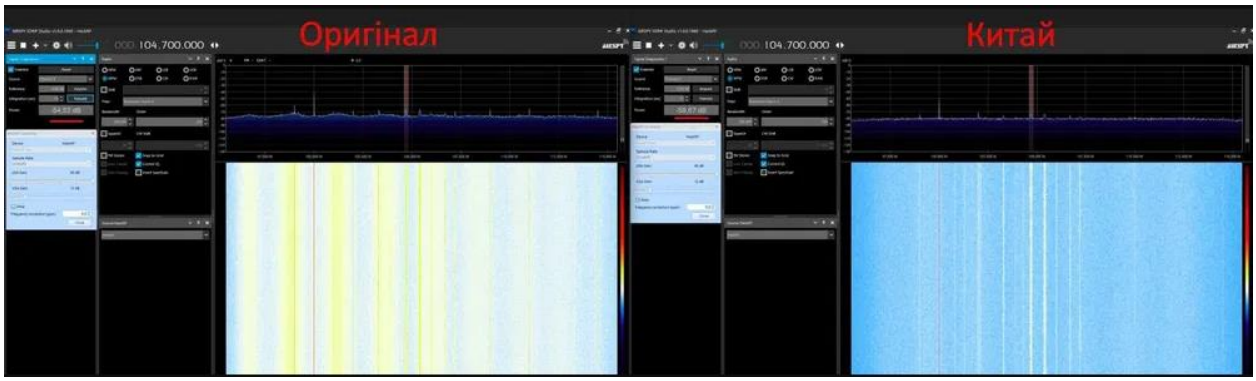


Рисунок 2.7 – Перевірка роботи китайської версії HACK-RF та оригіналу

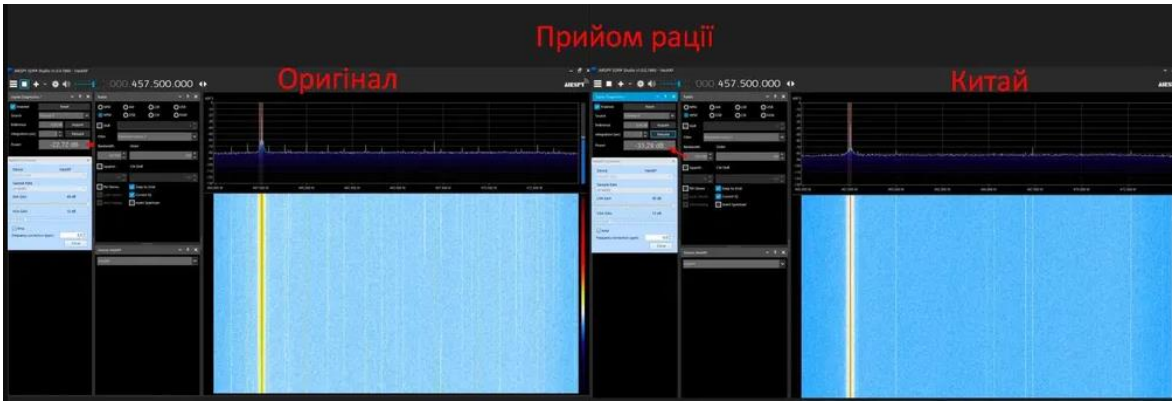


Рисунок 2.8 – Прийом рації оригінального приладу та її китайської версії

На рисунках 2.7 –2.8 ми бачимо, що у китайської версії невелика кількість сигналів, виділяється лише сигнал станції, що демонструє його меншу чутливість.

У китайського клона особливість подвійного перетворення частоти під час використання ZERO IF. 1-й гетеродин конвертера для кВ прийому – 120 МГц, 2-й гетеродин - вже перебудовується, вони мають сигнали прямокутної форми, тобто відбувається перетворення і на гармоніках (high order mixing products), з ослабленням всього 20-30дБ. Тому в режимі ZIF при НЧ прийомі ці перетворення на гармоніках можуть перебувати в смузі огляду, наприклад, при прийомі частоти 1 МГц в режимі ZIF, на частотах 700 і 500 кГц будуть побічні перетворення сигналу.

2.6 Опціональні пристрої для роботи платформи HACK-RF

Опціональні пристрої значно покращують роботу HACK-RF, зменшують розсіяні електромагнітні випромінювання, збільшують діапазон дії та інше, більш детально розглянемо деякі з них.

Антенна AT-Link Hack RF Edition (рис. 2.9) з довжиною кабелю 5 метрів і відмінним узгодженням. Вона виготовлена з нержавіючої сталі та пофарбована чорною порошковою фарбою.

Рисунок 2.9 – Антенна AT-Link Hack RF Edition

Використовуючи дану антену з`являється можливість розмістити її в кращих місцях, наприклад на дереві, за рахунок її довжини. Посилення антени 12 дБ дозволить без підсилювача розпізнати підліт дрона на частоті 2.4 ГГц на відстані близько 1.5-2 км.

Повнодіапазонний підсилювач (рис. 2.10) з високою лінійністю та наднизьким рівнем шуму в металевому корпусі має наступні параметри:

- Джерело живлення: 5 В 70 мА;
- Діапазон частот: 100к-6ГГц;
- Наднизький коефіцієнт шуму NF 0,4 дБ на частоті 1,95 ГГц;
- Високий коефіцієнт посилення частоті 1,95 ГГц, коефіцієнт посилення 20 дБ;
- Висока лінійність, вихід +35 дБм IP3;

– Висока стійкість до вхідної потужності +22 дБм CW;
– Стабільна робота;
– вхід/вихід 50 Ом;
– Роз'єм: гніздо SMA;
– Розмір: 45*45*18,5 мм (без урахування стиків);
– Вага: 46 г;
– 2 режиму живлення: -Від зовнішнього джерела; -роз'єм мікро-USB.

Рисунок 2.10 - Повнодіапазонний підсилювач

Завдяки даному підсилювачу можна збільшити чутливість, що підвищить можливість прийняти слабкі за потужністю сигнали.

Радіочастотний екран для HackRF (рис. 2.11). Основу екрану потрібно припаяти до плати, а сам екран встановлюється на основу.

Рисунок 2.11 - Радіочастотний екран для HackRF

Застосування даного пристрою допомагає зменшити розсіяні електромагнітні випромінювання, використовується при відсутності PortaPack.

3 ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ HACK-RF ДЛЯ ЗАДАЧ АВТОМАТИЗОВАНОГО РАДІОМОНІТОРИНГУ

HACK-RF є дуже багатофункціональним, відкриваючи безліч можливостей в різних сферах життя, тому що може використовуватися як приймач, так і як передавач. Завдяки даному пристрою більшість поставлених завдань РМ можна виконати. Враховуючи можливості даної платформи, вона може використовуватися також в РЕР та РЕБ. В даному розділі розглядається виконання деяких задач радіомоніторингу.

3.1 Застосування HACK-RF для прийому радіомовлення та декодування цифрових сигналів

Радіомовлення - один з оперативних засобів масової звукової інформації, що здійснюється за допомогою сукупності передавальних та приймаючих технічних засобів електрозв'язку.

Фіксованості повідомлення на радіо немає, цим і характеризуються особливості радіомовлення. Така передача інформації призначається на її одноразове сприйняття, коли вона у прямому ефірі. Доставка аудіоматеріалу кінцевому адресату закладена у самих технічних особливостях радіо: від комунікатора до безпосереднього споживача у будь-яку точку простору та у будь-який час, без посередників. Це гарантує радіомовленню найвищу оперативність засобів і охоплення максимальної потенційної аудиторії.

Для розгляду застосування HACK-RF для радіомовлення будемо використовувати АМ, вона комерційно використовується для даної задачі в діапазоні від 535 до 160 кГц. Цей діапазон буде використано під час дослідження для прослуховування АМ-радіоканалу. У цьому типі модуляції

амплітуда несучої хвилі пропорційно змінюється відносно форми сигналу, що передається.

Для проведення дослідження використовувалося GNU Radio. Це безкоштовний інструментарій розробки програмного забезпечення з відкритим вихідним кодом, який містить кілька блоків обробки для реалізації програмного радіо. Крім того, він дозволяє як створювати нові блоки, так і змінювати існуючі, програмуючи їх на Python.

Для дослідження була створена наступна схема, показана на рисунку 3.1.

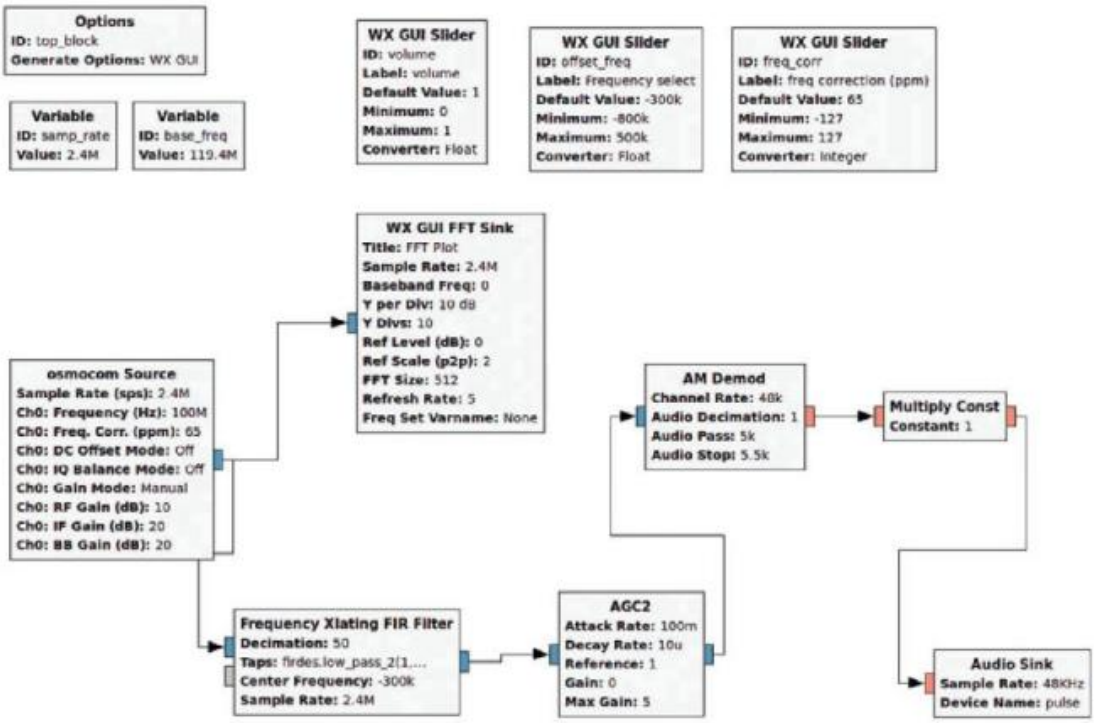


Рисунок 3.1 – Блок-схема синхронної демодуляції AM

Як можна помітити, спеціальний вихідний блок під назвою Osmocom Source block необхідний для забезпечення сигналу, який фіксує HackRF. Цей блок визначається частотою дискретизації та частотою кореляції та може використовуватися як для передачі, так і для прийому.

Крім джерела, фільтра, демодуляції та інших блоків, завжди необхідно включати приймальник, який є кінцевою точкою програми. У цьому випадку

було вибрано блок Audio Sink, щоб дозволити прослуховувати демодульований сигнал, просто підключивши гучномовець або навушники до комп’ютера. Крім того, було включено декілька графічних блоків. Це блоки графічного інтерфейсу WX і відповідні компоненти ковзної панелі, які показані на рисунку 3.2.

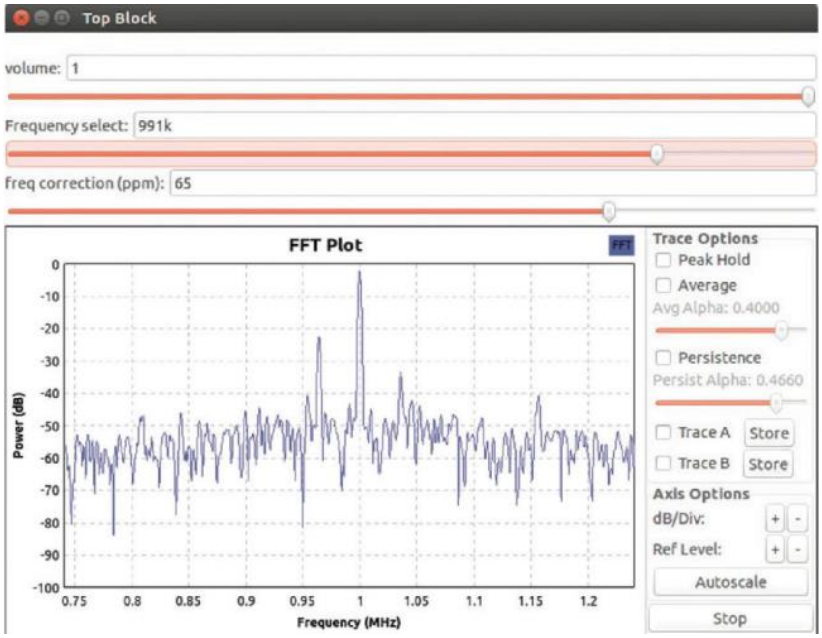


Рисунок 3.2 – Блок прийому WX GUI FFT, який фіксує AM-сигнал після демодуляції

Елементи пов'язані з параметрами системи, тому можна змінювати посилення прийому (гучність), діапазон частот та інші параметри в режимі реального часу, спостерігаючи за впливом на сигнал.

FM має кращу точність і завадостійкість, тому він активно використовується в FM-радіомовленні, а також в інших контекстах, таких як телеметрія або радар. FM-радіомовлення працює приблизно в діапазоні від 85 до 117 МГц. У цьому типі модуляції модулюючий сигнал пропорційний зміні між несучою та його центральною частотами.

Метою цього дослідження буде прослуховування деяких із комерційних FM-каналів. Тим не менш, слід зазначити, що FM демодуляцію важче виконати,

ніж AM. Таким чином, будуть необхідні інші компоненти, такі як Rational Resampler, Frequency Multiplier або блок отримання WBFM.

На рисунку 3.3 зображено результат цього дослідження. Слід зазначити, що блок WX GUI дозволяє відображати середні значення та/або пікові. Таким чином, можна чітко визначити, де можуть бути розташовані FM-канали.

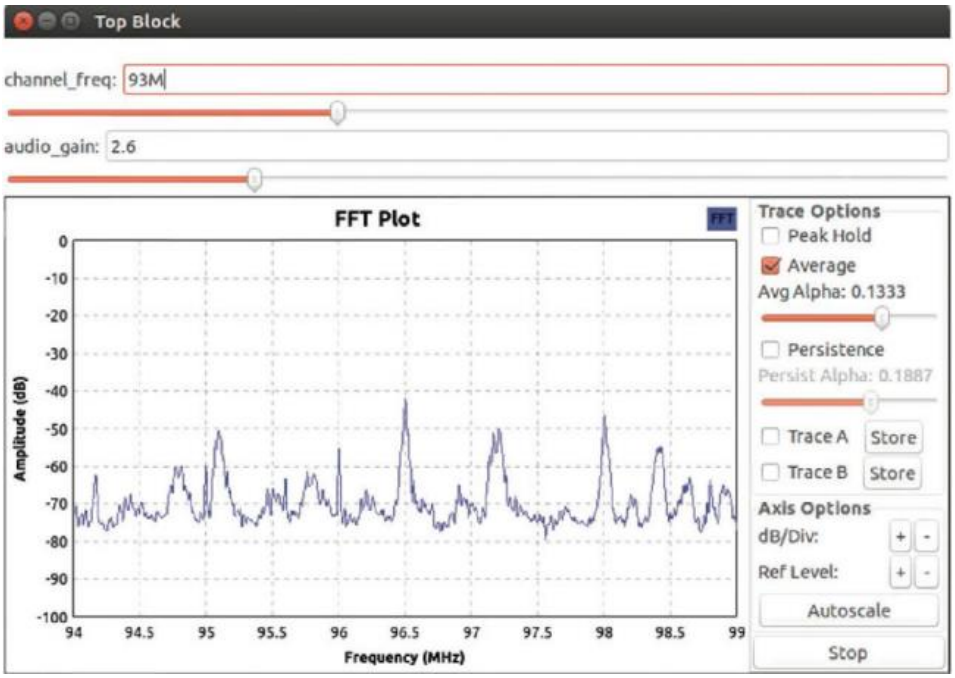


Рисунок 3.3 – Спектр FM

У системах передачі дискретних повідомлень у результаті демодуляції послідовність елементів сигналу перетворюється на послідовність кодових символів, після чого ця послідовність перетворюється на послідовність елементів повідомлення, що видається одержувачу [15]. Це перетворення називається декодуванням.

За допомогою апаратного програмно визначеного приймача, що працює з програмою SDRSharp та утилітою DSD+, можна дешево і просто прослуховувати незашифровані цифрові радіостанції, наразі вони є дуже популярними, а саме через те, що вони мають ряд переваг порівняно з традиційними аналоговими видами радіозв`язку. Проте цифровий радіозв`язок

набагато складніше прослуховувати через те, що потрібні спеціальні приймачі, вони досить дорогі, тому що можуть декодувати цифровий сигнал. Системи цифрового радіозв`язку можуть бути зашифровані, тому прослуховування стає майже неможливим, проте більшість користувачів залишають перемовини не зашифрованими через дороговизну, затримки переговорів, швидше розряджання акамуляторів портативних прийомо-передавачів, яким потрібно використовувати додаткову потужність для розшифровки даних, що надходять та відправки шифрованих даних. Найбільш розповсюджений набір стандартів для цифрового кодування APSO P25 або просто P25, який має 3 фази, але на даний момент широко застосованою є перша, яка може бути успішно декодована DSD+. DSD+ підтримує і інші стандарти.

За допомогою HACK-RF, який може приймати і виконувати дискретизацію сигналу, DSD+ та SDRSharp, можна приймати і декодувати різні стандарти цифрового зв`язку, за умови, що вони не зашифровані.

Послідовність виконання дослідження наступна:

1. В SDRSharp обираємо джерелом – обладнання, а саме HACK-RF

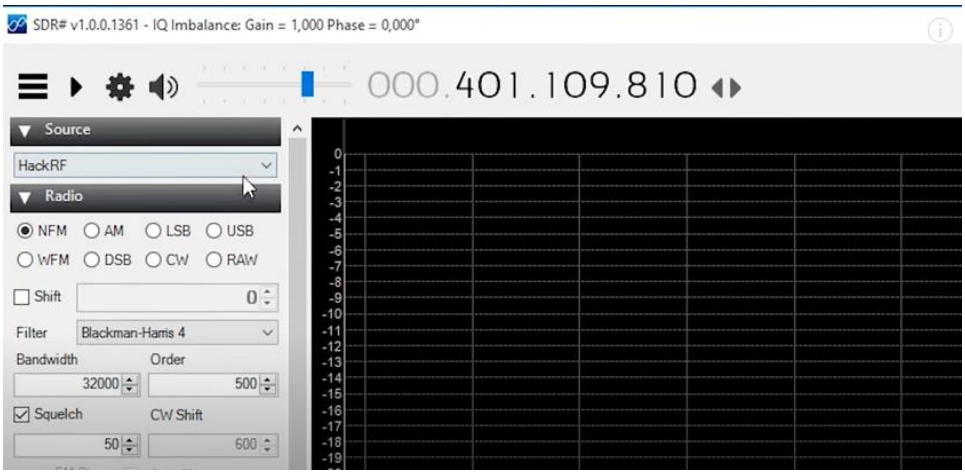


Рисунок 3.4 – Програмне вікно з вибором приймача

2. У DSD Interface обираємо звуковий пристрій.

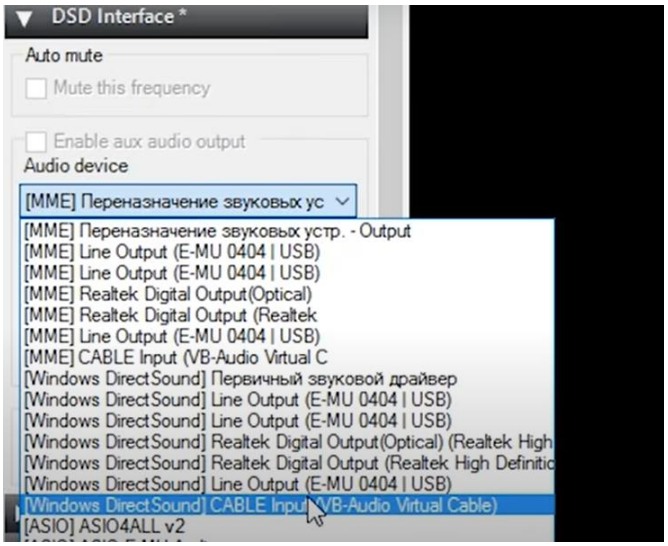


Рисунок 3.5 – Програмне вікно з вибором звукового пристрою

3. Натискаємо Start DSD. Обираємо звуковий вхід і вихід. Заходимо в налаштування і вводимо номера входа і виходу.

Рисунок 3.6 – Вікно з номерами входу/виходу

4. Запускаємо роботу програми, нажавши кнопку Start.

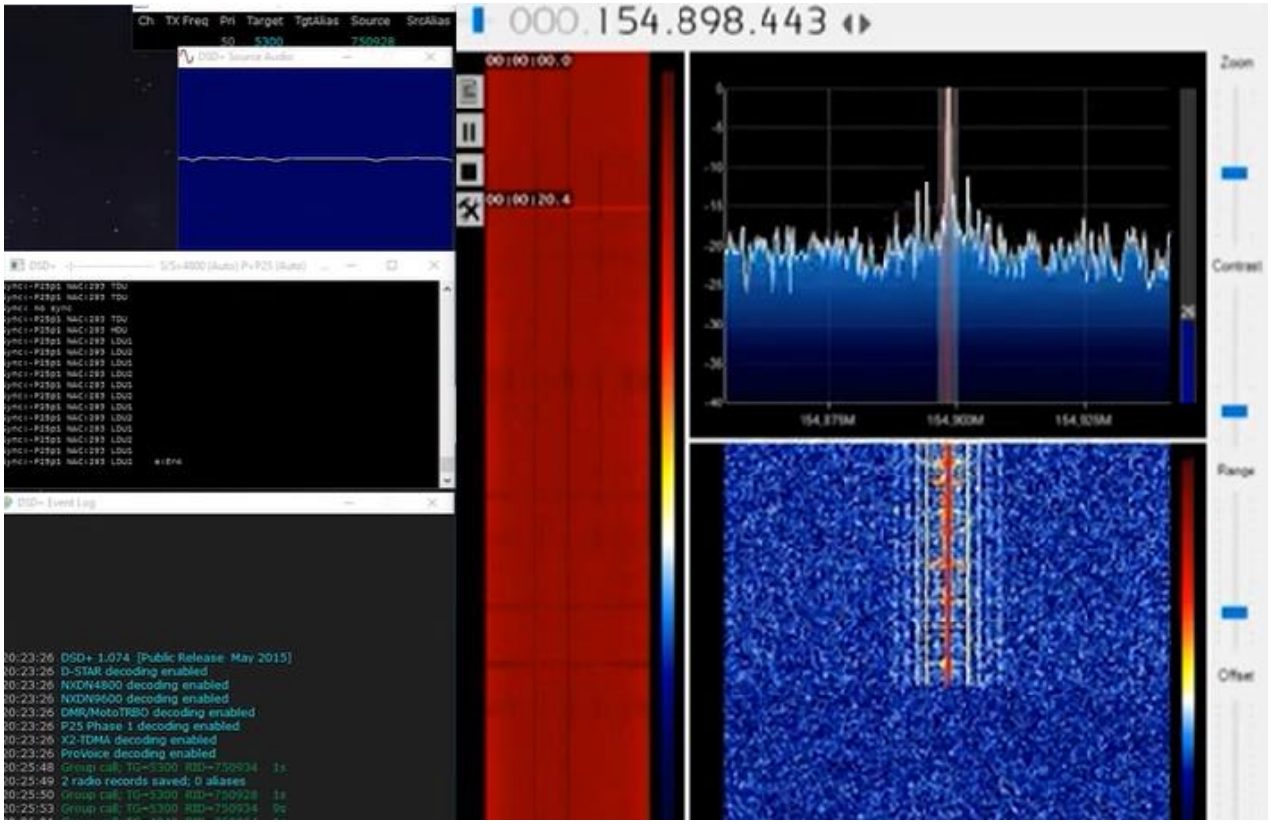


Рисунок 3.7 – Декодування цифрового радіозв’язку за допомогою DSD+ та SDRSharp

Розглянемо детальніше рис. 3.7: у верхньому чорному прямокутному вікні відображається поточна активність (канал, частота, пріорітет та інше); вікно,що знаходиться нижче відображає сигнал на вході ; далі вікно відображає поточну активність програми (якщо після sync вказана назва стандарта, то програма автоматично його визначила, якщо no sync, то передача не проходить. В налаштуваннях програми можна вказати необхідний стандарт. NAC – заголовки пакетів. TDU,LDU – фрейми стандарта); останнє вікно відображає поточні події, наприклад час тривалості з`єднання.

3.2 Використання HACK-RF для знаходження координат літака

Більшість літаків та інших літальних апаратів оснащені ретранслятором — пристроєм, який передає дані про місцезнаходження повітряного судна та

інші відомості про політ до Центру управління повітряним рухом. Цей сигнал може бути прийнятий недорогими приймачами, заснованими на технології, званої ADS-B.

ADS-B – це автоматичне залежне спостереження в режимі радіомовлення. Це технологічне рішення, що визначає координати літака використовуючи для цього систему GPS, і потім, транслює їх і інші дані (висота, швидкість, рейс тощо) про політ як в наземні центри диспетчерам, так і іншим літакам. ADS-B дозволяє пілотам і диспетчерам бачити одну і ту ж картину того, що відбувається, що підвищує взаєморозуміння між усіма учасниками руху, тим самим підвищуючи безпеку і гнучкість управління повітряним рухом [16].

Gqrx - це програмно-визначуване радіо з відкритим вихідним кодом (SDR) приймач реалізований з використанням GNU Radio та Qt GUI toolkit. В даний час він працює на Linux та Mac з обладнанням, що підтримується gr-osmosdr., включаючи Funcube Dongle, RTL-SDR, Airspy, HackRF, BladeRF, RFSpace, USRP та SoapySDR.

Використаємо Gqrx (встановлений на Ubuntu 12.04.2)для перевірки частоти 1090 МГц (рис. 3.8). На рисунку 3.8 майже нічого немає , хоча, якщо подивитися дуже уважно, можна помітити випадкові трохи більш зелені короткі горизонтальні лінії у водоспаді на цій частоті. Дійсно, передачі ADS-B дуже короткі (близько 200 мкс) і не дуже часті, тому велику частину часу в ефірі нічого немає.

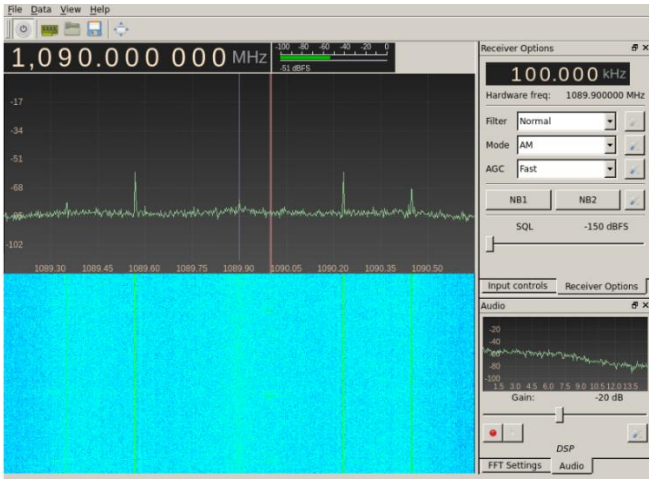


Рисунок 3.8 – Передача ADS-B

Dump 1090 – це декодер режиму S спеціально розроблений для пристроїв SDR.

Основні особливості:

– Надійне декодування слабких повідомлень, у режимі 1090 багато користувачів відзначають покращений діапазон у порівнянні з іншими популярними декодерами.

– Підтримка мережі: потік TCP30003 (MSG5...), необроблені пакети, HTTP.

– Вбудований HTTP-сервер, який відображає виявлені літаки на карті Google.

– Коригування одиночних помилок за допомогою 24-бітної CRC.

– Можливість декодування повідомлень DF11, DF17.

– Можливість декодування форматів DF, таких як DF0, DF4, DF5, DF16, DF20 та DF21, де контрольна сума пов'язана з адресою ICAO шляхом перебору поля контрольної суми з використанням нещодавно переглянутих адрес ICAO.

– Декодування необроблених зразків IQ із файлу (використовуючи параметр командного рядка --ifile).

– Інтерактивний режим інтерфейсу командного рядка, в якому виявлені в даний час літаки відображаються у вигляді списку, що оновлюється при надходженні додаткових даних.

– Розшифровка координат CPR та розрахунок треку за швидкістю.

– Потокова передача TCP-сервера та отримання необроблених даних від/до підключених клієнтів (використовуючи --net).

Щоб захопити трафік прямо з пристрою та відобразити захоплений трафік у стандартному виведенні потрібно запустити програму без будь-яких параметрів:

./dump1090

Щоб запустити програму в інтерактивному режимі:

./dump1090 --interactive

Щоб запустити програму в інтерактивному режимі за допомогою мережі та підключитися за допомогою браузера до http://localhost:8080 , щоб побачити трафік у реальному часі:

./dump1090 --interactive --net

В інтерактивному режимі можна отримати менш насичений інформацією, але більш «аркадний» висновок, коли екран оновлюється кожну секунду, відображаючи всі помічені літаки з деякою додатковою інформацією, такий як висота над рівнем моря і номер рейсу, витягнутої з отриманого режиму S. пакети.

Dump 1090 в інтерактивному режимі показує польоти (а також шум - і його більше, ніж зазвичай через зміну тайм-ауту входу з 60 на 600 секунд), що працює з -metric опцією, таким чином, висота в метрах, а швидкість км/год (рис. 3.9).

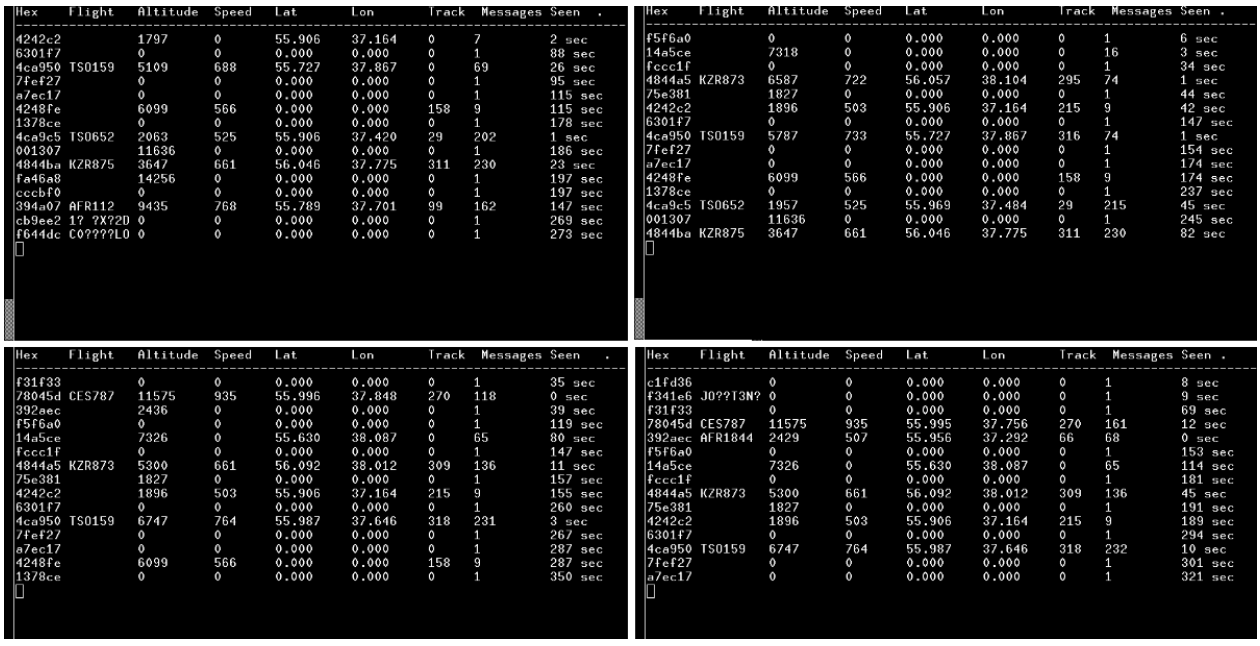


Рисунок 3.9 – DUMP 1090 в інтерактивному режимі

На рисунку 3.9 показано, що рейс AFR112 це "рейс Air France з Парижа, Франція (CDG) до Шанхаю, Китай (PVG)", і він не приземляється і не злітає в

обраному аеропорту - але його "бачать" через ADS -B. Так само CES787, мабуть, є «рейсом China Eastern Airlines з Шанхаю, Китай (PVG) до Риму, Італія (FCO)», на висоті понад 11,5 км і швидкості 935 км/год.

dump1090 у неінтерактивному режимі, то консоль відобразить захвачений трафік в стандартному вигляді (рис. 3.10 - 3.11).

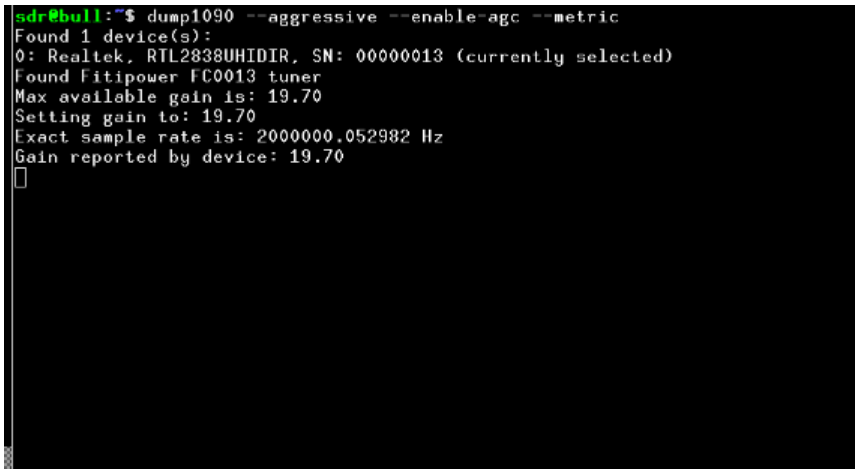


Рисунок 3.10 – DUMP 1090 у неінтерактивному режимі

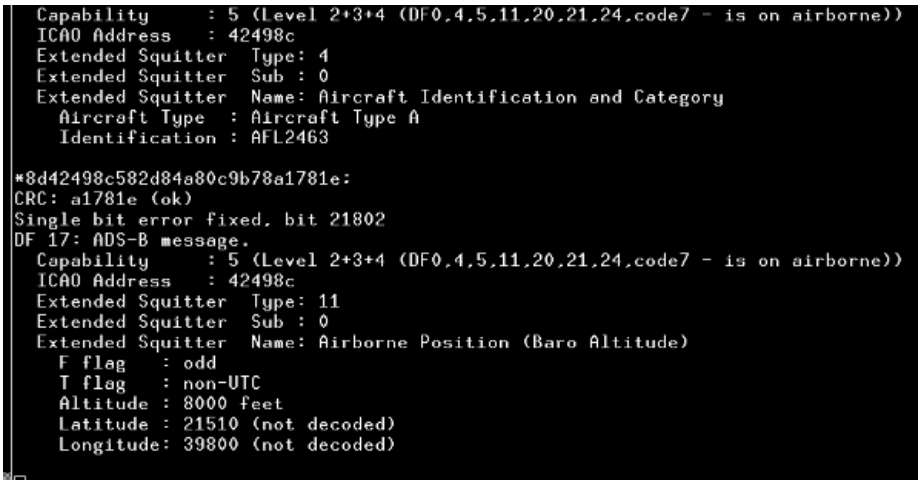


Рисунок 3.11 – DUMP 1090 в неінтерактивному режимі, за кілька секунд

3.3 Дослідження радіосигналів, що випромінює БпЛА

Для виявлення дронів використовують: радіочастотні аналізатори, акустичні датчики, оптичні датчики та радари.

За допомогою HACKRF One можна виявити БПЛА, а також знешкодити його за потребою.

Нова функція HACKRF під назвою HackRF Sweep дозволяє керувати ультрашироким спектром на видатній швидкості 6 ГГц/с, що дозволяє використовувати надширокосмуговий моніторинг шуму.

Послідовність дій для підключення нової функції та її використання:

1. Оновити HackRF за допомогою команд наведених на рис.3.12.

```
https://github.com/mossman/hackrf/wiki/Updating-Firmware
hackrf_spiflash -w hackrf_one_usb.bin (After completed, reset device.)
hackrf_cpldjtag -x firmware/cpld/sgpio_if/default.xsvf (LEDs blinking
indicates completed. Reset device again.)
hackrf_info (Verify successful update.)
```

Рисунок 3.12 – Необхідні команди для оновлення HackRF

2. Ввести команду наведену на рис. 3.13 та підключити HackRF.

```
root@kali:~/Downloads/hackrf-2017.02.1/firmware-bin# hackrf_spiflash -w hackrf_one_usb.bin
File size 21960 bytes.
Checking target device compatibility
Erasing SPI flash.
Writing 21960 bytes at 0x000000.
root@kali:~/Downloads/hackrf-2017.02.1/firmware-bin#
```

Рисунок 3.13 – Команда з каталогу

3. Оновити CPL. Після чого світлодіоди почнуть мерехтіти і HackRF потрібно від’єднати, після підключити знову.

```
root@kali:~/Downloads/hackrf-2017.02.1# hackrf_cpldjtag -x firmware/cpld/sgpio_if/default.xsvf
File size 37629 bytes.
LED1/2/3 blinking means CPLD program success.
LED3/RED steady means error.
Wait message 'Write finished' or in case of LED3/RED steady, Power OFF/Disconnect the HackRF.
```

Рисунок 3.14 – Оновлення CPL

4. Запустити HackRF info. Повинна бути відповідь від HackRF.

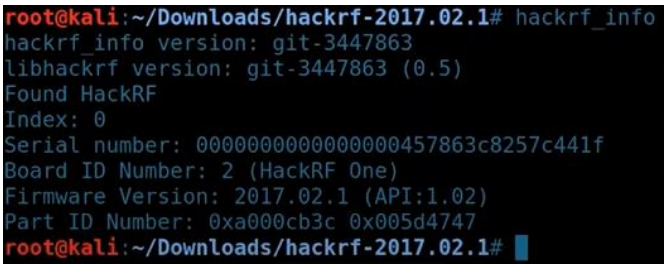


Рисунок 3.15 – HackRF info

5. Ввести команду sweep.

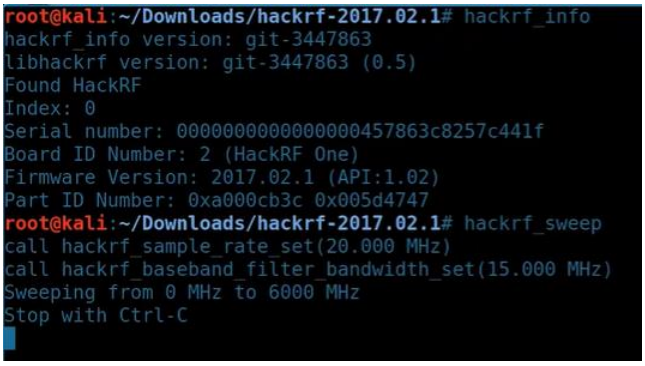


Рисунок 3.16 – Команда sweep

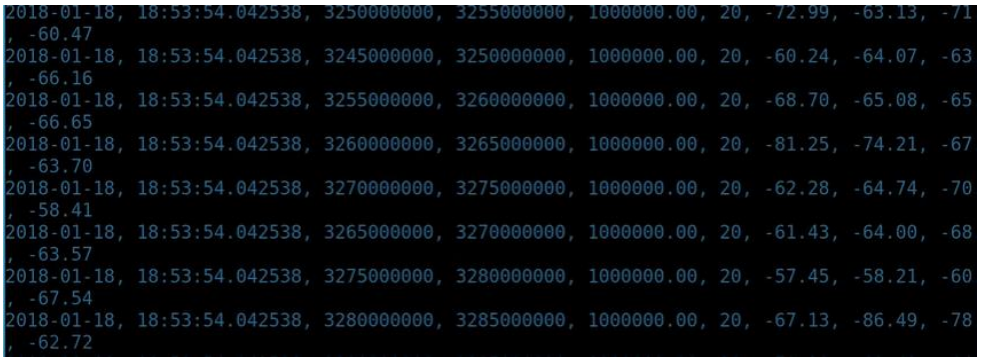


Рисунок 3.17 – Відповідь на команду sweep

6. Ввести qspectrunanalyzer.

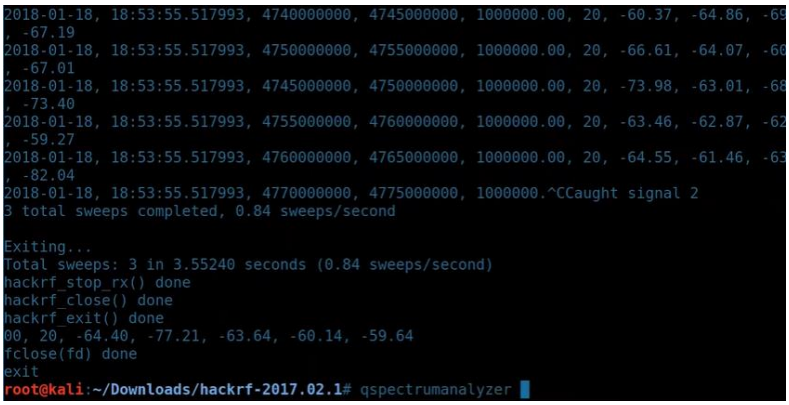


Рисунок 3.18 – Команда qspectrunanalyzer

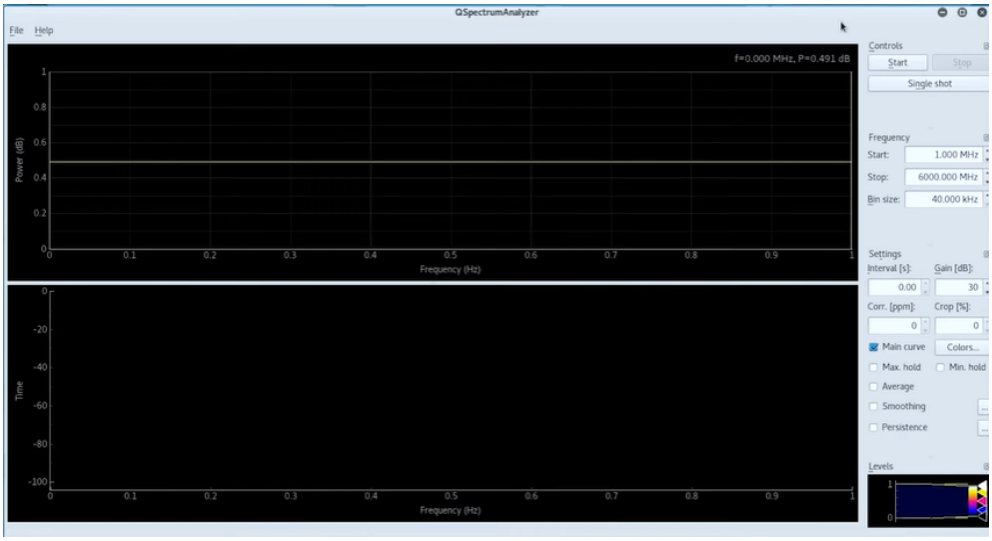


Рисунок 3.19 – Відповідь на команду qspectrunanalyzer

7. Встановити необхідні налаштування.

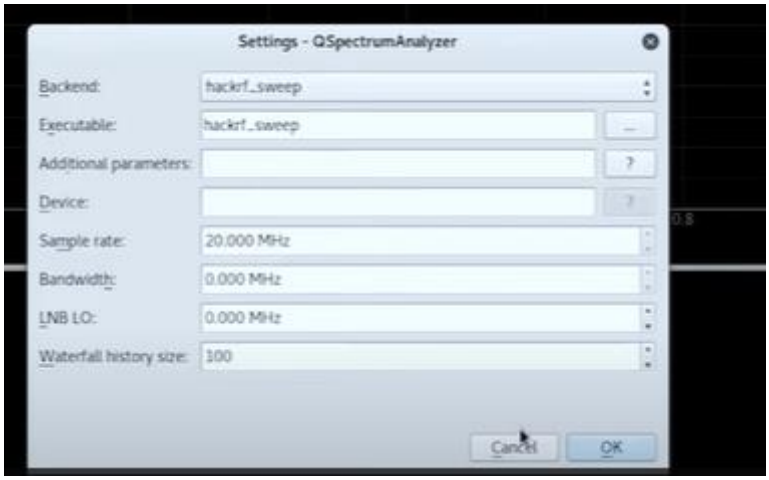


Рисунок 3.20 – Налаштування

8. Натиснути Start. З’явиться графік аналізатору спектра, що охоплює 6 ГГц. Курсор, який наводиться на графіку вказує на частоту та потужність. Якщо необхідно спіймати всі сигнали поблизу можна встановити прапорець максимального утримання, дозволити програмі працювати кілька хвилин після чого шукати найсильніші сигнали. Якщо ми наведемо курсор на пік найсильніших сигналів ми можемо побачити їх частоти.

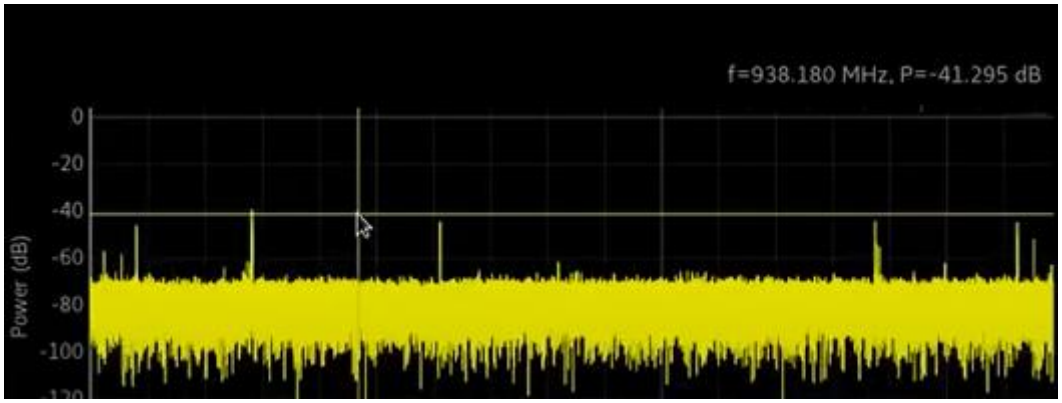


Рисунок 3.21 – Графік аналізатору спектра

Для перевірки чи змінюється сигнал (стає сильнішим коли приближаємо, стає слабшим коли віддаляємо HACK-RF) необхідно приєднати до HACK-RF антену. Якщо необхідно дізнатися звідки точно надходять сигнали потрібно приєднати зонд ближнього поля. Зонд ближнього поля призначений для виявлення магнітних полів, які випромінюються вертикально від поверхні друкованих та монтажних плат і можуть застосовуватися для дослідження струмової петлі. Діапазон частот від 30 МГц до 3 ГГц.

Рисунок 3.23 – Досліджувана установка

Найбільш популярні дрони працюють на частоті 2,4 ГГц і 5,8 ГГц, знаючи ці частоти можна виявити БпЛА за допомогою даної функції HACK-RF.

HACK-RF може не тільки виявити БпЛА, а й допомогти завданню РЕБ, наприклад за допомогою спуфінга, при умові що квадракоптер має GPS.

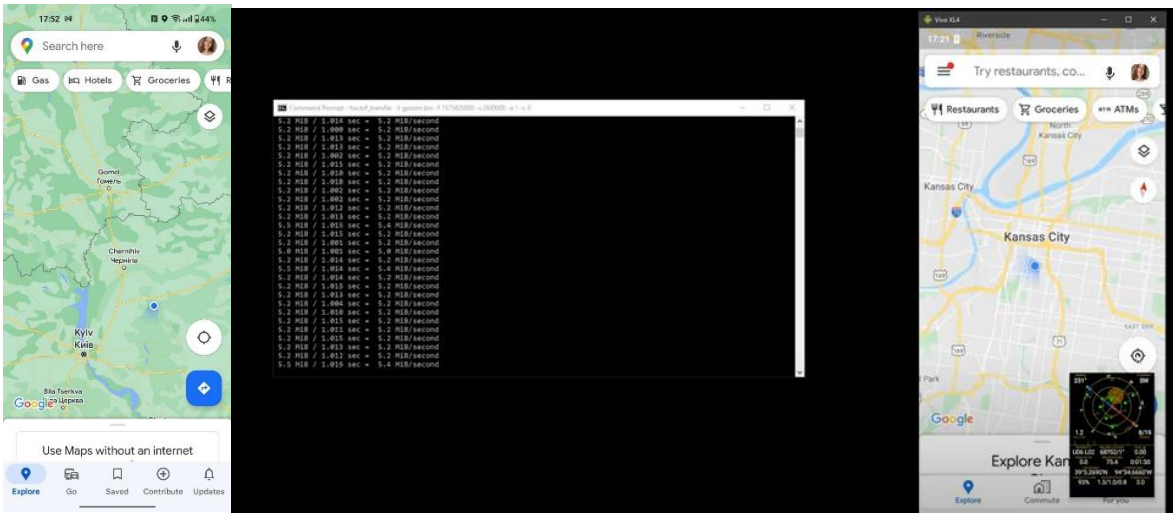
Спуфінг (від англійського слова spoofing) - це кібер-атака, в рамках якої шахрай видає себе за якесь надійне джерело, щоб отримати доступ до важливих даних або інформації. Така заміна (спуфінг-атака) може відбуватися через веб-сайти, електронну пошту, телефонні дзвінки, текстові повідомлення, IP-адреси та сервери [17].

Спуфінг-атака на GPS-приймач працює наступним чином: широкомовно передаючи трохи більш потужний сигнал, ніж отриманий від супутників GPS, такий, щоб бути схожим на ряд нормальних сигналів GPS [18]. Імітовані сигнали змушують одержувача неправильно визначати своє місцерозташування, вважаючи його таким, як задав атакуючий. Для проведення GPS-спуфінгу необхідно точно знати місцерозташування жертви, аби структурувати імітуючий сигнал з належними затримками. Дана атака проводиться повільно, щоб не спричинити втрату сигнального блокування.

Після атаки на дрон вірогідніше всього він буде висіти в повітрі або включить аварійну посадку, також можливо, що він розіб’ється.

Спуфінг за допомгою HACK-RF можна виконати в кілька способів, а саме:

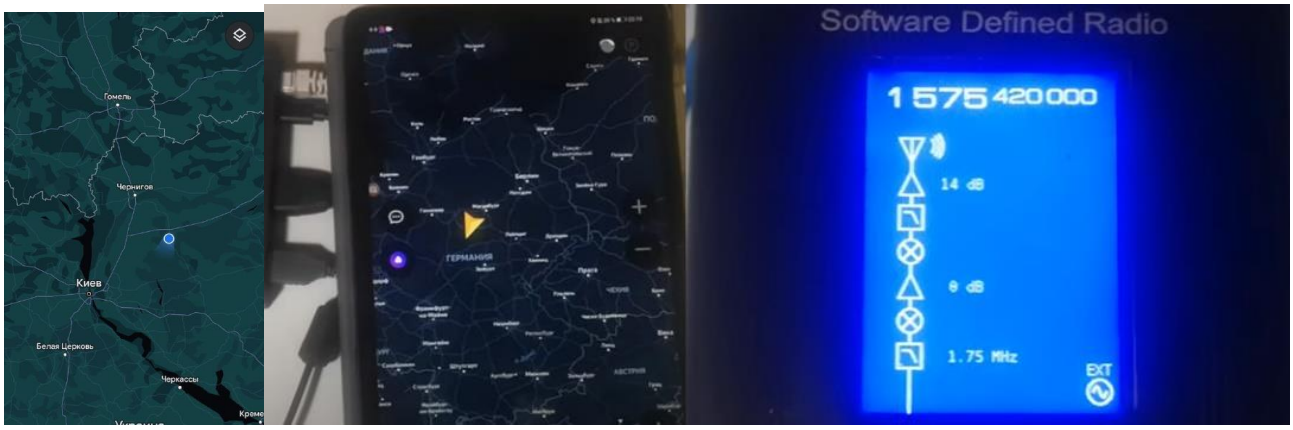
– заміна геолокації в Windows;



а) б)

Рисунок 3.24 – Spoofing атака через Windows: а) початкові координати; б) координати після спуфінг атаки

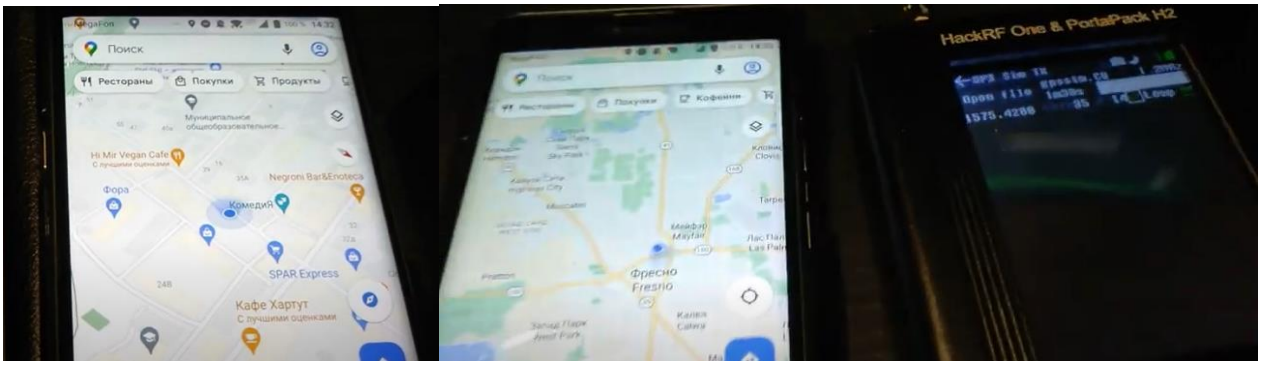
– підміна геолокації за допомогою Double SSH Tunnel Manager та HackRF ONE;



а) б)

Рисунок 3.25 – Spoofing атака: а) початкове місцезнаходження; б) місцезнаходженння після проведення атаки

– підміна координат за допомогою HackRF PortaPack.



а) б)

Рисунок 3.26 – Spoofing атака PortaPack: а) початкове місцезнаходження; б) місце знаходження після проведення атаки

ВИСНОВКИ

В кваліфікаційній роботі було проведене дослідження застосування платформи HACK-RF для задач автоматизованого радіомоніторингу.

В ході роботи було розглянуто особливості і тенденції розвитку моніторингу. Спираючись на результати дослідження тенденцій розвитку радіомоніторингу, можна з впевненістю стверджувати, що такі комплекси вже є обов'язковим елементом системи управління.

Розглянуто технологія SDR, платформа HACK-RF. Була підкреслена оптимальність обраної платформи серед інших SDR та запропоновані опціональні пристрої для покращення її роботи.

Проведене дослідження застосування HACK-RF для прийому радіомовлення та декодування, використовуючи різні методи дослідження. AM та FM-радіомовлення досить легко досліджується за допомогою GNU Radio, результатом роботи стало знаходження та демодуляція AM- та FM-каналів. Результатом дослідження декодування було прослуховування сигналів на частоті 154 МГц. За рахунок великого функціоналу обраної платформи дані дослідження могли бути проведені різними способами, з використанням ПК, PortaPack та різних програм. Також дослідження виявлення сигналів літака та БпЛА. Завдяки декодеру Dump 1090 та технологічному рішенню ADS-B було виявлено сигнали літаків, а завдяки функції Sweep виявлено дрони. Запропоновано методи РЕБ за допомогою HACK-RF, а саме спуфінг-атака, що може не просто вивести з ладу літальний апарат, а в деяких випадках і знищити його.

ПЕРЕЛІК ПОСИЛАНЬ

1. Довідник з радіомоніторингу / Під заг. ред. П.В. Слободянюка. – Ніжин: ТОВ "Видавництво "Аспект-Поліграф", 2008. 588 С.

2. Гаценко (S.S. Hatsenko) С., Писаренко (R.V. Pysarenko) Р., Лук'янчіков (I.M. Lukianchykov) І., Ошкодер (S.V. Oshkoder) С., Ніколаєнко (V.P. Nykolaienko) В., & Приходько (O.G. Prykhodko) О. (2020). ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ РАДІОМОНІТОРИНГОМ. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, (67), 5–17.

3. Рембовскии А.ММ Ашнхмин А.В., Козьмин В.А. Радномониторинг: задачи, методы, средства / Под ред. А.М. Рембовского.- М.: Горячая линияТелеком^2006. 492 с

4. Weber C., Peter M., Felhauer T. Automatic modulation classification technique for radio monitoring //Electronics Letters. – 2015. – Т. 51. – №. 10.С. 796.

5. Регламент радиосвязи. Сборник рабочих материалов по международному регулированию планирования и использования радиочастотного спектра.- М.: 2004.

6. Закон України „Про радіочастотний ресурс України*' від 24.06.2004 р. № 1876-1V із змінами і доповненнями.

7. Благодарней В.Г., Ступак В.С. Основні терміни у сфері користування радіочастотним ресурсом: Словник-довідник / За ред. П.В. Слободянюка. - Ніжин: ТОВ „Видавництво „Аспект-Поліграф", 2006. 336 с

8. Рябенький В.М. Жуйков В.Я. Ямненко Ю.С. Заграничний А.В. „Схемотехніка: Пристрої цифрової електроніки – Київ, 2016. 399 с.

9. Слободянюк П.В. Радиомониторинг: вчера, сегодня, завтра / П.В. Слободянюк, В.Г. Благодарный. - Прилуки: ООО «Издательство «Аір-Поліграф», 2009. 296 с.

10. SDR и HackRF для начинающих : сайт URL: https://hackware.ru/?p=8249

11. Програмно обумовлена радіосистема: веб-сайт: сайт URL: https://ru.wikipedia.org/wiki/Программно_определяемая_радиосистема

12. Kenington P.B. RF and baseband techniques for Software Defined Radio / P.B. Kenington. – Artech House, 2005.337 с.

13. Немного про устройство современного радио на примере HackRF One : сайт URL: https://habr.com/ru/post/499376/

14. . Передача радиосигналов с помощью HackRF : сайт URL: https://habr.com/ru/post/372177/

15. Беркман Л.Н., Отрох С.І., Тарбаєв С.І., Чумак Н.С. Загальні поняття про сигнали та канали зв'язку. Навчальний посібник підготовлено для самостійної роботи студентів вищих навчальних закладів – Київ: ДУТ ННІТІ, 2017. – 132 с.

16. ADS-B Technologies : сайт URL: http://www.ads-b.com/ (дата звернення 20.04.2021).

17 Спуфинг (spoofing) – кибератака: сайт URL: https://www.tadviser.ru/index.php

18. Що таке спуфінг і як запобігти атаці? ПОРАДИ: сайт URL: https://cybercalm.org/novyny/shho-take-spufing-i-yak-zapobigty-atatsi-porady/