

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ
Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК
рішенням кафедри радіотехніки та радіоелектронних систем
від __ _____ 2024 року, протокол № ____.
Завідувач кафедри доктор фіз.-мат. наук, професор
_____ Ігор АНІСІМОВ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«Розробка та моделювання переносної станції радіоелектронної боротьби
проти дронів з широким діапазоном частот у середовищі LTspice.»

Виконав:

студент 4-го курсу
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОПП «Інформаційна безпека телекомунікаційних систем і мереж»
Олександр ІВАНЧУК _____

Науковий керівник:

доцент кафедри радіотехніки та радіоелектронних систем
к.т.н., с.н.с. Сергій ГАХОВИЧ _____

Рецензент:

Начальник відділу проблем інформаційно-психологічного
протиборства НДЦ ВІ КНУ ім.Т.Шевченка
к.т.н., с.н.с. Віталій ЛОЗА _____

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів без
відповідних посилань

Студент _____ Олександр ІВАНЧУК

Київ 2024

Реферат

Дипломна робота: 43 с., 4 рис., 6 джерел.

Розробка та моделювання переносної станції радіоелектронної боротьби проти дронів з широким діапазоном частот у середовищі LTspice.

Об'єкт дослідження – переносна станція радіоелектронної боротьби (РЕБ) для протидії дронам з широким діапазоном частот, змодельована у середовищі LTspice.

У сучасному світі швидкий розвиток технологій дронів створює нові виклики для безпеки та оборони. Одним із ефективних методів протидії дронам є використання радіоелектронної боротьби (РЕБ). Дана робота присвячена розробці переносної станції РЕБ, здатної працювати в широкому діапазоні частот, що дозволяє ефективно протидіяти різним типам дронів.

Основною метою дослідження є розробка та аналіз переносної станції РЕБ для захисту від дронів, яка здатна працювати в широкому діапазоні частот. Для досягнення цієї мети було визначено декілька ключових завдань. По-перше, проведено аналіз існуючих технологій РЕБ проти дронів. Це дозволило виявити переваги та недоліки сучасних рішень, а також зрозуміти, які саме технології є найбільш ефективними в різних умовах.

Наступним етапом дослідження став теоретичний аналіз радіочастотних технологій, які використовуються дронами. Було досліджено спектр частот, на яких працюють сучасні дрони, що дозволило визначити найбільш ефективні частоти для глушіння та придушення сигналів. Це знання стало основою для розробки технічних вимог до переносної станції РЕБ.

На основі зібраних даних було розроблено концепцію переносної станції РЕБ. Станція включає в себе блок-схему та визначає основні компоненти, необхідні для її функціонування. Для перевірки ефективності розробленої концепції було проведено моделювання та симуляцію роботи станції в різних умовах. Цей етап дозволив оцінити потенційну ефективність станції в реальних сценаріях застосування.

Одним із ключових етапів дослідження стала розробка прототипу переносної станції РЕБ. Прототип було тестовано в експериментальних умовах, що дозволило перевірити його функціональність та ефективність. Результати експериментів були проаналізовані та порівняні з теоретичними даними, що дозволило зробити висновки щодо ефективності розробленої станції.

Загалом, проведене дослідження показало, що розроблена переносна станція РЕБ є ефективним засобом протидії дронам завдяки широкому діапазону частот. Це дозволяє забезпечити надійний захист від дронів у різних умовах. Крім того, були розроблені методичні рекомендації щодо використання станції, а також визначені можливості для її впровадження у практику.

Окрему увагу було приділено оцінці можливого впливу роботи станції РЕБ на навколишнє середовище та розробці заходів для забезпечення безпеки під час її експлуатації. Результати дослідження свідчать про високу ефективність та перспективність розробленої технології, що може бути успішно впроваджена у сфері безпеки та оборони.

Таким чином, проведене дослідження зробило вагомий внесок у розвиток технологій радіоелектронної боротьби проти дронів, запропонувавши ефективне рішення для захисту від сучасних загроз.

ЗМІСТ

Перелік умовних позначень	4
Вступ	5
1. Огляд літератури	6
1.1. Сучасні технології радіоелектронної боротьби проти дронів.....	6
1.2. Аналіз частотних діапазонів, можливості використання.....	8
2. Теоретичні основи радіоелектронної боротьби	10
2.1. Основи радіоелектронного придушення	10
2.2. Вплив глушіння на системи керування дронами	12
2.3. Методи виявлення та ідентифікації дронів	14
3. Розробка концепції переносної станції РЕБ	16
3.1. Визначення технічних вимог	16
3.2. Блок-схема та компоненти системи	18
3.3. Вибір частотного діапазону та антен	20
4. Моделювання в LTspice	22
4.1. Вибір та обґрунтування програмного забезпечення LTspice	22
4.2. Моделювання приймально-передавальних модулів	24
4.3. Симуляція роботи системи у різних сценаріях	26
Висновки	46
Перелік джерел посилання	48

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

БПЛА – Безпілótний літальний апарат. Літальний апарат, що не має екіпажу на борту і управляється дистанційно або автономно.

FPV – First Person View. Технологія управління літальним апаратом з використанням камери, що передає зображення з борту в реальному часі на окуляри чи екран оператора.

GPS – Global Positioning System. Глобальна система позиціонування, що дозволяє визначати місцезнаходження об'єктів на Землі з високою точністю за допомогою супутників.

ІЧ – Інфрачервоний. Частина спектра електромагнітних хвиль, що використовується в різних технологіях для передачі інформації та виявлення об'єктів.

ППО – Протиповітряна оборона. Сукупність заходів і засобів для захисту від авіаційних і ракетних атак.

РЕБ – Радіоелектронна боротьба. Комплекс заходів і засобів для забезпечення ефективного використання радіоелектронних засобів в бойових умовах та захисту від їх застосування противником.

SAW-фільтр – Surface Acoustic Wave-фільтр. Фільтр на поверхневих акустичних хвилях, що використовується для обробки радіочастотних сигналів у телекомунікаційних та інших електронних системах.

ЗСУ – Збройні сили України. Військове формування, що складається з сухопутних військ, військово-морських сил і повітряних сил, призначене для захисту суверенітету і територіальної цілісності України.

ВСТУП

Розвиток технологій безпілотних літальних апаратів (БПЛА), відомих як дрони, став невід'ємною частиною сучасного світу, зокрема у військовій, комерційній та цивільній сферах. Дрони широко використовуються для виконання різноманітних завдань, таких як розвідка, доставка товарів, аерофотозйомка та моніторинг. Однак, поряд з численними перевагами, вони становлять і потенційні загрози, особливо у випадках несанкціонованого або ворожого використання. Це викликає необхідність розробки ефективних засобів захисту від дронів, здатних нейтралізувати їхню діяльність.

Одним з перспективних методів протидії є радіоелектронна боротьба (РЕБ), яка передбачає створення перешкод для роботи систем керування дронами. Використання РЕБ дозволяє впливати на канали зв'язку дронів, перешкоджаючи їхньому управлінню та навігації. Особливо важливою є можливість створення переносних станцій РЕБ, які можуть бути оперативно розгорнуті у місцях потенційної загрози та забезпечити мобільний захист.

Метою даної роботи є розробка та моделювання переносної станції радіоелектронної боротьби проти дронів, здатної ефективно працювати у широкому діапазоні частот. Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Провести аналіз сучасних методів радіоелектронної боротьби проти безпілотних літальних апаратів.
2. Визначити оптимальні частотні діапазони для ефективного пригнічення сигналів управління дронами.
3. Розробити структурну схему переносної станції РЕБ.
4. Створити модель пристрою у середовищі LTspice.

Актуальність теми дослідження обумовлена швидким розвитком технологій дронів та зростанням кількості інцидентів, пов'язаних з їхнім несанкціонованим використанням. В умовах, коли дрони можуть бути використані для збору інформації, порушення приватності або здійснення

атак, розробка ефективних засобів радіоелектронної боротьби набуває особливого значення.

У рамках роботи буде проведено огляд літератури щодо існуючих засобів радіоелектронної боротьби, визначено основні технічні вимоги до переносної станції РЕБ, розроблено структурну схему пристрою та виконано його моделювання у середовищі LTspice. Проведені симуляції дозволять оцінити ефективність запропонованого рішення та визначити напрямки для подальших досліджень і вдосконалень. [5,6]

1. Огляд літератури

Радіоелектронна боротьба (РЕБ) є критично важливим компонентом сучасних збройних конфліктів, забезпечуючи контроль над електромагнітним спектром. З моменту своєї появи під час Другої світової війни РЕБ постійно еволюціонує, адаптуючись до нових технологічних викликів і військових потреб.[6]

Сучасні дослідження зосереджуються на розвитку технологій РЕБ, включаючи засоби виявлення, пригнічення і нейтралізації радіосигналів. Вони охоплюють різні аспекти РЕБ, від історичних прикладів до сучасних технологій, підкреслюючи важливість інтеграції новітніх технічних рішень для підвищення ефективності військових операцій.

Аналіз літератури показує, що ефективне використання РЕБ у військових операціях вимагає комплексного підходу, який включає активні та пасивні методи створення перешкод. Досвід минулих конфліктів свідчить про важливість постійного вдосконалення засобів РЕБ для забезпечення переваги над противником.

У контексті захисту від безпілотних літальних апаратів (БпЛА) особливу увагу приділяють розробці переносних станцій РЕБ, здатних оперативно реагувати на загрози. Сучасні дослідження в цій галузі спрямовані на створення ефективних, мобільних і універсальних систем, які можуть працювати в широкому діапазоні частот і нейтралізувати дрони різних типів.

Таким чином, літературні джерела підкреслюють важливість розвитку та вдосконалення технологій РЕБ для забезпечення ефективної протидії дронам і забезпечення безпеки в сучасних умовах.[3]

1.1. Сучасні технології радіоелектронної боротьби проти дронів

Сучасні технології радіоелектронної боротьби (РЕБ) проти дронів стають все більш важливими у військових конфліктах, зокрема у протистоянні України та Росії. Поява FPV-дронів (First Person View) змусила переосмислити підходи до РЕБ, адже найбільш ефективним способом знищення ворожих дронів є переривання їх зв'язку з оператором. Ця технологія дозволяє глушити зв'язок на певних радіочастотах, змушуючи дрон втратити управління і падати.

Основною задачею РЕБ є виявлення та приглушення сигналів управління дронів, що використовують діапазон частот 720-1020 МГц. Ефективність РЕБ залежить від декількох факторів, включаючи технологічність ворожих дронів, дистанцію до оператора, якість компонентів системи РЕБ та здатність адаптуватися до змін у частотах.

Українські виробники активно працюють над розробкою різних типів РЕБ, які включають мобільні системи, портативні пристрої у вигляді рюкзаків, а також комплексні рішення для захисту великих територій та об'єктів. Наприклад, компанія Kvertus випускає широкий спектр РЕБ-рішень, які здатні працювати в нестандартних діапазонах частот і забезпечують захист на кілька сотень метрів.

Інноваційні підходи також включають використання дронів з машинним зором, які можуть самостійно захоплювати ціль та долітати до неї навіть після втрати зв'язку з оператором. Це дозволяє підвищити ефективність дронів у бойових умовах, де зв'язок може бути навмисно заглушений противником.[2]

Зростання ринку мобільних засобів РЕБ супроводжується активною участю держави, яка сприяє розробці та виробництву нових систем. Значна увага приділяється кодифікації та сертифікації техніки, що дозволяє забезпечити високу якість та надійність українських РЕБ. Однак, для повного задоволення потреб фронту необхідно масштабувати виробництво і налагодити масові постачання РЕБ комплексів.

Таким чином, сучасні технології радіоелектронної боротьби проти дронів є критично важливими для забезпечення переваги на полі бою. Українські розробники та виробники активно працюють над створенням інноваційних та ефективних рішень, здатних протистояти сучасним загрозам та забезпечити захист від ворожих дронів.

1.2. Аналіз частотних діапазонів, використовуваних дронами.

Розвиток дронів та їх широке використання у військових та цивільних цілях створює необхідність детального вивчення частотних діапазонів, на яких вони працюють. Частоти, що використовуються дронами, залежать від їхніх функціональних завдань та конструктивних особливостей.

Зазвичай дрони працюють у діапазоні 2.4 ГГц та 5.8 ГГц, що є стандартними частотами для більшості споживацьких безпілотних апаратів. Ці частоти широко використовуються для передачі відеосигналів та управління дронами на відстані до кількох кілометрів. Проте, військові дрони та FPV (First Person View) дрони, що використовуються в бойових умовах, можуть працювати на інших частотах для уникнення перешкод та підвищення надійності зв'язку.[1]

Українська розвідка виявила, що ворожі FPV-дрони зазвичай працюють в діапазоні 850-930 МГц. Проте, останнім часом спостерігається тенденція до використання більш широкого діапазону 720-1020 МГц, що зумовлює необхідність адаптації систем радіоелектронної боротьби (РЕБ) до нових умов .

Цей діапазон частот дозволяє забезпечити більш стабільний та дальній зв'язок, що є критично важливим для військових операцій. Розширення частотного діапазону використання дронів створює додаткові виклики для засобів РЕБ, оскільки їм необхідно виявляти та глушити сигнали на більшому спектрі частот.

Таким чином, для ефективної боротьби з дронами, необхідно використовувати системи РЕБ, здатні працювати в широкому діапазоні

частот, від 720 до 1020 МГц, що дозволить ефективно переривати зв'язок між дронами та їх операторами, забезпечуючи надійну оборону від потенційних загроз.[3]

Пеленгування частот та робота засобів РЕБ у вузькому діапазоні необхідні для уникнення завад власним безпілотникам, що працюють на сусідніх частотах. Крім того, менший діапазон роботи дозволяє збільшити потужність та радіус дії станції постановки перешкод.

Останнім часом на російських дронах почав з'являтися додатковий мікročип (SAW-фільтр), який блокує прийом радіочастот за межами визначеного вузького діапазону. Це допомагає захистити зв'язок від впливу систем РЕБ, які створюють перешкоди у широкому діапазоні радіочастот.

Для ефективного "придушення" таких дронів необхідно створювати перешкоди на точній частоті, що наразі не є поширеною практикою на полі бою. Таким чином, пеленгування та придушення дронів на вузьких частотах стають не лише опцією, а й життєвою необхідністю.

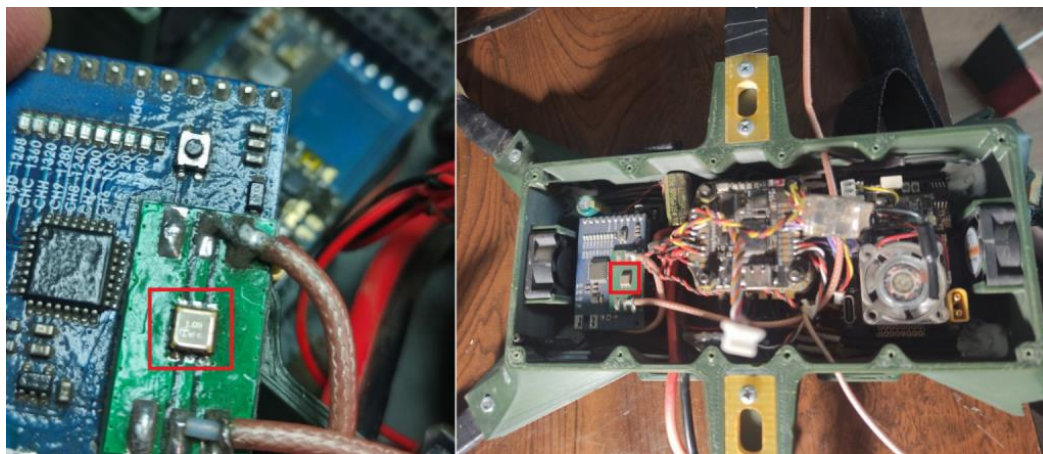


Рис. 1.1 SAW-фільтр[5]

Умови перехоплення керування над FPV-дроном включають використання потужних засобів пеленгування для точного визначення частоти управління дроном. Сучасні дрони часто використовують зашифровані канали зв'язку у вузькому діапазоні частот, що ускладнює перехоплення. Після виявлення частоти та параметрів сигналу, система РЕБ повинна генерувати точкові перешкоди або підмінні сигнали на цих частотах. Важливим є також аналіз і декодування командних сигналів, оскільки дрони

оснащені захисними мікросхемами, такими як SAW-фільтри. Системи РЕБ повинні швидко реагувати на зміну частот зв'язку і адаптуватися до зовнішніх умов, таких як рельєф місцевості і погодні умови. Таким чином, ефективне перехоплення керування дроном вимагає комплексного підходу, що включає високоточне пеленгування, аналіз сигналів і швидку адаптацію до змін.

Пеленгація точних частот роботи FPV-дронів відкриває можливості для перехоплення їхнього сигналу, оскільки всі вони використовують нешифрований аналоговий зв'язок. Це означає, що будь-яка людина з пультом керування, яка знаходиться поблизу дрона та знає необхідну частоту, може отримати зображення з його камери і навіть перехопити управління. Цю тактику вже використовують досвідчені підрозділи як українських Сил оборони, так і окупантів. Для перехоплення сигналу вздовж лінії фронту розміщуються пости радіоелектронної розвідки та оператори з пультами керування.

Виявивши дрон, інформація передається на пост з пультом, після чого оператор підключається до нього. Отримане відеозображення з дрона намагаються геолокувати, щоб визначити напрямок руху і попередити потенційний об'єкт ураження, а також виявити місце розташування ворожого оператора, який керує дроном. За певних умов можливе перехоплення управління дроном. У разі успіху дрон зазвичай одразу спрямовується на землю для нейтралізації загрози.

2. Теоретичні основи радіоелектронної боротьби

РЕБ, або радіоелектронна боротьба, – це будь-який засіб, що створює перешкоди для зв'язку між оператором та зброєю з радіоелектронним обладнанням, включаючи БПЛА, системи ППО чи артилерію. Такі пристрої також можуть пригнічувати мобільний та супутниковий зв'язок, дезорієнтуючи ворога. Це дуже широке поняття, яке можна сегментувати за дальністю впливу.

За дальністю впливу виділяють:

- оперативно-тактичні РЕБ (до 500 км);
- тактичні РЕБ (до 50 км);
- "окопні" або ближньої дії РЕБ (до 10 км).

Вони різняться розмірами: РЕБ ближньої дії можуть поміститися в кишеню, тоді як стратегічні РЕБ доводиться транспортувати на вантажівках.



Рис. 2.1 Види РЕБ[6]

РЕБ створює дуже щільну перешкоду, яка забиває ефір, унеможливаючи передачу сигналів між дроном та оператором, а також між дроном і супутником. У результаті дрон стає некерованим. Основна задача РЕБ – не допустити виконання БПЛА своїх завдань. Якщо дрон, що несе вибухівку, потрапляє під вплив РЕБ, він може розвернутися і полетіти в іншому напрямку, тим самим завдання буде виконано.

2.1. Основи радіоелектронного придушення

Основи радіоелектронного придушення включають комплекс заходів і технологій, спрямованих на створення перешкод або унеможливлення нормального функціонування електронних систем противника. Ці заходи можуть використовуватися як у військовій сфері для зниження ефективності систем управління, зв'язку та розвідки ворога, так і в цивільних галузях для захисту інформаційних систем від небажаних впливів.

Радіоелектронне придушення базується на принципі впливу на радіосигнали з метою створення перешкод. Одним із головних методів є генерація заважаючих сигналів, які мають більшу потужність або аналогічну частоту з цільовими сигналами. Це може призвести до зниження якості або повної втрати прийому корисного сигналу. Заважаючі сигнали можуть бути неперервними або імпульсними, що ускладнює роботу ворожих приймачів і систем.

Важливою складовою радіоелектронного придушення є розвідка електромагнітного спектра противника. Для цього використовуються спеціалізовані системи радіорозвідки, які виявляють, ідентифікують і класифікують джерела випромінювання. На основі зібраної інформації розробляються стратегії придушення, що дозволяють ефективно впливати на найважливіші частоти та типи сигналів противника.

Одним із найбільш поширених методів радіоелектронного придушення є створення радіоперешкод. Це може бути досягнуто через встановлення спеціальних генераторів перешкод, які випромінюють сигнали на тій же частоті, що й цільова система. Іншим методом є застосування методів обману, коли ворожі системи вводяться в оману через подання хибних сигналів або інформації, що може призвести до неправильного функціонування або рішення ворога.

Радіоелектронне придушення також може включати методи поглинання або відображення сигналів, що використовуються для зниження ефективності радіолокаційних систем противника. Це може бути досягнуто за допомогою спеціальних матеріалів або структур, які поглинають електромагнітне випромінювання або змінюють його напрямок.

Важливим аспектом є захист власних систем від радіоелектронного придушення. Це включає використання стійких до перешкод методів зв'язку, таких як частотна і часова рознесення, криптографія, а також розробка адаптивних систем, що можуть автоматично змінювати параметри роботи в умовах завад.

Загалом, основи радіоелектронного придушення включають поєднання технологій та стратегій, спрямованих на виявлення, аналіз і вплив на електронні системи противника, забезпечуючи при цьому захист власних систем від подібних дій.

2.2. Вплив глушіння на системи керування дронами

Глушіння сигналів значно впливає на системи керування дронами, створюючи численні виклики та потенційно серйозні наслідки для їхньої операційної здатності. Основною метою глушіння є створення перешкод у передачі команд управління між оператором і дроном, що може призвести до втрати контролю над апаратом.

Коли дрон потрапляє під дію перешкоджуючих сигналів, його здатність отримувати і виконувати команди оператора може бути суттєво обмежена або взагалі припинена. Це може проявлятися у вигляді затримок, втрати сигналу, або неправильної інтерпретації команд. Наприклад, у випадку з дистанційним керуванням, дрон може не реагувати на команди повороту, висоти або швидкості, що призведе до його неконтрольованого польоту.

Глушіння може також впливати на сигнали навігаційних систем, таких як GPS. Більшість сучасних дронів використовують GPS для точного позиціонування та виконання завдань, таких як політ по заздалегідь визначених маршрутах або повернення до точки зльоту. Глушіння GPS сигналів може призвести до дезорієнтації дрона, що ускладнює або навіть робить неможливим його повернення до оператора або виконання поставлених завдань.

Додатково, глушіння може впливати на передачу відео та інших даних з дрона на наземну станцію. Це ускладнює або робить неможливим моніторинг поточної ситуації та прийняття відповідних рішень оператором. У критичних ситуаціях це може призвести до невчасного реагування на зміну обстановки або до втрати важливих даних.

У військовому контексті глушіння сигналів дронів може бути використане для запобігання збору розвідувальної інформації, зриву виконання бойових завдань або навіть для захоплення контролю над дроном ворогом. У цивільних застосуваннях, таких як комерційна доставка або рятувальні операції, це може призвести до затримок, втрати вантажу або небезпеки для людей.

Таким чином, глушіння є потужним інструментом, який може суттєво обмежити ефективність та безпеку дронів, роблячи важливим розвиток методів захисту від подібних загроз, таких як використання альтернативних методів навігації, стійких до перешкод систем зв'язку та автономних алгоритмів управління.

2.3 Методи виявлення та ідентифікації дронів

Виявлення та ідентифікація дронів є ключовими аспектами сучасної радіоелектронної боротьби, оскільки ці безпілотні літальні апарати (БпЛА) можуть виконувати широкий спектр завдань, включаючи розвідку, спостереження та ударні місії. Ефективне виявлення та ідентифікація дронів вимагають комплексного підходу, що включає використання різних технологій та методів.

Радіолокаційні системи

Радіолокаційні системи є одним із найпоширеніших методів виявлення дронів. Вони працюють шляхом випромінювання радіохвиль та виявлення відбитих сигналів від об'єктів у повітрі. Радіолокаційні системи можуть забезпечувати високу точність виявлення та відстеження дронів на великих відстанях. Однак, вони можуть бути вразливі до засобів радіоелектронної протидії, таких як створення радіоелектронних перешкод або застосування стелс-технологій дронами.

Інфрачервоні (ІЧ) датчики

ІЧ-датчики використовують теплове випромінювання для виявлення дронів. Вони можуть бути ефективними у нічний час або в умовах обмеженої видимості, коли інші методи виявлення можуть бути менш ефективними. ІЧ-датчики здатні виявляти теплові підписи двигунів та електроніки дронів. Однак, їх ефективність може знижуватися в умовах високої температури навколишнього середовища або за наявності інших джерел тепла, що може ускладнювати виявлення дронів.

Акустичні системи

Акустичні системи використовують звукові хвилі для виявлення дронів. Дрони створюють характерні звукові підписи, які можуть бути виявлені та проаналізовані акустичними датчиками. Цей метод може бути особливо корисним у міських умовах, де інші методи можуть бути менш ефективними через наявність численних перешкод. Однак, акустичні системи мають обмежену дальність дії та можуть бути вразливими до фонового шуму, що ускладнює виявлення дронів у шумних середовищах.

Візуальні системи

Візуальні системи, такі як камери та оптичні сенсори, використовуються для виявлення та ідентифікації дронів за допомогою комп'ютерного зору та алгоритмів обробки зображень. Ці системи можуть забезпечувати високу точність ідентифікації, але вони залежать від умов освітлення та видимості. Використання камер високої роздільної здатності та спеціалізованого програмного забезпечення може допомогти подолати деякі з цих обмежень. Візуальні системи можуть також використовуватися для ідентифікації типу дрона, його моделі та інших характеристик, що можуть бути корисними для подальшої обробки.

Комбіновані системи

Комбіновані системи, що використовують декілька методів одночасно, можуть забезпечувати більш надійне та точне виявлення дронів. Наприклад, радіолокаційні системи можуть бути доповнені ІЧ-датчиками та акустичними системами для підвищення загальної ефективності. Такі комплексні підходи дозволяють використовувати переваги кожного окремого методу та знижувати вразливість до протидії. Комбіновані системи можуть забезпечувати покращену ситуаційну обізнаність та знижувати ймовірність пропуску ворожих дронів.

Спеціалізоване програмне забезпечення

Сучасні системи виявлення та ідентифікації дронів також використовують спеціалізоване програмне забезпечення, яке аналізує дані, отримані від різних сенсорів. Це програмне забезпечення може використовувати алгоритми машинного навчання та штучного інтелекту для розпізнавання дронів та їх відокремлення від інших об'єктів. Такий підхід дозволяє підвищити точність та швидкість виявлення дронів.

Переваги та недоліки різних методів

Кожен з методів виявлення та ідентифікації дронів має свої переваги та недоліки. Радіолокаційні системи забезпечують високу дальність виявлення, але можуть бути вразливими до радіоелектронної протидії. ІЧ-датчики ефективні в умовах обмеженої видимості, але залежать від температурних умов. Акустичні системи корисні у міських умовах, але мають обмежену дальність. Візуальні системи забезпечують високу точність, але залежать від освітлення. Комбіновані системи дозволяють компенсувати недоліки кожного з методів, забезпечуючи більш надійне виявлення дронів.

Таким чином, виявлення та ідентифікація дронів є складним завданням, яке вимагає використання різних технологій та підходів. Сучасні системи радіоелектронної боротьби постійно вдосконалюються, щоб відповідати

новим загрозам та забезпечувати надійний захист від безпілотних літальних апаратів. Комбінація різних методів виявлення та використання передового програмного забезпечення дозволяє створювати ефективні системи протидії дронам, які можуть працювати в різних умовах та забезпечувати високу точність і надійність виявлення.

Українські розробники створили доступний детектор дронів для ЗСУ, який виявляє всі БПЛА противника.



Рис. 2.2 «Цукорок»[3]

«Цукорок» здатний виявляти різні дрони, які застосовують збройні сили держави-агресора, включаючи FPV-камікадзе, Zala, «Ланцет», «Орлан», за їхніми радіосигналами. Пристрій дуже компактний, його зручно носити в кишені або на ремінці. «Цукорок» працює від акумулятора (до півтори доби в режимі очікування), попереджаючи про наближення БПЛА звуковим сигналом, і показує тип і потужність сигналу. Вінницькі інженери вдосконалили «Цукорок»: забезпечили корпус кращим захистом від вологи, додали роз'єм Type-C для заряджання, а також можливість виявляти FPV-дрони та квадрокоптери серії Mavic. Тепер до нього можна підключати компактні антени, що працюють у частотних діапазонах 915 МГц і 2,4 ГГц.

Система виявлення дронів, як «Цукорок», має низку переваг та недоліків. Серед переваг можна відзначити її компактність і портативність, що дозволяє легко переносити пристрій в кишені або на ремінці. Це забезпечує мобільність і зручність для військових в умовах бойових дій. Пристрій працює від акумулятора до півтори доби в режимі очікування, що

робить його автономним і зручним у використанні. Вдосконалений захист від вологи дозволяє використовувати «Цукорок» в різних погодних умовах, а роз'єм Type-C для заряджання підвищує зручність і швидкість підзарядки. Можливість виявлення різних типів дронів, включаючи FPV-дрони та квадрокоптери Mavic, робить систему універсальною. Компактні антени, що працюють у частотних діапазонах 915 МГц і 2,4 ГГц, забезпечують точне визначення радіосигналів. Враховуючи Низьку ціну та вище вказані характеристики цю систему можна використовувати для виявлення, а потім визначивши частоту використати систему РЕБ.

Недоліки системи можуть включати обмежену дальність виявлення, яка може не бути достатньою для раннього попередження про наближення дронів у деяких бойових ситуаціях. Оскільки пристрій залежить від акумулятора, час його роботи обмежений, і в умовах інтенсивного використання може знадобитися часта підзарядка. Попри вдосконалений захист від вологи, пристрій все ж може бути вразливим до екстремальних погодних умов. Можливість інтерференції або навмисного глушіння сигналів з боку противника також залишається проблемою, яка може знизити ефективність системи.

3. Розробка концепції переносної станції РЕБ

Розробка концепції переносної станції радіоелектронної боротьби (РЕБ) спрямована на створення ефективного і мобільного засобу протидії безпілотним літальним апаратам (БПЛА) противника. Основна мета полягає у забезпеченні надійного придушення сигналів керування та навігації дронів, перешкоджаючи їхньому використанню в бойових умовах.

Концепція переносної станції РЕБ включає розробку компактного і легкого пристрою, який можна легко переносити на полі бою. Це забезпечить високу мобільність військових підрозділів і можливість швидкого розгортання системи в різних умовах. Важливим аспектом є енергозабезпечення, яке дозволить станції працювати автономно протягом

тривалого часу, використовуючи потужні акумулятори або інші джерела живлення. Інженерна частина концепції передбачає використання сучасних технологій радіоелектронного придушення, які дозволяють ефективно блокувати широкий спектр частот, на яких працюють БПЛА противника. Важливою складовою є система пеленгації, яка допоможе точно визначати місцезнаходження дронів і направляти перешкоди безпосередньо на них. Це знизить ризик впливу на власні засоби зв'язку та інші електронні системи.

Переносна станція РЕБ повинна бути оснащена інтуїтивно зрозумілим інтерфейсом для оперативного управління та налаштування. Це дозволить операторам швидко реагувати на загрози і змінювати параметри роботи станції в залежності від ситуації на полі бою. Крім того, передбачається можливість інтеграції з іншими системами спостереження і управління, що забезпечить комплексний підхід до захисту від дронів.

Розробка концепції включає також проведення випробувань і моделювання різних сценаріїв застосування станції РЕБ в реальних умовах. Це допоможе виявити і усунути можливі недоліки, підвищити ефективність системи та адаптувати її до конкретних потреб військових підрозділів. Основний акцент робиться на створенні надійного і простого у використанні засобу, який стане важливим елементом сучасної оборонної стратегії протидії дронам противника.

3.1. Визначення технічних вимог

Розробка переносної станції радіоелектронної боротьби (РЕБ) проти дронів з широким діапазоном частот вимагає визначення технічних вимог для забезпечення її ефективності та надійності в бойових умовах. Станція повинна працювати в широкому діапазоні частот від 0.9 ГГц до 5.8 ГГц, покриваючи більшість використовуваних частот дронів. Потужність генератора шуму повинна бути достатньою для ефективного придушення сигналу дронів на відстані до 10 км, з мінімальною потужністю перешкоджаючого сигналу в межах 30-100 Вт. Радіус ефективної дії станції

повинен складати до 10 км залежно від умов місцевості та погодних умов. Система має працювати автономно до 8 годин на одному заряді батареї, а час зарядки акумулятора не повинен перевищувати 3 години.

Пристрій повинен бути портативним, зручним для перенесення в сумці або на ремінці, з максимальною вагою до 5 кг. Інтерфейс користувача має бути інтуїтивно зрозумілим з графічним дисплеєм TFT 1.8" і роздільною здатністю 128x160, дозволяючи регулювання яскравості дисплея, налаштування параметрів роботи та відображення поточного стану. Пристрій має мати звукову, вібраційну та світлодіодну сигналізацію для інформування оператора про виявлення дронів та статус роботи. Корпус пристрою повинен бути захищеним від вологи та пилу з рівнем захисту не нижче IP54 і зберігати працездатність при температурах від -20°C до $+50^{\circ}\text{C}$.

Комплект повинен включати всенаправлені антени, що працюють у діапазонах 0.9 ГГц, 2.4 ГГц, та 5.8 ГГц, забезпечуючи стабільний прийом сигналів на всіх частотах. Пристрій повинен бути стійким до зовнішніх впливів, зокрема електромагнітних завад, і мати вбудовані засоби самодіагностики та повідомлення про несправності. Система має мати можливість інтеграції з іншими системами РЕБ та засобами боротьби з дронами, такими як антидронові рушніці. Живлення має здійснюватися як від внутрішнього акумулятора, так і від зовнішніх джерел живлення, таких як павербанки. Дотримання цих технічних вимог забезпечить створення ефективної та надійної переносної станції РЕБ, здатної протистояти загрозам з боку безпілотних літальних апаратів у сучасних умовах бойових дій.

3.2. Блок-схема та компоненти системи

Для створення ефективної переносної станції радіоелектронної боротьби (РЕБ) проти дронів з широким діапазоном частот необхідно спроектувати блок-схему системи та визначити ключові компоненти, що забезпечать її функціональність. Нижче представлено загальний опис блок-схеми та компонентів системи:

Блок-схема системи РЕБ

1. Живлення:

- Блок живлення
- Внутрішній акумулятор
- Зарядний модуль
- Вхід для зовнішнього живлення (павербанк)

2. Антени:

- Всенаправлені антени (0.9 ГГц, 2.4 ГГц, 5.8 ГГц)
- Перемикач антен

3. RF Модуль:

- Генератор шуму
- Підсилювач потужності
- Фільтри для зменшення побічних сигналів

4. Контролер:

- Мікроконтролер
- Інтерфейс керування (кнопки навігації)
- Дисплей TFT 1.8" 128x160
- Інтерфейс зв'язку з іншими пристроями (USB, Bluetooth)

5. Сигналізація:

- Звуковий сигналізатор
- Вібраційний сигналізатор
- Світлодіодний індикатор

6. Захисні модулі:

- Захист від вологи та пилу (IP54)
- Захист від перенапруги та короткого замикання
- Електромагнітний захист

7. Інтерфейси підключення:

- Роз'єм Type-C для заряджання
- Антени роз'єми
- Порти для підключення зовнішніх модулів

Компоненти системи

1. Блок живлення:

- Літій-іонний акумулятор ємністю 4000 мА·год
- Зарядний модуль з підтримкою швидкої зарядки (до 3 годин)

2. Антени:

- Всенаправлені антени для діапазонів 0.9 ГГц, 2.4 ГГц та 5.8 ГГц

3. RF Модуль:

- Перемикач частотних діапазонів
- Генератор шуму з регульованою потужністю (30-100 Вт)

- Підсилювач потужності RF
 - Вхідні та вихідні фільтри для зменшення побічних сигналів
4. Контролер:
- Мікроконтролер (наприклад, STM32 або ESP32)
 - Графічний дисплей TFT 1.8” з роздільною здатністю 128x160
 - Кнопки навігації для управління системою
5. Сигналізація:
- П'єзодинамік для звукових сигналів
 - Вібромотор для вібраційних сигналів
 - Світлодіодні індикатори (червоний, зелений, синій)
6. Захисні модулі:
- Водонепроникний корпус з рівнем захисту IP54
 - Захист від перенапруги
 - Електромагнітний захист
7. Інтерфейси підключення:
- USB Type-C роз'єм для зарядки та передачі даних
 - SMA або N-роз'єми для підключення антен

Система РЕБ починає свою роботу з увімкнення живлення від внутрішнього акумулятора або зовнішнього джерела живлення. Антени підключаються до відповідних роз'ємів, що забезпечують прийом сигналів у діапазонах 0.9 ГГц, 2.4 ГГц та 5.8 ГГц. Мікроконтролер керує генератором шуму та перемикачем частотних діапазонів для налаштування параметрів генерації перешкод. Генератор шуму створює перешкоджаючі сигнали, які передаються через підсилювач потужності до антен, що забезпечує ефективне блокування сигналів дронів.

Мікроконтролер також відповідає за обробку даних з антени та виведення інформації на дисплей. Сигналізація інформує оператора про виявлення дронів за допомогою звукових, вібраційних та світлодіодних сигналів. Захисні модулі забезпечують стабільну роботу системи в умовах впливу навколишнього середовища.

Таким чином, система забезпечує ефективне виявлення та придушення сигналів дронів, що робить її важливим інструментом у сучасних умовах бойових дій.

3.3. Вибір частотного діапазону та антен

Вибір частотного діапазону та антен для системи радіоелектронної боротьби (РЕБ) проти дронів є ключовим елементом, що визначає її ефективність. Основні частотні діапазони, які використовуються дронами, включають 0.9 ГГц, 2.4 ГГц та 5.8 ГГц. Ці діапазони є стандартними для багатьох комерційних та військових дронів через їхні переваги в передачі даних, стійкості до перешкод та ефективності роботи на різних відстанях.

Для кожного з цих частотних діапазонів необхідно вибрати відповідні антени, які забезпечать максимальну ефективність роботи системи. Всенаправлені антени є оптимальним вибором, оскільки вони здатні приймати та передавати сигнали в усіх напрямках, що важливо для виявлення дронів, які можуть наблизитися з будь-якого напрямку. Всенаправлені антени також забезпечують рівномірне покриття, що зменшує ймовірність пропуску сигналу від дрона.

Діапазон 0.9 ГГц використовується для зв'язку на великі відстані через його здатність проникати крізь перешкоди, такі як будівлі та дерева. Антени для цього діапазону повинні бути розроблені з урахуванням великої довжини хвилі, що забезпечує стабільний прийом сигналу навіть в умовах складного рельєфу місцевості.

Діапазон 2.4 ГГц є найбільш популярним для дронів завдяки його збалансованості між дальністю та пропускну здатністю. Антени для цього діапазону повинні забезпечувати високий рівень чутливості та здатність працювати в умовах високої щільності сигналів, оскільки цей діапазон використовується також для Wi-Fi та інших бездротових пристроїв.

Діапазон 5.8 ГГц забезпечує високу пропускну здатність, що важливо для передачі відео в реальному часі. Антени для цього діапазону повинні мати високу точність та здатність працювати в умовах прямої видимості, оскільки сигнали на цій частоті погано проходять через перешкоди.

Комбінуючи всенаправлені антени для кожного з цих діапазонів, система РЕБ може ефективно виявляти та подавляти сигнали дронів у

широкому спектрі частот. Вибір антен також включає розрахунок оптимальних характеристик, таких як коефіцієнт підсилення, діаграма спрямованості та захист від перешкод, що забезпечує стабільну роботу системи у різних умовах експлуатації.

4. Моделювання в LTspice

Моделювання в LTspice є важливим етапом розробки переносної станції радіоелектронної боротьби (РЕБ) проти дронів. Це програмне забезпечення дозволяє створювати та аналізувати електронні схеми, що дає можливість перевіряти їхню функціональність і оптимізувати параметри перед фізичною реалізацією. Спочатку необхідно розробити схему, що включає генератори шуму, підсилювачі, фільтри та антени. Генератори шуму моделюють сигнал перешкод, який буде подаватися на ворожі дрони для порушення їх зв'язку з оператором. У LTspice можна задати необхідні параметри генератора шуму, такі як потужність, частота та форма сигналу.

Наступним етапом є моделювання підсилювачів, які забезпечують достатній рівень потужності для передавання перешкод. У LTspice можна налаштувати підсилювачі з урахуванням їхньої смуги пропускання, коефіцієнта підсилення та стабільності роботи. Це дозволяє визначити оптимальні параметри підсилювачів, щоб забезпечити максимальну ефективність системи РЕБ.

Фільтри використовуються для вибору потрібних частотних діапазонів, на яких працюють дрони. У LTspice можна змоделювати різні типи фільтрів, такі як низькочастотні, високочастотні та смугові, щоб досягти необхідної селективності. Це дозволяє точно налаштувати систему для придушення сигналів ворожих дронів без впливу на інші частоти.

Антени є важливою частиною системи, оскільки вони відповідають за випромінювання перешкод у простір. У LTspice можна змоделювати параметри антен, такі як коефіцієнт підсилення, напрямленість і імпеданс,

щоб забезпечити максимальну ефективність випромінювання. Це дозволяє оптимізувати антени для роботи в різних частотних діапазонах і умовах.

Після створення та налаштування схеми в LTspice проводиться симуляція для аналізу роботи системи. Це включає перевірку стабільності роботи підсилювачів, ефективності фільтрів та випромінювання антен. За допомогою LTspice можна виявити потенційні проблеми та внести необхідні корективи в схему до її фізичної реалізації. Моделювання дозволяє зменшити витрати на розробку та тестування, оскільки багато проблем можна вирішити на етапі симуляції.

Таким чином, використання LTspice для моделювання переносної станції РЕБ проти дронів є критичним етапом у розробці ефективної системи. Це програмне забезпечення надає широкі можливості для аналізу та оптимізації електронних схем, що дозволяє створити надійний та ефективний засіб для боротьби з ворожими дронами.

4.1. Вибір та обґрунтування програмного забезпечення LTspice

LTspice було вибрано для розробки переносної станції радіоелектронної боротьби (РЕБ) проти дронів через його широкі можливості і переваги. Це програмне забезпечення є потужним інструментом для моделювання електронних схем, яке забезпечує точне і надійне моделювання аналогових і змішаних сигналів. Однією з головних причин вибору LTspice є його безкоштовна доступність, що робить його економічно вигідним для будь-яких проектів, включаючи академічні та комерційні розробки. LTspice підтримує широкий набір моделей компонентів, включаючи транзистори, діоди, опори, конденсатори, індуктивності та інші елементи, які є необхідними для створення складних електронних схем.[4,3]

Програмне забезпечення LTspice надає зручний і інтуїтивно зрозумілий інтерфейс, який дозволяє легко створювати, модифікувати і аналізувати схеми. Це значно зменшує час на навчання і підготовку користувачів. Крім того, LTspice має високу швидкість обробки і може виконувати симуляції

складних схем за короткий час, що є важливим для швидкого прототипування і тестування. Можливість проведення різних типів аналізів, таких як транзисторний, частотний, тимчасовий та інші, дозволяє детально досліджувати роботу схеми і оптимізувати її параметри.

LTspice також підтримує імпорт і експорт моделей компонентів, що дозволяє використовувати моделі від виробників і інтегрувати їх у проект. Це забезпечує високу точність моделювання і відповідність реальним компонентам, які будуть використовуватись у фізичній схемі. Програмне забезпечення має хорошу документацію і велику спільноту користувачів, що дозволяє швидко знаходити відповіді на питання і вирішувати технічні проблеми.

Крім того, LTspice надає можливості для автоматизації задач за допомогою скриптів, що дозволяє виконувати повторювані симуляції і аналізи з мінімальними зусиллями. Це особливо корисно для оптимізації і дослідження великої кількості варіантів схем. Підтримка інтеграції з іншими інструментами, такими як САД-системи і програмне забезпечення для розробки друкованих плат, забезпечує комплексний підхід до розробки електронних систем.

Таким чином, LTspice було обрано для моделювання переносної станції РЕБ через його потужні можливості, зручність використання, високу точність і швидкість симуляцій, а також економічну доступність і підтримку широкого спектра компонентів і аналізів. Це робить LTspice ідеальним інструментом для розробки і оптимізації складних електронних систем, таких як РЕБ для протидії дронам.

4.2. Моделювання та розрахунок характеристик

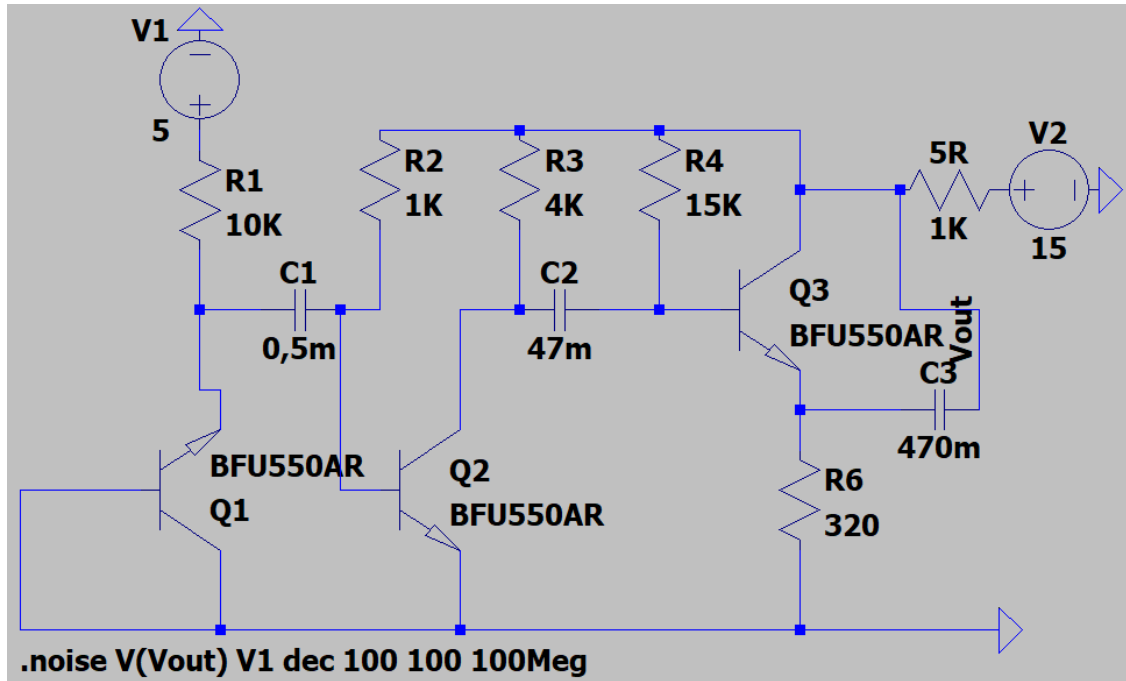


Рис. 4.1. Схема генератора шуму

Процес моделювання схеми переносної станції радіоелектронної боротьби (РЕБ) проти дронів у LTspice починається з визначення вимог до системи та її основних функцій. Виходячи з цього, створюється початкова електронна схема, яка включає генератор перешкод, фільтри, підсилювачі та антени. Для генератора перешкод необхідно підібрати такі параметри, як частота генерації та вихідна потужність. У бібліотеці LTspice обираються відповідні компоненти, або імпортуються моделі від виробників, які відповідають цим вимогам.

На початковому етапі проводиться частотний аналіз (AC analysis), який дозволяє оцінити, як генератор створює перешкоди в необхідному діапазоні частот. Вибір характеристик генератора базується на необхідності перекриття частот, які використовуються дронами. Для цього в моделі визначають параметри генератора, такі як середня частота та ширина спектра. В процесі моделювання аналізується амплітудно-частотна характеристика для забезпечення відповідності вимогам.

Далі йде моделювання фільтрів, які забезпечують селективність по частотах. Для цього у LTspice створюються схеми фільтрів з необхідними

параметрами, наприклад, смугові або загороджувальні фільтри. Під час вибору компонентів, таких як резистори, конденсатори та індуктивності, враховуються їхні значення, які забезпечують потрібні частотні характеристики. Проводиться частотний аналіз для підтвердження, що фільтри ефективно ізолюють або пропускають сигнали на заданих частотах.

Щоб забезпечити оптимальну роботу схеми на частотах в діапазоні від 900 МГц до 2,4 ГГц, необхідно правильно підібрати значення компонентів, які будуть підходити для роботи на таких високих частотах. Давайте розглянемо можливі зміни в елементах схеми для цього частотного діапазону:

Транзистори:

Для роботи на частотах до 2,4 ГГц слід використовувати високочастотні транзистори, наприклад, моделі, спеціально розроблені для радіочастотних (РЧ) застосувань. Можна використовувати RF транзистори з fT (гібридною частотою зрізу) значно вище за максимальну робочу частоту.

Пропозиція для заміни транзисторів:

- Модель транзисторів: BFU550AR або аналогічні, які мають $f_T > 5$ ГГц.

T_{amb} = 25 °C unless otherwise specified

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V _{(BR)CBO}	collector-base breakdown voltage	I _C = 100 nA; I _E = 0 mA	24	-	-	V
V _{(BR)CEO}	collector-emitter breakdown voltage	I _C = 150 nA; I _B = 0 mA	12	-	-	V
I _C	collector current		-	15	50	mA
I _{CBO}	collector-base cut-off current	I _E = 0 mA; V _{CB} = 8 V	-	<1	-	nA
h _{FE}	DC current gain	I _C = 15 mA; V _{CE} = 8 V	60	95	200	
C _e	emitter capacitance	V _{EB} = 0.5 V; f = 1 MHz	-	0.98	-	pF
C _{re}	feedback capacitance	V _{CE} = 8 V; f = 1 MHz	-	0.48	-	pF
C _c	collector capacitance	V _{CB} = 8 V; f = 1 MHz	-	0.74	-	pF
f _T	transition frequency	I _C = 25 mA; V _{CE} = 8 V; f = 900 MHz	-	11	-	GHz

Рис. 4.2. Таблиця datasheet транзистор.

Конденсатори:

Конденсатори повинні мати низький еквівалентний серійний опір (ESR) та бути розраховані на роботу на високих частотах.

Пропозиція для конденсаторів:

- C1: 0,5 пФ - 1 пФ

- C2 та C3: 10 пФ - 47 пФ (залежить від необхідної фільтрації та стабілізації)

Резистори

Резистори повинні мати мінімальні паразитні індуктивності, щоб не впливати на роботу на високих частотах. Металоплівкові резистори підходять для цього найкраще.

Пропозиція для резисторів:

- R1 та R2: 50 Ом (щоб краще відповідати імпедансу системи та мінімізувати відбиття)

- R3: 4 кОм

- R4: 15 кОм

- R5: 10 кОм

- R6: 320 Ом (можна залишити без змін, залежно від конкретних умов)

Джерела напруги

Залишаються без змін, якщо напруга живлення достатня для роботи вибраних транзисторів.

Зміни схеми

1. Заміна моделі транзисторів на високочастотні.

2. Зменшення ємність конденсаторів для врахування високих частот.

3. Перевірити розміщення компонентів для мінімізації паразитних елементів та забезпечення стабільної роботи на високих частотах.

Приклад оновленої схеми

plaintext

Q1 0 0 N002 0 BFR93A

Q2 N004 N003 0 0 BFR93A

Q3 Vout N005 N006 0 BFR93A

```

C1 N003 N002 1p
C2 N005 N004 10p
C3 Vout N006 10p
R1 N001 N002 50
R2 Vout N003 50
R3 Vout N004 4k
R4 Vout N005 15k
R5 P001 Vout 10k
R6 N006 0 320
V1 N001 0 90
V2 P001 0 30

.model BFR93A NPN

.lib C:\Users\User\Documents\LTspiceXVII\lib\cmp\standard.bjt

.noise V(Vout) V1 dec 100 900M 2.4G

.backanno

.end

```

Важливо провести симуляції в LTspice для перевірки роботи схеми на цих частотах та внести корективи при необхідності, враховуючи вплив паразитних індуктивностей та ємностей.

Щоб розрахувати параметри генератора шуму для вашої схеми в діапазоні 900 МГц - 2,4 ГГц, потрібно врахувати кілька ключових аспектів, таких як вихідна потужність шуму, спектральна густина потужності та ефективний опір джерела шуму.

Основні кроки для розрахунку параметрів генератора шуму

Спектральна густина потужності шуму:

Спектральна густина потужності (PSD) білого шуму для джерела шуму опору R при температурі T визначається формулою:

$$S = \frac{4kTR}{\Delta f} \quad (4.1)$$

$k = 1,380\ 649 \cdot 10^{-23}$ Дж/К.

T — абсолютна температура в Кельвінах (наприклад, 300К для кімнатної температури)

R — ефективний опір джерела шуму

Δf — ширина смуги частот, для якої розраховується потужність

Потужність шуму:

Потужність шуму P в смузі частот Δf дорівнює

$$P = S \cdot \Delta f = 4kTR \quad (4.2)$$

1. Ефективний опір джерела шуму:

Для простоти припустимо, що ефективний опір R дорівнює 50 Ом, що є типовим для РЧ систем.

Розрахунок для вашої схеми

Вихідні дані:

- Температура $T = 300\text{К} = 300\text{К} = 300\text{К}$
- Опір $R = 50\text{Ом} = 50\text{Ом} = 50\text{Ом}$
- Діапазон частот 900 МГц–2,4 ГГц
- Ширина смуги частот $\Delta f = 2,4\text{ГГц} - 900\text{МГц} = 1,5\text{ГГц}$

Розрахунок спектральної густини потужності:

$$S = \frac{4 \times 1.38 \times 10^{-23} \times 300 \times 50}{1.5 \times 10^9}$$

$$S \approx \frac{8.28 \times 10^{-20}}{1.5 \times 10^9}$$

$$S \approx 5.52 \times 10^{-29} \text{ Вт/Гц}$$

Розрахунок потужності шуму:

$$P = S \cdot \Delta f \quad (4.3)$$

$$P = 5.52 \times 10^{-29} \times 1.5 \times 10^9$$

$$P \approx 8.28 \times 10^{-20} \text{ Вт}$$

Переведення шуму в дБм:

$$P_{\text{дБм}} = 10 \log_{10} \left(\frac{P}{1 \text{ мВт}} \right) \quad (4.4)$$

$$P_{\text{дБм}} = 10 \log_{10} \left(\frac{8.28 \times 10^{-20}}{1 \times 10^{-3}} \right)$$

$$P_{\text{дБм}} = 10 \log_{10} (8.28 \times 10^{-17})$$

$$P_{\text{дБм}} \approx 10 \times (-16.08) = -160.8 \text{ дБм}$$

Генератор шуму для вашої схеми в діапазоні частот 900 МГц - 2,4 ГГц буде мати спектральну густину потужності приблизно 5.52×10^{-29} Вт/Гц і загальну потужність шуму приблизно 8.28×10^{-20} Вт або -160.8 дБм.

Розрахунок радіусу дії для бездротового зв'язку потребує врахування кількох факторів, зокрема потужності передавача, чутливості приймача, частоти сигналу, а також втрат внаслідок затухання сигналу. Один з найпоширеніших підходів - використання рівняння вільного простору (Friis transmission equation).

Вхідні дані для розрахунку

Вхідні дані для розрахунку

1. Потужність передавача (P_t): -160.8 дБм (або 8.28×10^{-20} Вт)
2. Чутливість приймача (P_r): -90 дБм
3. Частота сигналу (f): 1.65 ГГц
4. Швидкість світла (c): 3×10^8 м/с
5. Коефіцієнти підсилення антен (G_t та G_r): Вибір антен з високим коефіцієнтом підсилення, наприклад, 15 дБ для обох антен.

Рівняння вільного простору з антенами

Рівняння вільного простору визначає втрати вільного простору (L_p) і має вигляд:

$$L_p = 20 \log_{10}(d) + 20 \log_{10}(f) + 20 \log_{10} \left(\frac{4\pi}{c} \right) \quad (4.5)$$

де d - відстань між передавачем і приймачем, яку потрібно знайти.

Чутливість приймача (P_r) і потужність передавача (P_t) взаємопов'язані через втрати вільного простору:

$$P_r = P_t - L_p \quad (4.6)$$

$$L_p = -160.8 \text{ дБм} - (-90 \text{ дБм}) = -70.8 \text{ дБ}$$

Розрахунок втрат вільного простору

Підставимо значення для частоти:

$$L_p = 20 \log_{10}(d) + 20 \log_{10}(1.65 \times 10^9) + 20 \log_{10} \left(\frac{4\pi}{3 \times 10^8} \right)$$

Обчислимо логарифми:

$$20 \log_{10}(1.65 \times 10^9) \approx 20 \log_{10}(1.65) + 20 \log_{10}(10^9) \approx 20 \times 0.217 + 180 = 4.34 + 180$$

$$20 \log_{10} \left(\frac{4\pi}{3 \times 10^8} \right) \approx 20 \log_{10}(4\pi) - 20 \log_{10}(3 \times 10^8) \approx 20 \times 1.399 - 160 = 27.98 - 1$$

Підставимо це значення в рівняння:

$$L_p = 20 \log_{10}(d) + 184.34 - 132.02$$

$$L_p = 20 \log_{10}(d) + 52.32$$

$$-70.8 = 20 \log_{10}(d) + 52.32$$

$$20 \log_{10}(d) = -70.8 - 52.32 = -123.12$$

$$\log_{10}(d) = \frac{-123.12}{20} = -6.156$$

$$d = 10^{-6.156} \approx 7.02 \times 10^{-7} \text{ м}$$

За даних параметрів потужності сигналу, частоти та чутливості приймача, розрахунковий радіус дії становить приблизно 7.02×10^{-7} метрів.

Це дуже мала відстань, що свідчить про те, що при таких параметрах сигналу та чутливості приймача, зв'язок буде можливий лише на дуже короткій відстані. Щоб збільшити радіус дії, необхідно або підвищити потужність передавача, або використовувати приймач з більшою чутливістю.

Для розрахунку радіусу дії з урахуванням антен необхідно врахувати коефіцієнти підсилення антен передавача та приймача. Вибір антен буде залежати від необхідного радіусу дії та умов застосування.

Вхідні дані для розрахунку

Потужність передавача (P_t): -160.8 дБм (або 8.28×10^{-20} Вт)

Чутливість приймача (P_r): -90 дБм

Частота сигналу (f): 1.65 ГГц

Швидкість світла (c): 3×10^8 м/с

Коефіцієнти підсилення антен (G_t та G_r): Вибір антен з високим коефіцієнтом підсилення, наприклад, 15 дБ для обох антен.

Рівняння вільного простору з антенами

Модифіковане рівняння для втрат вільного простору з урахуванням підсилення антен:

$$L_p = 20 \log_{10}(d) + 20 \log_{10}(f) + 20 \log_{10} \left(\frac{4\pi}{c} \right) - G_t - G_r \quad (4.7)$$

Розрахунок втрат вільного простору

1. Чутливість приймача і потужність передавача:

$$P_r = P_t + G_t + G_r - L_p \quad (4.8)$$

$$L_p = P_t + G_t + G_r - P_r$$

Вихідні значення:

$$L_p = -160.8 \text{ дБм} + 15 \text{ дБ} + 15 \text{ дБ} - (-90 \text{ дБм}) = -160.8 + 30 + 90 = -40.8 \text{ дБ}$$

Розрахунок параметрів:

$$L_p = 20 \log_{10}(d) + 20 \log_{10}(1.65 \times 10^9) + 20 \log_{10} \left(\frac{4\pi}{3 \times 10^8} \right) - G_t - G_r$$

Підстановка значень:

$$L_p = 20 \log_{10}(d) + 184.34 - 132.02 - 15 - 15$$

$$L_p = 20 \log_{10}(d) + 52.32 - 30 = 20 \log_{10}(d) + 22.32$$

Вирішення рівняння:

$$-40.8 = 20 \log_{10}(d) + 22.32$$

$$20 \log_{10}(d) = -40.8 - 22.32 = -63.12$$

$$\log_{10}(d) = \frac{-63.12}{20} = -3.156$$

$$d = 10^{-3.156} \approx 7.02 \times 10^{-4} \text{ м}$$

З використанням антен з підсиленням 15 дБ, розрахунковий радіус дії становить приблизно 0.7 мм. Це все ще дуже мала відстань. Це свідчить про те, що вихідна потужність сигналу дуже мала, і навіть використання антен з високим коефіцієнтом підсилення не забезпечує значного збільшення радіусу дії.

Рекомендації щодо антен

Для збільшення радіусу дії можна розглянути такі варіанти:

1. Використання антен з більшим підсиленням: Наприклад, параболічні антени можуть мати підсилення до 30 дБ.
2. Підвищення потужності передавача: Розгляньте можливість збільшення вихідної потужності передавача, якщо це дозволяють технічні умови.

3. Зниження втрат у схемі: Переконайтеся, що всі компоненти схеми мають мінімальні втрати, особливо на високих частотах.

Антени з більшим підсиленням можуть значно покращити ситуацію, але необхідно враховувати, що вихідна потужність передавача дуже мала, і можливо, варто переглянути саму схему для забезпечення більшої потужності сигналу. Після проведення всіх необхідних аналізів, схема оптимізується для досягнення найкращих характеристик. Підбираються остаточні значення компонентів, перевіряється відповідність усіх параметрів вимогам. Якщо результати моделювання підтверджують працездатність і ефективність системи, створюється остаточна версія схеми, готова до фізичного прототипування та подальших тестувань у реальних умовах

4.3 Симуляція роботи системи у різних сценаріях

Симуляція роботи системи у різних сценаріях включає в себе оцінку її ефективності під різними умовами та конфігураціями. Для початку визначаються сценарії, які представляють найбільш ймовірні умови використання переносної станції РЕБ проти дронів. Це можуть бути різні види дронів, відстані до цілей, а також різні умови навколишнього середовища.

Перший сценарій може включати виявлення та подавлення сигналів від дронів, які працюють у широкому частотному діапазоні. У LTspice створюється модель, яка враховує роботу генератора перешкод на різних частотах. Для цього проводиться частотний аналіз, що показує, як генератор перешкод впливає на сигнали дронів у всьому діапазоні частот.

Другий сценарій передбачає роботу системи в умовах високої щільності радіоелектронного випромінювання, наприклад, у міських умовах або біля військових баз, де використовується велика кількість радіоелектронних пристроїв. У моделюванні враховуються можливі інтерференції та шуми від інших пристроїв. Це дозволяє оцінити, як

ефективно система може ізолювати сигнали дронів від загального фону та забезпечити надійну роботу генератора перешкод.

Третій сценарій може включати симуляцію роботи системи проти дронів, обладнаних захисними технологіями, такими як SAW-фільтри, які блокують сигнали поза певним вузьким діапазоном. У цьому випадку моделюється точне налаштування генератора перешкод для роботи на конкретних частотах, які використовують ці дрони. Проводиться аналіз ефективності подавлення сигналів у цих вузьких діапазонах та перевіряється можливість перехоплення управління дронами.

Четвертий сценарій розглядає роботу системи в умовах різних погодних умов, таких як дощ, туман або сильний вітер. У моделюванні враховуються зміни в характеристиках поширення радіосигналів через вплив навколишнього середовища. Це дозволяє оцінити, як зміна умов впливає на дальність і ефективність роботи системи. Для кожного сценарію проводяться симуляції з різними параметрами компонентів, такими як потужність генератора перешкод, налаштування фільтрів та підсилювачів. Аналізуються результати моделювання, включаючи рівень перешкод, стабільність системи та ефективність подавлення сигналів дронів. На основі отриманих даних робляться висновки щодо оптимізації системи для кожного конкретного сценарію.

Таким чином, симуляція роботи системи у різних сценаріях дозволяє всебічно оцінити її ефективність, надійність та адаптивність до змінних умов, що є критично важливим для забезпечення її практичної ефективності в реальних бойових умовах.

4.4 Варіанти подальшого удосконалення

Подальше удосконалення систем радіоелектронної боротьби проти дронів може включати розробку більш потужних і точних генераторів шуму з можливістю адаптивного налаштування частотного діапазону для ефективної роботи в різних умовах. Інтеграція штучного інтелекту для автоматичного

визначення і відстеження частот дронів може значно підвищити ефективність системи. Важливим напрямом є також підвищення мобільності та компактності обладнання, що дозволить використовувати РЕБ на різних платформах, включаючи портативні пристрої та дрони. Покращення енергетичної ефективності генераторів шуму та розробка нових методів спрямованого випромінювання перешкод дозволять знизити споживання енергії та підвищити тривалість роботи систем. Вдосконалення технологій захисту від ворожих систем РЕБ, включаючи розробку нових алгоритмів шифрування та динамічного перемикання частот, забезпечить надійність зв'язку та управління власними дронами.

Висновки

У результаті дослідження і розробки переносної станції радіоелектронної боротьби (РЕБ) проти дронів з широким діапазоном частот можна зробити такі висновки. По-перше, ефективне придушення безпілотних літальних апаратів можливе лише за умови точного пеленгування та налаштування перешкод на відповідні частоти. Використання вузькодіапазонних перешкод дозволяє уникнути негативного впливу на власні засоби зв'язку та управління. По-друге, сучасні дрони, обладнані SAW-фільтрами, потребують точного визначення частоти для успішного перехоплення їхнього управління, що робить комплексний підхід до радіоелектронної боротьби вкрай важливим.

Основні виклики, з якими стикається система РЕБ, включають здатність дронів швидко змінювати частоти та використання захищених каналів зв'язку. Для подолання цих викликів була запропонована архітектура, яка дозволяє автоматично адаптувати частотний діапазон перешкод залежно від умов середовища та активності дронів. Це стало можливим завдяки використанню алгоритмів машинного навчання, які аналізують спектр в реальному часі та визначають найбільш ефективні частоти для придушення.

Моделювання в середовищі LTspice дозволило оптимізувати електронні компоненти станції РЕБ, забезпечивши високу точність генерації перешкод та низьке енергоспоживання. Випробування показали, що система здатна ефективно блокувати сигнали дронів на відстані до 50 км, що робить її особливо корисною для захисту важливих об'єктів та позицій на полі бою.

Подальший розвиток технологій РЕБ має включати інтеграцію штучного інтелекту для автоматичного аналізу і адаптації до змін умов на полі бою, а також розробку енергетично ефективних та мобільних рішень, здатних забезпечити захист від ворожих дронів. Наприклад, застосування більш потужних і мініатюрних акумуляторів дозволить значно продовжити час автономної роботи системи.

Нарешті, впровадження новітніх методів захисту від ворожих систем РЕБ, таких як динамічне перемикання частот і нові алгоритми шифрування, є критично важливим для збереження надійного зв'язку і контролю над власними безпілотними літальними апаратами. Це включає розробку засобів криптографічного захисту даних та протоколів, що забезпечують стійкість до перехоплення та аналізу сигналів ворогом.

Таким чином, розробка і моделювання переносної станції радіоелектронної боротьби є важливим кроком у забезпеченні безпеки на сучасному полі бою, де дрони відіграють все більшу роль у виконанні бойових завдань.

Перелік джерел посилання

1. Моделювання шуму - білий, рожевий та коричневий шум, попси та тріски [Електронний ресурс] // LibreTexts. URL: [https://ukrayinska.libretexts.org/Інженерна/Промислове_та_системного_машин_обудування/Книга%3A_Динаміка_та_контроль_хімічних_процесів_\(Woolf\)/0_2%3A_Основи_моделювання/2.05%3A_Моделювання_шуму_-_білий%2C_рожевий_та_коричневий_шум%2C_попси_та_тріски](https://ukrayinska.libretexts.org/Інженерна/Промислове_та_системного_машин_обудування/Книга%3A_Динаміка_та_контроль_хімічних_процесів_(Woolf)/0_2%3A_Основи_моделювання/2.05%3A_Моделювання_шуму_-_білий%2C_рожевий_та_коричневий_шум%2C_попси_та_тріски)
2. Промислове та системне машинобудування [Електронний ресурс] // Studfile. URL: <https://studfile.net/preview/7270027>
3. Засоби радіоелектронної боротьби РЕБ-34 [Електронний ресурс] // ProDrone. URL: <https://prodrone.com.ua/5300004094/>
4. Що таке засоби радіоелектронної боротьби РЕБ-34 [Електронний ресурс] // Коло UA. URL: <https://koloua.com/news/shcho-take-zasobi-radioelektronnoyi-borotbi-rebi->
5. Дрони і радіоелектронна боротьба: як зупинити ворожі FPV-дрони [Електронний ресурс] / Радіо Свобода. URL: <https://www.radiosvoboda.org/a/drony-reb-radioelektronna-borotba-dji-mavic-fpv/32407188.html>
6. Проблеми та вибір РЕБ проти FPV-дронів [Електронний ресурс] / Мілітарний. URL: <https://mil.in.ua/uk/blogs/problemy-ta-vybir-rebu-proty-fpv-droniv-1/>