Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _Електронної та біомедичної інженерії__
(повна назва)

Кафедра __Мікроелектроніки, електронних приладів та пристроїв__
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти_____другий (магістерський) _____

____Дослідження широкосмугових джерел електромагнітних завад для систем РЕБ_____
(тема)

Виконав:
здобувач 2 року навчання
групи ЕППм-23-1
_____Білецький В.В._____
(прізвище, ініціали)
Спеціальність __171 - Електроніка___
_____
(код і повна назва спеціальності)
Тип програми ____освітньо-професійна___
(освітньо-професійна або освітньо-наукова)
Освітня програма _Електронні прилади та_
_пристрої_____
(повна назва освітньої програми)

Керівник ___проф. Грицунов О. В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет___Електронної та біомедичної інженерії_____
(повна назва)

Кафедра_____Мікроелектроніки, електронних приладів та пристроїв_____
(повна назва)

Рівень вищої освіти_____другий (магістерський)_____

Спеціальність_____171 - Електроніка_____
(код і повна назва)

Тип програми_____освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)

Освітня програма____Електронні прилади та__пристрої_____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві __Білецькому Владиславу Валерійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи ___Дослідження широкосмугових джерел електромагнітних завад_____
__для систем РЕБ_____

затверджена наказом університету від _06_ ___грудня_____2024 р. № _1283Ст___

2. Термін подання студентом роботи до екзаменаційної комісії _10_ ____01____ 2025 р.

3. Вихідні дані до роботи Дослідити перспективні конструкції та можливі функціональні та принципові схеми широкосмугового генератора електромагнітних завад з такими____ попередніми (орієнтовними) параметрами:_____
діапазон частот: 900 МГц … 5800 Мгц;_____
середня потужність по діапазону, не менше: 10 Вт;_____
час автономної роботи, не менше: 4 год;_____
маса, не більше: 12 кг_____

4. Перелік питань, що потрібно опрацювати в роботі:
Мета роботи, аналіз проблеми і постановка задачі, огляд наявних засобів РЕБ, порівняльний аналіз конструкцій, варіанти функціональних і принципових схем, висновки_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри)
Відомість кваліфікаційної роботи: 1
Слайди презентації: 15

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Аналіз предметної галузі	01.10.2024	Виконано
2	Огляд існуючих засобів РЕБ	15.10.2024	Виконано
3	Аналіз проблеми широкосмугових РЕБ	15.11.2024	Виконано
4	Підготовка пояснювальної записки	30.11.2024	Виконано
5	Спецчастина	30.12.2024	Виконано
6	Підготовка презентації та доповіді	05.01.2025	Виконано
7	Попередній захист	06.01.2025	Виконано
8	Нормоконтроль	10.01.2025	Виконано
9	Занесення диплому в електронний архів	11.01.2025	Виконано
10	Допуск до захисту у зав. кафедри	14.01.2025	Виконано

Дата видачі завдання 13 вересня 2024 р.

Здобувач _____
(підпис)

Керівник роботи _____ проф. Грицунов О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота магістра містить 42 сторінки, 26 рисунків, 1 таблицю, 9 джерел.

РЕБ, ШИРОКОСМУГОВІ ДЖЕРЕЛА ЗАВАД, ШУМ, ПРОТИДІЯ БПЛА

Метою роботи є дослідження існуючої проблеми використання широкосмугових джерел завад для протидії використання ворогом малих БПЛА.

В результаті виконання роботи було проаналізовано існуючі проблеми використання широкосмугових джерел завад і запропоновано програмно-апаратний комплекс, який вирішує проблему зниження ефективності РЕБ при використанні широкого діапазону випромінення, шляхом аналізу використовуваних частот і динамічною їх зміною.

ABSTRACT

The Master’s certification work includes 42 pages, 26 figures, 1 table, 9 sources.

ELECTRONIC WARFARE, BROADBAND INTERFERENCE SOURCES, NOISE, COUNTERMEASURES AGAINST UAV

The purpose of the work is to analyze existing problem of broadband interference sources against UAVs that are used by the enemy.

As a result of the work, the existing problem of broadband interference sources’ usage was analyzed and the program-hardware bundle that solves the problem of decreasing of efficiency of usage Electronic Warfare tools in broadband mode using analysis of used bandwidth and their dynamic change was suggested.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БПЛА - безпілотний літальний апарат.

РЕБ - радіоелектронна боротьба.

ППО - протиповітряна оборона.

РЛС - радіолокаційна станція.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 6
ВСТУП 8
1 ЗАГАЛЬНИЙ ОГЛЯД ПРОБЛЕМИ ШИРОКОСМУГОВИХ ДЖЕРЕЛ ЗАВАД 10
1.1 Огляд проблеми використання джерел завад для протидії використанню ворогом БПЛА 11
1.2 Огляд проблеми придушення сигналів в широкому спектрі 14
2 КЛАСИФІКАЦІЯ РАДІОЕЛЕКТРОННИХ ПЕРЕШКОД ТА ВИДИ ЇХНІХ ДЖЕРЕЛ 19
2.1 Маскуючі завади 20
2.2 Імітуючі завади 22
2.3 Засоби захисту від перешкод 23
3 ЦИФРОВА СХЕМА ВИБОРУ ЧАСТОТНИХ ДІАПАЗОНІВ 27
3.1 Програмна основа цифрової схеми 28
3.2 Технічні характеристики майбутнього виробу 32
4 СХЕМИ ТА ПРИСТРОЇ ДЛЯ ГЕНЕРАЦІЇ ШУМІВ 37
4.1 Огляд генераторів шуму із аналоговим керуванням 37
4.2 Цифрові генератори шуму 38
ВИСНОВКИ 41
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 42
Додаток А. Відомість кваліфікаційної роботи ..... **Ошибка! Закладка не определена.**
Додаток Б. Слайди презентації ..... **Ошибка! Закладка не определена.**

ВСТУП

Умови сучасної війни показали, що для ураження живої сили і техніки зовсім нема необхідності у прямому візуальному контакті, а іноді - навіть прямого вогневого контакту. Все частіше ми бачимо, як, використовуючи боєприпас чи техніку, що керується віддалено, як наші захисники так і війська супротивника наносять удари вглиб лінії бойових дій, при цьому залишаючись у відносній безпеці від прямого ураження. Керовані крилаті ракети можуть подолати сотні кілометрів, підлаштовуючи свою висоту, швидкість і навіть свою траєкторію використовуючи системи навігації, такі як GPS чи ГЛОНАСС.

Методи протидії системам навігації уже давно відомі, і не використовують прямих фізичних завад. Натомість, використовуються засоби, що здатні видавати свій спотворений сигнал за сигнал, наприклад, GPS, передаючи невірну інформацію.

Проте невід’ємною частиною сучасної війни є безпілотні літальні апарати (БПЛА), як бойові так і розвідувальні. Придушення сигналу GPS може ускладнити їх наведення, проте пілот завжди може скерувати засіб на базі відео із камери. Відносно малі теплові, акустичні і оптичні сигнатури значно ускладнюють виявлення таких засобів, а відносно невеликий розмір ускладнює їх ураження традиційними засобами ППО. Дані засоби, за невеликим виключенням, використовують радіосигнал для віддаленого керування, що робить очевидним необхідність розробки принципово нових засобів радіоелектронної боротьби (РЕБ) для їх виявлення у повітрі до їх безпосереднього наближення до цілі і знешкодження. Цілі РЕБ в даному випадку можна розділити на 4 основні напрями:

- виявлення БПЛА у повітрі, виявлення його траєкторії, і, в перспективі, знаходження джерела керівного сигналу;
- перехоплення сигналу камери, що дозволить зрозуміти ціль і полегшити ураження такого БПЛА;

- перехоплення керування, що дозволить відвести БПЛА в зону, де він не зможе нанести шкоди;
- придушення сигналів керування або сигналу камери, що зробить неможливим керування даним БПЛА.

Розібравши дані цілі, можна зробити висновок, що ціль пункту 1 досяжна на базі наявних засобів радіолокаційної і гібридної розвідки. Цілі пункту 2 та 3 у перспективі можуть бути корисними, проте потребують значних зусиль, приймаючи до уваги захист цифрового сигналу (наприклад шифрування і використання ключів команд, що не дадуть змогу надіслати команди, ідентичні командам керування), а також зважаючи на складність використання подібних засобів на декількох цілях одночасно. Тому найбільш універсальною і ефективною методикою боротьби буде досягнення цілі номер 4, тобто унеможливлення керування ворогом усіма зафіксованими БПЛА.

Для досягнення цієї цілі необхідна розробка генераторів завад, які унеможливлять або ускладнять проходження сигналу. Основною проблемою розробки є факт того, що передача сигналу може вестись на декількох різних частотах (наприклад, метод динамічного перемикання частот, що дозволяє перемикатися на іншу частоту в умовах завад). Саме тут розробка широкосмугових джерел завад набуває свою актуальність, бо саме придушення сигналу у широкому спектрі частот зробить неможливим перемикання і відновлення сигналів.

Основною проблемою широкосмугових РЕБ на даний час є факт того, що розмір діапазону завад напряму пов’язаний із потужністю випромінення, а в умовах бойових дій це впливає на фізичні параметри даного засобу, такі як потужність джерел живлення і батарей, матеріал, що використовується у даних засобах, системи охолодження і як результат - на розмір засобу.

Метою дипломної роботи є дослідження і розробка джерела завад, яке зможе ефективно вести випромінення у широкому спектрі частот, і при цьому ефективно використовуючи енергію і маючи прийнятні розміри для встановлення і транспортування.

1 ЗАГАЛЬНИЙ ОГЛЯД ПРОБЛЕМИ ШИРОКОСМУГОВИХ ДЖЕРЕЛ ЗАВАД

Для того, щоб проаналізувати проблему, яку має вирішити широкосмугове джерело завад у складі комплексів РЕБ, треба декомпозувати ціль і проаналізувати технічні проблеми і труднощі кожного із елементів. Почнемо із того, які проблеми наразі є із протидією використанню ворогом БПЛА. Особливо звернемо увагу на відносно малі БПЛА, які активно використовуються на лінії бойових дій, так як більші (у порівнянні із розмірами звичайних літальних апаратів) визначаються існуючими системами ППО, і піддаються типовим методам боротьби із ними. Для виявлення безпілотників використовуються:

- системи радіопеленгації/радіомоніторингу випромінювання БПЛА (комплекси РТР);
- РЛС (насамперед активні РЛС);
- комплекси оптико-електронного спостереження;
- системи шумопеленгації.

Після виявлення БПЛА в повітряному просторі, можна переходити до його знищення. Основними засобами придушення та знищення БПЛА є:

- кінетичне ураження мети осколками зенітного снаряда чи зенітної ракети;
- перехоплення БПЛА дроном-винищувачем;
- руйнування корпусу БПЛА лазерним випромінюванням;
- ураження електроніки БПЛА потужним мікрохвильовим випромінюванням;
- ураження електроніки БПЛА електромагнітним імпульсом вибухового генератора;
- засоби радіоелектронного придушення.

1.1 Огляд проблеми використання джерел завад для протидії використанню ворогом БПЛА

Малі БПЛА створюють значно більше проблем для протидії, ніж більші, хоча принципи їх виявлення та ураження, зокрема за допомогою засобів ППО, схожі з тими, що застосовуються до традиційних літальних апаратів. Основною відмінністю малих БПЛА є їхня дуже мала ефективна площа розсіювання (ЕПР), що досягається завдяки компактним розмірам та широкому використанню пластику в конструкції. Крім того, ці дрони мають обмежену теплову, акустичну та оптичну сигнатури, що ускладнює їх виявлення.

Для подальшої класифікації приведемо таблицю класів БПЛА, із якими доводиться мати справу (таблиця 1.1). У даній роботі сконцентруємося саме на малих, бо використання їх противником значно ускладнює як оборону, так і наступ із ряду причин.

Таблиця 1.1 - Класифікація БПЛА

Клас	Категорія	Позначення	Найменування
Малі	I	n	Нано
		μ	Мікро
		Mini	Міні
Легкі	II	CR	Близької дії
Середні	III	SR	Малої дальності
		MR	Середньої дальності
	IV	MRE	Середньої дальності із підвищеною тривалістю польоту
		LADP	Маловисотний великої дальності
Важкі	V	LALE	Маловисотний із підвищеною тривалістю польоту
	V-VI	MALE	Середньовисотний із підвищеною тривалістю польоту
	VII	HALE	Висотний із підвищеною тривалістю польоту

Продовження таблиці 1.1

Клас	Категорія	Позначення	Найменування
Бойові	VIII	UCAV	Безпілотний ударний
		DEC	Фальш-ціль
		TGT	Повітряна мішень
Змішані	IX	OPA	Пілотований за вибором
		CMA	Переобладнаний пілотований

Навіть якщо БПЛА виявляються, виникає проблема їхнього ураження. Сучасні засоби ППО не були спеціально розраховані для боротьби з такими малими і низькошвидкісними цілями. Вартість зенітної ракети часто в кілька разів (а іноді й у десятки разів) перевищує вартість самого БПЛА, що робить таке використання озброєння економічно невигідним. Крім того, наявні системи наведення та підривники не завжди ефективні при ураженні таких малорозмірних цілей.

Ще однією проблемою є тактика «рою», коли на один об'єкт одночасно націлюються численні БПЛА, що летять з різних напрямків. Це призводить до виснаження боєзапасу і можливості прориву дронів до цілі.

Застосування низьковисотного польоту також ускладнює виявлення БПЛА, оскільки радіогоризонт обмежує його дальність. Для ефективної протидії БПЛА необхідно не лише вчасно їх виявити, а й фізично знищити або вивести з ладу їхні системи управління, навігації, спостереження чи інші критично важливі елементи.

Необхідно врахувати, що супротивник постійно вдосконалює засоби зв'язку та управління БПЛА за рахунок:

- застосування адаптивних активних ґрат БПЛА (в першу чергу для прийому сигналів від глобальних навігаційних систем);
- шифрування сигналів;
- відхилення від стандартних частот передачі;

- застосування шумоподібних сигналів (ШПС) та сигналів із псевдовипадковою перебудовою робочої частоти (ППРЧ, або FHSS – англ. Frequency-Hopping Spread Spectrum). Тому структурні перешкоди будуть ефективними лише проти:

а) стандартних глобальних навігаційних систем: GPS (L1 – 1575,42 МГц/L2 – 1227,6 МГц/L5 – 1176,45 МГц), ГЛОНАСС (L1 – 1602 МГц/L2 – 1246 МГц) , BeiDou (B1 – 1561,098 МГц/B2 – 1207,14 МГц/B3 – 1268,52 МГц), Galileo (E1 – 1575,42МГц/E6–1278,75МГц/E5–1191,79;

б) типових каналів стільникового зв'язку: CDMA800 (850-894 МГц), GSM900 (890-915, 935-960 МГц), GSM1800 (1710-1880 МГц), 3G (2110-2170 МГц), 8G (7 960, 925-960 МГц; 1,7-2,2, 2,5-2,7 ГГц), Wi-Fi (2,4-2,5, 4,9-6,425 ГГц);

в) каналів супутникових систем зв'язку "Інмарсат" (1518-1660,5 МГц), "Ірідіум" (1616-1626,5 МГц), Starlink;

Структурні перешкоди оптимально пригнічують канали зв'язку та навігації із заздалегідь відомими параметрами, (як за частотами, так і за структурою каналу, що пригнічується).

Генератори перешкод із перебудовою частоти раціонально використовувати проти:

- засобів радіозв'язку діапазону УКХ;
- засобів авіаційного радіозв'язку;
- інших нестандартних каналів зв'язку управління та навігації БПЛА.

При цьому засобами радіотехнічної розвідки (РТР) ці канали повинні бути розкриті в режимі реального часу і передані на придушення засобам РЕБ. Якщо засоби РТР не змогли їх розкрити, то генератори перешкод із перебудовою частоти повинні перейти в режим свіпування (від англ. «sweep», що значить «змах»), тобто швидке перемикання частотного діапазону від низьких до високих частот із певними часовими рамками, створюючи непостійну заваду у широкому спектрі і не даючи можливості передавачу обрати частоти без завад. Відкритим залишається питання періоду перебудови свіпуючого генератора, тобто як швидко проводити перебудову частоти генератора, а також границі

діапазону, оскільки спостерігається тенденція використання у засобах зв'язку та спостереження БПЛА нестандартних частот. Шумові загороджувальні перешкоди найменш ефективні з енергетичної точки зору при придушенні БПЛА, але безперечною перевагою даного типу перешкод є їхня універсальність при застосуванні. Причому під шумовою загороджувальною перешкодою слід розуміти не тільки перешкоду з модулюючим сигналом типу «білого шуму» (рис. 1.1)

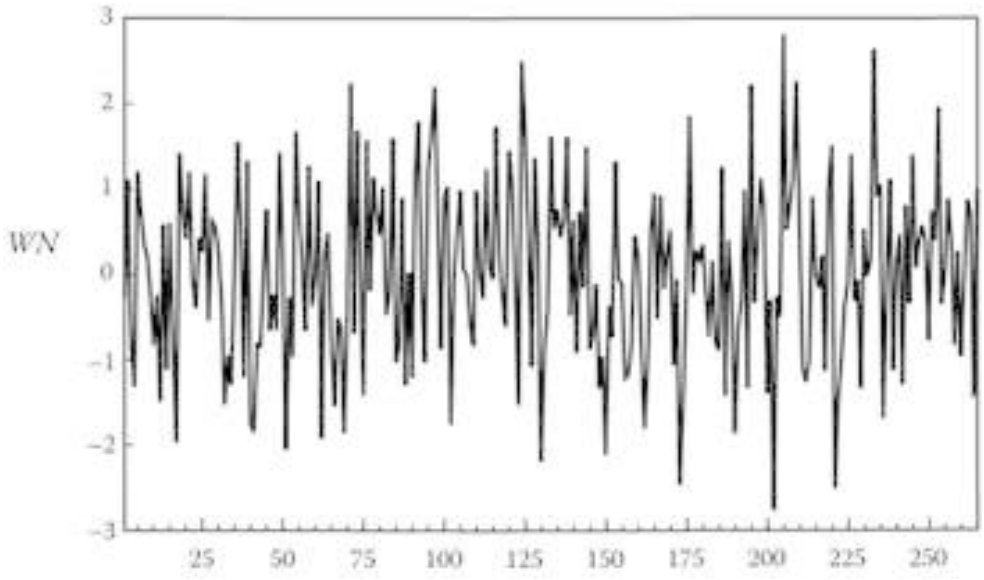


Рисунок 1.1 - Спектрограма білого шуму

1.2 Огляд проблеми придушення сигналів в широкому спектрі

Слід зазначити, що рівень сигналу РЕБ зменшується пропорційно квадрату відстані. Цю фундаментальну властивість радіосигналів неможливо оминути, і підтверджується вона формулою Введенського (формула 1.1), що описує залежність напруженості поля від відстані до випромінювача.

$$E = 2{,}18\frac{\sqrt{P \cdot G} \cdot h1 \cdot h2 \cdot k}{\lambda r^2}\ , \qquad (1.1)$$

де E - значення напруженості поля, що діє, мВ/м;

r - довжина траси зв'язку в км;

λ - довжина робочої хвилі передавача в метрах;

P - потужність передавача у кВт;

G - коефіцієнт посилення передавальної антени;

h1, h2 – висота підвісу передавальної та приймальних антен у метрах;

K – коефіцієнт, що враховує середовище поширення, лежить у межах 0,2-0,4.

При сталих потужності передавача, коефіцієнту посилання передавальної антени і висоті підвісу антен розуміємо, що один і той самий сигнал на різній відстані від випромінювача змінюватиме свою потужність квадратично відстані.

Окрім того, потужність сигналу на одиницю частоти залежить від ширини спектру, і описується наступною формулою (1.2):

$$P_{rad} = \frac{\mathrm{P}_{in}}{\Delta \mathrm{f}} \cdot G \ , \qquad (1.2)$$

де P rad - потужність на одиницю частоти;

P in - сумарна потужність передавача;

Δf - ширина діапазону (тобто різниця між найбільшою і найменшою частотами випромінення);

G - коефіцієнт посилення передавальної антени.

Таким чином, беручи до уваги вище приведені формули, можна привести конкретні приклади. Візьмемо стандартний канал 900 MHz для системи ERLS, який є найбільш розповсюдженим у побутових (так званих «любительських») дронах. Його діапазон в основному відрізняється на 25 MHz і лежить (для стандарту США) в межах від 902 MHz до 928 MHz, в якому використовується розбиття на окремі канали по 25 KHz кожен. Припустимо, ми знаємо сталу частоту і канал, на якому відбувається керування дроном, тому беремо умовно перший канал і підставляємо дані у формулу із рис. 3. Припустимо, що потужність нашого передавача дорівнює 100 Вт, таким чином отримуємо 0,4G

на кожні 100 Hz частоти в діапазоні 25 KHz. Приймемо це значення як стале для одного каналу, що використовується у БПЛА. Якщо ж прийомо-передавальні пристрої БПЛА можуть перемикатися між двома різними каналами, і ми знаємо обидва - то наш діапазон зростає вдвічі, і потужність на кожні 100 Hz частоти становитиме уже 0,2G, а згідно із формулою з рисунку 2 це значить (приведемо непряму аналогію потужності випромінення і значенням потужності поля), що якщо РЕБ із потужністю в 100 Вт може придушити один канал на відстані, наприклад, в 400 метрів (що можна назвати граничною відстанню для влучання зі стрілецької зброї по БПЛА, що втратив керування), то при роботі із двома каналами отримаємо (вирішивши рівняння із рисунку 1 відносно r і прийнявши інші показники сталими) зменшення відстані роботи у $\sqrt{2}$ (що приблизно дорівнює 1,4) рази, тобто на нашому прикладі - до приблизно 285 метрів. Якщо ж передавальний пристрій здатний охоплювати 4 керуючих частоти - то зменшення ефективної відстані буде до 200 метрів, і так далі.

Таким чином ми розуміємо, що придушення частот у більшому спектрі, що охоплював би всі канали ERLS, уже не має принципового сенсу, так як із такої невеликої відстані шкода, яку нанесе влучання БПЛА, буде заподіяна або безпосередній цілі, або оточенню (персоналу). Дана теза також не охоплює нестандартні частоти, які все частіше використовуються у пілотуванні, і для протидії яким смуга передачі повинна бути додатково розширена. Частково дану проблему вирішує використання свіп-передавача, який одночасно генерує заваду лише в одному із заданих каналів, але час від часу перемикається між каналами, не даючи можливості перебудувати керування на інший канал. Проте дана техніка буде мати сенс лише тоді, коли перемикання каналів керування відбувається за статичним законом (з меншого каналу на більший чи с більшого на менший), що дозволить розробити алгоритм перемикання. Використання ж псевдо-випадкового вибору каналу або аналіз і вибір каналу із найменшими завадами робить таку заваду неефективною.

Також, зниження ефективної дистанції потенційно можна компенсувати кількістю використаних генераторів завад (рисунок 1.2), проте така схема значно

впливає на результуючу вартість системи, і робить майже неможливим використання свіп-режиму за рахунок того, що генератори завад повинні бути синхронізовані (тобто кожен із генераторів завад в кожен проміжок часу повинен охоплювати один і той самий частотний діапазон).

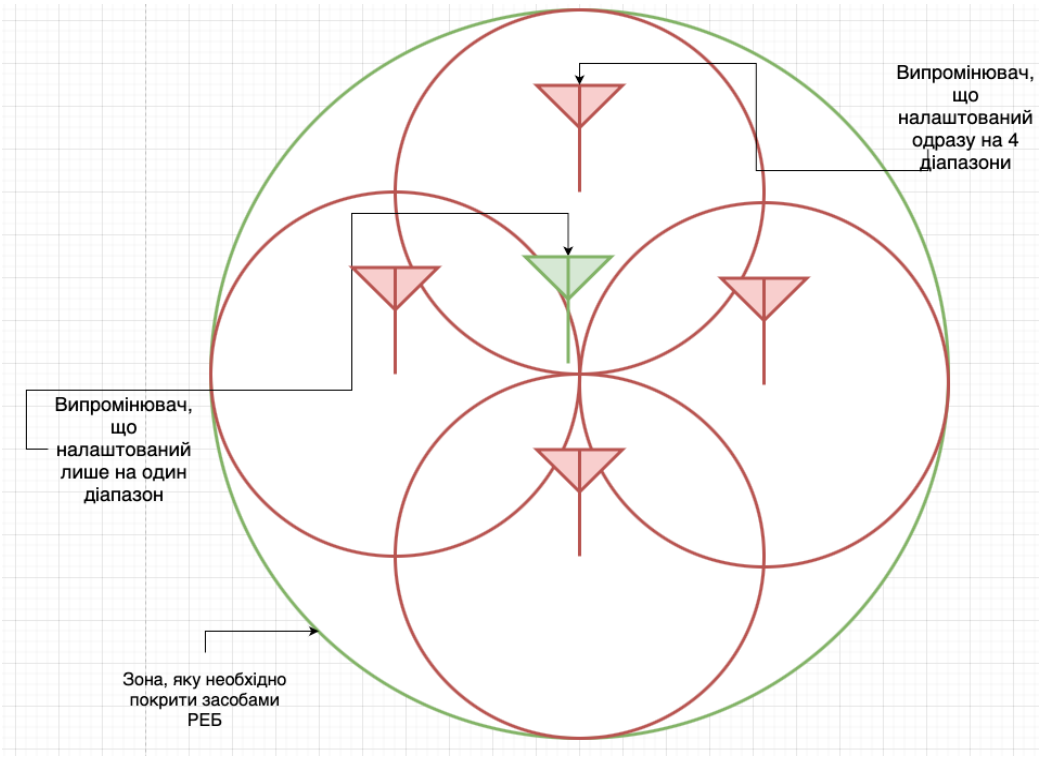


Рисунок 1.2 - Схема покриття широкої зони засобами РЕБ

Відкритим також залишається питання живлення таких засобів. Зазвичай польовий блок РЕБ споживає від 200 до 400 ват електроенергії, що, звісно, дозволяє заживити засіб на декілька годин за допомогою зарядної станції, але дані станції не виробляють, а лише акумулюють електроенергію, і їх необхідно перезаряджати. А отже що більше засобів РЕБ встановлено, то більшою буде витрата енергії.

Дана схема наочно показує, як на розрахунках, приведених вище, співвідносяться зони покриття. Якщо випромінювачем, налаштованим на один частотний діапазон, можна умовно покрити зону в 400м (зона, позначена зеленим кольором), то при налаштуванні на чотири діапазони зона покриття звужується до 200 метрів (зони, позначені червоним кольором), і для покриття

однієї і тієї самої ділянки уже необхідно 4 засоби РЕБ. Одночасно із тим ми бачимо, що деякі ділянки залишаються покритими слабше, проте в центральній частині є накладання охоплених ділянок. Звісно, даний приклад не покриває усіх можливих сценаріїв використання РЕБ, і, беручи до уваги топологічні особливості конкретної місцевості можна зробити цю схему більш ефективною, виносячи РЕБ від центру до країв зони, яку необхідно покрити засобами РЕБ, проте проблема перекриття деяких ділянок і недопокриття інших залишається, і якщо БПЛА зможе пройти повз краї зон - він потрапить в незахищений центр ділянки.

Особливо дана проблема актуальна у разі придушення БПЛА літакового типу, які, на відміну від малих (квадро- чи октокоптерного типу) при втраті сигналу продовжують пологе зниження до попередньо зазначеної точки. Це значить, що якщо зони перекриття РЕБ зможуть придушити керування літальним апаратом, то він продовжить свій рух до центру, що потенційно не є прикритим, і відновить своє керування безпосередньо над своєю цільовою ділянкою. За відкритими даними, БПЛА літакового типу, що летить на висоті 1км, при втраті керування може планувати на відстань до 10 км вздовж своєї попередньої траєкторії, що, з одного боку, дає більше часу на його збиття засобами фізичного впливу (зенітні боєприпаси, автоматична зброя, тощо), проте не дає повного захисту. А в межах міста дана проблема отримує додаткову актуальність. Для прикладу, площа міста Харків - 350 квадратних кілометрів, що дуже приблизно можна описати колом в 19 кілометрів у діаметрі. Існуючі стаціонарні засоби РЕБ якщо і можуть покрити таку зону, то лише в обмеженому частотному діапазоні, а БПЛА, який летів в центр і був придушений засобами РЕБ на околицях міста, зможе продовжити свій шлях до центру міста. Навіть БПЛА, що утратив керування, досить важко збити в межах міста, бо використання зенітних боєприпасів може потенційно нанести не меншу шкоду (уламками від вибуху може зачепити будівлі, що опинилися у радіусі вибуху), а мобільні вогневі групи, які могли б збити даний апарат із автоматичної зброї, мають можливість рухатись лише автомобільними дорогами в межах міста, тому час, за який вони

зможуть вийти на дистанцію пострілу до БПЛА значно збільшується. Таким чином розуміємо, що для ефективного прикриття міста зона, на якій відбувається придушення, має починатися мінімум за 10 кілометрів від міста (беручи за основу дані, приведені вище, що БПЛА буде планувати 10 кілометрів після втрати керування), що робить зону необхідного покриття окружністю у 29 кілометрів (що є недосяжним навіть для потужних стаціонарних засобів РЕБ). Для того ж, щоб прикрити місто кільцем із описаних вище засобів РЕБ, здатних забезпечити більше ніж 10 кілометрів прикриття (для того, щоб БПЛА літакового типу упав у передмісті, де потенційно нанесе менше шкоди, ніж при падінні у місті), потрібно не менше ніж 5 або 6 випромінювачів, що ускладнює процес і значно впливає на вартість схеми.

Відкритим залишається питання того, що стаціонарні засоби РЕБ можуть самі стати ціллю ворога, яку можна знищити за допомогою некерованих засобів, що не будуть чутливими до дії РЕБ. Це приводить нас до факту того, що замість використання декількох стаціонарних засобів необхідно використати менші, які можливо буде вільно переміщувати на кількасот метрів, не даючи ворогу можливості уразити їх, і час розгортання яких буде достатньо малим, щоб відновити роботу, не залишаючи ділянку неприкритою.

Нажаль поки що ми прийшли до взаємо-виключних зауважень. РЕБ меншого розміру не матиме достатньої потужності при використанні широкого діапазону частот, щоб ефективно виконувати свою функцію, в той час як засіб РЕБ, що матиме достатню потужність, не матиме можливості працювати в штатному режимі, а його використання і обслуговування може стати небезпечним.

2 КЛАСИФІКАЦІЯ РАДІОЕЛЕКТРОННИХ ПЕРЕШКОД ТА ВИДИ ЇХНІХ ДЖЕРЕЛ

Для більш глибокого розуміння генерації перешкод, необхідно розібрати і проаналізувати наявні джерела перешкод і механізми їх роботи.

Ми знаємо, що перешкоди бувають як природними, так і штучними. Аналізувати природні перешкоди немає сенсу, так як оперувати ними неможливо, однак треба розуміти, що вони мають бути враховані при побудові мережі РЕБ. Наприклад, як компас може видавати хибні дані за наявності поряд сильного магнітного поля, так і цифровий сигнал може бути спотворений або навіть загублений в несприятливих умовах (наприклад, супутниковий сигнал в умовах значної хмарності буде просто неможливий, проте радіосигнал навпаки може навіть підсилитися, як це можна побачити в сигналі телеефіру).

Штучна завада може бути як ненавмисною (наприклад, перетинання частотного спектру, при якому слабший сигнал буде губитися у більш сильному), так і навмисною (наприклад, дія РЕБ в конкретному діапазоні частот). У першому випадку завада повинна бути вирішена шляхом комунікації перед власне використанням частотного діапазону, наприклад, шляхом вибору різних каналів зв’язку у різних підрозділах, що унеможливить перетинання сигналів, або у випадку цифрового сигналу - методом підпису і фільтрації пакетів даних (таким чином кожен приймач розумітиме, який сигнал було передано йому, а який повинен бути проігнорований).

Другий випадок більш суттєвий. Треба розуміти, що використовуючи шумоподібне заглушення сигналу засобами РЕБ на конкретному діапазоні частот робить цей діапазон непридатним як для використання ворогом, так і для власних потреб. Доволі часто на полі бою зустрічаються ситуації, коли за недостатньої комунікації між підрозділами один підрозділ виконує придушення частотного діапазону, у той час інший безуспішно намагається використати цей діапазон для встановлення зв’язку або, наприклад, для керування власними БПЛА. Така ситуація може бути критичною і нести непоправну шкоду.

Також штучні джерела завад умовно можна розділити на два типи: маскуючі та імітуючі завади.

2.1 Маскуючі завади

Маскуючі завади ускладнюють отримання корисної інформації в заданому частотному діапазоні, що робить неможливим установлення зв’язку чи керування радіоелектронними приладами. Зачасту, це досягається генерацією шуму із достатньою силою сигналу, щоб перекрити корисний сигнал. Умовно зображено таку заваду на рисунку 2.1.

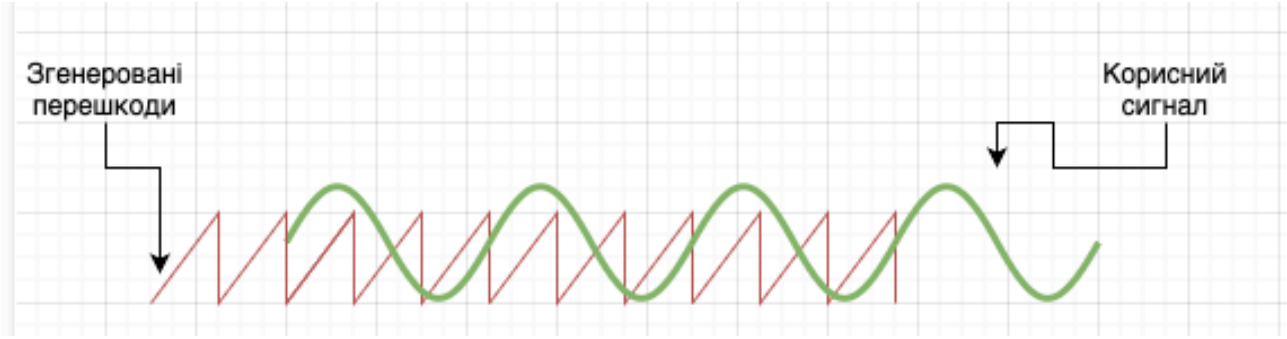


Рисунок 2.1 - Накладання корисного сигналу на перешкоду

На даному рисунку червоним виділено сигнал-заваду, який генерується засобами РЕБ на постійній основі. Якщо інше джерело намагається передати корисну інформацію (виділено зеленим кольором) у цьому самому діапазоні - сигнал змішується і губиться у генерованому шумі, таким чином отримання інформації передавачем ускладнюються чи навіть унеможливлюється.

До недоліків такого виду джерел завад треба також віднести те, що джерело завади саме по собі є потужним джерелом випромінювання, а значить легко може бути виявлене чи стати ціллю для протирадіолокаційних ракет ворога. Такий тип ракет не має віддаленого керування, а значить його неможливо придушити засобами РЕБ, і автоматично наводиться на сильне джерело радіосигналу, а це значить, що за наявності у ворога таких ракет у конкретній місцевості робить використання маскувальної завади занадто небезпечним. Зазвичай для захисту засобів маскуючого РЕБ використовують так звані фальш-цілі, які повинні видавати себе за антену РЛС і прийняти на себе вогонь протирадіолокаційних ракет.

Альтернативою є механічні завади, які самі по собі не є випроміненням, проте знижують коефіцієнт прохідності сигналу конкретної місцевості. До таких, наприклад, відносяться дипольні відбивачі, які є смужками металізованої стрічки, що спричиняють відбиття сигналу. Відстрілюючи у повітря капсули із такими смужками за допомогою спеціальної техніки можна створити умовну хмару, яка унеможливить проходження сигналу крізь неї на деякий проміжок часу (залежить від погодних умов, наприклад від швидкості вітру). Такі завади мають високу ефективність проти тропосферного або супутникового зв'язку, проте неефективні проти сигналів близького зв'язку, що пройде під хмарою.

Також ефективним є електромагнітний імпульс високої потужності, що може спричинити вихід із ладу контурів приймача за рахунок індукції у ньому високого струму, але генерація такого імпульсу потребує значної енергії (наприклад, такий імпульс генерується під час вибуху атомного боєприпасу у повітрі, або у малому радіусі розрядкою конденсаторів великої ємності), проте для використання на постійній основі вони не призначені і можуть нести шкоду як для ворога, так і для власної техніки.

2.2 Імітуючі завади

Більш технічно складними, проте іноді більш ефективними, є імітуючі завади. У такому випадку засіб РЕБ не просто генерує заваду на частотному діапазоні, а передає сигнал, який видає себе за корисний, проте несе заздалегідь неправдиву інформацію. Такі завади орієнтовані на конкретний тип інформації, конкретні протоколи даних і конкретні команди, проте можуть мати значущий ефект. Найпростіший приклад - це так званий GPS-spoofing, тобто підробка даних GPS-сигналу. Зазвичай будь-який GPS-приймач повинен увійти в контакт мінімум із трьома GPS-передавачами, які в свою чергу нададуть йому інформацію про широту, довготу і висоту над рівнем моря конкретної точки у просторі, в якій знаходиться приймач. Що більше передавачів взято у роботу - то більш точною буде інформація (для широко розповсюджених приймачів

допустимим є відхилення усього в декілька метрів), що робить можливим, наприклад, навігацію автомобіля на дорозі або навігацію БПЛА при заході на ціль. Проте якщо поряд є передавач, що видає себе за GPS, але передає заздалегідь невірну інформацію, то це може спотворити всю навігацію. Це можна побачити, наприклад, увімкнувши автомобільну навігацію у прифронтовому місті. У такому випадку навігатор покаже точку, яка знаходиться у десятках кілометрів від реального положення, а також покаже невірну інформацію про висоту і швидкість руху. Використовуючи такий тип завад можна, наприклад, атакувати ворожі БПЛА, передавши їм інформацію про те, що вони знаходяться занадто далеко від цілі, і відвести їх від заданого курсу туди, де вони не зможуть нанести шкоди, або передати їм неправдиву інформацію про їх висоту, спровокувавши зниження аж до самого зіткнення із землею. У випадку малих БПЛА, можна навіть змусити їх перейти на інший керівний сигнал, тим самим перехопивши керування. Проте слід розуміти, що такі засоби є значно більш технічно складними (наприклад у випадку підробки GPS-сигналу необхідним критерієм є те, що сила підробленого сигналу має бути приблизно такою ж, як сила реальних сигналів від супутників, що взяті в роботу, інакше приймач його проігнорує), і використання них може потребувати як значних навичок, так і дороговартісних засобів.

2.3 Засоби захисту від перешкод

Знаючи механізм роботи завад, можна зрозуміти, як ускладнити їх використання ворогом. Для цього існують як технічні методи, що обираються на етапі підготовки операції, так і комбіновані, що можуть бути застосовані при виявленні перешкод чи можуть бути спроектовані виробником конкретного радіотехнічного засобу в умовах використання виробу за присутності завад і задіяні на полі бою. Комбіновані засоби включають як попередні налаштування, так і механізми, що оцінюють заваду і дозволяють користувачу продовжити роботу.

Технічні засоби захисту включають наступні аспекти:

- раціональний вибір параметрів сигналу. Наприклад, вибір неочікуваних каналів для установлення радіозв'язку чи нестандартних каналів керування БПЛА, що може ускладнити виявлення керівного сигналу;
- інтервальний сигнал. Така техніка може використовуватись для унеможливлення виявлення сигналу, і базується вона на тому, що команди керування передаються не на постійній основі, а через деякі проміжки часу. Наприклад, БПЛА раз на декілька секунд чи хвилин отримує команду від центру керування, що редагує його курс, висоту чи швидкість руху на наступний проміжок часу. Таким чином сигнал не виявляється локаторами, що очікують постійну передачу інформації, і може бути пропущений;
- робота на кількох несучих частотах. У випадку відсутності керівного сигналу в заданому проміжку часу на одній частоті сигнал перемикається на іншу, заздалегідь відому для центра керування і очікує команд звідти. В такому випадку у разі, якщо БПЛА опинився у зоні дії однодіапазонного РЕБ, він втратить керування тільки на незначний проміжок часу, після чого перейде на інший канал (зачасту з протилежного боку нумерації каналів), який, імовірно, не буде перекритий РЕБ;
- селекція сигналів по напрямку приходу. Найпростіший захист може бути реалізований завдяки використанню направленої антени БПЛА, що отримуватиме слабший сигнал, який приходить зі сторони цілі його руху, та сильніший зі зворотнього боку. Більш складна реалізація побудована завдяки автокомпенсації перешкод, заснована на механізмі просторової кореляції і досягається за рахунок використання декількох антен. В такому випадку компенсаційна антена охоплює своєю пелюсткою бічні пелюстки основної антени. Обидва сигнали приходять на суматор, який виділить корисний сигнал, проте такий механізм є ефективним лише за умови дії однієї перешкоди.

До комбінованих засобів можна віднести наступні програмно-технічні рішення, що потребують вищої обчислювальної потужності контролеру приймача, наприклад:

- додаткова верифікація даних приймача. Наприклад, БПЛА може запам’ятовувати попередні показники сигналу GPS, і якщо наступний сигнал надасть йому інформацію про положення, що значно відрізняється від попереднього - він не змінюватиме курс і ігноруватиме показники;
- селекція сигналів по силі. Наприклад, при виявленні сигналу, що значно сильніший за задане обмеження, ігнорувати його команди;
- заздалегідь запрограмовані дії. Наприклад, БПЛА при втраті сигналу керування може повернутися до заданої точки, продовжити рух за тією самою траєкторією і з тією самою швидкістю, або навіть самоліквідуватися (вибухнути) за відсутності сигналу у деякому проміжку часу, якщо потрапляння БПЛА до рук ворога може нести загрозу.

Але знаючи, що одночасно передача все ще ведеться на одній частоті, і беручи до уваги факт того, що перелічені засоби генерації завад також відомі і ворогу, бо були розроблені ще десятки років тому, існує необхідність розробки нового принципу побудови РЕБ, який, використовуючи описані принципи, дозволить підвищити їх ефективність на полі бою.

Наприклад, замість підвищення потужності передавача генератора маскувальних завад (що веде за собою більше навантаження на батареї, необхідність охолодження передавачів і інші фізичні аспекти) треба розглядати системи, що зможуть звести ситуацію, у якій нам треба генерувати завади на широкому суцільному діапазоні частот, до ситуації, коли ми матимемо набір зі скінченного (ідеально - декілька одиниць) спектру каналів невеликого діапазону, в яких передача буде найбільш ефективною за рахунок мінімального зниження потужності випромінювача. Для цього замість аналогових засобів, що є компонентами сучасного РЕБ і подолання їх фізичних обмежень, треба рухатись у напрямку цифровізації процесу, а саме вводити додатковий керуючий елемент, що прийме рішення стосовно необхідних частот і ефективно згенерує заваду.

Існуючі цифрові генератори завад із плаваючою частотою частково покривають ці потреби, проте мають і власні недоліки. Генератори завад ведуть передачу на діапазоні частот, що є суцільним, тобто не даючи можливості

пропускати неактивні ділянки. Також використання генераторів із цифровим керуванням потребує синхронізації між підрозділами і отримання вказівок, а переналаштовування може займати час і бути достатньо складним, бо потребує достатньо великої кількості параметрів.

3 ЦИФРОВА СХЕМА ВИБОРУ ЧАСТОТНИХ ДІАПАЗОНІВ

Як найбільш універсальний (тобто той, що не потребує додаткових навичок у користувача) і ефективний у плані вартості розробки тип завад, будемо розглядати маскуючу заваду із шумоподібним сигналом. Імітуючі завади відкинуто через їх високу вартість і через те, що вони ефективні лише в обмеженому спектрі ситуацій, прямо не пов’язаних із використанням ворогом саме малих БПЛА як розвідувального, так і ударного типу. Не має сенсу підробляти сигнал GPS, якщо дроном може керувати людина, так само немає сенсу намагатися підробити команди керування, бо більшість польотних контролерів для БПЛА мають механізми підпису і шифрування сигналів. Проте придушення керівного сигналу все ще є ефективним. Малі БПЛА коптерного типу не здатні довго перебувати у повітрі через обмежений ресурс їх батарей і неможливість вільного планування, тому придушивши керівний сигнал можна досягнути успішної протидії такому типу загрози. Також інтервальний метод віддання команд неефективний для них із тієї самої причини, БПЛА не здатен летіти достатньо високо і довго, щоб очікувати на нові команди.

Проаналізувавши перелічені у попередньому пункті роботи методи генерації завад і захисту від них розуміємо, що для протидії малим БПЛА достатньо не дати ворогу можливості заздалегідь налаштуватися на частоти, що не будуть враховані при проектуванні РЕБ, а також унеможливити використання альтернативних каналів керування при перемиканні керуючої частоти. Все вказує на те, що система одночасно повинна покрити усі доступні частотні діапазони, охоплюючи також нестандартні діапазони, що неможливо із ряду причин, описаних у пункті 1 враховуючи витрати енергії і технічні особливості передачі широкосмугового сигналу.

Враховуючи описану ціль і існуючі недоліки розуміємо, що результатом повинна стати цифрова схема, яка буде виконувати передачу лише в одному частотному діапазоні в один проміжок часу, досягаючи максимальної

ефективності використання передавача, схожою до техніки свіпування, проте в автоматичному (або напів-автоматичному) режимі виявляти лише необхідні частотні діапазони, що прискорить перемикання каналів, пропускаючи ті, на який не виявлено передачі даних, що дозволить позбутися недоліків свіп-систем. Ця схема буде цифровою, бо аналогові методи не здатні до обробки такого набору інформації і прийняття програмних рішень, водночас вона повинна базуватися на існуючих методах і засобах, не призводячи до необхідності дороговартісної і довготривалої розробки. Для придушення частоти все ще використовуватиметься сигнал категорії білого шуму, так як такий сигнал достатньо важко вирізнити на значній відстані і легко отримати.

3.1 Програмна основа цифрової схеми

За основу цифрової схеми, здатної проаналізувати і виявити необхідні частотні діапазони, а також керувати випроміненням завад в засобах РЕБ, можна взяти схему, яка часто використовується у портативній акустичній техніці - Active Noise Cancellation, чи активного шумозаглушення (рис. 3.1).

На даній схемі мікрофон отримує сторонній сигнал (тобто шум, червоний сигнал на схемі), і передає його а контролер активного шумозаглушення. Контролер аналізує шум, генерує протифазу цього сигналу (синій сигнал на схемі), тобто розгортає фазу отриманого сигналу на 180 градусів, і підмішує з використанням так званого суматора цей сигнал до корисного сигналу (зелений на схемі), який зазвичай є аудіозаписом, що програється. Таким чином, при випроміненні динаміком корисного сигналу, протифаза шуму і сам шум гасять одне одного, і користувач схеми чує лише оригінальний сигнал.

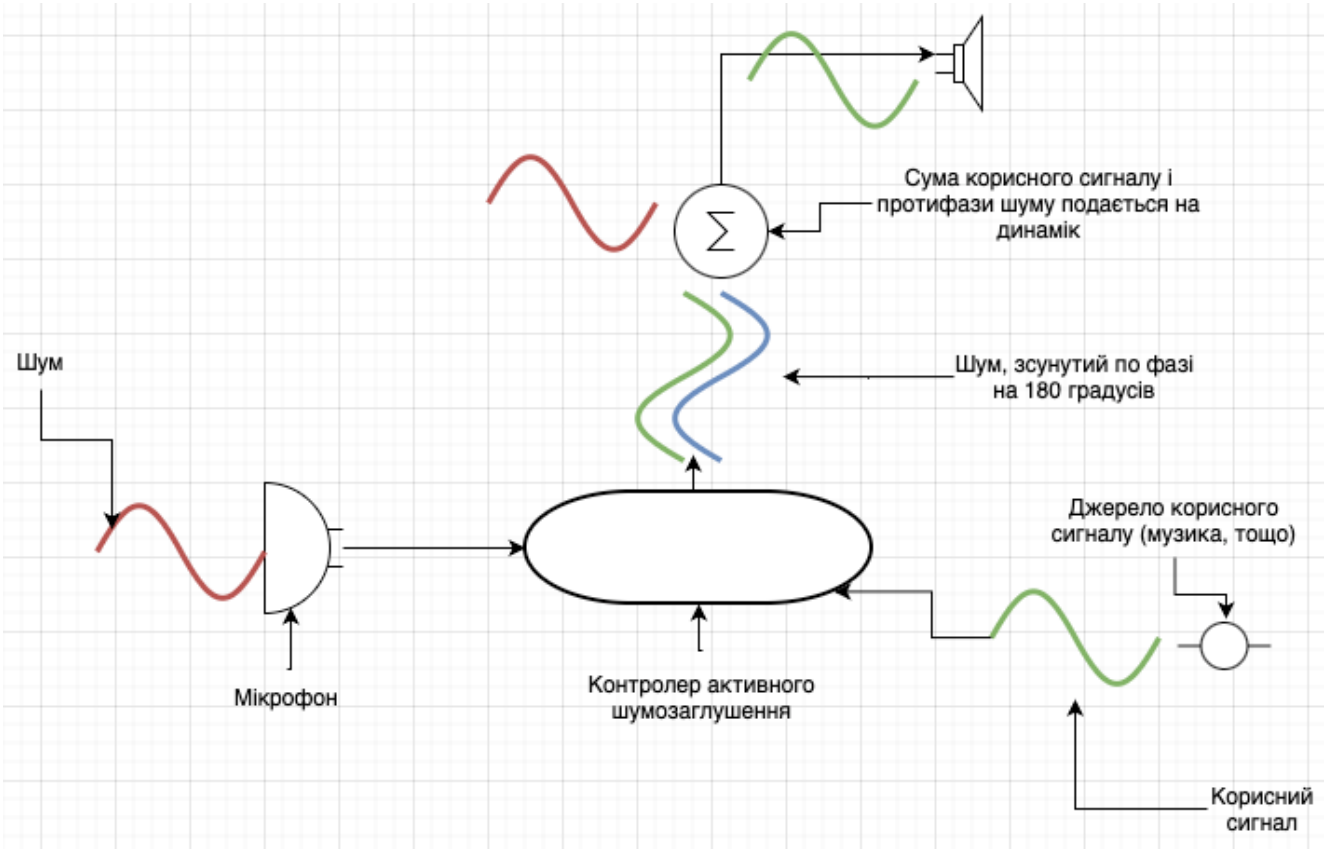


Рисунок 3.1 - Спрощена схема активного шумозаглушення

У випадку аудіосигналу, досить важливим критерієм є швидкість спрацювання контролеру та якість знегерованої протифази, що мінімально деформує корисний сигнал.

У випадку РЕБ, дана схема може бути спрощена наступним чином:

- контролер не має створювати саме протифазу сигналу, достатньо лише проаналізувати частоту, на якій присутній сигнал, і використати білий шум в даному діапазоні;
- корисний сигнал в даній схемі відсутній, тому можна знехтувати швидкістю спрацьовування контролеру і спотворенням сигналу, спровокованим накладанням протифази шуму;
- частотний діапазон керуючого сигналу достатньо рідко змінюється у часі, тому проводити сканування можна проводити із достатньо великим інтервалом і перемикатися між частотними

діапазонами у значно більшому проміжку часу (декілька секунд, що уже переважає над свіп-контролерами), дозволяючи придушувати сигнал більш ефективно.

Таким чином, отримуємо схему, описану на рисунку 3.2.

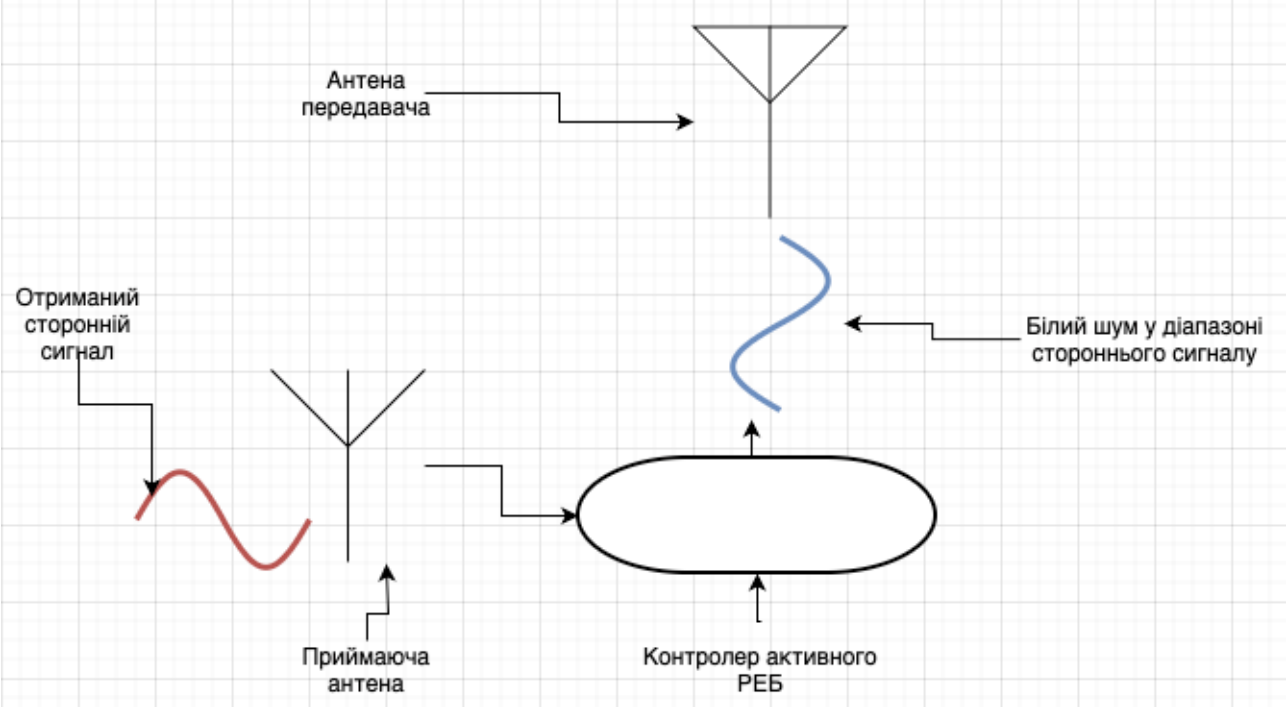


Рисунок 3.2 - Схема РЕБ із активним аналізом частоти

На даній схемі приймаюча антена фіксує сигнал, отриманий від стороннього джерела (керуючий сигнал для БПЛА). Контролер аналізує сигнал і виявляє діапазон, в якому він лежить. Далі контролер генерує білий шум у заданому діапазоні і передає його на антену передавача. Таким чином описаний засіб РЕБ одночасно веде випромінення лише в одному частотному діапазоні, а значить працює на своїй максимальній потужності.

Після фіксації сигналу контролер може перестати приймати дані з антени на деякий час (потенційно даний проміжок може бути від однієї до 10 секунд, бо зазвичай перемикання на резервний канал керування не відбувається миттєво), а під час наступного сканування пропускати ту частоту, на якій уже відбувається

випромінення, таким чином реалізуючи безшовне перемикання між діапазонами за необхідності.

Також дана схема може об’єднувати декілька описаних приладів в одну складну мережу, що дозволить вирішити існуючу проблему конфлікту частот РЕБ, яка відбувається за недостатньої синхронізації між підрозділами, що використовують РЕБ, і призводить до надлишкового покриття одного діапазону і недостатнього покриття іншого.

Для об’єднання у мережу можна використати схему master-slave, у якій один центральний пристрій отримує сигнал одночасно із декількох приймаючих антен (або уже оброблені дані із декількох контролерів), і передасть на усі контролери список діапазонів, у яких вони повинні випромінювати придушуючий сигнал (рисунок 3.3).

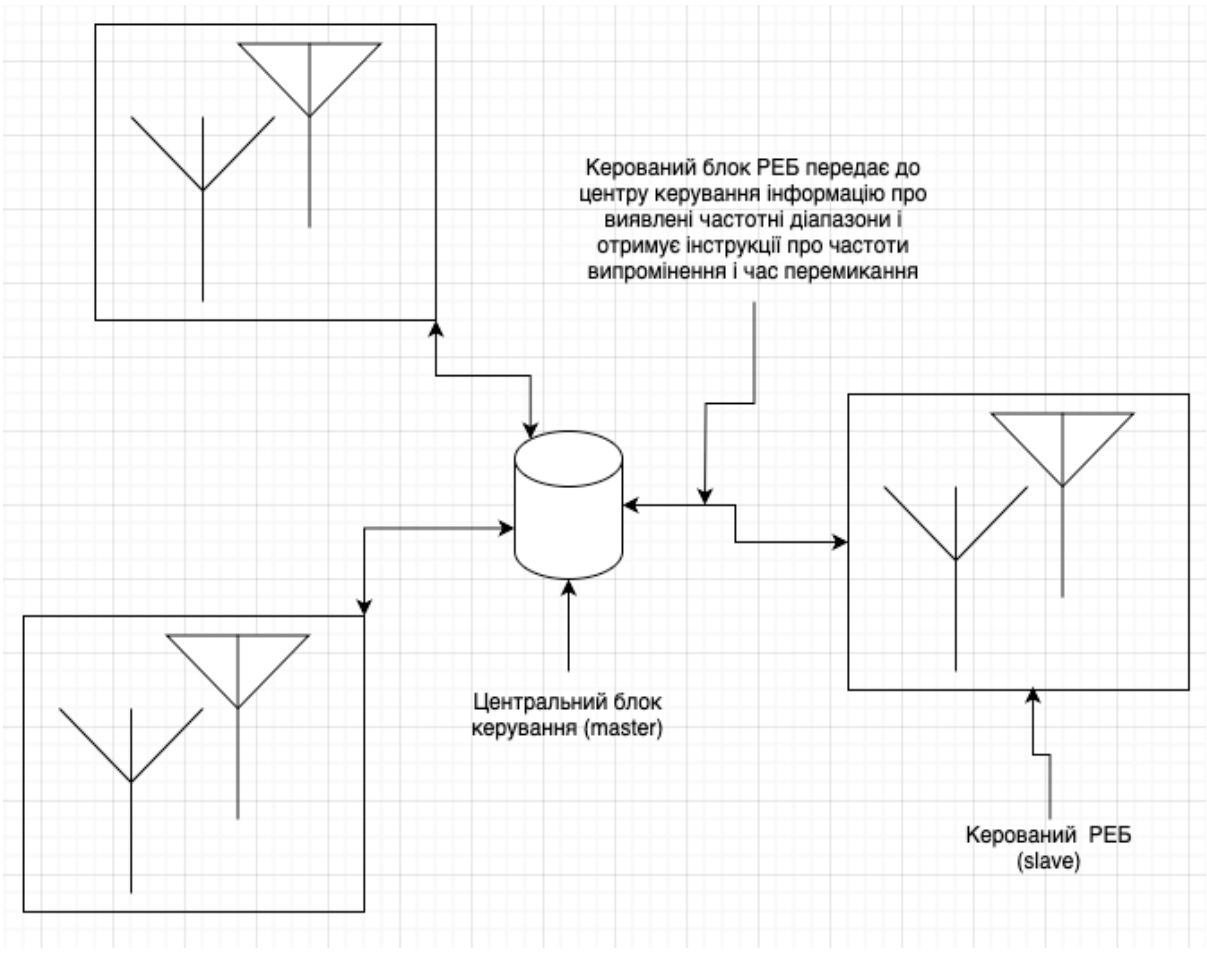


Рисунок 3.3 - Схема master-slave для об’єднання засобів у мережу

Також, за умови об’єднання динамічного РЕБ у мережу, можна створити систему ручного керування, де оператор зможе наочно відстежити, на яких частотах зараз працює РЕБ у всій мережі (а це значно спростить керування групою підрозділів, так як кожен із підрозділів, що відповідальний за окрему ділянку, не буде змушений окремо звітувати про використані частоти), а також за необхідністю вносити корективи, наприклад для забезпечення безперебійної роботи власних БПЛА чи засобів зв’язку у діапазонах, які не мають бути придушені засобами РЕБ. Для цього система має бути спроектована таким чином, що кожен із контролерів у мережі матиме окремі таблиці із записами про зафіксовані діапазони (тобто ті, які зафіксував хоча б один із пристроїв у мережі) і таблиці, які використовуються для випромінення білого шуму. Останні можуть бути перманентно вилучені зі сканування, таким чином жоден із контролерів не братиме до уваги частотні діапазони, на яких відбувається передача сигналу іншими РЕБ, і одночасно із тим кожен контролер зможе забезпечувати «наскрізні коридори», тобто частотні діапазони, на яких не буде працювати жоден РЕБ у мережі.

Для формалізації потреб і полегшення подальшого проектування, складемо технічне завдання для контролера.

3.2 Технічні характеристики майбутнього виробу

Як було описано вище, цифровий блок керування РЕБ повинен мати змогу працювати в двох режимах: режимі єдиного РЕБ (такий режим називають Standalone) і в режимі РЕБ-мережі. Для початку опишемо базові потреби першого режиму, спроектувавши послідовність процесів, що протікатимуть у пристрої за допомогою UML-діаграми (рисунок 3.4).

В базовому використанні від оператора фактично потрібна лише дві дії: увімкнути пристрій і задати частотні діапазони, які не повинні бути ним придушені, задля збереження можливості використовувати власні БПЛА та

встановлювати зв’язок на обмеженому наборі частот. Для одночасного спрощення налаштувань і унеможливлення втручання ворога в схему робочого процесу, зробимо введення параметрів можливим лише під час увімкнення пристрою.

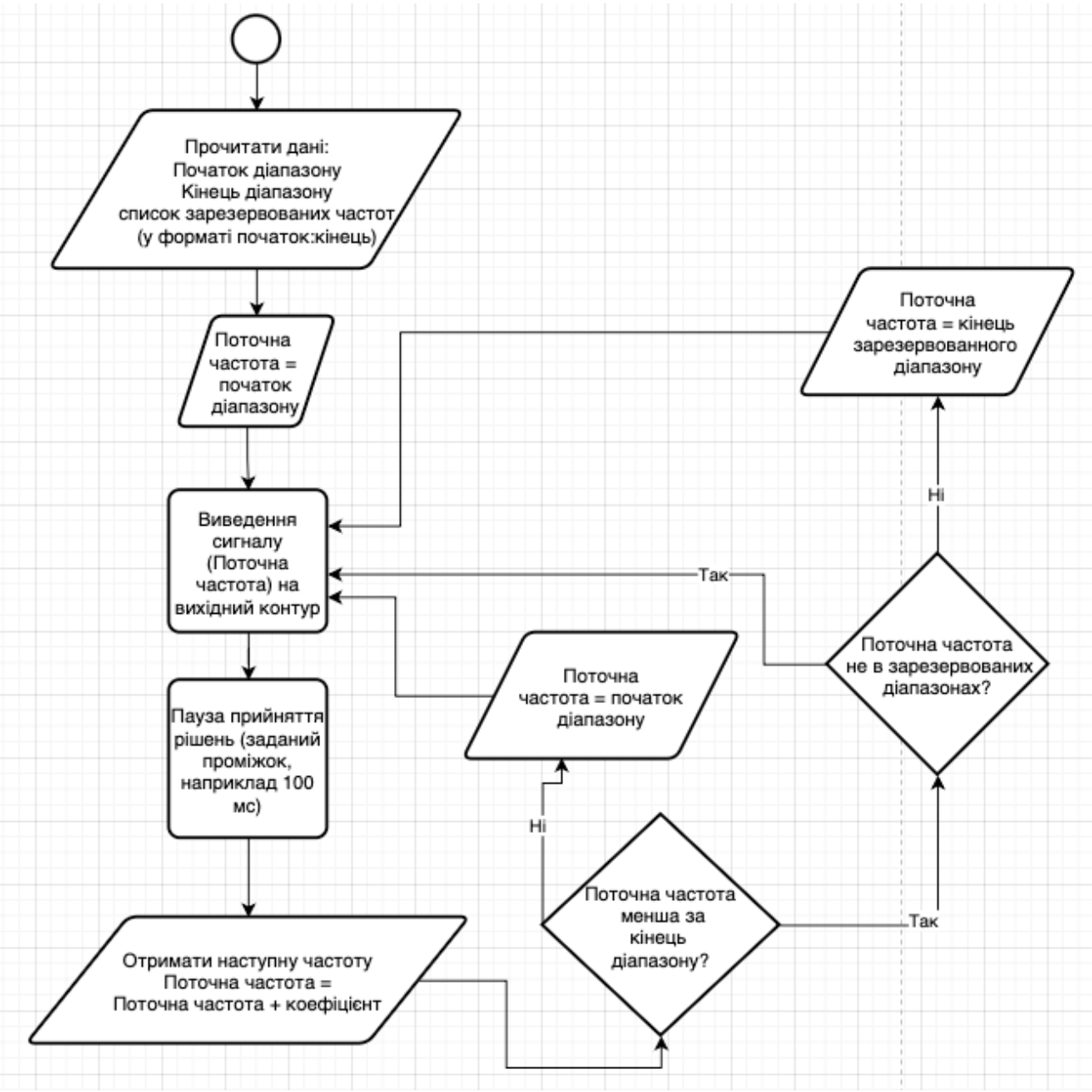


Рисунок 3.4 - Блок-схема логіки роботи Standalone режиму

Як бачимо, схема прийняття рішень доволі проста, і приводить нас у замкнутий цикл, який декілька разів на секунду збільшує базову частоту, поки не дійде до кінця діапазонів, пропускаючи обрані проміжки. Для такої простої логіки підійдуть прототипні плати класу ESP32, що значно спростить програмування пристрою і його подальші налаштування, а живлення плати всього в межах від 1 до 2 вата дозволить живити її від блока живлення підсилювача без впливу на його роботу. Для реалізації запам’ятовування списку частот, які були знайдені в ході сканування (що дозволить ефективніше перемикатися, пропускаючи частоти, на яких сигналів не зафіксовано), схема ускладнюється додатковим блоком. Режим сканування має отримати сигнал на заданих частотах (механізм схожий до режиму автоматичного сканування станцій звичайного FM-радіо), і запам’ятати ті частоти, які були знайдені. В подальшому ці значення можна обгорнути в такий самий список початок-кінець, що дозволить замість простого додавання коефіцієнту «перестрибувати» між значеннями, скорочуючи проміжки часу між перемиканнями несучих частот.

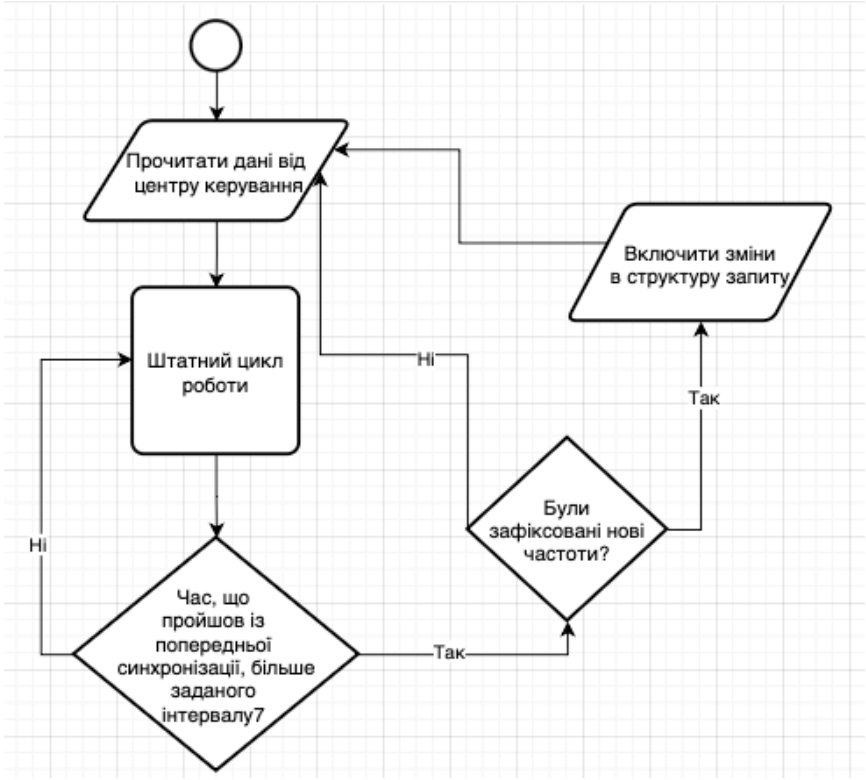
Також для отримання режиму мережі необхідно зробити дві додаткові зміни в схемі:

а) замість статичного уведення частот необхідно зробити запит на центр керування (фактично це така сама плата, яка замість основної логіки просто зберігає значення і може відповідати на запити). Структура відповіді повинна включати усі ті самі вхідні дані, і додатково описувати час, через який повинен бути зроблений запит на оновлення. Це необхідно для реалізації інтервального методу, який дозволить захиститися від перехоплення, а також дозволить приладу працювати із меншою кількістю переривань. Структура запиту може включати список частот, знайдених кожним із приладів, таким чином центр керування зможе комбінувати дані всієї мережі і координувати захист;

б) через проміжок часу, отриманий від центру керування, необхідно реалізувати переривання, під час якого прилад зробить новий запит для синхронізації.

Схема роботи описана на рисунку 3.5.

Запит включатиме список зафіксованих частот лише в тому випадку, коли з моменту останньої синхронізації було виявлено зміну. Це дозволить значно зменшити кількість даних, які будуть передаватися, що в свою чергу прямо пропорційно знижує час на виконання запиту. Також для додаткової оптимізації процесу, можна включати код-мітку, яка буде позначати актуальні дані. Якщо в структурі запиту пристрій передав той самий код, це значить що йому уже відома актуальна версія таблиці частот, і вона не буде включена у структуру відповіді, що в такому випадку міститиме лише новий інтервал



синхронізації.

Рисунок 3.5 - Схема роботи в режимі мережі

За потреби в структуру запитів і відповідей можна інтегрувати режим свій-чужий, реалізований на базі одноразових кодів і «ключового слова», яке буде налаштоване до початку роботи, що дозволить захистити всю схему від потенційних спроб втручання у її роботу ворогом.

4 СХЕМИ ТА ПРИСТРОЇ ДЛЯ ГЕНЕРАЦІЇ ШУМІВ

Отримавши базову частоту на попередньому кроці, необхідно згенерувати шумоподібний сигнал, що буде в подальшому підсилено і відправлено на антену. Для цих цілей використовується так званий генератор шуму. Генератори шуму можуть бути як цілком аналоговими, так і із цифровим керуванням, що дозволяє корегувати параметри шумів. Сам генератор шуму - це не виключно пристрій військового призначення, вони часто використовуються у лабораторіях і майстернях як джерело сигналу, який спостерігається в реальних системах і умовах.

4.1 Огляд генераторів шуму із аналоговим керуванням

Для генерації шуму аналоговим шляхом використовуються резистори високої потужності і так звані шумові діоди. За рахунок шуму, що виникає в резисторі, який додатково підсилюється підсилювачем, можна отримати простий генератор шуму, описаний на рисунку 4.1.

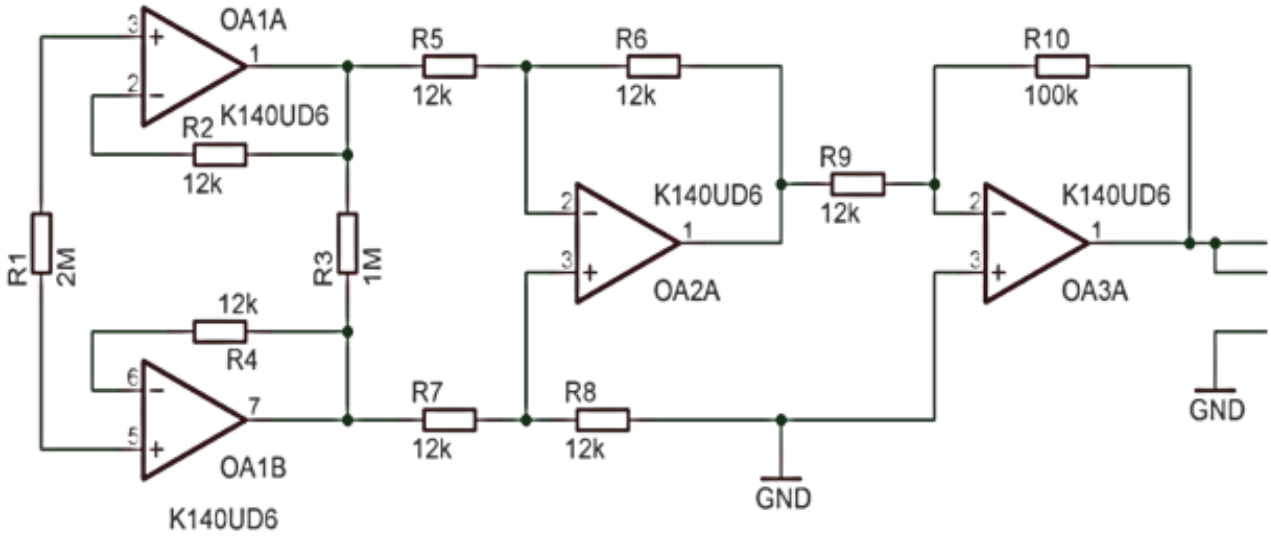


Рисунок 4.1 - Схема генератора шуму на базі резистору

Шум із такого генератора зазвичай підсилюють для отримання електроакустичного шуму для подальшого використання при розробці і калібруванні акустичної техніки (мікрофони, системи шумозаглушення, і навіть системи розпізнавання голосу) для отримання умов, близьких до умов реального використання майбутніх приладів.

Більш контрольований шум і такий, який дозволяє задати діапазони частот і щільність спектру, можна отримати із використанням напівпровідникових шумових діодів (рисунок 4.2).

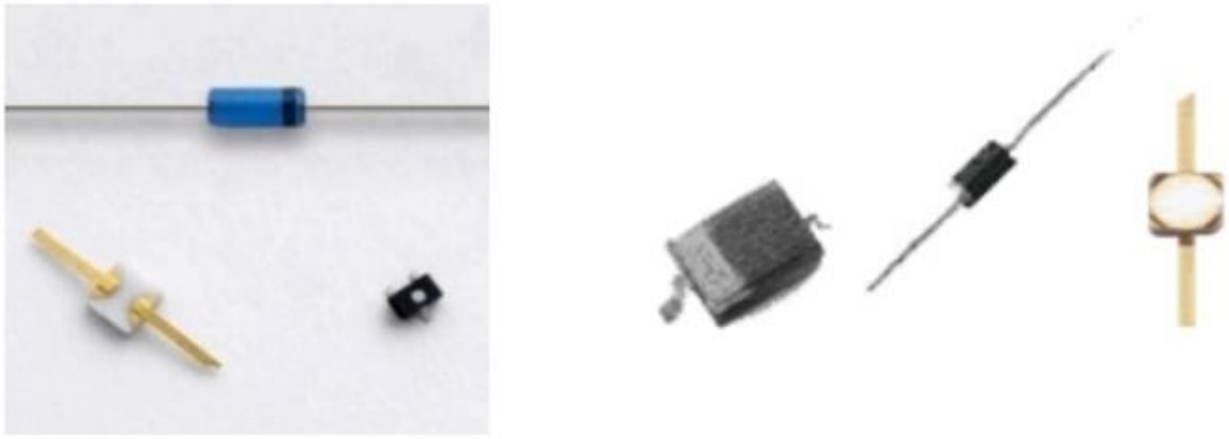


Рисунок 4.2 - Шумові діоди

У таких діодах шум з’являється за рахунок ударної іонізації або лавиноподібного примноження в областях переходів, що дозволяє отримати шум із випадковим розподіленням, а їх частота може досягати десятків гігагерц, що дозволяє використовувати їх у мікрохвильовій апаратурі та при розробці аналогово-цифрових перетворювачів.

4.2 Цифрові генератори шуму

Цифрові генератори шуму керуються за допомогою мікросхеми, яка дозволяє налаштувати частоти і форму вихідного сигналу, базуючись на

уведених даних, що відповідає потребам по генерації шуму, описаним в попередньому пункті. Для генерації шуму представлена схема із рисунку 4.3.

Рисунок 4.3 - Схема цифрового генератора шуму

На даній схемі задавальний генератор генерує неконтрольований (аналоговий) шум, який додатково підсилюється проміжковим підсилювача до рівня лінійного входу, що дозволить далі опрацювати його коректором АЧХ для змін спектральної щільності сигналу. Гетеродин в даній схемі є джерелом гармонійних коливань, тобто опорного сигналу, що в подальшому змішується із шумом на змішувачі. Після змішування сигнал подається на підсилювач і на передаючий випромінювач. Зазвичай подібна схема використовується для роботи, наприклад, телевізійного чи радіосигналу, і суть її полягає у тому, що високочастотний сигнал значно краще розповсюджується у просторі, ніж низькочастотний. Роль задавального генератора при цьому виконує вузол, що приймає низькочастотний слабкий сигнал (наприклад мікрофон), а гетеродин має постійну високочастотну характеристику. Після змішування ми отримуємо високочастотний сигнал, що змінюється в часі за законом низькочастотного, тобто повторює його характеристики і може бути обернений на приймальному

пристрої (тобто виділивши високочастотну частину ми отримуємо низькочастотний сигнал, аналогічний оригінальному, що може бути передано на динамік). Блок живлення у даному випадку живить усю схему, і його потужність використовується як для отримання базової частоти на гетеродині, так і для підсилення вихідного сигналу перед подачею його на випромінювач. У нашому ж випадку обернення сигналу не потрібне, бо ми не передаємо жодної корисної інформації, проте ми все ще повинні отримати деяку форму високочастотного сигналу.

Знаючи це розуміємо, що пристрій, що описаний в попередньому пункті, може бути використаний саме у якості гетеродину, тобто несуча частота, яка буде генерована на базі наших обчислень, буде змінюватись за нашими потребами на базі зафіксованих частот, на яких ведеться передача інформації воногом, і використана для того, щоб аналоговий шум, згенерований генератором шуму на базі резистору чи діоду, після змішування із несучою частотою утворив шумоподібний сигнал на заданій попередньо частоті. Шуму, утвореного на даному етапі, повинно бути достатньо, щоб перекрити корисний сигнал для команд керування чи радіопередачі, і зробити неможливим виділення голосу або команд із них.

ВИСНОВКИ

У проведених під час виконання роботи дослідженнях виявлено ключові особливості, притаманні веденню радіоелектронної боротьби проти різноманітних БПЛА і проблему застосування існуючих засобів РЕБ для протидії ворожим БПЛА, зокрема неефективність їх роботи в широкому спектрі частот і обмеження, із якими стикаються широкосмугові передавачі.

Методом декомпозиції отримано цілі, які можуть бути досягнуті за використання РЕБ для боротьби із БПЛА, проаналізовано доцільність виконання деяких із цих цілей і відповідність їх практичної користі до необхідних зусиль, що будуть затрачені на їх досягнення, в результаті чого обрано оптимальний напрям роботи, що дозволить у досяжні строки і з помірними витратами максимізувати користь використання РЕБ.

Проаналізовано основні радіочастотні діапазони, у яких ведеться передача сигналів керування БПЛА і стратегії, за якими може бути обрано частотний діапазон для системи зв’язку, який потрібно буде придушувати широкосмуговими джерелами завад. Із використанням відомих формул обчислено і виявлено порядок зменшення ефективності класичного широкосмугового генератора завад при одночасному придушенні сигналу у широкому діапазоні частот, що використовуються в класичному ERLS як прикладі найбільш типового засобу керування БПЛА.

Як результат, зроблено припущення відносно механізму, що матиме найбільшу ефективність із точки зору витрати енергії, що одночасно дозволить вести придушення декількох каналів зв’язку у широкому діапазоні без зниження радіусу дії завад, а також дозволить зберегти поточний порядок технічних характеристик (ємність і інші параметри батарей, температурний робочий діапазон і фізичні розміри) для джерела завад.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Макаренко С. І. Аналіз засобів та способів протидії безпілотним літальним апаратам // Системи управління, зв'язку та безпеки. 2020. № 2.

2. Макаренко С. І. Протидія безпілотним літальним апаратам" (монографія): "Наукоємні технології", ТОВ "Корпорація "Інтел Груп". 2020.

3. Никольский В.В., Никольская Т.И. Электродинамика и распространение радиоволн. – М.: Наука, 1989. – 544 с.

4. Моделирование электромагнитных полей в электротехнических устройствах / А.Е. Степанов, Ю.Г. Блавдзевич, З.Х. Борукаев и др. – К.: Техніка, 1990. – 188 с.

5. Нгуєн В.Х., Фан Н.З., Фам Х.Х. Ефективність впливів перешкод у системі глобальної навігації GPS// Євразійський Союз Вчених (ЕСУ). 2020. № 2.

6. Слюсар Ст. Радіолінії зв'язку з БПЛА Приклади реалізації // ЕЛЕКТРОНІКА: Наука, Технологія, Бізнес. 2010. №5.

7. Wyder, P.M., Chen, Y.-S., Lasrado, A.J., Pelles, R.J., Kwiatkowski, R., Comas, E.O., Kennedy, R., Mangla, A., Huang, Z., Hu, X., Xiong, Z., Aharoni, T., Chuang, T.-C. and Lipson, H. Autonomous drone hunter operating by deep learning and all-onboard computations in gps-denied environments, PloS One, 2019.

8. Craye, C. and Ardjoune, S. Spatio-temporal semantic segmentation for drone detection, 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE, 2019.

9. Dan Gettinger, “The Drone Databook,” Center for the Study of the Drone, 2019. https://dronecenter.bard.edu/projects/drone-proliferation/databook/