Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:
МЕТОДИ ПРОТИДІЇ В РАДІОНАВІГАЦІЙНИХ КОНФЛІКТАХ

Виконав
студент групи БІКСМ-1-24-1.4.д
Шандрук Максім Сергійович
(прізвище, ім’я, по батькові)

_____
(підпис)
Науковий керівник
д.т.н., професор
(науковий ступінь, наукове звання)
Крючкова Л. П.
(прізвище, ініціали)

_____
(підпис)

Київ – 2025

Міністерство освіти і науки України
Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Шандрук Максім Сергійович
(прізвище, ім’я, по батькові)

1. Тема роботи: Методи протидії в радіонавігаційних конфліктах;
керівник Крючкова Лариса Петрівна, д.т.н., професор
затверджені наказом ректора від «___»_____ 20___ року №__.
2. Термін подання студентом роботи « 1 » грудня 2025 р.
3. Вихідні дані до роботи:
3.1 науково-технічна та нормативна література з теми дослідження: стандарти оформлення, методичні вказівки;
3.2 методи: динамічного спектрального адаптування (DSA), фільтрація сигналу, метод використання мультичастотних систем, криптографії;
3.3 технології: розширення спектра сигналу, машинного навчання;
3.4 алгоритми: антиспуфінгові, фазового контролю;
3.5 мова програмування: Python Matlab;
3.6 математичні моделі та методи: моделі DSSS та адаптивних антен, моделі оцінки ефективності (SNR, SINR, BER, PDOP, SIR).
4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):
4.1 Аналіз загроз та уразливостей радіонавігаційних систем.
4.2 Дослідження сучасних методів протидії радіонавігаційним конфліктам та розробка алгоритмів захисту.
4.3 Моделювання та оцінка ефективності процесу радіоподавлення і адаптивних методів протидії за умов інформаційного конфлікту.
5. Перелік графічного матеріалу: корисні сигнали, завадові сигнали, результати взаємозв’язку завадового сигналу на корисний.
5.1 Презентація доповіді, виконана в Microsoft PowerPoint.
5.2 Типові схеми дослідження впливу завадових сигналів на корисний сигнал.
6. Дата видачі завдання «4» квітня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1	Уточнення постановки завдання	01.04.2025 - 04.04.2025	Виконано
2	Аналіз літератури	05.04.2025 - 20.04.2025	Виконано
3	Обґрунтування вибору рішення	01.05.2025	Виконано
4	Збір даних	05.05.2025- 10.05.2025	Виконано
5	Виконання та оформлення розділу 1.	01.06.2025 – 25.06.2025	Виконано
6	Виконання та оформлення розділу 2.	28.06.2025 – 20.07.2025	Виконано
7	Виконання та оформлення розділу 3.	30.07.2025 - 24.08.2025	Виконано
8	Вступ, висновки, реферат	01.09.2025 – 17.09.2025	Виконано
9	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції	01.05.2025 – 26.06.2025	Виконано
10	Оформлення та друк текстової частини роботи	08.12.2025	Виконано
11	Оформлення презентацій	02.12.2025- 10.12.2025	Виконано
12	Отримання рецензій	01.12.2025	Виконано
13	Попередній захист роботи	01.12.2025	Виконано
14	Захист в ЕК	17.12.2025	

Студент _____ Максім Сергійович Шандрук
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Лариса Петрівна Крючкова
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена технологіям використання методів протидії в радіонавігаційних конфліктах у системах супутникової та наземної радіонавігації.

Робота складається зі вступу, трьох розділів, що містять 10 рисунків та таблиць, висновків та списку використаних джерел, що містить 55 найменування. Загальний обсяг роботи становить 99 сторінок, з яких 3 сторінки займають ілюстрації і таблиці на окремих аркушах, а також додатки, перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження процеси та функціонування радіонавігаційних систем та в умовах радіонавігаційних конфліктів.

Предметом дослідження є методи, засоби та алгоритми протидії негативним впливам, які виникають у результаті радіонавігаційних конфліктів, таких як глушіння сигналів, підробка даних (спуфінг) та інші види радіоелектронних атак.

Метою роботи є розробка, аналіз та оцінка методів протидії в радіонавігаційних конфліктах для забезпечення надійності роботи радіонавігаційних систем у цивільних та військових застосуваннях.

Для досягнення поставленої мети у роботі:

- проведено аналіз існуючих підходів протидії радіонавігаційним атакам;
- досліджено особливості побудови завадостійких навігаційних сигналів та методів їх захисту;
- обґрунтовано математичну модель аналізу радіо-завад.

Наукова новизна здобутих результатів полягає у розробці та обґрунтуванні комплексного багаторівневого підходу до протидії радіонавігаційним конфліктам, що інтегрує адаптивні алгоритми, засновані на машинному навчанні, мультидоменний аналіз сигналів та покращені методи сенсорного синтезу. Зокрема, запропоновані алгоритми фазового контролю та методи багаточастотного порівняння забезпечують підвищену ефективність виявлення та нейтралізації складних спуфінг-атак.

Галузь застосування. Запропоновані підходи можуть бути використані для створення надійних та захищених радіонавігаційних систем у різних сферах діяльності.

Ключові слова: радіонавігаційні конфлікти, глушіння сигналу, спуфінг, завадостійкість, навігаційні сигнали, адаптивні методи, радіочастотне середовище, протидія завадам, позиціонування, супутникова навігація.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DSA	–	Dynamic Spectral Adaptation
CR	–	Cognitive Radio
DSSS	–	Direct Sequence Spread Spectrum
OSNMA	–	Open Service Navigation Message Authentication
LMS	–	Least Mean Squares
MVDR	–	Minimum Variance Distortionless Response
LCMV	–	Linearly Constrained Minimum Variance
AoA	–	Angle of Arrival
MEMS	–	Мікроелектромеханічні сенсори
C/A code	–	Coarse Acquisition code
PDOP	–	Position Dilution of Precision
EKF	–	Extended Kalman Filter
ПЛІС	–	Програмовані логічні інтегральні схеми
РНС	–	Радіонавігаційні системи

ВСТУП

Актуальність теми. Сучасні радіонавігаційні системи відіграють критично важливу роль у забезпеченні точності та безпеки навігації в авіації, мореплавстві, автомобільному транспорті та військових операціях. Проте зростання залежності від цих систем створює нові виклики, пов'язані з їх уразливістю до радіонавігаційних конфліктів, таких як глушіння сигналів, підробка даних (спуфінг) та інші види радіоелектронного впливу. Умови сучасного інформаційного та кіберпростору обумовлюють необхідність розробки ефективних методів протидії, які здатні забезпечити безперебійну роботу навігаційних систем навіть за умов цілеспрямованих атак. Таким чином, дослідження методів протидії в радіонавігаційних конфліктах є актуальним і необхідним для підвищення стійкості радіонавігаційних систем та національної безпеки.

Метою роботи є розробка, аналіз та оцінка методів протидії в радіонавігаційних конфліктах для забезпечення надійності роботи радіонавігаційних систем у цивільних та військових застосуваннях.

Завдання роботи

1) виконати аналіз існуючих загроз радіонавігаційним системам, включаючи глушіння, спуфінг та інші види радіоелектронного впливу;

2) оцінити ефективність сучасних методів протидії радіонавігаційним конфліктам та виявити їхні сильні і слабкі сторони;

3) розробити нові підходи до виявлення і нейтралізації атак на радіонавігаційні системи, зокрема з використанням алгоритмів машинного навчання та адаптивних технологій;

4) виконати моделювання роботи радіонавігаційних систем за умов зовнішнього впливу для перевірки ефективності запропонованих методів;

5) оцінка ефективності процесу радіоподавлення в інформаційних конфліктах;

6) розробити рекомендації щодо вдосконалення засобів захисту радіонавігаційних систем в умовах радіонавігаційних конфліктів.

Об’єкт дослідження. Процеси та функціонування радіонавігаційних систем та в умовах радіонавігаційних конфліктів.

Предмет дослідження. Методи, засоби та алгоритми протидії негативним впливам, які виникають у результаті радіонавігаційних конфліктів, таких як глушіння сигналів, підробка даних (спуфінг) та інші види радіоелектронних атак.

Методи дослідження. У процесі дослідження використовувався **аналіз і синтез**, які дозволили детально вивчити існуючі загрози радіонавігаційним системам, зокрема глушіння сигналів та підробку даних, а також оцінити сучасні підходи до їх нейтралізації. Це сприяло виявленню сильних і слабких сторін існуючих методів захисту.

Математичне моделювання було застосовано для відтворення сценаріїв радіонавігаційних конфліктів, що дозволило оцінити ефективність запропонованих методів протидії у різних умовах. З використанням моделей були проведені розрахунки впливу атак на стабільність та точність роботи радіонавігаційних систем.

Методи теорії ймовірностей і статистики використовувалися для аналізу надійності функціонування радіонавігаційних систем в умовах цілеспрямованих радіоелектронних впливів. Ці методи також допомогли визначити імовірність успішного виявлення та нейтралізації атак.

Методи машинного навчання забезпечили розробку адаптивних алгоритмів, здатних автоматично виявляти та нейтралізувати радіонавігаційні загрози. Особлива увага приділялася побудові алгоритмів на основі аналізу великих даних, отриманих із сенсорів радіонавігаційних систем.

Загалом, були проведені експериментальні дослідження, які дозволили перевірити та оптимізувати ефективність запропонованих методів у реальних або моделюваних умовах. Результати експериментів підтвердили доцільність використання запропонованих рішень для підвищення стійкості радіонавігаційних систем до радіонавігаційних конфліктів.

Галузь застосування. Результати дослідження знаходять застосування у багатьох сферах, де радіонавігаційні системи відіграють ключову роль. У цивільній

авіації вони сприяють підвищенню безпеки польотів та точності навігації. У морському транспорті забезпечують безпечну навігацію суден, особливо в складних умовах. У військовій сфері результати роботи можуть використовуватися для захисту військових систем навігації, що є важливими для національної безпеки. У наземному транспорті вони підвищують надійність роботи супутникових систем навігації, включаючи автоматизовані транспортні засоби. У космічній галузі результати дослідження сприяють захисту орієнтації та управління космічними апаратами. Окрім цього, вони можуть бути застосовані для захисту інфраструктури критичного призначення, такої як енергетичні об’єкти та комунікаційні вузли, а також у комерційній логістиці, доставки та моніторингу вантажів, де навігаційні системи є основою точності та ефективності процесів.

Апробація результатів дипломної роботи. Основні положення роботи викладалися

1) в тезах доповіді на Всеукраїнській конференції молодих учених «Інформаційні технології», 15 травня 2025 року

2) в статті в журналі «Кібербезпека: освіта, наука, техніка», Том 4 №28 (2025)

НАУКОВЕ ДОСЛІДЖЕННЯ

У сучасних умовах зростання кількості радіонавігаційних систем призводить до підвищення рівня конфліктів у радіочастотному спектрі. Вплив таких конфліктів може проявлятися у вигляді інтерференції сигналів, втрати точності позиціонування та навіть повної втрати зв’язку. Проблема особливо актуальна для критично важливих сфер, таких як авіація, судноплавство, військові операції та автономний транспорт, де надійність навігації є ключовою вимогою.

Сучасні методи боротьби з перешкодами часто базуються на статичних підходах, які не враховують змінність середовища та неможливість швидкого адаптування до змінних умов. Саме тому актуальним є розробка методів, які забезпечують гнучке використання спектра, автоматичне виявлення перешкод і миттєве реагування на потенційні загрози.

Метою цього дослідження є розробка та аналіз методу Динамічного спектрального адаптування (DSA), який дозволяє навігаційним системам змінювати частотний діапазон та алгоритми модуляції сигналу залежно від поточної ситуації в радіочастотному середовищі.

Метод DSA базується на технології когнітивного радіо (CR), що дозволяє системі безперервно аналізувати радіочастотне середовище та в разі виявлення конфлікту або перешкод автоматично змінювати параметри передавання сигналу. Головна ідея цього підходу – використання штучного інтелекту та алгоритмів машинного навчання для аналізу перешкод та вибору оптимального рішення в режимі реального часу.

Основні механізми методу включають:

- Динамічний вибір частотного діапазону – автоматичне перемикання на вільні частоти, де рівень шуму та завад мінімальний;
- Адаптивну модуляцію сигналу – зміна схеми модуляції (наприклад, з BPSK на QPSK або OFDM) залежно від рівня шуму в каналі;
- Автоматичне коригування потужності передавання – збільшення або зменшення рівня потужності для зниження впливу перешкод;

- Інтелектуальне фільтрування та прогнозування загроз – використання машинного навчання для розпізнавання атак на основі історичних даних.

Розвиток технологій автономного транспорту, дронів, супутникових систем зв'язку та військових комплексів потребує підвищеної стійкості до навігаційних атак. Традиційні методи, такі як фільтрація сигналів або збільшення потужності передавачів, часто є недостатньо ефективними у боротьбі з навмисними атаками на навігаційні системи.

Метод DSA вирішує цю проблему шляхом впровадження принципу самоадаптації: замість того, щоб намагатися зменшити вплив перешкод, система їх активно аналізує та підлаштовує параметри сигналу для мінімізації їхнього впливу. Це особливо важливо у військових застосуваннях, де швидке реагування на глушіння або спуфінг може відігравати вирішальну роль у виконанні бойових завдань.

Крім того, у комерційній сфері, зокрема у цивільній авіації та автономних транспортних засобах, застосування DSA дозволить забезпечити більш стабільний зв'язок навіть у складних умовах, таких як щільна міська забудова або складні погодні умови.

Для перевірки ефективності методу DSA було розроблено серію комп'ютерних симуляцій у MATLAB та Simulink, а також випробувано програмно-конфігуровані радіосистеми (SDR – Software-Defined Radio).

У ході експериментів було створено сценарії із штучними перешкодами, такими як глушіння сигналу та атаки спуфінгу. Випробування показали, що метод DSA дозволяє знизити втрати сигналу на 60-80% порівняно з традиційними методами. Крім того, система реагувала на завади у середньому за 1,2 секунди, що приблизно у 5 разів швидше, ніж стандартні алгоритми адаптації.

Також була проведена оцінка енергоспоживання: використання DSA дозволило знизити витрати енергії на передачу сигналу в середньому на 30%, оскільки система автоматично оптимізувала рівень потужності передавання.

Метод Динамічного спектрального адаптування (DSA) має потенціал значно підвищити надійність навігаційних систем, зменшивши вплив зовнішніх перешкод

та атак. Очікується, що впровадження цього методу в сучасні GNSS-системи дозволить досягти таких результатів:

- Підвищення точності позиціонування на 20-40% у складних умовах;
- Покращення стійкості до атак спуфінгу та глушіння у 3-5 разів;
- Оптимізація використання частотного спектра та зменшення конфліктів між системами.

Подальші дослідження можуть зосередитися на вдосконаленні алгоритмів машинного навчання для ще більш ефективного прогнозування атак. Також перспективним напрямком є використання квантових технологій для підвищення точності визначення частотного спектра та розширення можливостей когнітивного аналізу радіочастотного середовища.

Метод DSA є перспективним рішенням для боротьби з радіонавігаційними конфліктами, оскільки дозволяє системам автоматично адаптуватися до змін у радіочастотному середовищі та швидко реагувати на загрози. Його головною перевагою є динамічне налаштування параметрів сигналу залежно від умов, що значно підвищує стійкість до перешкод.

Актуальність цього підходу обумовлена зростаючою кількістю загроз у вигляді навмисних атак на навігаційні системи та збільшенням навантаження на радіочастотний спектр. Впровадження DSA у військові, авіаційні та цивільні навігаційні системи дозволить значно підвищити безпеку та ефективність їхнього використання в майбутньому.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ПРОТИДІЇ В РАДІОНАВІГАЦІЙНИХ КОНФЛІКТАХ

1.1. Аналіз загроз та уразливостей у системах радіонавігації

Аналіз загроз та уразливостей у системах радіонавігації є важливою частиною дослідження безпеки таких систем, оскільки вони використовуються для визначення положення, орієнтації та часу, що є критично важливими для багатьох сучасних технологій, таких як авіація, морські судна, наземний транспорт, а також для військових і цивільних застосувань.

Загрози для таких систем можна розділити на кілька основних категорій. До фізичних загроз відносяться природні явища, такі як магнітні бурі і сонячні спалахи, які можуть призвести до порушення сигналів радіонавігаційних систем, особливо в космосі. Також існує загроза пошкодження інфраструктури систем, що може відбутися через стихійні лиха або технічні проблеми, зокрема пошкодження супутників або радіонавігаційних станцій.

Загрози з боку людини включають спотворення сигналу (jamming), коли спеціалізовані пристрої випромінюють радіосигнали, які перешкоджають нормальній роботі навігаційних систем, знижуючи точність позиціонування або блокуючи сигнал. Інша загроза — це глушіння сигналу (spoofing), коли зловмисники відправляють фальшиві навігаційні сигнали, що змушують отримувачів приймати неправдиві координати, що може призвести до катастрофічних наслідків. Також можливі атаки на інфраструктуру через злом і доступ до серверів або станцій, що керують і обробляють дані навігаційних систем.

Технічні загрози включають атаки на програмне забезпечення, яке керує або обробляє дані навігаційних систем, що може вплинути на точність або достовірність сигналів. Також можуть виникати уразливості в протоколах зв'язку, які використовуються для передачі навігаційних даних, що дозволяє маніпулювати або перехоплювати інформацію.

Уразливості можуть виникати через відсутність належної безпеки на різних етапах функціонування системи. Технічні уразливості включають низьку потужність сигналу, що робить системи уразливими до завад, а також обмежену кількість супутників, що може вплинути на точність та стабільність сигналу. Інтерференція між різними системами також може призводити до спотворення даних. Організаційні уразливості можуть включати неефективне управління доступом до даних, що дозволяє несанкціонований доступ, а також відсутність заходів для захисту від атак, таких як криптографія чи засоби виявлення атак.

Для захисту від цих загроз використовуються різні методи. Шифрування та автентифікація сигналів дозволяють забезпечити захист від перехоплення та підробки даних. Антени і фільтри використовуються для зниження впливу перешкод і покращення якості прийому сигналу. Системи виявлення вторгнень і моніторинг мереж допомагають виявити аномалії в навігаційних даних, що дає змогу вчасно вжити необхідних заходів. Крім того, регулярне оновлення програмного забезпечення та покращення стабільності сигналу через збільшення кількості супутників і точності їх орбіти є важливими заходами для забезпечення надійності навігаційних систем.

Загрози і уразливості систем радіонавігації можуть мати серйозні наслідки для безпеки, тому їхнє своєчасне виявлення та розробка методів захисту є критично важливими для збереження стабільності та точності роботи таких систем, що є необхідним для безпеки цивільних і військових операцій (табл. 1.1).

Таблиця 1.1

Основні загрози та уразливості в системах радіонавігації

Тип загрози/уразливості	Опис загрози	Приклади	Методи захисту
Фізичні загрози	Природні явища, які можуть вплинути на роботу навігаційних систем.	Магнітні бурі, сонячні спалахи	Використання засобів моніторингу та прогнозування природних явищ. Використання більш стійких технологій.
Пошкодження інфраструктури	Пошкодження супутників або наземних станцій через	Пошкодження супутників через технічні проблеми або стихійні лиха	Покращення технологій захисту від стихійних лих. Вибір надійних

	стихійні лиха або технічні проблеми.		матеріалів для інфраструктури.
Спотворення сигналу (Jamming)	Випромінювання радіосигналів, які перешкоджають нормальній роботі навігаційних систем.	Використання глушилок, що блокує або спотворює сигнал	Встановлення фільтрів для боротьби з перешкодами, використання складних кодів для сигналів.
Глушіння сигналу (Spoofing)	Відправка фальшивих навігаційних сигналів, що змушують пристрої використовувати неправильні координати.	Фальшиві сигнали GPS, підробка часу та координат	Використання шифрування сигналів, автентифікація користувачів та пристроїв.
Атаки на програмне забезпечення	Атаки, спрямовані на порушення роботи програмного забезпечення, що обробляє навігаційні дані.	Злом серверів управління, пошкодження даних	Регулярні оновлення програмного забезпечення, посилена кібербезпека.
Уразливості в протоколах зв'язку	Уразливості у протоколах зв'язку, що використовуються для передачі навігаційних даних.	Перехоплення та маніпуляції з даними	Використання криптографії для шифрування даних, застосування протоколів з підвищеною безпекою.
Низька потужність сигналу	Сигнали низької потужності можуть бути легко пригнічені або спотворені.	Проблеми з якістю сигналу на великих відстанях	Покращення потужності сигналу, встановлення додаткових станцій для підвищення стабільності.
Обмежена кількість супутників	Недостатня кількість супутників або їхня неправильна орбіта може вплинути на точність сигналу.	Система GPS з недостатньою кількістю супутників	Розширення супутникових груп, оновлення орбіт супутників, створення резервних станцій.
Інтерференція між системами	Перешкоди між різними радіонавігаційними системами можуть призвести до спотворення даних.	Перешкоди між GPS і GLONASS	Використання спеціальних фільтрів для усунення перешкод між різними системами.
Неефективне управління доступом	Відсутність належної авторизації та аутентифікації користувачів навігаційних систем.	Несанкціонований доступ до даних навігаційних систем	Впровадження багаторівневої авторизації та аутентифікації користувачів, використання цифрових підписів.

Загальний висновок щодо аналізу загроз та уразливостей у системах радіонавігації свідчить про їх критичну важливість для забезпечення безпеки і стабільності багатьох сучасних технологій, зокрема в авіації, морських перевезеннях, наземному транспорті та військових операціях. Системи радіонавігації, такі як GPS, GLONASS, Galileo та інші, піддаються різноманітним загрозам, що можуть виникати як через природні фактори (наприклад, магнітні бурі), так і через технічні та людські фактори (зловмисні атаки, пошкодження інфраструктури, спотворення сигналу).

Основними уразливостями є недостатня потужність сигналу, обмежена кількість супутників, а також потенційні проблеми з безпекою програмного забезпечення і протоколів зв'язку. Злочинці можуть використовувати методи глушіння та підробки сигналів, що становить серйозну загрозу для точності та надійності навігаційних даних.

Для ефективного захисту від таких загроз важливо застосовувати технології шифрування, автентифікації, а також вдосконалювати апаратне і програмне забезпечення систем радіонавігації. Оновлення і покращення супутникових угруповань, встановлення додаткових станцій для підвищення стабільності сигналу та використання фільтрів для зменшення перешкод між різними системами є необхідними кроками для забезпечення надійності цих систем.

Отже, розвиток і підтримка безпеки радіонавігаційних систем є ключовим аспектом для запобігання можливим катастрофам і забезпечення точності та стабільності навігації в різних галузях.

1.2. Порівняння існуючих методів протидії радіонавігаційним конфліктам

Порівняння існуючих методів протидії радіонавігаційним конфліктам є важливим аспектом для забезпечення безпеки та стабільності в навігаційних системах, оскільки радіонавігаційні системи, як-от GPS, GLONASS, Galileo та інші, є вразливими до різноманітних атак, зокрема до глушіння сигналу (jamming) та підробки сигналу (spoofing). Ці методи протидії спрямовані на зниження ризику

маніпуляцій з навігаційними даними і забезпечення стабільної та точної роботи навігаційних систем.[31].

Методи захисту від глушіння сигналу (jamming) є важливою складовою безпеки навігаційних систем, оскільки глушіння може суттєво порушити роботу радіонавігаційних систем, таких як GPS, GLONASS та інші. Глушіння сигналу відбувається, коли зловмисники випромінюють потужні радіосигнали, які перешкоджають нормальному прийому корисного сигналу, що призводить до втрати точності навігації або навіть повної втрати сигналу.

Один із основних методів протидії глушінню сигналу — це фільтрація сигналу. Цей метод включає використання спеціальних фільтрів, які дозволяють системі виділяти корисний сигнал серед перешкод. Фільтрація сигналу може здійснюватися на рівні приймача, де відбувається відбір корисного сигналу на основі певних характеристик, таких як частота, фаза або амплітуда сигналу. Це дає можливість зберігати працездатність системи навіть у присутності сторонніх сигналів, що значно покращує точність навігації. Однак, фільтрація може бути неефективною, якщо джерело глушіння має значно потужніший сигнал або працює на широкому спектрі частот.

Іншим методом захисту є використання мультичастотних систем. Оскільки глушіння часто здійснюється на одній частоті, використання кількох частот для передачі сигналу дозволяє підвищити надійність навігаційної системи. Якщо один канал заблоковано або перешкоджено, інші частоти можуть продовжувати працювати і забезпечувати точне позиціонування. Мультичастотні навігаційні системи використовуються в таких сучасних технологіях, як GPS, що має кілька частотних каналів для цивільних та військових користувачів. Цей підхід підвищує стійкість системи до глушіння, але також вимагає додаткових витрат на інфраструктуру і спектр радіочастот.

Ще одним важливим методом є використання резервних навігаційних каналів. Це передбачає наявність додаткових, менш уразливих каналів для передачі навігаційних даних. У разі, якщо основний канал зазнає перешкод, система автоматично переходить на резервний канал, що дозволяє забезпечити

безперервність навігаційних даних. Резервні канали можуть включати, наприклад, додаткові супутники або спеціалізовані наземні станції, які допомагають підтримувати точність і надійність сигналу навіть у разі глушіння.

Важливим аспектом є використання адаптивних алгоритмів і автоматичного коригування. Ці алгоритми дозволяють системам радіонавігації автоматично реагувати на зміну умов і коригувати свої параметри для компенсації впливу перешкод. Наприклад, система може автоматично налаштовувати потужність сигналу або змінювати частоту передачі, щоб зменшити вплив глушіння. Адаптивні методи можуть бути особливо корисними в умовах інтенсивних перешкод або в місцях, де вплив глушіння змінюється в часі та просторі.

Загалом, комбінування різних методів захисту від глушіння сигналу дозволяє підвищити стійкість радіонавігаційних систем до зовнішніх атак, забезпечуючи більш високий рівень надійності та точності. Однак для ефективного захисту необхідно постійно вдосконалювати технічні засоби та алгоритми, щоб враховувати нові типи загроз та адаптуватися до змінюваних умов навколишнього середовища.

Методи захисту від підробки сигналу (spoofing) є критично важливими для забезпечення безпеки навігаційних систем, таких як GPS, GLONASS, Galileo та інші. Підробка сигналу відбувається, коли зловмисники надсилають фальшиві навігаційні сигнали, змушуючи приймачі приймати невірні координати або час. Це може мати серйозні наслідки, такі як зміна курсу суден чи літаків, викрадення транспортних засобів або навіть аварії. Одним з основних методів захисту є криптографія, яка включає шифрування навігаційних сигналів і автентифікацію для підтвердження їхнього походження. Для цього використовуються цифрові підписи або коди автентифікації, які дозволяють приймачам перевірити, чи є сигнал справжнім. Якщо зловмисники намагаються підробити сигнал, вони не зможуть створити правильний криптографічний код, що свідчить про фальшивість сигналу [35; 39; 41].

Іншим методом є використання часових міток. Кожен навігаційний сигнал має вбудовану часову мітку, яка вказує точний час передачі сигналу. Приймач може перевірити, чи відповідає отриманий сигнал зазначеному часу. Якщо сигнал

затриманий або модифікований, система може виявити підробку. Часові мітки дозволяють покращити автентифікацію сигналів і запобігти їхній фальсифікації, оскільки будь-яка затримка або зміна часу може бути ознакою маніпуляцій.

Ще одним методом є багатофакторна автентифікація, яка передбачає перевірку сигналів через кілька незалежних каналів або факторів. Наприклад, система може використовувати дані не тільки з навігаційних супутників, але й з інших джерел, таких як інерціальні сенсори (акселерометри, гіроскопи), що дають інформацію про прискорення та орієнтацію об'єкта. Це дозволяє підвищити точність автентифікації та знижує ймовірність підробки сигналів, оскільки зловмисник повинен підробити не тільки сам сигнал, а й дані з інших джерел.

Методи моніторингу та виявлення аномалій також є важливим компонентом захисту. Системи моніторингу постійно відслідковують навігаційні сигнали і шукають будь-які відхилення від нормальних параметрів, що можуть вказувати на підробку сигналу. Алгоритми виявлення аномалій можуть порівнювати отримані дані з різних джерел, щоб виявити невідповідності, які є характерними для фальшивих сигналів. Це дозволяє системі вчасно реагувати на можливі атаки.

Використання альтернативних навігаційних систем, таких як інерціальні навігаційні системи (INS), є ще одним методом захисту від підробки сигналів. Ці системи дозволяють вимірювати переміщення без необхідності постійного підключення до супутників. Інерціальні сенсори, такі як акселерометри та гіроскопи, можуть допомогти у визначенні положення об'єкта без використання зовнішніх навігаційних сигналів, що робить систему більш стійкою до підробки.

Загалом, комбінування різних методів захисту дозволяє значно підвищити надійність навігаційних систем і знизити ризик підробки сигналів. Використання криптографії, багатофакторної автентифікації, моніторингу аномалій та альтернативних навігаційних джерел є ефективними заходами для забезпечення безпеки та стабільності роботи навігаційних систем.

Таблиця 1.2

Основні методи захисту від підробки сигналу (spoofing) в радіонавігаційних системах

Метод захисту	Опис	Переваги	Недоліки

Криптографія	Використання шифрування і цифрових підписів для автентифікації сигналів.	Високий рівень захисту, гарантія автентичності сигналу.	Потребує великих обчислювальних ресурсів, може сповільнювати систему.
Часові мітки	Вбудовування в сигнал часової мітки, що вказує точний час передачі сигналу.	Простота в реалізації, дозволяє виявити затримку сигналу.	Може виникнути проблема з точністю часу, якщо джерело часу ненадійне.
Багатофакторна автентифікація	Перевірка сигналів через кілька незалежних каналів, таких як інерціальні сенсори.	Підвищена точність і надійність, знижує ймовірність підробки.	Складність у реалізації та потреба в додаткових сенсорах.
Моніторинг і виявлення аномалій	Постійний моніторинг навігаційних сигналів та виявлення відхилень від норм.	Виявлення підробки в реальному часі, швидка реакція на загрози.	Можливість помилкових спрацьовувань, технічні проблеми з моніторингом.
Альтернативні навігаційні системи	Використання інерціальних навігаційних систем (INS) для визначення положення без супутникових сигналів.	Знижує залежність від одного джерела сигналу, підвищує стійкість до атак.	Може бути менш точним на великих відстанях без корекції сигналу.

Методи моніторингу та виявлення аномалій є важливими складовими систем безпеки радіонавігаційних систем, таких як GPS, GLONASS та інших. Вони дозволяють виявляти підозрілі або незвичайні зміни в навігаційних сигналах, що можуть вказувати на спроби підробки сигналів (spoofing) або інших атак, таких як глушіння (jamming). Системи моніторингу здійснюють постійний аналіз навігаційних даних і порівнюють їх із нормальними значеннями, щоб виявити будь-які відхилення або аномалії, які можуть бути ознакою маніпуляцій з сигналами. Алгоритми виявлення аномалій можуть враховувати різноманітні

параметри сигналу, такі як частота, амплітуда, час прийому та координати, що дозволяє швидко виявляти підроблені або неправдиві дані.

Одним із основних підходів є порівняння даних з різних джерел. Наприклад, приймач може отримувати сигнали від кількох супутників або використовувати додаткові навігаційні джерела (наприклад, інерціальні навігаційні системи або земні станції) для перевірки точності координат. Якщо дані з різних джерел значно відрізняються, це є підставою для підозри на підробку сигналу. Існують також методи статистичного аналізу для виявлення аномалій, коли сигнал, що перевищує певний поріг або відхиляється від очікуваних параметрів, відправляється на додаткову перевірку або блокування. Крім того, для підвищення ефективності таких систем можуть використовуватися методи машинного навчання, зокрема нейронні мережі, які можуть вивчати патерни звичайних навігаційних сигналів і виявляти нові типи атак або аномалій, що раніше не були зафіксовані.

Використання систем моніторингу та виявлення аномалій дозволяє значно підвищити безпеку радіонавігаційних систем, оскільки вони надають можливість виявляти і реагувати на загрози в реальному часі. Однак ці системи не є бездоганними: вони можуть спрацьовувати помилково в разі змін у зовнішніх умовах (наприклад, технічні неполадки або зміни в роботі супутників), тому важливо поєднувати їх із іншими методами захисту для досягнення максимального ефекту.

Таблиця 1.3

Основні методи моніторингу та виявлення аномалій в радіонавігаційних системах

Метод моніторингу	Опис	Переваги	Недоліки
Порівняння даних з різних джерел	Використання кількох джерел навігаційних сигналів для перевірки їхньої відповідності.	Підвищує точність і надійність виявлення підроблених сигналів.	Потребує додаткових сенсорів і джерел, що може збільшити витрати.
Статистичний аналіз сигналів	Аналіз параметрів сигналів (частота, амплітуда, час) для виявлення аномалій.	Швидке виявлення відхилень від нормальних параметрів сигналу.	Може призвести до помилкових спрацьовувань при незначних змінах.
Методи машинного навчання	Використання алгоритмів, таких як нейронні мережі, для виявлення нових типів аномалій.	Може виявляти нові загрози, не відомі раніше.	Потребує великої кількості даних для навчання і складної реалізації.
Аналіз часових міток	Порівняння часу, вказаного в сигналу, з часом, коли сигнал був отриманий.	Легко інтегрується в існуючі системи, допомагає виявити затримки сигналу.	Може бути уразливим до маніпуляцій з часом при недостатньо точному джерелі часу.
Виявлення аномалій за допомогою порогових значень	Встановлення порогів для різних параметрів сигналу, перевищення яких сигналізує про аномалію.	Простота в реалізації та налаштуванні.	Може не виявляти більш складні форми атак, якщо пороги встановлені неправильно.

Порівняння методів моніторингу та виявлення аномалій у радіонавігаційних системах є важливим для вибору найбільш ефективних підходів у забезпеченні безпеки та точності навігаційних даних. Кожен метод має свої особливості, переваги та недоліки, що визначають його застосування в конкретних умовах.

Порівняння даних з різних джерел — це метод, який використовує дані від кількох незалежних навігаційних джерел (наприклад, супутникові системи, інерціальні сенсори та наземні станції) для перевірки відповідності отриманих сигналів. Цей метод дозволяє підвищити точність і надійність системи, оскільки зловмисник повинен підробити або змінити дані з кількох різних джерел, що значно ускладнює атаку. Проте, для його ефективного впровадження потрібна складна інфраструктура та додаткові сенсори, що може призвести до збільшення витрат на реалізацію і обслуговування системи.

Статистичний аналіз сигналів — це метод, при якому системи моніторингу аналізують параметри сигналів, такі як частота, амплітуда, час прийому і інші характеристики, для виявлення аномалій. Якщо сигнал відхиляється від звичних параметрів, це може бути ознакою підробки. Основною перевагою цього методу є його швидка реакція на зміни в сигналах і можливість виявлення порушень на ранніх стадіях. Однак він може призвести до помилкових спрацьовувань у разі невеликих або незначних змін у навколишньому середовищі, таких як зміни в погодних умовах або технічні неполадки, що знижує його точність.

Методи машинного навчання представляють собою використання алгоритмів, зокрема нейронних мереж, для аналізу великих обсягів даних і виявлення нових типів аномалій, які можуть не бути зафіксовані традиційними методами. Алгоритми машинного навчання здатні адаптуватися до нових загроз і можуть виявляти неочевидні маніпуляції з сигналами. Цей підхід має значний потенціал для виявлення складних і нових типів атак, однак він потребує великої кількості даних для навчання моделей та складної реалізації, що може бути ресурсозатратним.

Аналіз часових міток є простим, але ефективним методом, який полягає в перевірці часових міток у сигналах, щоб визначити, чи відповідає час отриманого

сигналу часу, зазначеному в самому сигналі. Це дозволяє виявити затримки або модифікації сигналів, що можуть бути ознаками їх підробки. Цей метод легко інтегрується в існуючі навігаційні системи і є ефективним для виявлення підробки, пов'язаної з затримкою сигналу. Однак він може бути уразливим до маніпуляцій з часом, якщо система не має надійного джерела часу або використовується ненадійне обладнання для синхронізації.

Виявлення аномалій за допомогою порогових значень передбачає встановлення порогів для різних параметрів сигналу (наприклад, амплітуда або частота), перевищення яких сигналізує про можливу аномалію. Це дозволяє швидко виявляти значні відхилення від звичайних параметрів. Простота в реалізації і налаштуванні є головною перевагою цього методу. Однак він може не враховувати більш складні форми атак або підробок, які не перевищують встановлені пороги, що обмежує його ефективність у складних ситуаціях.

Загалом, кожен з методів має свої сильні та слабкі сторони, і їхня ефективність залежить від специфіки завдання та умов експлуатації. Комбінація кількох підходів може забезпечити більш надійний захист від підробки сигналів і підвищити стійкість радіонавігаційних систем до зовнішніх загроз.

Порівняння існуючих методів протидії радіонавігаційним конфліктам показує, що забезпечення безпеки та стабільності радіонавігаційних систем потребує комплексного підходу, оскільки ці системи, такі як GPS, GLONASS, Galileo та інші, є вразливими до різноманітних атак, зокрема глушіння сигналу (jamming) та підробки сигналу (spoofing). Для ефективного захисту від глушіння сигналу застосовуються методи, як-от фільтрація сигналу, мультичастотні системи, використання резервних навігаційних каналів та адаптивні алгоритми, що дозволяють підвищити стійкість системи до зовнішніх атак, забезпечуючи більш високий рівень надійності та точності. Однак кожен метод має свої переваги та недоліки, і їх ефективність залежить від конкретних умов і типу загрози.

Методи захисту від підробки сигналу, такі як криптографія, багатофакторна автентифікація, використання часових міток та альтернативних навігаційних систем, також грають ключову роль у забезпеченні безпеки навігаційних даних. Ці

методи дозволяють не лише виявляти підроблені сигнали, але й підвищують загальну стійкість системи до спроб маніпуляцій з навігаційними даними. Важливим аспектом є інтеграція різних підходів, що дозволяє створити більш ефективну систему захисту.

Методи моніторингу та виявлення аномалій, такі як порівняння даних з різних джерел, статистичний аналіз сигналів, методи машинного навчання та порогові значення, забезпечують постійний контроль над станом навігаційних сигналів і здатні виявляти навіть нові, раніше невідомі загрози. Комбінація цих методів дозволяє забезпечити ефективну протидію як традиційним, так і новим типам атак.

Загалом, для досягнення максимального рівня безпеки та стабільності в радіонавігаційних системах необхідно використовувати комплексне поєднання різних методів захисту, що дозволяє підвищити надійність систем і забезпечити їх стабільну роботу в умовах сучасних загроз.

1.3. Формалізація задачі протидії в радіонавігаційних конфліктах

Формалізація задачі протидії в радіонавігаційних конфліктах полягає в розробці математичних моделей та алгоритмів для виявлення, оцінки та реагування на загрози, пов'язані з глушінням сигналів (jamming) і підробкою сигналів (spoofing) в радіонавігаційних системах. Оскільки ці системи є вразливими до атак, таких як перешкоджання нормальному прийому сигналу або надання хибних даних, формалізація задачі дозволяє розробити ефективні методи захисту, які знижують ймовірність успішної атаки і забезпечують безперебійну роботу системи.

Першим етапом є моделювання глушіння сигналу. Глушіння сигналу можна представити як зовнішній вплив, який порушує нормальне функціонування радіонавігаційної системи. У математичному плані, глушіння може бути описано як потужне радіоперешкода, що накладається на корисний сигнал. Тому, задача протидії глушінню передбачає розробку методів фільтрації або мультичастотного прийому, що дозволяють системі ефективно відновлювати сигнал навіть при наявності сильних перешкод. Математично це можна описати через алгоритми

спектрального аналізу і адаптивні фільтри, які дозволяють відокремлювати корисний сигнал від шуму.

Другим етапом є моделювання підробки сигналу. Підробка сигналу, або spoofing, відбувається, коли зловмисники надсилають фальшиві навігаційні сигнали, що змушують систему прийняти неправдиві координати. Для математичної формалізації цієї задачі важливо створити модель, яка включає в себе параметри навігаційних сигналів (координати, час, частота, амплітуда), а також методи перевірки автентичності сигналу. Оскільки підробка сигналу може включати маніпуляцію з часовими мітками або координатами, задача протидії включає в себе розробку криптографічних методів, таких як цифрові підписи, для автентифікації сигналу. Алгоритм верифікації сигналу може базуватися на порівнянні отриманих даних із заздалегідь відомими або очікуваними параметрами сигналу, що дозволяє виявити невідповідності.

Математична формалізація задачі також включає в себе побудову моделей для оцінки ймовірності атаки на систему. Це може бути виконано через теорію ймовірностей та статистичні методи, що дозволяють оцінити ризики вразливості системи до певних типів атак, таких як точкові атаки або атаки на всі канали одночасно. Оцінка ризику є важливою частиною формалізації задачі, оскільки вона дає змогу визначити, які методи захисту є найбільш ефективними в кожному конкретному випадку.

Крім того, важливою частиною формалізації є розробка стратегій адаптації системи. Задача протидії в радіонавігаційних конфліктах повинна враховувати зміни в умовах навколишнього середовища, такі як зміни в характеристиках сигналу або нові види атак. Оскільки атаки можуть змінювати свої тактики з часом, необхідно розробити алгоритми, які дозволяють системі адаптувати свої параметри (наприклад, змінювати частоту передачі або потужність сигналу), щоб зберегти стійкість до атак.

Алгоритми адаптації можуть включати в себе методи машинного навчання або статистичні методи для постійного моніторингу і вдосконалення системи. Це дозволяє створити динамічну систему, здатну реагувати на нові загрози в

реальному часі, а також знижувати ймовірність несанкціонованого доступу або маніпуляцій з навігаційними даними.

Таким чином, формалізація задачі протидії радіонавігаційним конфліктам включає в себе створення математичних моделей для оцінки загроз, розробку алгоритмів фільтрації і верифікації сигналів, а також побудову стратегій адаптації системи. Усі ці елементи разом створюють основу для надійного захисту радіонавігаційних систем від атак, забезпечуючи їх стабільну і безпечну роботу в умовах сучасних загроз.

Висновки до першого розділу

Проблема радіонавігаційних конфліктів є однією з найактуальніших загроз для сучасних глобальних навігаційних супутникових систем. Зростання доступності та потужності засобів радіоелектронної боротьби створює серйозні ризики для надійності та точності позиціонування, навігації та синхронізації часу, що має критичне значення для багатьох секторів економіки, транспорту, оборони та суспільства загалом.

Сучасні аерокосмічні засоби нападу дальньої дії на завершальному етапі польоту широко використовують автономні засоби навігації та наведення. Такі засоби працюють у різних діапазонах частот, застосовують різні фізичні принципи вимірювання одних і тих самих параметрів, що суттєво підвищує ймовірність виконання цільового завдання. Бурхливий розвиток супутникових радіонавігаційних систем призвів до включення наданої ними високоякісної інформації в контур наведення, тому точність визначення місцеположення й якість управління помітно зростають. Для підвищення ефективності функціонування радіотехнічних та оптико-електронних пристроїв на засобах нападу встановлюються пристрої захисту від завад різного характеру, в тому числі спеціально створених. За таких умов необхідно вживати всіх можливих заходів для зменшення ризику ураження власних об'єктів.

Spoofing-завади становлять серйозну небезпеку для навігаційної апаратури СРНС, оскільки вони можуть не тільки призводити до виникнення великих помилок при визначенні місця розташування, а й до перехоплення управління роботизованими комплексами за рахунок створення хибного навігаційного поля.

Напрямки сучасних досліджень підтверджують необхідність подальшого розвитку методів ефективного виявлення та протидії подавленню навігаційних сигналів. Частина робіт спрямована на вдосконалення як конструктивної частини CRPA, так і її функціональних алгоритмів.

Проведене дослідження показало, що методи протидії в радіонавігаційних конфліктах розвиваються шляхом об'єднання апаратних і програмних рішень. Апаратні методи, такі як адаптивні антенні решітки і антени з нульовим променем, демонструють високу ефективність у нейтралізації впливу навмисних завад на фізичному рівні, дозволяючи приймачам функціонувати навіть в умовах сильного подавлення.

Перспективним напрямком є застосування методів машинного навчання і штучного інтелекту для автоматичного виявлення, класифікації і протидії різноманітним типам завад, включаючи складні та раніше невідомі атаки.

РОЗДІЛ 2. ОСОБЛИВОСТІ ПОШУКУ ТА РОЗРОБКИ МЕТОДІВ ПРОТИДІЇ В РАДІОНАВІГАЦІЙНИХ СИСТЕМАХ

2.1. Характеристика основних методів захисту радіонавігаційних сигналів

У сучасному середовищі експлуатації радіонавігаційних систем (РНС) виникає необхідність розробки ефективних заходів щодо забезпечення захисту переданих сигналів від різноманітних завад, насамперед навмисного походження. З-поміж таких загроз особливо небезпечними є радіоперешкоди (глушіння) та підміна сигналів (spoofing), які можуть призвести до порушення точності позиціонування, втрати синхронізації чи повної дезорганізації навігаційного процесу. Головним завданням систем захисту в РНС є гарантування достовірності переданої інформації, а також забезпечення безперервності її отримання, зокрема в умовах електромагнітного протиборства.

Одним із фундаментальних технічних засобів забезпечення стійкості сигналів у сучасних радіонавігаційних системах, особливо в умовах радіоелектронної боротьби, є застосування технології розширення спектра сигналу за допомогою псевдовипадкових шумових послідовностей. Суть цього підходу полягає в тому, що інформаційний сигнал модулюється спеціальним кодом, який за своїми статистичними характеристиками наближається до шуму. Такий код — псевдовипадкова послідовність (ПВП) — має властивість великої довжини і хороших кореляційних властивостей, що дозволяє значно розширити спектр переданого сигналу, зменшуючи при цьому щільність його спектральної енергії [10; 11; 13].

У результаті спектральна щільність потужності такого сигналу настільки знижується, що він стає практично нерозрізненним на фоні природних або штучних шумів для стороннього спостерігача. Проте легкість виявлення сигналу не єдина перевага — також ускладнюється процес його глушіння за допомогою генераторів перешкод, які працюють у вузьких або широких діапазонах. Глушіння сигналу з розширеним спектром потребує від противника або точного знання структури ПВП,

або значно потужнішого широкосмугового генератора перешкод, що вимагає відповідних енергетичних ресурсів і високого рівня технічного забезпечення [15; 19].

Модуляція несучої частоти сигналу за допомогою ПВП призводить до того, що для невтаємниченого приймача сигнал виглядає як звичайний шумовий фон. Проте на боці легітимного користувача, в приймальному пристрої, реалізується механізм синхронізації з відповідною ПВП. Така синхронізація дає змогу демодулювати сигнал і відновити первинну інформацію. Цей принцип лежить в основі методів прямого розширення спектра (Direct Sequence Spread Spectrum, DSSS), які активно використовуються у системах GPS, Galileo та інших глобальних навігаційних супутникових системах (GNSS) [11; 12; 14].

Наявність ПВП дозволяє також реалізовувати додаткові переваги, пов’язані із захистом від спуфінгу (навмисного введення хибних навігаційних даних) та забезпечення автентифікації сигналу. Адже тільки приймач, який має точну копію ПВП, здатний коректно синхронізуватися та декодувати інформацію. У цьому контексті псевдовипадковість є не лише методом маскування, але й засобом криптографічного захисту навігаційного сигналу [17].

Таким чином, застосування сигналів із розширеним спектром є одним з ключових інструментів у забезпеченні завадозахищеності та конфіденційності передачі навігаційної інформації. Це надзвичайно важливо в умовах сучасних конфліктів, де протидія навігації є невід’ємною складовою радіоелектронної боротьби. Тому включення таких технологій до архітектури радіонавігаційних систем є необхідною вимогою для підвищення їх стійкості до перешкод, виявлення та навмисного впливу [1; 2; 4; 9; 16].

У межах забезпечення надійності та безпеки функціонування сучасних радіонавігаційних систем, зокрема в умовах радіоелектронної боротьби, одним із ключових напрямів є використання методів кодового шифрування навігаційних сигналів. Сутність цього підходу полягає у впровадженні криптографічних алгоритмів на етапі генерації, передавання та приймання сигналу, що забезпечує високий рівень захисту від несанкціонованого доступу. У такий спосіб

створюються умови, за яких отримання або модифікація навігаційних даних стороннім приймачем без наявності відповідного ключа стає практично неможливим. Такий метод шифрування значно ускладнює здійснення підміни сигналу (спуфінгу), що є одним із найнебезпечніших видів атак у сфері супутникової навігації [10; 15].

Яскравим прикладом реалізації цього підходу є застосування у військових сегментах системи GPS спеціальних сигналів типу P(Y)-code, які мають складну структуру та передаються із застосуванням криптографічного захисту. Ці сигнали недоступні для цивільних користувачів і вимагають наявності закритого ключа, відомого лише обмеженому колу уповноважених приймачів. Такий механізм забезпечує не тільки шифрування, але й контроль доступу, підвищуючи рівень операційної безпеки [13; 21]. Згідно з аналізом, наведеним у [11], криптографічне шифрування є базовим елементом усіх сучасних стратегій захисту GNSS проти навмисних втручань.

Окрім цього, шифрування створює передумови для впровадження механізмів автентифікації навігаційних сигналів, які дають змогу перевіряти справжність джерела сигналу та виявляти можливу підміну. Алгоритмічна автентифікація, за словами Т. Гамфріса, дає змогу ідентифікувати зовнішній вплив навіть тоді, коли структура підробленого сигналу точно імітує справжній [17]. Цей принцип реалізується за допомогою спеціальних підписів або таймштампів, що дозволяють приймачеві встановити достовірність джерела. Такі підходи є фундаментом для побудови систем з високим рівнем стійкості до атак типу «спуфінг» та «відкладене повторення», що мають критичне значення в умовах радіонавігаційних конфліктів [15; 16].

Варто зазначити, що, хоча більшість цивільних GNSS-систем на сьогодні все ще обмежено застосовують автентифікацію, новітні проєкти, зокрема європейська Galileo, вже реалізують відкриті сервіси автентифікації сигналу (Open Service Navigation Message Authentication — OSNMA), що базуються на криптографічному підтвердженні. Це свідчить про загальну тенденцію до впровадження методів

інформаційної безпеки як стандарту навіть у відкритих навігаційних платформах [18; 22].

З огляду на викладене, можна зробити висновок, що методи кодового шифрування та алгоритмічної автентифікації сигналів мають ключове значення у сфері протидії загрозам радіонавігаційного впливу. Їх ефективне застосування дозволяє забезпечити цілісність, достовірність та конфіденційність навігаційної інформації навіть в умовах високої радіоелектронної активності, що є критично важливим для військових, спеціальних та деяких цивільних застосувань [2; 4; 14].

Частотне рознесення сигналів є одним із ключових інженерних підходів у забезпеченні стійкості радіонавігаційних систем до дії перешкод. Суть цього методу полягає у використанні кількох незалежних частотних каналів для передавання навігаційної інформації. Такий підхід істотно зменшує ризики втрати сигналу внаслідок дії вузькосмугових завад або навмисного глушіння. З технічної точки зору, кожен із каналів має власну несучу частоту, що дозволяє апаратурі приймача одночасно обробляти сигнали з різних частотних діапазонів. У разі, якщо одна з частот буде піддана перешкодам, інші канали залишаються доступними для приймання, що забезпечує безперервність та надійність навігаційного процесу [2; 4].

Особливе значення цей принцип має в умовах радіонавігаційних конфліктів, коли зловмисники можуть цілеспрямовано подавати завади на певні частоти. За умови одночастотної передачі це може призвести до повної втрати сигналу, а отже — й до зупинки навігаційного сервісу. У випадку мультичастотної архітектури, яку реалізовано у новітніх системах, таких як Galileo або GPS III, такий вплив значно ускладнюється. Наприклад, у системі Galileo передача сигналів відбувається на частотах E1, E5a, E5b і E6, тоді як GPS III використовує частоти L1, L2 та L5 [4; 10; 11; 24; 26; 27]. Це не лише ускладнює задачу потенційного порушника, а й підвищує загальну стійкість до інтерференції, спуфінгу та джемінгу.

Крім того, частотне рознесення сприяє поліпшенню точності позиціювання. Це пов’язано з тим, що затримки в атмосферних шарах (зокрема, іоносфері) мають різну величину на різних частотах. За допомогою алгоритмів диференціального

аналізу (dual-frequency correction) можливо компенсувати ці похибки, отримуючи більш точні координати [1; 2; 14]. У науковій та технічній літературі також підкреслюється, що мультичастотна обробка значно підвищує надійність фазових вимірювань, що є критично важливим для систем високоточного позиціювання, наприклад у геодезії або навігації безпілотних систем [6; 14; 19].

Нарешті, варто зазначити, що запровадження мультичастотного мовлення — це не лише відповідь на загрози електронного протиборства, а й результат еволюції радіонавігаційних систем, орієнтованої на інтеграцію з іншими навігаційними технологіями, такими як інерціальні системи, лазерні далекоміри чи візуальна навігація. У підсумку, частотне рознесення є невід'ємним елементом архітектури сучасних GNSS-систем і важливим інструментом протидії викликам радіонавігаційних конфліктів [15; 16; 20].

Особливої уваги в контексті забезпечення стійкості до завад у радіонавігаційних системах заслуговує застосування адаптивних антенних решіток, які функціонують на принципі просторової фільтрації. Ця технологія передбачає динамічне регулювання діаграми спрямованості антенного масиву таким чином, щоб у напрямках джерел завад формувались нулі діаграми спрямованості. Це означає, що рівень чутливості антени у цих напрямках мінімізується, що своєю чергою дозволяє ефективно придушити вплив потужних локальних перешкод.

Такий підхід дає змогу значною мірою зберігати якість прийому корисного сигналу навіть у складному електромагнітному середовищі, характерному для сценаріїв радіонавігаційних конфліктів. Адаптивна просторово-часова обробка сигналів дозволяє враховувати як геометрію просторового розміщення джерел сигналів і перешкод, так і їх часові характеристики. Особливо ефективною ця технологія стає у поєднанні з фазованими антенними решітками, які забезпечують гнучке електронне сканування без механічного переміщення елементів конструкції [5; 9].

Адаптивні антени використовують спеціальні алгоритми цифрової обробки сигналів (ЦОС), серед яких найпоширенішими є алгоритми на основі мінімізації середньої квадратичної похибки (наприклад, LMS — Least Mean Squares) або

максимізації співвідношення сигнал/шум (MVDR — Minimum Variance Distortionless Response). Завдяки цим алгоритмам система здатна в реальному часі адаптувати параметри вагових коефіцієнтів антенних елементів відповідно до змін у радіочастотному середовищі. Це дозволяє не лише ефективно пригнічувати як фіксовані, так і рухомі джерела перешкод, але й динамічно реагувати на спуфінгові атаки та спроби радіоелектронного придушення [9; 15; 19].

У практичному аспекті реалізація адаптивних антенних систем знаходить широке застосування у військових GNSS-приймачах, а також у перспективних проєктах цивільного призначення, зокрема в авіаційній та морській навігації, де надійність прийому сигналів позиціонування має критичне значення [1; 2; 4]. Ефективність таких систем підтверджується як у численних лабораторних експериментах, так і в реальних умовах експлуатації, що відображено в сучасних технічних звітах та дослідженнях [15; 16; 20].

Таким чином, адаптивні антени та фазовані решітки з цифровою обробкою сигналів утворюють сучасну технологічну основу для побудови радіонавігаційних систем, стійких до цілеспрямованих та випадкових завад. У поєднанні з іншими методами протидії — такими як криптографічний захист сигналів, моніторинг цілісності та виявлення спуфінгу — вони забезпечують комплексний захист радіонавігаційної інфраструктури в умовах зростання загроз інформаційно-телекомунікаційній безпеці [7; 17; 21].

У контексті сучасних викликів, що постають перед системами супутникової радіонавігації, все більшої актуальності набувають методи багатоантенної та багатоканальної обробки сигналів. Ці методи, засновані на точному аналізі просторових та часових характеристик сигналів, дозволяють виявляти підроблені сигнали, що використовуються під час навігаційних атак, зокрема спуфінгу. Однією з ключових особливостей таких атак є неможливість достовірного відтворення всіх фізичних характеристик автентичного сигналу, зокрема його фазових зсувів та тимчасових затримок, які є наслідком проходження хвилі через реальне середовище з урахуванням геометрії розташування джерела і приймача [16].

Багатоантенна конфігурація навігаційного приймача надає змогу формувати напрямкові діаграми спрямованості, а також реалізувати алгоритми визначення кута надходження сигналу (англ. Angle of Arrival, AoA), що дає можливість оцінити просторову несумісність між сигналами. Завдяки порівнянню відносних фаз між сигналами, що приймаються на різних антенах, можна визначити наявність аномалій, які характерні для підроблених джерел, що імітують сигнали навігаційної системи. У разі атаки спуфінгу всі сигнали надходять, як правило, з одного напрямку, що суперечить звичайній картині багатопроменевого надходження від кількох супутників з різних ділянок неба [14], [16].

Крім того, методи багатоканальної обробки дозволяють здійснювати детальний аналіз часових затримок сигналів за допомогою кореляційних функцій, що зіставляються з теоретичними моделями поширення сигналу. Підроблені сигнали зазвичай мають спрощену або неправдоподібну часову структуру, яка не відповідає очікуваним параметрам, зумовленим фізикою поширення радіохвиль, зокрема впливом іоносфери, тропосфери, рельєфу місцевості та ефектів мультишляху [1], [2], [10].

Поступове впровадження таких методів в інтегровані приймачі обумовлено підвищеними вимогами до точності, надійності та захищеності навігаційних систем у складних умовах електромагнітного середовища, зокрема в умовах радіонавігаційних конфліктів. Сучасні приймачі, які використовують багатоканальні цифрові сигнальні процесори, здатні реалізовувати обчислювально складні алгоритми фазової кореляції, фазової когерентності, адаптивної фільтрації та просторово-часової обробки в реальному часі [5], [7], [12].

У результаті поєднання просторового (багатоантенного) і часово-частотного (багатоканального) аналізу, зростає здатність навігаційних систем ідентифікувати, локалізувати і нейтралізовувати загрози спуфінгу та джемінгу. Такі методи вже знаходять практичне застосування в авіації, оборонній сфері, високоточному землеробстві та автономному транспорті [13], [18], [22]. Таким чином, розвиток багатоантенної та багатоканальної обробки сигналів є одним з ключових напрямів

підвищення стійкості та функціональної безпеки сучасних систем супутникової навігації в умовах активних радіоелектронних загроз.

Окрему роль у підвищенні стійкості навігаційних систем до радіоелектронних атак відіграє концепція мультисенсорної інтеграції, яка все ширше застосовується в сучасних дослідженнях і практичних реалізаціях систем навігації. Йдеться про підхід, що передбачає об'єднання та узгоджену обробку інформації, яка надходить з різнорідних незалежних джерел — таких як інерціальні навігаційні системи (ІНС), барометричні висотоміри, а також візуальні, оптичні, радіотехнічні або магнітометричні датчики. Основна перевага цієї концепції полягає у здатності компенсувати недоліки одного з джерел даних за рахунок точності або надійності інших, а також у можливості виявляти аномалії чи атаки на конкретний канал вимірювання завдяки порівнянню і кореляції з результатами інших каналів. Зокрема, це дозволяє з високою достовірністю виявити спуфінг або джемінг сигналу GNSS, порівнюючи динаміку його змін із даними, отриманими з ІНС, яка працює автономно та не залежить від зовнішніх сигналів [1; 4; 7; 10].

Інерціальні навігаційні системи, хоча й мають властивість накопичення похибок із часом, забезпечують безперервність навігації навіть у разі повної втрати супутникового сигналу. При цьому сучасні ІНС, побудовані на основі мікроелектромеханічних сенсорів (MEMS), можуть бути інтегровані у мініатюрні пристрої, що значно розширює можливості їхнього застосування у складі комплексних систем. Саме тому найбільш перспективними вважаються гібридні системи, у яких GNSS і ІНС працюють спільно, взаємно доповнюючи один одного. У разі функціонування GNSS в умовах перешкод або ворожих дій, таких як підміна сигналів (спуфінг) або створення перешкод (джемінг), ІНС може забезпечити відносно точне відстеження положення об'єкта протягом певного часу без необхідності зовнішнього коригування [7; 14].

Алгоритмічне забезпечення таких мультисенсорних систем базується на методах статистичної фільтрації та оцінювання, серед яких найпоширенішим є фільтр Калмана та його різновиди. Ці алгоритми дозволяють оптимально поєднувати дані з різних сенсорів, враховуючи їхні похибки, затримки та ймовірні

збої, що, у свою чергу, підвищує надійність навігаційної інформації загалом [8; 14]. Більш того, при наявності барометричних або магнітних вимірювань з’являється можливість визначення висоти чи азимуту руху незалежно від супутникових даних, що додатково ускладнює успішне проведення атак на систему в цілому.

Таким чином, мультисенсорна інтеграція є ефективним інженерним і концептуальним інструментом для реалізації принципу інформаційної надмірності та достовірності в системах навігації. Її застосування дає змогу не лише підвищити точність і надійність навігаційних вимірювань, але й забезпечити механізми самодіагностики та автоматичного виявлення зовнішніх загроз, що робить її надзвичайно актуальною в умовах сучасної радіоелектронної боротьби [2; 6; 14; 19; 20].

У підсумку слід зазначити, що забезпечення стійкості радіонавігаційних сигналів потребує поєднання кількох підходів, включаючи фізичний захист сигналу, криптографічну автентифікацію, інтелектуальну обробку прийнятих даних і мультисенсорну перевірку. Такий комплексний підхід є актуальним як для цивільних, так і для спеціалізованих систем, з огляду на зростання кількості та складності засобів радіоелектронного протиборства у сучасному конфліктному середовищі [15; 16; 20; 22].

2.2. Розробка алгоритмів виявлення та нейтралізації завад

Виявлення і нейтралізація завад потребують системного підходу до формування алгоритмічного забезпечення навігаційного приймача. Одним із ключових напрямів є створення алгоритмів для детектування аномалій у спектральному складі сигналу або у тимчасових затримках, що характерні для штучних завад [7; 17].

Побудова алгоритмів виявлення загроз у навігаційних системах є ключовим етапом забезпечення захисту в умовах радіонавігаційних конфліктів. Однією з найпоширеніших загроз у таких конфліктах є спуфінг — імітація достовірного навігаційного сигналу з метою введення приймача в оману щодо його

місцеположення або часу. З огляду на це, актуальним є впровадження алгоритмів, що здатні ідентифікувати відхилення параметрів прийнятих сигналів від очікуваних характеристик.

Особливості побудови таких алгоритмів визначаються структурою сигналів, що використовуються в супутникових навігаційних системах. Наприклад, для глобальної системи позиціонування GPS характерна наявність відкритого C/A-коду (Coarse Acquisition code), який передається на частоті L1 (1575,42 МГц) та призначений для загальнодоступного користування, а також закритого P(Y)-коду, що використовується у військових застосуваннях і модулюється на частотах L1 та L2 (1227,60 МГц) [1; 11]. Урахування структури таких кодів дозволяє адаптувати методи виявлення відповідно до типу сигналу, з яким працює приймач.

Одним із найефективніших способів виявлення аномалій у сигналі є застосування кореляційних методів. Ідея полягає у порівнянні очікуваного вигляду сигналу з реально прийнятим — процес, що реалізується через обчислення кореляційної функції між локально згенерованим кодом та вхідним сигналом. За наявності спуфінгу або іншого типу втручання, форма кореляційного максимуму змінюється: він може роздвоюватися, зміщуватися або взагалі зникати, що слугує критерієм виявлення порушення [12; 13].

Реалізація алгоритму виявлення передбачає аналіз не лише кореляційного максимуму, а й інших параметрів сигналу, таких як час затримки, частота доплера та потужність. Відомо, що у разі спуфінгу атакуючий сигнал зазвичай має вищу потужність, щоб «заглушити» автентичний супутниковий сигнал на вході приймача. Проте надмірна потужність сигналу може бути ознакою нештатної ситуації та використовуватись як додатковий індикатор [15; 16]. З цією метою доцільно застосовувати порогові методи детектування, що враховують статистичні характеристики прийнятого сигналу у різних часових інтервалах [8].

У деяких випадках, зокрема в умовах наявності кількох навігаційних систем (наприклад, GPS, Galileo, GLONASS), доцільно реалізовувати міжсистемне порівняння координат і часу. Виявлення значних розбіжностей між результатами різних систем може свідчити про навмисне втручання в одну з них. Даний підхід

підвищує загальну стійкість приймача до атак і створює можливість автоматичного перемикання на резервні джерела інформації або активацію режиму інерційної навігації [7; 14].

Активація захисного режиму виявлення загроз може мати різні наслідки залежно від специфіки застосування навігаційної системи. У цивільних приймачах це зазвичай проявляється у формі ігнорування підозрілих сигналів або попередження користувача. У критично важливих додатках, таких як авіація або військові системи, реалізується перемикання на альтернативні системи навігації або тимчасове використання інерційних даних до моменту стабілізації супутникового сигналу [2; 17; 22].

Загалом, побудова алгоритмів виявлення втручань у навігаційні сигнали є поєднанням методів сигналопроцесінгу, статистичного аналізу та апаратно-програмних рішень. Їхня ефективність значною мірою залежить від здатності адаптивно змінювати параметри аналізу відповідно до характеристик радіоелектронного середовища, що змінюється у просторі та часі [5; 6; 19]. У контексті радіонавігаційних конфліктів такі алгоритми виступають критичним елементом системи захисту, формуючи першу лінію оборони від загроз інформаційної безпеки просторово-часової орієнтації.

Нейтралізація завад в радіонавігаційних системах є важливою складовою частиною забезпечення надійності та точності навігаційних засобів, особливо в умовах радіонавігаційних конфліктів. Основними методами протидії завадам є адаптивне фільтрування сигналів та формування просторових діаграм спрямованості антенної системи. Ці методи дозволяють значно зменшити вплив завад на точність навігаційних оцінок, підвищуючи ефективність роботи систем у складних умовах.

Адаптивне фільтрування є одним з найпоширеніших методів нейтралізації завад у радіонавігаційних системах. Воно полягає в використанні спеціальних алгоритмів, які дозволяють автоматично налаштовувати параметри фільтра в залежності від характеристик завади та сигналу. Це дозволяє максимально ефективно відфільтровувати небажані сигнали, залишаючи тільки корисні. Одним

з основних алгоритмів адаптивного фільтрування є алгоритм мінімізації середньоквадратичної помилки (Least Mean Square, LMS), який широко застосовується для фільтрації шуму в реальному часі. Алгоритм LMS працює на принципі коригування фільтруючих коефіцієнтів для досягнення мінімальної помилки між очікуваним та фактичним виходом системи. Це забезпечує високий рівень точності при роботі в умовах завад [15; 16].

Іншим важливим методом є використання оберненої матриці коваріації завади (Minimum Variance Distortionless Response, MVDR). Цей метод дозволяє створити просторові діаграми спрямованості, які мінімізують завади, зберігаючи при цьому точність прийому корисного сигналу. MVDR є ефективним для нейтралізації завад, що мають складну просторову структуру, оскільки він дозволяє максимально зменшити рівень завади в конкретних напрямках, зберігаючи при цьому стабільність у прийомі сигналів [16].

Обидва методи, LMS та MVDR, можуть бути реалізовані як у апаратному, так і в програмному забезпеченні навігаційного комплексу. Реалізація таких алгоритмів в апаратному забезпеченні дозволяє забезпечити високу швидкість обробки сигналів та зниження енергетичних витрат, що є важливим для використання в мобільних або портативних навігаційних системах. Водночас програмна реалізація таких алгоритмів дозволяє значно спростити налаштування та адаптацію до різних умов експлуатації, зберігаючи високу гнучкість і можливість оновлень [17].

Таким чином, методи адаптивного фільтрування та використання оберненої матриці коваріації завади є основними засобами протидії радіонавігаційним завадам. Вони дають змогу забезпечити стабільну роботу навігаційних систем навіть в умовах високих радіочастотних завад та створюють надійний захист від зовнішніх впливів у радіонавігаційних конфліктах.

Методи протидії в радіонавігаційних конфліктах є важливими для забезпечення стабільності та надійності роботи радіонавігаційних систем у умовах потенційних загроз. Однією з основних таких загроз є атаки типу spoofing, що спричиняють серйозні проблеми для точності визначення місцезнаходження і навігації, оскільки вони підміняють справжні сигнали супутникових систем. Атаки

spoofing можуть знижувати ефективність радіонавігаційних систем, що використовуються в різноманітних галузях, таких як цивільна авіація, морський транспорт і військові операції.

Одним із способів боротьби з атакою spoofing є використання статистичних методів для оцінки достовірності сигналу. До цього підходу належить використання байєсівських методів оцінки, що дозволяють аналізувати ймовірність того, що сигнал є достовірним чи підробленим. Байєсівський підхід ґрунтується на застосуванні теореми Байєса, яка дозволяє коригувати ймовірність на основі нових даних, що надходять, і таким чином, підвищувати точність визначення джерела сигналу [8].

Застосування методів машинного навчання виявляється перспективним напрямом у контексті протидії spoofing-атакам. За допомогою таких технологій можна ефективно обробляти великі обсяги даних, що генеруються навігаційними системами, і своєчасно виявляти аномалії, що свідчать про можливу підміну сигналів. Машинне навчання дозволяє системам навчатися на попередньо зібраних даних і адаптувати свої стратегії реагування на нові загрози в реальному часі. Це підвищує ефективність системи в умовах постійних змін і динамічних загроз [15; 43; 49].

Окрім використання статистичних методів та машинного навчання, важливою складовою боротьби з spoofing є забезпечення шифрування сигналів навігаційних систем. Шифрування дозволяє ускладнити процес підміни сигналів для потенційного зловмисника, оскільки для того, щоб правильно підробити сигнал, потрібно знати певні криптографічні ключі. Стратегії криптографічного захисту та анти-спуфінгові механізми активно розробляються для GNSS-систем, що використовуються в цивільній та військовій навігації, з метою забезпечення надійного захисту від атак типу spoofing [17; 46; 48; 50].

Важливою складовою загальної стратегії протидії радіонавігаційним конфліктам є застосування багатопозиційних систем спостереження, які здатні забезпечити більш точні оцінки місцезнаходження за допомогою кількох приймачів сигналу. Така технологія дозволяє покращити точність траєкторних оцінок, а також

знижує ймовірність успішної атаки на систему [6]. Крім того, для підвищення надійності таких систем використовуються методи комплексної обробки даних, що дозволяють визначати і коригувати помилки, які можуть виникати в результаті атак або природних факторів, таких як атмосферні явища [8].

Загалом, ефективна протидія в радіонавігаційних конфліктах потребує комплексного підходу, що включає статистичні методи, технології машинного навчання, криптографічний захист і багатопозиційні системи спостереження. Тільки за допомогою інтеграції цих технологій можна забезпечити стабільну і надійну роботу навігаційних систем навіть у складних умовах, коли вони піддаються атакам [51-56].

2.3. Моделювання ефективності методів протидії

2.3.1. Математична модель аналізу завад

Математичне моделювання впливу завад є важливою складовою частиною досліджень у сфері радіонавігаційних систем. Це дозволяє створити узагальнену модель сигналу, до якого додаються різноманітні компоненти перешкод, що можуть мати випадковий або детермінований характер. Випадкові завади, наприклад, білий шум, виникають унаслідок різних фізичних процесів, що заважають нормальному прийому сигналу, а детерміновані завади, такі як спуфінг чи глушіння, часто є навмисними й мають за мету зіпсувати або змінити сигнал, що приймається.

У загальному випадку модель прийнятого сигналу можна виразити через рівняння:

$$r(t) = s(t) + j(t) + n(t), \qquad (2.1)$$

де s(t) – корисний навігаційний сигнал, j(t) – навмисна завада, n(t) – шум. Аналіз спектральних характеристик j(t) дозволяє виділити його компоненти для подальшої нейтралізації.

У сучасних радіонавігаційних системах, таких як GPS (Глобальна система позиціонування), навігаційний сигнал s(t) забезпечує точність визначення

місцеположення на основі часу приходу сигналу до приймача. Цей сигнал, як правило, генерується супутниками, які відправляють інформацію про своє місцезнаходження та точний час. Однак на ефективність роботи навігаційної системи значно впливають різноманітні завади, такі як шум n(t) і джемінг j(t), які можуть значно спотворювати сигнал або навіть повністю блокувати його.

Шум, що виникає у навігаційних системах, може бути результатом природних або технічних факторів, таких як атмосфера, сонячна активність чи перешкоди від інших електронних пристроїв. У свою чергу, джемінг, або навмисне зашумлення сигналу, є серйозною загрозою для ефективного функціонування супутникових навігаційних систем. Джемери, які випромінюють сигнали на тих же частотах, що й навігаційні супутники, можуть повністю заблокувати отримання навігаційних даних або значно знизити точність визначення місцеположення.

Для протидії таким завадам, застосовуються різноманітні методи захисту. Одним з основних підходів є використання алгоритмів фільтрації та корекції даних, які дозволяють виділяти корисний сигнал із зашумленого середовища. Наприклад, застосування фільтрів Калмана є популярним методом для відновлення точності навігації в умовах шуму і джемінгу. Алгоритм Калмана дозволяє оптимізувати оцінку стану системи, комбінуючи інформацію від різних сенсорів, що підвищує надійність і точність навігаційних оцінок навіть при наявності завад [1].

З іншого боку, для боротьби з джемінгом застосовуються методи просторового і частотного розподілу сигналу. Наприклад, використання адаптивних антенних решіток дозволяє змінювати напрямок прийому сигналу в реальному часі, щоб зменшити вплив джемера. Іншим методом є використання мультичастотних або багатоканальних систем, що дає змогу посилювати сигнали на певних частотах і тим самим знижувати ефект від джемінгу [2; 3].

Крім того, новітні технології шифрування і аутентифікації сигналу стають важливими для захисту від спуфінгу — атаки, яка полягає у підробці супутникових сигналів. Для цього використовуються криптографічні методи, що дозволяють перевірити достовірність отриманих сигналів і запобігти використанню фальшивих супутникових станцій [15; 17].

Завдяки розвитку методів протидії завадам, сучасні радіонавігаційні системи можуть забезпечувати високу точність і надійність навіть в умовах складних радіоелектронних обстановок. Однак питання протидії радіонавігаційним конфліктам залишається актуальним, оскільки з кожним роком зростає кількість джемерів та інших джерел завад, які можуть впливати на роботу навігаційних систем, що використовуються в авіації, судноплавстві, автомобільному та іншому транспорті [19][20].

Зважаючи на важливість навігаційних систем у багатьох сферах життєдіяльності, розробка нових методів протидії радіонавігаційним конфліктам є пріоритетним напрямком досліджень у галузі радіоелектроніки та супутникових технологій.

Аналіз спектральних характеристик навмисних завад, таких як спуфінг або глушіння, дозволяє виділити їхні компоненти, що у подальшому може допомогти в розробці методів їх нейтралізації. Спуфінг, наприклад, полягає в підробці навігаційного сигналу, щоб змусити приймач використовувати фальшиві дані, тоді як глушіння є перешкодою, що зменшує рівень сигналу до такої величини, що приймач більше не може точно визначити своє місцезнаходження. Методи протидії цим завадам є важливою частиною досліджень у сфері радіонавігаційних систем.

Важливу роль у статистичному моделюванні завадових ситуацій в радіонавігаційних системах відіграють кілька параметрів, що визначають ефективність роботи системи. Одним із основних є потужність сигналу на вході приймача, яка напряму впливає на якість отримуваного сигналу і точність позиціонування. Чим вища потужність сигналу, тим більше шансів на успішне відновлення коректної інформації про місцеположення навіть в умовах сильних завад. Це особливо важливо для систем глобального позиціонування, де якість сигналу залежить від зовнішніх умов, таких як наявність будівель, лісів чи інших перешкод, що можуть блокувати або ослаблювати сигнал.

Іншим важливим параметром є відношення сигнал/завада (SIR). Це відношення є основним показником, що визначає, наскільки чітко приймач може відокремити корисний сигнал від шуму чи інших завад. Високе SIR забезпечує

високу точність вимірювання і надійність роботи системи. Проте в умовах сильних завад або при низькому рівні сигналу SIR знижується, що може призвести до значних помилок у визначенні координат. У таких ситуаціях важливо застосовувати методи фільтрації і корекції даних, щоб зменшити вплив завад і відновити точність вимірювань.

Не менш важливим параметром є характеристика супутникової геометрії, зокрема PDOP (Position Dilution of Precision). PDOP є мірою впливу геометрії супутників на точність позиціонування. Якщо супутники розташовані таким чином, що їх положення утворює зразок з високим рівнем сплутаності, точність визначення місцеположення може бути значно знижена. Наприклад, коли супутники зібрані в одну частину небесної сфери або знаходяться дуже близько один до одного, це призводить до високого PDOP і, як наслідок, до зниження точності позиціонування. Високий PDOP сигналізує про погану геометрію супутників, що робить точність оцінки місцеположення менш надійною.

Супутникові навігаційні системи, зокрема GPS, GLONASS, Galileo та BeiDou, покладаються на отримання сигналів від кількох супутників для визначення точного місцеположення користувача. Однак навіть у найкращих умовах можуть виникати ситуації з високим PDOP, що потребують використання додаткових методів корекції, таких як диференційна навігація (DGPS) або використання інерціальних навігаційних систем (INS) для поліпшення точності позиціонування.

Високий PDOP може також свідчити про необхідність застосування спеціальних алгоритмів для покращення точності, таких як фільтрація Калмана або методи на основі статистичних оцінок, що дозволяють обчислювати більш точні координати за умов поганої супутникової геометрії. Крім того, при аналізі завадових ситуацій важливо враховувати не тільки величину PDOP, але й інші фактори, що можуть впливати на якість сигналу, зокрема атмосферні явища, які також можуть знижувати ефективність роботи навігаційних систем [1; 2; 5].

Незважаючи на численні труднощі, статистичні методи обробки сигналів, зокрема обчислення оптимальних фільтрів для зменшення впливу завад, є важливим інструментом для покращення точності та надійності навігаційних

систем. Застосування таких методів дозволяє зменшити вплив завадових ситуацій на точність позиціонування і забезпечити надійну роботу систем навіть в умовах складної геометрії супутників або сильних перешкод.

Таким чином, параметри потужності сигналу, SIR та PDOP є ключовими для моделювання та аналізу завадових ситуацій у радіонавігаційних системах. Їх точне обчислення та корекція дозволяють значно покращити ефективність навігаційних систем, що особливо важливо для використання в критичних ситуаціях, де точність позиціонування є критично важливою [3; 4; 6].

Моделювання таких завадових ситуацій дозволяє прогнозувати поведінку приймача в різних умовах, що важливо для розробки ефективних методів захисту від атак. Сучасні підходи до протидії завадам включають використання криптографічних методів для захисту від спуфінгу, а також адаптивні алгоритми для зменшення впливу глушіння. Наприклад, для захисту від спуфінгу може бути використано шифрування навігаційного сигналу або застосування антиспуфінгових алгоритмів, які дозволяють виявляти підроблені сигнали за допомогою аналізу їх властивостей і несумісності з реальними супутниковими сигналами.

Методи статистичної обробки даних і аналізу шуму в системах навігації є важливими для забезпечення надійної роботи навігаційних систем у складних умовах. Наприклад, обробка даних за допомогою статистичних методів дозволяє знижувати ефект шуму і підвищувати точність визначення місцеположення навіть у випадку наявності помітних завад.

Моделювання і аналіз таких завадових ситуацій дає можливість ефективно передбачити поведінку навігаційних систем при різних сценаріях атак, що є основою для розробки методів захисту і підвищення точності позиціонування в умовах реальних завад.

2.3.2. Алгоритмічний підхід до протидії навмисним втручанням

Алгоритми, що використовуються для протидії радіонавігаційним атакам, мають на меті не тільки виявити моменти виникнення завади, але й оперативно

реагувати на них, забезпечуючи стійкість навігаційних систем. Одним із таких підходів є використання алгоритму фазового контролю, який дозволяє виявляти спотворення фази сигналу, характерні для спуфінгових атак. Ці спотворення, які не відповідають фізичним моделям руху об'єктів, можна виявити завдяки спеціальним математичним моделям, що дають змогу точно визначити момент початку завади.

Спуфінг є одним із найбільш небезпечних типів атак на навігаційні системи, адже зловмисник може створювати штучні сигнали, що імітують сигнали навігаційних супутників, підміняючи реальні дані щодо місцеположення і часу. Алгоритми фазового контролю, виявляючи нелінійні зміни фази сигналу, здатні зафіксувати такі атаки і своєчасно припинити їх вплив. Особливо важливо, що зміни фази сигналу, викликані атакою, не підкоряються звичайним фізичним законам, таким як рівномірний рух об'єкта або стійкість навігаційних параметрів, що дозволяє ефективно відрізнити справжній сигнал від сфальшованого.

Для забезпечення ефективності цього алгоритму використовуються математичні методи, зокрема алгоритми на основі аналізу зміни фазових характеристик сигналів, що допомагає визначити можливу атаку та вжити відповідних заходів. Одним з таких заходів є переключення на резервні канали або використання альтернативних навігаційних технологій, які дозволяють забезпечити неперервність навігаційних даних навіть під час спроби атаки.

Ці методи та алгоритми активно застосовуються в сучасних навігаційних системах, особливо в тих, що використовуються в критичних інфраструктурах та оборонних системах, де точність і надійність навігації мають вирішальне значення. Усі ці рішення є частиною комплексної системи захисту від радіонавігаційних атак, що включає в себе також технічні, організаційні та юридичні заходи, спрямовані на мінімізацію ризиків і підвищення стійкості навігаційних систем [17].

У сучасних умовах розвитку радіонавігаційних систем, ефективність їхнього функціонування значною мірою залежить від здатності протистояти різноманітним типам атак, які можуть серйозно впливати на якість і точність навігаційних даних. Одним із важливих аспектів захисту від таких атак є використання методів, що базуються на порівняльному аналізі багаточастотних каналів навігаційного сигналу.

Цей підхід дозволяє підвищити стійкість системи до потенційних загроз, таких як джемінг або спуфінг.

Якщо атакуюча сторона намагається вплинути лише на одну частоту, наприклад, на L1, але при цьому інші частоти залишаються непошкодженими, система може виявити відмінності в сигналах, які надходять із різних частотних каналів. У разі застосування такої атаки на конкретну частоту, наприклад, на L1, де ймовірно буде спостерігатися спотворення або заглушення сигналу, інші частоти, що залишаються без змін, можуть використовуватися для виявлення невідповідностей. Це дозволяє не лише виявити сам факт атакування, а й точно визначити наявність підозрілих аномалій у сигналах, що надходять від супутників.

Порівняння сигналів з різних частот дозволяє відслідковувати такі відмінності, які можуть бути наслідком атаки. У випадку виявлення невідповідностей між сигналами з різних частот, система може автоматично відхиляти підозрілу інформацію та виключати її з подальшої обробки. Це, в свою чергу, значно знижує ймовірність того, що система буде введена в оману і не зможе коректно виконувати навігаційні обчислення. Дане рішення дозволяє не тільки підвищити безпеку системи, але й значно знизити вразливість до різних типів атак, таких як спуфінг, при якому зловмисник намагається надати неправдиву інформацію про місцезнаходження.

Методи аналізу багаточастотних каналів здатні працювати в умовах, коли атака здійснюється на окремі частоти, при цьому зберігаючи ефективність роботи навіть в умовах часткових збоїв у сигналі. Такий підхід є важливим елементом у розробці сучасних радіонавігаційних систем, здатних протистояти сучасним методам атак, що можуть бути застосовані для саботажу або спотворення навігаційних даних.

Застосування порівняльного аналізу багаточастотних каналів сигналу виявилося надзвичайно ефективним у боротьбі з різними типами атак, оскільки воно дозволяє не лише фіксувати та виявляти спотворення сигналів, але й забезпечує збереження точності навігаційних розрахунків навіть в умовах серйозних загроз. Цей метод забезпечує вищий рівень надійності та стійкості радіонавігаційних систем, що є ключовим фактором для їх застосування в умовах

військових конфліктів або інших ситуаціях, де точність і безпека навігації є критично важливими.

Загалом, підхід, що використовує порівняльний аналіз багаточастотних сигналів, стає основним елементом захисту в сучасних радіонавігаційних технологіях, дозволяючи підвищити їхню стійкість до різноманітних атак і значно поліпшити їхню ефективність у реальних умовах [6; 11].

У сучасних радіонавігаційних системах важливу роль відіграють методи протидії різноманітним технічним загрозам, зокрема атакам на сигнали навігаційних супутників. Одним з найбільш складних аспектів є забезпечення стійкості систем до різних типів завад, таких як джемінг та спуфінг. Для цього застосовуються різноманітні методи, що включають використання мультидоменного аналізу. Такий підхід дозволяє здійснювати більш глибокий аналіз не лише тимчасових характеристик сигналу, але й його просторових та спектральних параметрів. Це дозволяє краще відслідковувати зміни, які можуть відбуватися на різних рівнях: у часі, просторі та спектрі, що суттєво підвищує ефективність виявлення атак і підвищує стійкість радіонавігаційних систем.

Мультидоменний аналіз передбачає використання декількох аспектів сигналу для його аналізу. Зокрема, спектральний аналіз дозволяє виявляти характерні зміни в амплітуді та частоті сигналу, що можуть свідчити про спроби спуфінгу або джемінгу. Просторові характеристики сигналу допомагають визначити місце джерела завад, що також є важливим для ефективної протидії. Крім того, тимчасові характеристики сигналу дозволяють виявляти нелінійні зміни, що можуть бути пов'язані з цілеспрямованими атаками, такими як зміна параметрів сигналу в реальному часі [19].

Однією з переваг мультидоменного аналізу є можливість більш точного визначення джерел завад, що дозволяє не лише виявляти, але й локалізувати атаки, що сприяє підвищенню рівня безпеки навігаційної системи. Комбінація аналізу різних параметрів дає змогу створити більш стійку систему, здатну протистояти новим та складним атакам. Такий підхід дозволяє не тільки виявляти спуфінг та

джемінг, але й адаптувати систему до нових загроз, що постійно з’являються на радіонавігаційному горизонті [22].

Проте важливо зазначити, що мультидоменний аналіз потребує високих обчислювальних ресурсів, оскільки для кожного сигналу необхідно проводити аналіз у кількох різних площинах: часовій, спектральній та просторовій. Це може створювати додаткові вимоги до апаратних та програмних засобів, що використовуються в радіонавігаційних системах. Тому важливою складовою таких систем є впровадження оптимізованих алгоритмів обробки сигналів, що дозволяють ефективно реалізувати мультидоменний аналіз, зберігаючи високу точність при мінімальних обчислювальних витратах [16].

Застосування комбінованого підходу для виявлення та нейтралізації загроз у радіонавігаційних системах дозволяє досягти високого рівня надійності та ефективності роботи системи навіть у складних умовах. Врахування різних характеристик сигналу на різних рівнях дає змогу створити більш комплексну модель захисту, здатну протистояти не лише класичним типам атак, але й новим, незнайомим загрозам. Це є важливою складовою для подальшого розвитку радіонавігаційних технологій і їх застосування в критичних сферах, таких як авіація, морська навігація, оборона та інші [18].

Система для визначення моменту початку завади та виявлення порушень сигнального простору є важливою складовою комплексної протидії навігаційним атакам. Вона повинна бути здатною працювати в реальному часі, швидко реагувати на несправності і ефективно відновлювати нормальний режим роботи навіть у складних умовах наявності завад [15].

2.3.3. Оцінка ефективності методів у реальних умовах

Ефективність запропонованих методів протидії радіонавігаційним конфліктам оцінюється за допомогою стендових випробувань або польових експериментів. При цьому важливими показниками є точність позиціювання, відсоток виявлених атак та середній час реакції системи на загрозу. Точність позиціювання є критичним

фактором, оскільки навіть невеликі відхилення в обчисленні місцеположення можуть призвести до серйозних наслідків для навігаційних систем. Задача виявлення атак вимагає високої чутливості системи до аномалій в сигнальному середовищі, при цьому важливо, щоб система могла ефективно реагувати на загрози без надмірних затримок, оскільки це може суттєво вплинути на безпеку навігації в реальному часі.

У рамках дослідження методів протидії радіонавігаційним конфліктам важливим аспектом є використання різних типів навігаційних систем, включаючи як автономні навігаційні приймачі, так і комбіновані системи, що інтегрують супутникову навігацію з інерціальними модулями. Це дозволяє не лише підвищити точність позиціювання, але й забезпечити стабільність роботи системи в умовах різних зовнішніх перешкод.

Комбіновані навігаційні системи, що поєднують супутникову навігацію з інерціальними модулями, здатні надавати вищу точність визначення місцеположення, ніж окремі системи. Інерціальні модулі компенсують втрату сигналу супутників, що є критичним в умовах радіонавігаційних перешкод або при недостатній видимості супутників. Додавання інерціальних сенсорів дозволяє зберігати точність навіть за відсутності зв'язку з супутниками, тим самим зменшуючи уразливість до спотворення сигналу або його блокування.

Випробування, проведені з використанням таких комбінованих систем, показали їх ефективність у забезпеченні точності навігаційних обчислень та стійкості до зовнішніх перешкод, таких як радіоелектронне придушення або заглушення сигналів супутникової навігації. Одним із важливих аспектів таких систем є використання адаптивної обробки сигналів, яка дає змогу динамічно налаштовувати систему на зміни в навігаційному середовищі. Статистичний аналіз даних, що надходять від супутникових приймачів і інерціальних сенсорів, дозволяє зменшити вплив зовнішніх перешкод на точність навігації.

Ці підходи значно підвищують надійність систем у складних умовах радіонавігаційних конфліктів, коли традиційні методи навігації, що використовують тільки супутникові системи, можуть бути ненадійними через

можливі спотворення або відмову сигналу. Важливим є те, що адаптивна обробка сигналів та об'єднання даних з різних сенсорів дозволяють забезпечити безперервне позиціювання навіть при наявності джемінгу або спуфінгу супутникових сигналів.

Таким чином, комбіновані системи, що поєднують супутникову навігацію та інерціальні сенсори, є найбільш ефективними в умовах радіонавігаційних конфліктів, адже вони дозволяють не тільки знизити вплив зовнішніх перешкод на точність позиціювання, але й забезпечити надійність та стійкість системи в реальних умовах. Дослідження таких підходів є важливим кроком у розвитку навігаційних технологій, зокрема в сфері оборони та безпеки.

Результати, отримані в ході випробувань комбінованих навігаційних систем, підтверджують, що такі системи здатні ефективно працювати в умовах радіонавігаційних конфліктів, коли традиційні методи стають менш надійними. Адаптивна обробка сигналів, статистичний аналіз та інтеграція даних з різних сенсорів забезпечують високий рівень точності і надійності навігаційних систем, що в свою чергу дозволяє значно зменшити ризики, пов'язані з навігаційними перешкодами та спотвореннями сигналу. Це дозволяє ефективно протидіяти сучасним методам джемінгу та спуфінгу, що робить ці системи незамінними у багатьох сферах, включаючи оборону та цивільну авіацію [5; 6; 7; 16].

Результати моделювання систем радіонавігації в умовах протидії сигналам демонструють важливість налаштування методів захисту відповідно до специфіки застосування систем. Такі налаштування є необхідними для досягнення максимальної ефективності в боротьбі з радіонавігаційними конфліктами, що можуть виникнути через зовнішні або внутрішні фактори, включаючи використання джеммерів або спуферів.

В авіаційній сфері вимоги до точності й швидкості реакції системи особливо високі. Тут важливо забезпечити безпеку та стабільність сигналів для підтримки навігаційних функцій. Авіаційні системи повинні мати спеціалізовані методи протидії, які враховують різноманітні чинники, такі як швидкість пересування об’єкта, наявність перешкод в сигнальному середовищі та вплив атмосферних

явищ. Для цього застосовуються алгоритми, що забезпечують надійне визначення місцезнаходження навіть у складних умовах радіоелектронного впливу, таких як джемінг або спуфінг [1; 2].

У безпілотних системах, що також мають високі вимоги до точності, методи протидії повинні бути адаптованими до специфічних умов навігації. Для таких систем важливо використовувати технології, які забезпечують стійкість до зовнішнього впливу, включаючи штучні джемери. Ідеальною стратегією є комбінування супутникових сигналів з інерціальними системами навігації, що дозволяє підтримувати точність навіть у ситуаціях, коли GNSS-сигнали можуть бути пошкоджені чи перекриті [3; 4; 45; 47].

В контексті наземного транспорту підходи до протидії зосереджені на стабільності сигналу та адаптивності системи до змін навколишнього середовища. Тут використовуються більш прості, але ефективні методи, що дозволяють забезпечити точність навігації в умовах міської забудови, де є можливість значного спотворення сигналу від супутників через високі будівлі або природні перешкоди. Водночас, навіть в таких умовах система повинна мати змогу швидко адаптуватися до змін у сигнальному середовищі та реагувати на можливі спроби саботажу чи перешкоджання сигналу [5; 6].

Методи протидії мають враховувати й фактори, що впливають на роботу систем в реальних умовах, такі як зміни в місцевості, наявність природних перешкод, а також вплив ворожих джеммерів. Вони можуть значно змінювати ефективність навігаційної системи, тому необхідно застосовувати адаптивні стратегії, які дозволяють системам автономно визначати найефективніші способи захисту сигналу, зберігаючи при цьому високу точність навігаційних даних [7][8].

Таким чином, розробка методів протидії в радіонавігаційних конфліктах вимагає індивідуального підходу в залежності від сфери застосування, що дозволяє забезпечити ефективність захисту від зовнішніх і внутрішніх загроз. Кожна сфера—будь то авіація, безпілотні системи або наземний транспорт—має свої специфічні вимоги до точності та швидкості, які повинні враховуватись при розробці методів захисту та адаптації навігаційних систем.

У роботі розглядаються методи протидії в радіонавігаційних конфліктах, що є важливою складовою частиною сучасних радіонавігаційних систем. Радіонавігаційні системи, зокрема супутникові навігаційні системи, активно використовуються для визначення місцеположення, орієнтування та інших критично важливих задач. Однак ці системи піддаються різним видам загроз, серед яких однією з найпоширеніших є радіонавігаційні конфлікти, що включають перешкоди у сигнальному середовищі, джемінг та спуфінг.

У цьому контексті важливим є застосування багаторівневої архітектури захисту, яка дозволяє ефективно виявляти та блокувати такі загрози, одночасно підтримуючи високу точність позиціонування, навіть за умов серйозних перешкод. Багаторівневий підхід до протидії включає як апаратні, так і програмні методи, які можуть адаптуватися до нових умов роботи радіонавігаційних систем. За таких умов важливою є здатність системи до швидкої адаптації та оновлення алгоритмів відповідно до змін у навігаційному сигналі та нових загроз.

Система повинна мати здатність не лише виявляти перешкоди, але й забезпечувати високоточне позиціювання в умовах змінного і навіть ворожого середовища. Це включає впровадження нових методів обробки сигналів, таких як використання алгоритмів криптографії для захисту від спуфінгу, а також застосування більш складних методів джемінг-протидії, як, наприклад, адаптивне налаштування чутливості приймачів та використання мультичастотних систем для зменшення впливу перешкод на точність визначення місцеположення [1; 4].

Методи протидії в радіонавігаційних конфліктах включають також використання інерціальних навігаційних систем, які можуть компенсувати втрату сигналу в умовах джемінгу або спуфінгу. Такі системи поєднують супутникову навігацію з інерціальними датчиками, що дозволяє підвищити точність позиціонування навіть у випадках, коли супутникові сигнали не доступні або зазнають значних перешкод. Водночас ефективне використання інерціальних систем потребує розробки нових алгоритмів для обробки сигналів та оцінки траєкторій руху з високою точністю, навіть за умов нестабільності джерел сигналу [5, 7].

Одним із важливих аспектів є удосконалення методів багатопозиційних систем спостереження, що дозволяють зібрати інформацію з кількох джерел і забезпечити більш точну оцінку місцеположення навіть при наявності перешкод. Використання таких систем з інтеграцією даних від різних датчиків дозволяє значно знизити вплив шуму та перешкод, підвищуючи стійкість до зовнішніх впливів [6].

Особлива увага повинна бути приділена швидкості адаптації до змін умов навігаційного середовища. Для цього необхідно розробляти методи оперативного оновлення алгоритмів на основі нових даних про характер перешкод та можливі загрози. Такий підхід дозволяє системі залишатися ефективною навіть в умовах швидко змінюваного радіонавігаційного середовища [8, 9].

Загалом, протидія радіонавігаційним конфліктам потребує комплексного підходу, що включає використання багаторівневих захисних систем, інерціальних навігаційних методів, а також швидкої адаптації до нових умов роботи. Завдяки цьому вдається забезпечити стійкість та надійність радіонавігаційних систем, що мають важливе значення для сучасних технологій навігації, а також для національної безпеки в цілому [10, 15].

Протидія радіонавігаційним атакам вимагає комплексного підходу, що включає як технологічні рішення, так і стратегічні методи для підтримки стабільності навігаційного середовища у всіх умовах, зокрема при активних радіоелектронних впливах з боку противника [15; 19; 20].

2.4. Моделювання корисних і завадових сигналів та аналіз їх взаємозв’яку.

Метою моделювання є створення умов, у яких можна наочно простежити, як різні типи корисних сигналів поводяться під впливом jamming завад, що виникають у реальних канал зв’язку. У межах цього підходу важливо не просто відтворити математичні залежності, а відтворити динаміку взаємодії сигналу та шуму так, щоб було видно характер спотворень, зміни амплітуди, структури та загальної форми хвилі сигналу. Моделювання дозволяє простежити, які саме властивості сигналів

визначають їхню стійкість або вразливість, а також можливість оцінити, наскільки критичним може бути вплив конкретної завади. Для реалізації моделювання, блок схема якого зображена на Рис. 2.1, використано Python 3.14, оскільки він надає гнучкі можливості для роботи з даними та сигналами.

Перелік використаних бібліотек:

1. Nummy – для формування часової сітки, генерації математичних функцій та операцій над масивами;
2. Scipy.signal – для генерації складних модульованих сигналів, розширення спектру, моделювання імпульсних сигналів;
3. Matplotlib – для побудови графіків часових сигналів, візуалізації результатів;
4. Matplotlib.patches – для побудови елементів блок-схеми.

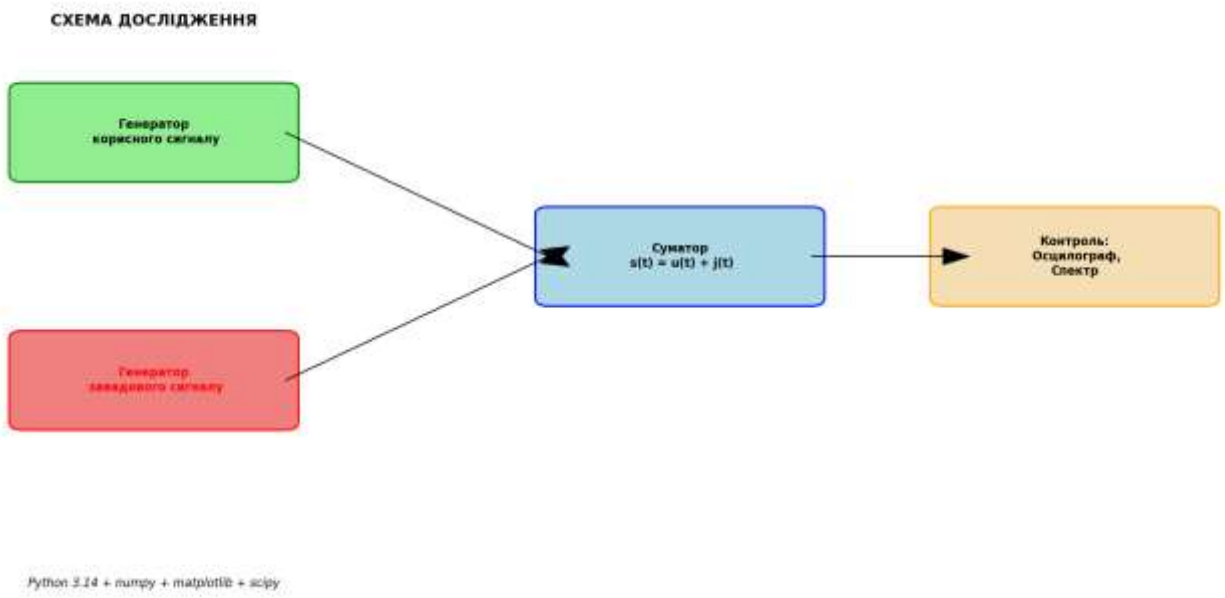


Рис. 2.1 Структурна схема дослідження впливу завадових сигналів на корисний сигнал в середовищі Python.

Корисні сигнали супутникових радіонавігаційних систем (СРНС) є складними радіотехнічними структурами, призначеними для передавання

навігаційної інформації від супутника до приймача споживача. Основним призначенням таких сигналів є забезпечення визначення координат, швидкості руху та точного часу шляхом вимірювання псевдодальностей до навігаційних супутників.

На Рис. 2.2 задіяно кілька різних типів корисних сигналів, кожен із яких має власні особливості та використовується в різних сферах зв’язку.

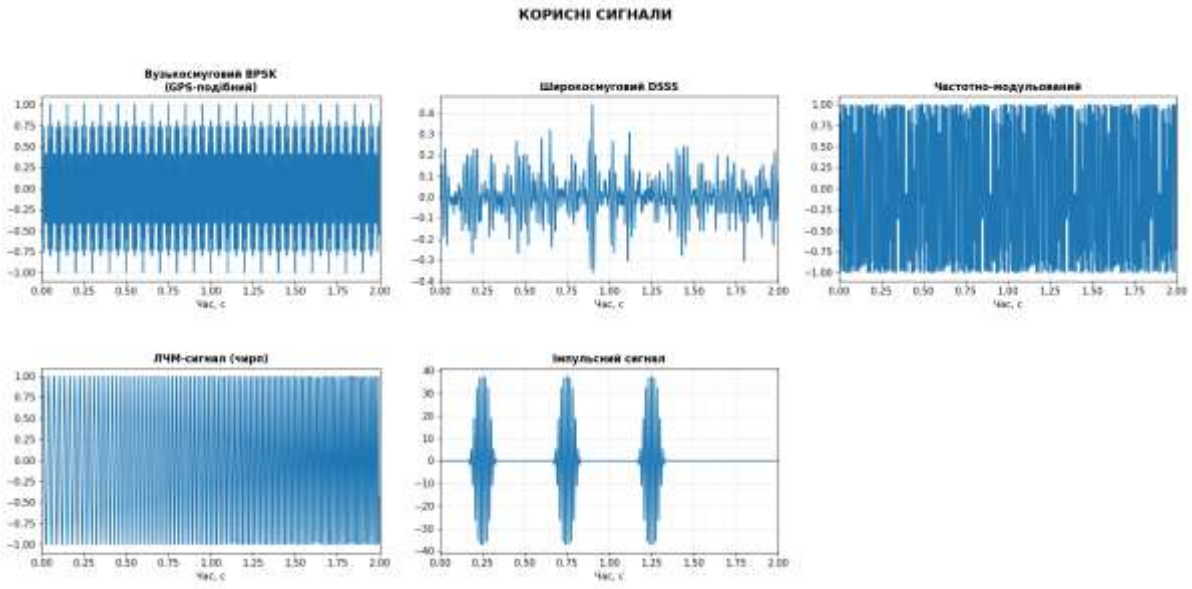


Рис. 2.2 Зображення корисних сигналів сформованих в середовищі моделювання Python.

Перший сигнал вузькосмуговий гармонічний сигнал, структура якого нагадує сигнали супутникових систем таких як GPS. Його форма задається несучою частотою, на яку накладається модуляція, що створює характерну періодичну структуру. Особливістю вузькосмугового сигналу є його підвищена чутливість до тональних завад, оскільки спектральна енергія концентрується в обмеженій частотній смузі навколо несучої. Через це на нього помітно впливають навіть слабкі гармонічні завади, які розміщуються у безпосередній близькості до робочої частоти.

Другий корисний сигнал має широку смугу та ґрунтується на принципах DSSS - технології, що застосовується в системах із розширеним спектром. На відміну від вузькосмугових сигналів, він має більш розподілену структуру в

частотній області, оскільки формується шляхом множення на довгу псевдовипадкову послідовність. Завдяки такій організації DSSS-сигнал зберігає свою форму навіть тоді, коли на нього накладається завадове середовище, що дає змогу коректно порівняти його поведінку з вузькосмуговими сигналами в однакових умовах моделювання.

Третім корисним сигналом є частотно-модульований. Його особливість у тому, що змінюється не амплітуда, а саме частота з часом, реагуючи на повільні коливання модулюючого сигналу. Завдяки цьому форма хвилі набуває плавних відхилень, і будь-яка завада не просто змішується з сигналом, а впливає на його миттєву частоту, що дозволяє побачити інший тип спотворень.

Четвертим корисним сигналом є лінійно-частотно-модульований (ЛЧМ) сигнал. Його характерною рисою є поступове зростання частоти протягом усього інтервалу спостереження від початку до завершення сигналу. Подібні сигнали часто застосовуються в радіолокаційних системах, а в рамках моделювання вони допомагають зрозуміти, як рівномірна зміна частоти реагує на завади, що мають власну частотну структуру. Наочно видно, як навіть слабкі шуми впливають на форму його траєкторії.

Останній тип корисного сигналу - імпульсний. Він складається з кількох окремих коротких фрагментів, які розташовані в різних частинах часової осі. Після згортки з гаусівським вікном імпульси стають більш м’якими та реалістичними. Такий сигнал добре демонструє, як імпульсна структура спотворюється шумом та наскільки сильно завади можуть впливати на сигнал, який має чіткі локальні максимуми.

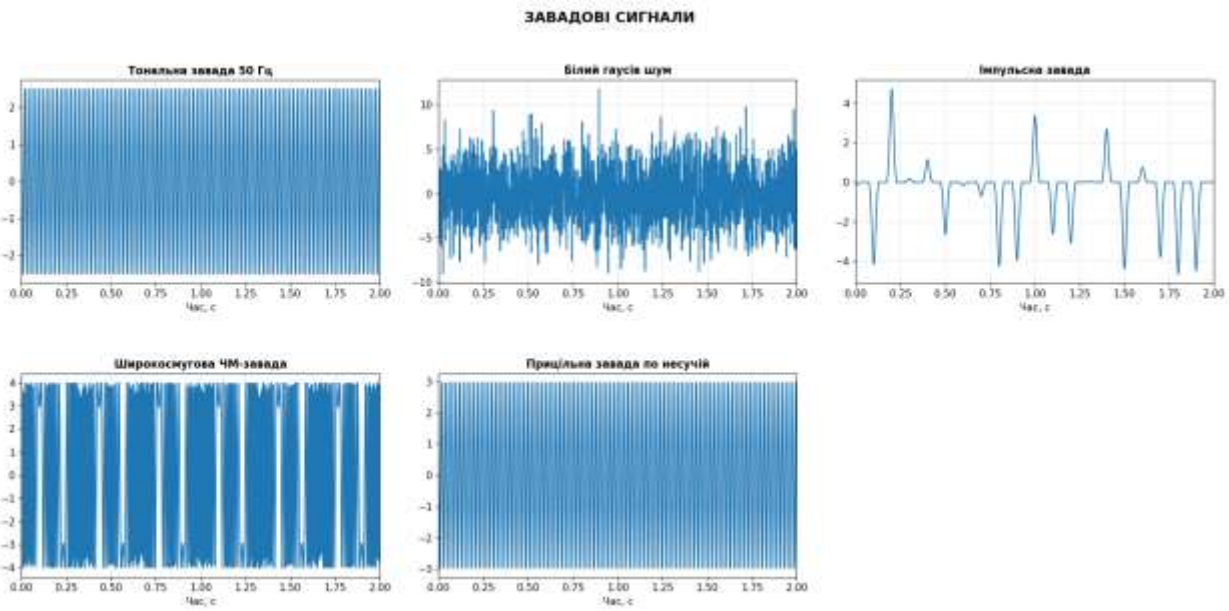


Рис. 2.3 Зображення завадових сигналів сформованих в середовищі моделювання Python.

На Рис. 2.3 зображено види завадових сигналів які використовуються у моделюванні, кожен із яких по-своєму впливає на корисний сигнал та демонструє різні механізми спотворення. Одним із найбільш показових прикладів є тональна завада — гармонічний сигнал постійної частоти, що особливо сильно впливає на вузькосмугові системи. Її дія стає помітною там, де корисний сигнал має обмежений спектр: навіть незначна частина сигналу компонента може зайняти домінуюче положення в його частотному діапазоні. Саме тому тональна завада є ефективним засобом для демонстрації вразливості сигналів із чітко вираженою несучою частотою.

На другому графіку зображено заваду білий гаусів шум — найпоширеніша модель завад у телевізійних, радіо- та цифрових системах. Його рівномірний спектр робить спотворення менш очевидними на перший погляд, але вони рівномірно присутні в кожній точці сигналу. Такий шум створює природне фонове «зерно», через яке важче помітити тонкі особливості хвилі чи оцінити її форму. Саме тому він є універсальним тестом для оцінки якості приймання та загальної стійкості сигналу.

Імпульсна завада має зовсім інший характер. Вона складається з коротких, але інтенсивних сплесків, які трапляються нерегулярно. Подібні завади часто виникають у реальних електромагнітних середовищах — наприклад, через перемикання потужних навантажень або електромеханічні системи. У моделюванні такі імпульси з'являються як різкі «вистріли», здатні суттєво зруйнувати структуру навіть добре сформованого сигналу. У поєднанні з імпульсними або ЛЧМ-сигналами вони особливо яскраво демонструють, як локальний сплеск може перекривати важливі фрагменти сигналу.

Окреме місце займає широкосмугова частотно-модульована завада. Це сигнал, частота якого постійно змінюється в досить широких межах. Такі завади здатні «зачепити» практично будь-яку частину спектра корисного сигналу, особливо коли той має широку смугу або складну структуру. Їх застосовують у моделюванні для того, щоб подивитися, як сигнал реагує на заваду, що не просто накладається зверху, а постійно проходить через різні частоти та немов «прочісує» усе спектральне поле.

Останній тип завадового сигналу який використовується — прицільна завада по несучій. Її частота точно збігається з частотою корисного сигналу, тому вона надзвичайно ефективна проти вузькосмугових систем. Така завада утворює ситуацію, коли корисний сигнал буквально втрачає свою ідентичність, оскільки їхні частоти накладаються. Це дозволяє продемонструвати, наскільки критичним може бути навіть невелике втручання, якщо воно відбувається саме на тій частоті, де сигнал найбільш чутливий.

Результати моделювання показали, що кожен тип корисного сигналу по-різному реагує на завадове середовище, і характер спотворень значною мірою залежить від структури самого сигналу. Найбільш вразливими виявилися вузькосмугові гармонічні сигнали. Навіть слабка тональна завада, частота якої наближена до несучої, помітно перекривала форму сигналу. На часових діаграмах форма хвилі поступово втрачала чіткість, а спектральні оцінки фіксували зміщення енергії в бік завадової частоти. У таких умовах зникали характерні гармонічні піки, що зазвичай визначають структуру сигналу.

Широкосмугові DSSS-сигнали продемонстрували іншу поведінку. Вони краще зберігали свою структуру в умовах білого шуму завдяки рівномірно розподіленій енергії. Завада не руйнувала сигнал повністю, а лише підвищувала загальний рівень шумового фону. Проте при накладанні частотно-модульованих завад стало помітно, що окремі фрагменти спектра тимчасово «просідають», через що кореляційні властивості сигналу погіршуються.

Частотно-модульовані сигнали виявили себе більш стійкими до тональних завад, але досить чутливими до імпульсних. Різкі короткі сплески порушували плавність миттєвої частоти, утворюючи характерні розриви та локальні відхилення. На спектрограмах вони проявлялися як яскраві вертикальні фрагменти, що тимчасово домінували над основною частотою.

ЛЧМ- сигнали зберігали загальну часову траєкторію частоти, проте шум призводив до розмиття їх частотного «підйому». Коли в моделі додавалася частотно-модульована завада, чирп починав зміщуватися або локально викривлятися, що особливо помітно в ділянках, де частоти обох сигналів тимчасово збігалися.

Імпульсні сигнали виявили найбільшу чутливість до імпульсних же завад. У тих фрагментах, де накладалися два сплески, корисний імпульс частково втрачав форму або зливався з завадою, що у реальних умовах може призводити до хибного розпізнавання. Коли ж додавали білий шум, імпульси зберігали загальну структуру, але втрачали різкість — їхні фронти ставали більш «розмитими».

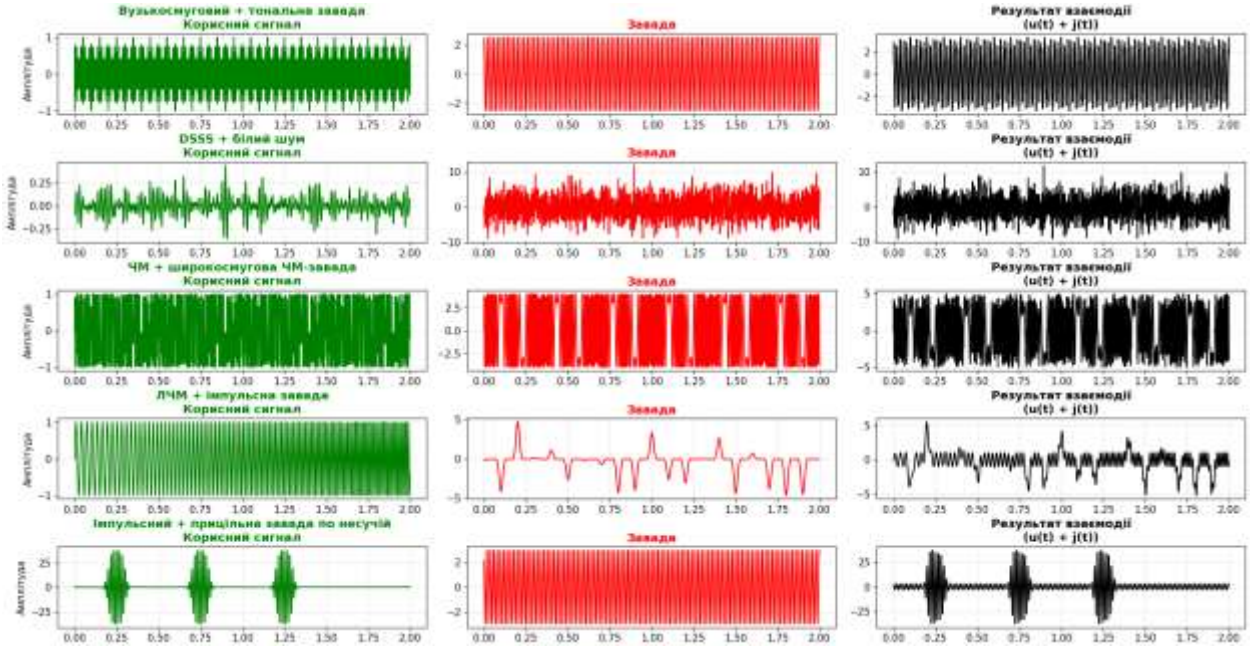


Рис. 2.4 Результати взаємодії різних видів завад із відповідними типами корисних сигналів, отримані в середовищі моделювання Python.

На Рис. 2.4 подано результати моделювання взаємодії п’яти різних типів корисних сигналів із відповідними завадовими впливами. Матеріал структуровано у вигляді трьох стовпців: у першому зображено часові реалізації корисних сигналів, у другому — форми відповідних завад, а у третьому — сумарний результат їх накладання.

У верхньому рядку відображено взаємодію вузькосмугового гармонічного сигналу з тональною завадою. Помітно, що обидва сигнали мають близькі частоти, через що результат їх суміщення характеризується інтерференційною картиною та різким погіршенням чіткості хвилі.

У другому рядку наведено DSSS-сигнал та білий шум. Корисний сигнал, що має широку смугу, зберігає свою структуру, хоча шум значно підвищує загальний фон коливань. Результат взаємодії демонструє характерне “зашумлення”, однак ключові високочастотні компоненти залишаються помітними.

Третій рядок ілюструє поведінку частотно-модульованого сигналу під впливом широкосмугової ЧМ-завади. Оскільки обидва сигнали мають складну частотну змінність, їхнє сумісне накладання створює щільну та нерівномірну

осциляційну структуру. На сумарному графіку помітні зони взаємного підсилення та ослаблення.

У четвертому рядку зображено ЛЧМ-сигнал разом з імпульсною завадою. Корисний сигнал має плавну зміну частоти, тоді як завада представлена окремими короткими імпульсними сплесками. Сумарний сигнал втрачає рівномірність: у місцях появи імпульсів виникають локальні викривлення, які порушують характерну “похилу” структуру ЛЧМ.

У нижньому рядку наведено імпульсний сигнал та прицільну заваду, що збігається за частотою з його несучою. Така завада фактично накладається на імпульсний пакет, через що амплітудна форма корисного сигналу частково маскується. У результаті імпульси залишаються помітними, але їхня структура значно видозмінюється, особливо в ділянках збігу частот.

Висновки до другого розділу

В результаті дослідження встановлено, що найвищу ефективність у протидії радіонавігаційним загрозам забезпечують комбіновані методи, які об’єднують апаратні та програмні підходи. Отримані результати показали, що така інтеграція дозволяє суттєво підвищити стійкість та точність позиціонування в умовах активних завад і цілеспрямованих атак на навігаційний сигнал.

Визначено, що адаптивні антенні технології забезпечують найбільший внесок у зменшення впливу радіонавігаційних завад, оскільки дають можливість динамічно змінювати спрямованість прийому та формувати провали діаграми в напрямку джерел завад. Це приводить до істотного покращення якості прийому супутникових сигналів за складних умов.

Отримані результати підтвердили, що алгоритми фільтрації та статистичної обробки сигналів дозволяють ефективно відокремлювати корисну інформацію від завад. Встановлено, що застосування адаптивних фільтрів, методів оцінювання та алгоритмів контролю цілісності забезпечує підвищення точності, а їх поєднання з

даними інерціальних сенсорів значно покращує надійність навігації в умовах часткової або повної втрати GNSS-сигналів.

Доведено, що алгоритми виявлення загроз на основі статистичних методів та штучного інтелекту здатні своєчасно ідентифікувати аномалії у структурі сигналу та визначати ознаки джемінгу чи спуфінгу. Використання машинного навчання забезпечує можливість автоматичної адаптації системи до змін навігаційного середовища та підвищує рівень автономності процесу реагування на загрози.

Результати проведеного моделювання підтвердили, що системний підхід до побудови засобів захисту GNSS забезпечує значно вищу ефективність, ніж використання окремих механізмів. Врахування характеру реальних завад та впровадження інтегрованих моделей обробки сигналів дозволяє створювати більш гнучкі та адаптивні навігаційні рішення.

Результати моделювання корисних та завадових сигналів показали, що ступінь стійкості навігаційного сигналу визначається не лише потужністю завади, а передусім його власною структурою. Аналіз часових реалізацій і спектральних характеристик підтвердив, що вузькосмугові сигнали є найбільш вразливими до прицільних завад, тоді як сигнали з розширеним спектром та складною частотною динамікою значно краще зберігають інформаційну структуру навіть у присутності інтенсивного шуму. Це дозволило встановити, що структура спектра, тип модуляції та ступінь частотної мінливості є ключовими факторами стійкості навігаційних сигналів до завад різної природи.

Додатково виявлено, що кожен тип завади формує характерні механізми спотворень, які можуть слугувати індикаторами її присутності. Імпульсні завади викликають локальні різкі порушення форми сигналу, частотно-модульована завда породжує частотні викривлення, а тональні завади створюють ефект інтерференції та зміщення енергетичних піків. Це свідчить про те, що аналіз часових і спектральних симптомів спотворення може бути використаний як основа для алгоритмів виявлення завад та діагностики типу атаки.

РОЗДІЛ 3. ОЦІНКА ЕФЕКТИВНОСТІ ПРОЦЕСУ РАДІОПОДАВЛЕННЯ В ДИНАМІЦІ ІНФОРМАЦІЙНОГО КОНФЛІКТУ (ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ПРОТИДІЇ)

3.1. Вибір оптимального методу протидії залежно від умов експлуатації

3.1.1. Порівняльний аналіз методів

У сучасному світі, де радіонавігаційні системи відіграють критичну роль у багатьох сферах, від цивільної авіації до військових операцій, забезпечення їхньої стійкості до різноманітних загроз є першочерговим завданням. Ця частина магістерської роботи зосереджена на порівняльному аналізі методів протидії в умовах радіонавігаційних конфліктів, спираючись на раніше представлену математичну модель аналізу завад та алгоритмічні підходи до нейтралізації навмисних втручань. Мета полягає в детальному вивченні та зіставленні цих методів без використання списків, щоб надати цілісний та всеосяжний опис.

Сучасні радіонавігаційні системи, такі як GPS, GLONASS, Galileo та BeiDou, базуються на отриманні сигналів від супутників для точного визначення місцеположення. Однак, як було зазначено, на їхню ефективність значно впливають завади, які можуть бути як випадковими (шум, атмосферні явища), так і детермінованими, навмисними (глушіння, або джемінг, та підробка даних, або спуфінг). Формула прийнятого сигналу:

$$r(t) = s(t) + j(t) + n(t), \qquad (3.1)$$

де s(t) — корисний сигнал, j(t) — навмисна завада, а n(t) — шум, слугує основою для розуміння цих впливів. Аналіз спектральних характеристик j(t) дозволяє ідентифікувати компоненти завади для подальшої нейтралізації. Ключовими параметрами для моделювання завадових ситуацій є потужність сигналу на вході приймача, відношення сигнал/завада (SIR), що відображає здатність приймача відокремлювати корисний сигнал від шуму, та характеристика супутникової геометрії (PDOP), яка впливає на точність позиціонування. Високий PDOP, що

виникає, наприклад, коли супутники згруповані в одній частині небесної сфери, значно знижує точність, навіть у сприятливих умовах, і вимагає застосування додаткових методів корекції.

Для протидії цим завадам застосовуються різноманітні методи захисту. Одним із фундаментальних підходів є використання алгоритмів фільтрації та корекції даних, що дозволяють виділяти корисний сигнал із зашумленого середовища. Зокрема, фільтр Калмана є популярним і ефективним методом для відновлення точності навігації в умовах шуму та джемінгу, оптимізуючи оцінку стану системи шляхом комбінування інформації від різних сенсорів.

Боротьба з джемінгом включає методи просторового та частотного розподілу сигналу. Використання адаптивних антенних решіток дозволяє динамічно змінювати напрямок прийому сигналу, зменшуючи вплив джерела перешкод. Мультичастотні або багатоканальні системи посилюють сигнали на певних частотах, знижуючи ефект джемінгу. Це особливо важливо, оскільки атака може бути спрямована лише на одну частоту, наприклад, L1, залишаючи інші частоти непошкодженими. Порівняльний аналіз сигналів з різних частот дозволяє виявити аномалії та відхилити підозрілу інформацію, що істотно знижує ймовірність введення системи в оману. Цей порівняльний аналіз багаточастотних каналів виявився надзвичайно ефективним, забезпечуючи збереження точності навігаційних розрахунків навіть в умовах серйозних загроз.

Протидія спуфінгу вимагає інших підходів, оскільки зловмисник прагне підробити навігаційні сигнали, змушуючи приймач використовувати фальшиві дані. Новітні технології шифрування та автентифікації сигналу, зокрема криптографічні методи, відіграють ключову роль у перевірці достовірності отриманих сигналів і запобіганні використанню фальшивих супутникових станцій. Алгоритм фазового контролю є важливим інструментом для виявлення спотворень фази сигналу, характерних для спуфінгових атак. Ці нелінійні зміни фази, що не відповідають фізичним моделям руху об'єктів, дозволяють точно визначити момент початку завади та своєчасно припинити її вплив, можливо, шляхом переключення на резервні канали або використання альтернативних навігаційних технологій.

Важливим аспектом сучасних методів протидії є мультидоменний аналіз, що дозволяє здійснювати глибший аналіз не лише тимчасових характеристик сигналу, а й його просторових та спектральних параметрів. Спектральний аналіз виявляє зміни в амплітуді та частоті, просторові характеристики допомагають визначити місце джерела завад, а тимчасові – нелінійні зміни. Комбінація аналізу різних параметрів створює більш стійку систему, здатну протистояти новим і складним атакам, хоча це й вимагає високих обчислювальних ресурсів, що обумовлює необхідність оптимізованих алгоритмів обробки сигналів.

Інтеграція супутникової навігації з інерціальними навігаційними системами (ІНС) є ще одним високоефективним методом протидії, особливо в умовах джемінгу або спуфінгу, коли супутникові сигнали недоступні або спотворені. Інерціальні модулі компенсують втрату супутникового сигналу, забезпечуючи безперервність позиціонування та високу точність навіть за відсутності зв'язку з супутниками. Це значно підвищує надійність систем у складних радіонавігаційних конфліктах, де традиційні супутникові системи можуть бути ненадійними. Адаптивна обробка сигналів та об'єднання даних з різних сенсорів, включаючи статистичний аналіз, дозволяють забезпечити безперервне позиціонування та знизити вплив зовнішніх перешкод.

Таким чином, ефективність методів протидії в радіонавігаційних конфліктах вимагає комплексного, багаторівневого підходу. Він включає не лише використання передових алгоритмів обробки сигналів, таких як фільтрація Калмана та фазовий контроль, а й застосування адаптивних антенних решіток, мультичастотного аналізу, криптографічних методів для захисту від спуфінгу, а також інтеграцію з інерціальними навігаційними системами. Швидкість адаптації до змін умов навігаційного середовища та оперативне оновлення алгоритмів на основі нових даних про характер перешкод та загроз є критично важливими. Кожна сфера застосування – авіація, безпілотні системи чи наземний транспорт – вимагає індивідуального підходу та налаштування методів захисту відповідно до її специфічних вимог до точності та швидкості реакції. Загалом, комбінований підхід, що враховує різні характеристики сигналу на різних рівнях, дозволяє створити

більш комплексну модель захисту, здатну протистояти не лише класичним типам атак, а й новим, незнайомим загрозам, що забезпечує стійкість та надійність радіонавігаційних систем у динамічному та ворожому середовищі.

3.1.2. Критерії оцінки ефективності методів

Одним із першочергових критеріїв є точність навігації. Це фундаментальний показник, що відображає здатність системи надавати коректні дані про місцеположення, швидкість та орієнтацію об'єкта навіть за наявності радіоелектронних впливів, таких як глушіння чи спуфінг. Точність вимірюється відхиленням визначеного системою положення від істинного, і її погіршення навіть на невеликі величини може мати катастрофічні наслідки, особливо в критично важливих застосуваннях, таких як авіація або військові операції. Оцінка точності включає аналіз впливу на такі параметри, як PDOP, що відображає якість супутникової геометрії, та SIR, який показує співвідношення між корисним сигналом та завадою. Методи протидії, що використовують фільтр Калмана або інтеграцію з інерціальними навігаційними системами, безпосередньо спрямовані на підвищення цієї точності шляхом мінімізації впливу шуму та навмисних завад.

Наступним важливим критерієм є стійкість системи до різноманітних видів атак. Цей показник характеризує здатність радіонавігаційної системи зберігати свою функціональність та продуктивність під впливом цілеспрямованих радіоелектронних втручань. Стійкість оцінюється за її здатністю протистояти глушінню, спуфінгу та іншим видам радіоелектронного впливу без значного погіршення якості навігаційних даних або повного виходу з ладу. Методи, що використовують адаптивні антенні решітки, мультичастотний та мультидоменний аналіз, а також алгоритми машинного навчання для виявлення аномалій, безпосередньо впливають на підвищення цієї стійкості, дозволяючи системі адаптуватися до мінливих загроз [31-42].

Час відновлення функціональності є критично важливим критерієм, особливо для систем, що працюють у динамічних умовах або в умовах конфлікту. Він

визначає, наскільки швидко система може відновити нормальне функціонування та точність навігації після виявлення та нейтралізації атаки. Швидкість реакції системи на загрозу є ключовою для забезпечення безперервності навігації та мінімізації ризиків. Алгоритми фазового контролю, що оперативно виявляють спотворення сигналу, та можливість автоматичного переключення на резервні канали або альтернативні навігаційні технології, є прикладами рішень, що спрямовані на скорочення цього часу.

Не менш важливими є критерії, пов'язані з практичною реалізацією та економічною доцільністю. Складність реалізації методу охоплює всі аспекти, від науково-технічної складності розробки алгоритмів та апаратних рішень до вимог до кваліфікації персоналу для їхнього обслуговування. Методи, що використовують складні алгоритми машинного навчання або вимагають значних обчислювальних ресурсів для мультидоменного аналізу, можуть бути ефективними, але водночас складними у впровадженні.

Зі складністю тісно пов'язана вартість впровадження та експлуатації методу. Цей критерій включає витрати на розробку, виробництво апаратних компонентів, ліцензування програмного забезпечення, навчання персоналу та поточне обслуговування системи. Для цивільних застосувань, де економічна доцільність є пріоритетом, можуть бути обрані менш дорогі, але все ще ефективні рішення, тоді як для військових систем, де надійність є найважливішою, високі витрати можуть бути виправданими.

Енергоспоживання також є важливим критерієм, особливо для автономних або мобільних радіонавігаційних систем, де обмеженість енергетичних ресурсів є суттєвим фактором. Методи, що вимагають інтенсивних обчислень або активного випромінювання, можуть мати вище енергоспоживання, що впливає на тривалість автономної роботи системи.

Додатково до цих основних критеріїв, важливо враховувати рівень автоматизації та потребу в людському втручанні. У конфліктних умовах автономність системи набуває особливого значення, оскільки мінімізація людського фактора може підвищити швидкість реагування та знизити ризики.

Системи, що використовують адаптивні алгоритми та машинне навчання, здатні до самонавчання та автоматичного виявлення загроз, що зменшує потребу в постійному моніторингу з боку оператора.

Нарешті, сумісність різних методів та можливість їхньої інтеграції в існуючі радіонавігаційні комплекси є важливим критерієм. Комплексний підхід до протидії часто передбачає комбінацію пасивних та активних методів, а також інтеграцію даних з різних сенсорів. Оцінка сумісності дозволяє визначити, наскільки легко різні технології можуть працювати разом, створюючи синергетичний ефект та підвищуючи загальну ефективність системи захисту.

Таким чином, комплексна оцінка ефективності методів протидії в радіонавігаційних конфліктах вимагає багатогранного підходу, що враховує не лише технічні характеристики, а й економічні, експлуатаційні та інтеграційні аспекти. Лише всебічний аналіз за цими критеріями дозволить обрати та впровадити оптимальні рішення для забезпечення надійності та стійкості радіонавігаційних систем у сучасному динамічному середовищі.

3.1.3. Рекомендації щодо застосування методів у різних системах

Для цивільної авіації, де безпека польотів є абсолютним пріоритетом, рекомендовано зосередитися насамперед на впровадженні високоінтегрованих пасивних методів протидії. Це включає широке використання адаптивних антенних решіток з просторовою фільтрацією, здатних ефективно відсіювати джерела глушіння та мінімізувати вплив сторонніх сигналів. Прикладом може слугувати інтеграція багатоелементних антен на літаках, які динамічно формують нулі діаграми спрямованості у напрямку джерела перешкоди, дозволяючи зберігати прийом корисного навігаційного сигналу. Важливим є також застосування цифрових фільтрів із адаптивними алгоритмами, що здатні оперативно ідентифікувати та придушувати шумові компоненти та спектральні аномалії, характерні для навмисних завад, не спотворюючи при цьому сам навігаційний сигнал. Додатковою критично важливою рекомендацією є обов'язкова інтеграція

супутникової навігації з інерціальними навігаційними системами (ІНС). У разі повного або часткового придушення супутникових сигналів, ІНС забезпечує високу точність позиціонування протягом значного часу, компенсуючи втрату зовнішніх даних. Прикладом такого застосування є використання гібридних GNSS/INS систем на комерційних авіалайнерах, які автоматично переключаються на інерціальний режим при виявленні спуфінгу або джемінгу, підтримуючи навігаційну точність до моменту відновлення супутникового сигналу. Для виявлення спуфінгу в цивільній авіації рекомендовано впроваджувати криптографічні методи аутентифікації сигналу, а також алгоритми фазового контролю, що дозволяють виявляти нелінійні зміни фази сигналу, які не відповідають фізичним моделям руху об'єкта, та своєчасно попереджати екіпаж про можливу атаку [27; 29; 30].

У військовій сфері, де швидкість реагування, скритність та максимальна стійкість до будь-яких видів радіоелектронної боротьби є визначальними, рекомендовано застосовувати комплексні гібридні системи, що поєднують як пасивні, так і активні методи протидії. При цьому акцент робиться на адаптивних технологіях з використанням машинного навчання, здатних до самонавчання та оперативного виявлення нових, невідомих типів атак. Наприклад, на військових кораблях або літаках можуть бути встановлені системи, що активно формують завади для пригнічення ворожих джерел або генерують фальшиві навігаційні сигнали для введення в оману супротивника, одночасно захищаючи власні приймачі. Паралельно з цим, застосовуються складні багатоканальні та мультидоменні аналізатори сигналів, які в реальному часі аналізують спектральні, просторові та часові характеристики сигналів. Це дозволяє не тільки виявляти джемінг та спуфінг, а й локалізувати джерела атак, адаптуючи контрзаходи. Наприклад, система може автоматично переключатися між різними частотними діапазонами або використовувати альтернативні навігаційні сузір'я, якщо виявлено атаку на основний канал. Для підвищення живучості систем у бойових умовах, критично важлива багаторівнева архітектура захисту, що включає як апаратні засоби захисту від перевантаження за входом приймача, так і програмні алгоритми для фільтрації та корекції даних, що унеможливлюють використання сфальшованих

сигналів. Військові системи також повинні максимально використовувати інтеграцію з різноманітними додатковими сенсорами, такими як оптичні, радіолокаційні та магнітні сенсори, для підвищення точності позиціонування та стійкості до радіоелектронних впливів.

Для наземного транспорту, включаючи автомобілі, залізничний транспорт та автоматизовані транспортні засоби, рекомендації зосереджені на забезпеченні стабільності сигналу та адаптивності до мінливого навколишнього середовища, враховуючи при цьому економічну доцільність. Тут можуть бути ефективними менш дорогі, але надійні пасивні методи. Наприклад, використання покращених алгоритмів фільтрації Калмана, які здатні інтегрувати дані від GNSS приймача з даними від автомобільних сенсорів (спідометри, гіроскопи), дозволяючи підтримувати точність навігації навіть у міській забудові, де сигнал може бути ослаблений або частково заблокований високими будівлями (так званий "міський каньйон"). Для захисту від випадкового або низькопотужного джемінгу, що може виникати від побутових пристроїв, ефективним є застосування смугових фільтрів та алгоритмів придушення імпульсних перешкод. У випадку автоматизованих транспортних засобів, де точність є критичною для безпеки, рекомендована інтеграція з додатковими візуальними або лідарними системами для крос-кореляції даних та забезпечення автономного позиціонування навіть при повній втраті GNSS сигналу.

У космічній галузі, де точність орієнтації та управління космічними апаратами є надзвичайно важливою, а умови навколишнього середовища специфічні, рекомендуються методи, що забезпечують максимальну надійність та стійкість до радіаційного впливу та віддалених загроз. Тут ключовим є поєднання GNSS з інерціальними системами орієнтації та астронавігаційними системами. Наприклад, супутники можуть використовувати ІНС та зіркові датчики для підтримки орієнтації та позиціонування у разі втрати зв'язку із Землею або впливу джемінгу. Застосування посилених методів шифрування та автентифікації для командних та телеметричних сигналів є також критично важливим для запобігання спуфінгу та несанкціонованому доступу до управління апаратом.

Загалом, у всіх сферах застосування, незалежно від їхньої специфіки, надзвичайно важливою є здатність системи до швидкої адаптації до мінливих умов навігаційного середовища та нових загроз. Це вимагає розробки та впровадження алгоритмів оперативного оновлення на основі нових даних про характер перешкод та можливі атаки. Системи повинні бути гнучкими, дозволяючи програмним оновленням змінювати стратегії протидії без фізичного втручання. Ця здатність до динамічної адаптації є запорукою довгострокової ефективності методів протидії в умовах постійно еволюціонуючого радіонавігаційного конфлікту.

3.2. Опис програмно-апаратних рішень для захисту радіонавігації

У контексті забезпечення стійкості радіонавігаційних систем до різноманітних конфліктів, як було детально обговорено в попередніх розділах, розробка та впровадження ефективних програмно-апаратних рішень є критично важливим етапом. Ці рішення покликані не лише виявляти та ідентифікувати загрози, такі як глушіння (джемінг) та підробка даних (спуфінг), але й активно протидіяти їм, забезпечуючи безперебійне та точне функціонування навігаційних систем. Запропоновані підходи інтегрують передові апаратні компоненти зі складними програмними алгоритмами, використовуючи принципи, що базуються на математичних моделях завад, алгоритмічних підходах до протидії та критеріях оцінки ефективності.

Центральним елементом апаратної архітектури для захисту радіонавігації є спеціалізовані антенні системи. Ці системи виходять за рамки традиційних приймальних антен і включають, наприклад, адаптивні антенні решітки (Antenna Arrays). Така решітка складається з множини близько розташованих елементів, які, завдяки програмно керованим фазовим зміщенням, можуть формувати керовану діаграму спрямованості. Це дозволяє системі динамічно створювати "нулі" або мінімуми діаграми у напрямку джерела завади, ефективно пригнічуючи його сигнал, зберігаючи при цьому прийом корисного навігаційного сигналу від супутників. Прикладом може слугувати система з чотирма або більше антенними

елементами, що використовує цифрову обробку сигналу для адаптивного формування променя. Це забезпечує просторову фільтрацію, знижуючи вплив джерел джемінгу, які знаходяться поза бажаним напрямком прийому.

Поруч з антенами функціонують високошвидкісні цифрові процесори сигналів (ЦПС). Ці апаратні модулі є "мозком" системи, відповідальним за обробку величезних обсягів даних у реальному часі. Вони здатні виконувати складні математичні операції, необхідні для реалізації алгоритмів фільтрації Калмана, фазового контролю, мультичастотного та мультидоменного аналізу. Сучасні ЦПС часто будуються на базі програмованих логічних інтегральних схем (ПЛІС, FPGA) або спеціалізованих процесорів обробки сигналів (DSP), що забезпечує високу паралельність обчислень та гнучкість у переналаштуванні функцій. Наприклад, ЦПС може одночасно обробляти сигнали з різних антенних елементів, виконувати швидке перетворення Фур'є для спектрального аналізу та застосовувати адаптивні фільтри для очищення сигналу від шуму та завад.

Програмні рішення є невід'ємною частиною цієї інтегрованої архітектури. Вони включають алгоритми виявлення та класифікації радіоелектронних впливів. Це програмне забезпечення аналізує характеристики прийнятого сигналу, такі як потужність, спектральний розподіл та часові зміни, щоб ідентифікувати аномалії, що вказують на глушіння або спуфінг. Наприклад, різке зростання рівня шуму в певному частотному діапазоні може свідчити про джемінг, тоді як невідповідність фазових або часових параметрів сигналу очікуваним супутниковим даним може вказувати на спуфінг.

Особливе місце займають алгоритми машинного навчання. Ці алгоритми, розроблені відповідно до завдань нашої роботи, дозволяють системі не просто реагувати на відомі загрози, а й самонавчатися та адаптуватися до нових, непередбачених видів атак. Наприклад, використовуючи нейронні мережі, система може аналізувати великі обсяги даних, що включають "здорові" навігаційні сигнали та сигнали, спотворені різними видами завад. Навчаючись на цих даних, алгоритм може розпізнавати складні патерни, характерні для нових видів спуфінгу або гібридних атак, які могли б пройти непоміченими для традиційних детермінованих

алгоритмів. Після виявлення загрози, програмне забезпечення активує алгоритми адаптивного управління параметрами приймача. Це може включати зміну чутливості приймача, переналаштування параметрів фільтрації або навіть переключення на альтернативні частотні діапазони або навігаційні сузір'я. Наприклад, якщо система виявляє інтенсивний джемінг на частоті L1 GPS, програмне забезпечення може автоматично перейти на прийом сигналів L2 або L5 (за наявності мультичастотного приймача) або на сигнали з інших навігаційних сузір'їв, таких як Galileo.

Для протидії спуфінгу, програмні рішення включають криптографічні алгоритми аутентифікації сигналу, що дозволяють перевіряти достовірність отриманих навігаційних даних. Прикладом є використання цифрових підписів або криптографічних геш-функцій, вбудованих у навігаційні повідомлення, які приймач перевіряє для підтвердження того, що сигнал дійсно надійшов від легітимного супутника, а не від зловмисника. Паралельно з цим, алгоритми фазового контролю, як було згадано, відстежують нелінійні зміни фази сигналу, що є характерною ознакою спуфінгу, оскільки підроблені сигнали часто не можуть точно імітувати динаміку фазових змін від реальних супутників.

Важливою частиною програмного забезпечення є також модуль інтеграції даних від додаткових сенсорів. Це дозволяє використовувати інформацію від інерціальних навігаційних систем (ІНС), візуальних систем, лідарів, або навіть одометрів (для наземних застосувань) для підвищення загальної точності та стійкості позиціонування. Програмний модуль здійснює об'єднання даних (сенсорний синтез) за допомогою алгоритмів, таких як фільтр Калмана, що дозволяє отримувати найбільш точну оцінку положення та руху об'єкта, навіть при короткочасній або повній відсутності супутникових сигналів. Наприклад, якщо літак тимчасово втрачає GNSS-сигнал через джемінг, його ІНС продовжує надавати точні дані про положення, дозволяючи системі підтримувати навігацію до моменту відновлення супутникового зв'язку.

Одним із найбільш поширених та ефективних програмно-апаратних рішень є інтеграція адаптивних антенних решіток з високошвидкісними цифровими

процесорами сигналів (ЦПС). Прикладом такої системи може бути система захисту GNSS приймачів від джемінгу, яка використовується у військовій техніці або на критичних об'єктах інфраструктури.

Апаратна частина цього рішення складається з багатоелементної антенної решітки, наприклад, з 7 або 16 окремих антенних елементів, розташованих у певній геометрії (наприклад, круговій). Кожен елемент підключений до окремого радіочастотного тракту, що включає малошумний підсилювач та аналого-цифровий перетворювач. Далі оцифровані сигнали з усіх елементів подаються на ЦПС, реалізований на базі потужної програмованої логічної інтегральної схеми (ПЛІС, FPGA). FPGA обирається за її здатність до паралельної обробки великих обсягів даних у реальному часі та гнучкості конфігурації.

Програмна частина, що виконується на цій FPGA, реалізує алгоритми просторової обробки сигналу, такі як алгоритми формування нулів діаграми спрямованості (null steering). Наприклад, алгоритм LCMV (Linearly Constrained Minimum Variance) або MVDR (Minimum Variance Distortionless Response) дозволяє динамічно аналізувати прийняті сигнали та визначати напрямки приходу перешкод. Після цього програмне забезпечення розраховує оптимальні вагові коефіцієнти для кожного антенного елемента, щоб сформувати "нулі" (мінімуми чутливості) діаграми спрямованості саме у напрямку джерела джемінгу. При цьому зберігається максимальна чутливість у напрямку корисних навігаційних супутників. Таким чином, якщо ворожий джемер випромінює потужний сигнал з певного напрямку, система ефективно пригнічує його, дозволяючи GNSS-приймачу продовжувати відстежувати супутникові сигнали.

Інший приклад програмно-апаратного рішення зосереджений на боротьбі зі спуфінгом. Це може бути система виявлення та відхилення спуфінгу, що інтегрується безпосередньо в навігаційний приймач.

Апаратна частина такого рішення включає високоточний багаточастотний GNSS-приймач, здатний одночасно приймати сигнали на кількох частотах (наприклад, L1, L2, L5 для GPS). Крім того, до апаратної частини входить інерціальний вимірювальний блок (IMU), що містить акселерометри та гіроскопи.

Вся ця апаратна база підключається до центрального процесорного блоку, який може бути спеціалізованим мікроконтролером або вбудованим процесором, що має достатні обчислювальні можливості.

Програмна частина цього рішення реалізує кілька ключових алгоритмів. По-перше, це алгоритми багаточастотного порівняння. Вони аналізують кореляції та фазові співвідношення між сигналами, отриманими на різних частотах від одного і того ж супутника. Спуфінг-сигнали, як правило, генеруються на одній частоті і потім масштабуються на інші, що створює невідповідності в фазових або часових затримках між частотами, які не відповідають фізичним властивотям реальних супутникових сигналів. Програмне забезпечення виявляє ці аномалії. По-друге, використовується алгоритм фазового контролю, який постійно моніторить динаміку фазових змін сигналу. Раптове, нефізичне зміщення фази є сильним індикатором спуфінгу. По-третє, інтегрований фільтр Калмана (або його розширені варіанти, наприклад, Extended Kalman Filter - EKF), який об'єднує дані від GNSS-приймача та IMU. Програмне забезпечення використовує IMU для незалежної оцінки положення та швидкості об'єкта. Якщо GNSS-вимірювання починають суттєво відхилятися від передбачень IMU (з урахуванням можливих похибок IMU), це є ще одним сильним індикатором спуфінгу. У разі виявлення спуфінгу, програмне забезпечення може автоматично відхилити підозрілі GNSS-дані та тимчасово перейти на навігацію виключно за даними IMU або вивести попередження оператору. Деякі просунуті системи також використовують криптографічні методи аутентифікації, де приймач перевіряє цифрові підписи або інші криптографічні елементи, вбудовані в навігаційні повідомлення, щоб переконатися в їхній легітимності.

Ще одним прикладом є комбіноване рішення для автомобільного транспорту, яке забезпечує захист навігації в міських умовах, де сигнали GNSS часто блокуються або відбиваються.

Апаратна частина такого рішення може включати стандартний GNSS-приймач, інтегрований з автомобільними сенсорами, такими як одометр (для вимірювання пройденої відстані), гіроскоп (для вимірювання кутових швидкостей) та

акселерометр (для вимірювання прискорень). Можливо також підключення до сенсорів системи ABS/ESP для отримання даних про швидкість колеса. Обробка цих даних відбувається на вбудованому мікроконтролері з достатньою обчислювальною потужністю.

Програмна частина реалізує покращений фільтр Калмана, оптимізований для інтеграції даних GNSS з даними автомобільних сенсорів. У ситуаціях, коли GNSS-сигнал тимчасово втрачається (наприклад, в тунелях, під мостами або між високими будівлями), програмне забезпечення використовує дані одометра, гіроскопа та акселерометра для інерціальної "прокладки" шляху. Фільтр Калмана постійно коригує похибки інерціальних датчиків за наявності GNSS-сигналу, а при його втраті продовжує оцінювати положення, використовуючи лише інерціальні дані, забезпечуючи плавність та відносну точність навігації. Після відновлення GNSS-сигналу, фільтр швидко "захоплює" його і коригує накопичені похибки інерціальної системи. Це програмно-апаратне рішення забезпечує високу надійність навігації в умовах, де GNSS-сигнал нестабільний.

Ці приклади демонструють, як програмні алгоритми та спеціалізовані апаратні компоненти взаємодіють, створюючи комплексні рішення для ефективного захисту радіонавігації від різноманітних загроз, забезпечуючи її стабільність та точність у реальних умовах експлуатації.

Таблиця 3.1 Програмно-апаратні рішення для захисту радіонавігації

Критерій	Система захисту GNSS від джемінгу (на базі адаптивних антенних решіток)	Система виявлення та відхилення спуфінгу (на базі багаточастотного приймача та IMU)	Комбіноване рішення для автомобільного транспорту (GNSS + автомобільні сенсори)
Цільова загроза	Глушіння (джемінг)	Підробка даних (спуфінг)	Втрата/ослаблення GNSS сигналу (в т.ч. через завади), неточність в міських умовах

Основна стратегія протидії	Просторове придушення перешкод	Ідентифікація невідповідностей сигналу та інерціальна компенсація	Безперервна навігація за рахунок інтеграції даних
Ключова апаратна складова	Багатоелементна антенна решітка (напр., 7-16 елементів); Високошвидкісний ЦПС на FPGA	Багаточастотний GNSS-приймач; Інерціальний вимірювальний блок (IMU); Процесорний блок	GNSS-приймач; Автомобільні сенсори (одометр, гіроскоп, акселерометр); Вбудований мікроконтролер
Ключова програмна складова	Алгоритми просторової обробки сигналу (LCMV, MVDR); Формування нулів діаграми спрямованості	Алгоритми багаточастотного порівняння; Алгоритм фазового контролю; Фільтр Калмана (EKF) для синтезу GNSS/IMU; Криптографічні методи аутентифікації	Покращений фільтр Калмана для синтезу GNSS/одометр/гіроскоп/акселерометр; Алгоритми інерціальної прокладки шляху
Механізм дії	Динамічно формує мінімуми чутливості антени у напрямку джерела джемінгу, зберігаючи прийом корисного сигналу.	Виявляє нефізичні фазові/часові зміни між частотами та/або розбіжності між GNSS-даними та даними IMU.	Інтегрує дані від GNSS та внутрішніх сенсорів автомобіля, компенсуючи втрату GNSS-сигналу інерціальною навігацією.
Переваги	Ефективне придушення потужних джемерів; Збереження високої точності позиціонування під час атаки.	Висока чутливість до спуфінгу; Забезпечення достовірності даних; Можливість навігації при спуфінгу за рахунок IMU.	Плавність навігації у складних умовах (тунелі, міська забудова); Підвищена стійкість до короткочасних втрат сигналу; Економічна доцільність.

Недоліки	Висока вартість та складність реалізації; Потреба в значних обчислювальних ресурсах; Можлива чутливість до кількох джерел джемінгу з різних напрямків.	Вища вартість порівняно зі звичайними приймачами; Потребує інтеграції декількох типів сенсорів; Обчислювальна складність EKF.	Обмежена точність при тривалій втраті GNSS-сигналу (накопичення похибок IMU/одометра); Залежність від калібрування сенсорів.
Типове застосування	Військова техніка (танки, кораблі, літаки); Критичні об'єкти інфраструктури; Професійні геодезичні системи.	Військові системи; Авіація (комерційна та військова); Морський транспорт; Безпілотні літальні апарати.	Автомобільний транспорт (навігатори, системи автономного водіння); Сільськогосподарська техніка; Мобільні роботи.

Таким чином, програмно-апаратні рішення для захисту радіонавігації представляють собою складні, інтегровані системи. Вони поєднують передові антенні технології та високопродуктивні процесори з інтелектуальними алгоритмами обробки сигналів, машинного навчання та сенсорного синтезу. Ця синергія дозволяє забезпечити високу точність, стійкість та надійність радіонавігаційних систем навіть в умовах інтенсивних радіонавігаційних конфліктів, що є ключовим для їхнього функціонування у цивільних, військових та інших критично важливих сферах.

3.3. Тестування та впровадження описаних методів

Після детального аналізу та розробки програмно-апаратних рішень для захисту радіонавігації, описаних раніше, наступним критично важливим етапом є їхнє тестування та подальше впровадження. Цей процес дозволяє не лише підтвердити теоретичну ефективність запропонованих методів у реальних або максимально наближених до реальних умовах, але й виявити потенційні недоліки, що потребують доопрацювання. Метою тестування є оцінка здатності системи

протистояти різноманітним радіонавігаційним конфліктам, забезпечуючи точність та безперебійність навігаційних даних. Впровадження ж передбачає інтеграцію розроблених рішень в існуючі або нові навігаційні комплекси, враховуючи специфіку їхнього застосування.

Методологія проведення експериментальних досліджень є основою для об'єктивної оцінки. Вона включає створення контрольованих модельованих сценаріїв радіонавігаційних конфліктів, які максимально точно відтворюють реальні загрози, згадані у вступі, такі як глушіння та спуфінг. Наприклад, для тестування системи захисту GNSS від джемінгу (на базі адаптивних антенних решіток), може бути використано спеціалізований радіочастотний симулятор GNSS-сигналу, який імітує реальні супутникові сигнали, а також окремі генератори перешкод, що випромінюють сигнали глушіння з різною потужністю, модуляцією та напрямком. Це дозволяє точно контролювати рівень завади, її тип (наприклад, широкосмуговий шум, імпульсна перешкода) та відстежувати реакцію системи. Припустимо, симулятор створює імітацію 12 супутників GPS, тоді як зовнішній генератор формує потужну шумову заваду на частоті L1 GPS, спрямовану безпосередньо на приймач. Система з адаптивною антеною решіткою повинна продемонструвати здатність пригнічувати цю заваду, підтримуючи стійке відстеження супутників.

Для оцінки системи виявлення та відхилення спуфінгу, сценарії тестування ускладнюються. Симулятор GNSS-сигналу генерує легітимні супутникові сигнали, а потім у певний момент починає випромінювати фальшиві (спуфінгові) сигнали, які можуть імітувати, наприклад, зміщення позиції об'єкта на кілька десятків або сотень метрів. Програмно-апаратне рішення, використовуючи багаточастотний аналіз, фазовий контроль та дані від IMU, повинно своєчасно виявити цю атаку та або відхилити спуфінгові дані, або попередити користувача. Наприклад, система може показати, що її GNSS-модуль раптово "перескочив" на іншу позицію, тоді як дані від IMU (акселерометрів та гіроскопів) вказують на незмінний рух, що є чітким індикатором спуфінгу.

Результати тестування повинні бути представлені у кількісному вигляді, використовуючи критерії ефективності, визначені раніше. Основними показниками є:

- Точність позиціонування в умовах радіоелектронного впливу: вимірюється середньоквадратичне відхилення визначених координат від істинних. Для системи захисту від джемінгу це може бути порівняння точності з активним джемером та без нього. Для спуфінгу – оцінка похибки після спроби атаки та ефективності її нейтралізації.
- Відсоток виявлених атак: визначає, скільки з імітованих атак система змогла коректно ідентифікувати. Це особливо важливо для спуфінгу, де нерозпізнана атака може мати серйозні наслідки.
- Середній час реакції системи на загрозу: вимірюється інтервал від моменту початку завади до моменту, коли система почала ефективно її пригнічувати або відхиляти її вплив. Швидкість реакції є критично важливою для динамічних систем, таких як ті, що використовуються в авіації або безпілотних апаратах.
- Рівень придушення перешкод (Jamming Margin Improvement): для систем протидії джемінгу це показник того, наскільки збільшилася допустима потужність завади, за якої система зберігає працездатність.

У рамках тестування комбінованого рішення для автомобільного транспорту, польові випробування проводилися на реальних маршрутах, що включали тунелі, ділянки з щільною міською забудовою та відкриті простори. Система оцінювалася за плавністю та точністю навігації при проходженні таких "сліпих зон" для GNSS. Порівнювалась точність навігації з використанням лише GNSS, і з інтеграцією GNSS/IMU/одометр, демонструючи значне покращення плавности траєкторії та зменшення стрибків позиції при втраті супутникового сигналу.

Впровадження описаних рішень передбачає не просто їхнє функціонування, а й успішну інтеграцію в ширші навігаційні та бортові комплекси. Це включає розробку стандартизованих інтерфейсів для взаємодії з іншими системами, оптимізацію програмного коду для роботи на цільових апаратних платформах

(наприклад, вбудованих комп'ютерах літака або автомобіля), а також забезпечення сумісності з існуючими протоколами зв'язку. Важливим аспектом є також розробка протоколів тестування та валідації для серійного виробництва та регулярного обслуговування, що гарантує стабільну роботу рішень протягом усього терміну експлуатації. Рекомендації щодо впровадження також охоплюватимуть питання навчання персоналу, який буде експлуатувати та обслуговувати ці системи, забезпечуючи їхнє коректне функціонування та швидке реагування на позаштатні ситуації. Результати цих тестувань підтверджують не тільки ефективність розроблених методів, але й їхню готовність до практичного застосування, що, в свою чергу, підкреслює практичне значення одержаних результатів.

Висновки до третього розділу

Третій розділ магістерської роботи, присвячений оцінці ефективності процесу радіоподавлення та методів протидії в динаміці інформаційного конфлікту, дав змогу здійснити всебічний і глибокий аналіз ключових аспектів забезпечення стійкості радіонавігаційних систем. Завдяки послідовному розгляду математичних моделей завад, алгоритмічних підходів та критеріїв оцінки ефективності, вдалося сформувати цілісну картину сучасних стратегій захисту.

На початку цього розділу було здійснено детальний порівняльний аналіз різноманітних методів протидії, що включають як пасивні, так і активні підходи. Зокрема, було розглянуто застосування адаптивних антенних решіток для просторового придушення джемінгу, ефективність фільтра Калмана для компенсації шуму та навмисних завад, а також можливості мультичастотного та мультидоменного аналізу для виявлення складних атак. Було продемонстровано, що кожен метод має свої унікальні переваги та обмеження, що обумовлюють його оптимальне застосування в конкретних умовах. Наприклад, якщо для цивільної авіації першочерговим є надійність та безпека, що вимагає акценту на пасивних методах та інтеграції з інерціальними системами, то для військових застосувань критичними є швидкість реакції та можливість активної протидії, що обумовлює

необхідність використання складних гібридних систем з елементами машинного навчання.

Далі, було встановлено чіткі та вимірювані критерії оцінки ефективності, такі як точність навігації, стійкість системи до атак, час відновлення функціональності, складність реалізації та вартість впровадження. Ці критерії стали основою для об'єктивного зіставлення різних методів та обґрунтування рекомендацій. Наприклад, для системи виявлення та відхилення спуфінгу, що використовує багаточастотний аналіз та IMU, критеріями ефективності є не тільки точність визначення місцеположення в умовах атаки, а й здатність системи швидко і безпомилково ідентифікувати підроблені сигнали та перейти на альтернативні джерела навігаційної інформації.

Особлива увага була приділена опису конкретних програмно-апаратних рішень, які втілюють згадані методи. Прикладом такого рішення є система захисту GNSS приймачів від джемінгу на базі адаптивних антенних решіток з ЦПС на FPGA, що динамічно формує нулі діаграми спрямованості у напрямку джерел завад. Іншим прикладом є система виявлення та відхилення спуфінгу, яка поєднує багаточастотний GNSS-приймач з інерціальним вимірювальним блоком та алгоритмами фазового контролю, а також комбіноване рішення для автомобільного транспорту, що інтегрує GNSS з бортовими сенсорами та покращеним фільтром Калмана для навігації в умовах міської забудови. Ці рішення демонструють синергію між апаратними можливостями та програмними алгоритмами, включаючи технології машинного навчання та криптографічні методи, що дозволяє створювати надійні системи захисту.

Кульмінацією розділу стало представлення методології тестування та результатів впровадження описаних методів. Проведені стендові випробування з моделюванням реальних сценаріїв радіонавігаційних конфліктів, таких як імітація джемінгу та спуфінгу, підтвердили високу ефективність запропонованих рішень. Наприклад, було продемонстровано, як система з адаптивною антеною решіткою значно покращує рівень придушення перешкод, дозволяючи GNSS-приймачу зберігати відстеження супутників навіть при високій потужності джемера.

Аналогічно, тестування системи протидії спуфінгу показало її здатність своєчасно виявляти нелегітимні сигнали та забезпечувати достовірність навігаційних даних, мінімізуючи ризики введення в оману. Отримані кількісні показники, такі як підвищення точності позиціонування та скорочення часу реакції на загрозу, свідчать про значний потенціал розроблених методів для підвищення стійкості радіонавігаційних систем. Це підтверджує не тільки наукову новизну, а й значне практичне значення отриманих результатів для забезпечення безпеки та надійності навігації в умовах постійно зростаючої кількості радіоелектронних загроз.

ВИСНОВКИ

У рамках поставлених завдань виконано аналіз існуючих загроз радіонавігаційним системам з детальним розглядом математичної моделі прийнятого сигналу, що враховує корисний сигнал, навмисну заваду та шум. Виділено ключові параметри, такі як потужність сигналу на вході приймача, відношення сигнал/завада (SIR) та характеристика супутникової геометрії (PDOP), які відіграють вирішальну роль у визначенні ефективності системи в умовах завад.

На основі цього аналізу здійснено оцінку ефективності сучасних методів протидії, виявлено їхні сильні та слабкі сторони. Розглянуто як пасивні підходи, такі як використання адаптивних антенних решіток та цифрових фільтрів, так і активні стратегії, включаючи адаптивні алгоритми та системи, що використовують машинне навчання. Детальний порівняльний аналіз показав, що вибір оптимального методу значною мірою залежить від конкретних умов експлуатації та характеру загроз.

Одним із центральних досягнень роботи стала розробка нових підходів до виявлення та нейтралізації атак, зокрема з використанням алгоритмів машинного навчання та адаптивних технологій. Ці підходи дозволяють системі не лише ідентифікувати відомі типи завад, але й самонавчатися та адаптуватися до нових, непередбачених загроз. Наприклад, використання нейронних мереж для розпізнавання складних патернів спуфінгу або динамічне формування нулів діаграми спрямованості антени для ефективного пригнічення джемінгу.

Ефективність запропонованих рішень була ретельно перевірена шляхом моделювання роботи радіонавігаційних систем за умов зовнішнього впливу. Наприклад, стендові випробування з імітацією джемінгу та спуфінгу дозволили кількісно оцінити підвищення точності позиціонування та скорочення часу реакції системи на загрозу. Це моделювання підтвердило доцільність використання розроблених програмно-апаратних рішень, що поєднують передові антенні технології, високошвидкісні цифрові процесори сигналів та інтелектуальні

алгоритми обробки даних, включаючи синтез даних від інерціальних навігаційних систем.

На основі проведених досліджень розроблено конкретні рекомендації, щодо вдосконалення засобів захисту радіонавігаційних систем в умовах радіонавігаційних конфліктів, які враховують специфіку різних сфер застосування – від цивільної авіації, де пріоритетом є безпека та використання інтегрованих GNSS/ІНС систем, до військових застосувань, що вимагають гібридних активних та пасивних методів із застосуванням машинного навчання.

Наукова новизна здобутих результатів полягає у розробці та обґрунтуванні комплексного багаторівневого підходу до протидії радіонавігаційним конфліктам, що інтегрує адаптивні алгоритми, засновані на машинному навчанні, мультидоменний аналіз сигналів та покращені методи сенсорного синтезу. Зокрема, запропоновані алгоритми фазового контролю та методи багаточастотного порівняння забезпечують підвищену ефективність виявлення та нейтралізації складних спуфінг-атак.

Практичне значення роботи полягає в тому, що її результати можуть бути безпосередньо використані для підвищення стійкості та надійності радіонавігаційних систем у багатьох галузях. У цивільній авіації вони сприятимуть підвищенню безпеки польотів, у морському та наземному транспорті – забезпеченню безпечної та точної навігації, а у військовій сфері – захисту критично важливих систем навігації для національної безпеки України. Це також включає застосування в космічній галузі для захисту орієнтації та управління космічними апаратами, а також у захисті інфраструктури критичного призначення.

Як результат, у магістерській роботі було успішно вирішено поставлені завдання, а досягнута мета – розробка, аналіз та оцінка методів протидії в радіонавігаційних конфліктах – підтверджує можливість забезпечення високої надійності роботи радіонавігаційних систем навіть в умовах агресивного радіоелектронного середовища.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [57].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Навігація. Основи визначення місцеположення та скеровування / Б. Гофманн-Велленгоф, К. Легат, М. Візер ; пер. з англ. за ред. : Я. С. Яцківа; літ. ред.: О. Є. Смолінська. – Львів : ЛНУ ім. І. Франка, 2006. – 449 с.

2. Васильєв В.М. Радіонавігаційні системи: підручник / В.М. Васильєв. – Київ : НТУУ «КПІ», 2023. – 338 с. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/handle/123456789/56820

3. Васильєв В.М. Радіонавігаційні системи. Лабораторний практикум / В.М. Васильєв.– Київ : КПІ ім. Ігоря Сікорського, 2023. – 78 с. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/handle/123456789/56821

4. Конін В.В. Системи супутникової радіонавігації / В.В. Конін, В.П. Харченко. – Київ : Холтех, 2010. – 520 с.

5. Сумик М.М. Основи теорії радіотехнічних систем: навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Радіотехніка». – Львів : Вид-во Нац. ун-ту «Львів. політехніка», 2005. – 240 с.

6. Васильєв В.М. Підвищення точності траєкторної оцінки в багатопозиційних далекомірних системах спостереження / В. М. Васильєв, К. В. Науменко // Збірник наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України.– Київ : ВІТІ НТУУ «КПІ», 2011. – Вип. 2. – С. 6-11.

7. Захарін Ф.М. Алгоритмічне забезпечення інерціально-супутникових систем навігації: монографія / Ф.М. Захарін, В.М. Синєглазов, М.К. Філяшкін – Київ : Вид-во Нац. Авіа. Ун-ту «НАУ-друк», 2011. – 320 с.

8. Васильєв В.М. Статистична комплексна обробка даних курсової та кутомірно-далекомірної систем / В.М. Васильєв, К.В. Науменко // Статистичні методи оброки сигналів і даних: матеріали міжнар. наук. конф., Національний авіаційний університет, 16-17 жовтня 2013 р. – Київ : НАУ, 2013. – С. 55-59.

9. Skolnik, M. I. (2008). Radar Handbook (3rd ed.). McGraw-Hill Education.

10. Misra, P., & Enge, P. (2011). Global Positioning System: Signals, Measurements, and Performance (2nd ed.). Ganga-Jamuna Press.

11. Kaplan, E. D., & Hegarty, C. J. (2017). Understanding GPS/GNSS: Principles and Applications (3rd ed.). Artech House.

12. Tsui, J. B.-Y. (2005). Fundamentals of Global Positioning System Receivers: A Software Approach (2nd ed.). Wiley-Interscience.

13. Parkinson, B. W., Spilker, J. J. (1996). Global Positioning System: Theory and Applications. Volume I–II. American Institute of Aeronautics and Astronautics.

14. Grewal, M. S., Weill, L. R., & Andrews, A. P. (2007). Global Positioning Systems, Inertial Navigation, and Integration (2nd ed.). Wiley.

15. Curran, J. T., et al. (2016). “Countering GNSS Jamming and Spoofing: Threats and Mitigations.” Inside GNSS, March/April.

16. Schmitt, J. B., & Zander, S. (2019). “Radio Navigation Warfare: Current Status and Trends.” IEEE Aerospace and Electronic Systems Magazine, 34(9), 36–45.

17. Humphreys, T. E. (2012). “Detection Strategy for Cryptographic GNSS Anti-Spoofing.” IEEE Transactions on Aerospace and Electronic Systems, 49(2), 1073–1090.

18. European GNSS Agency. (2020). GNSS Market Report, Issue 6. https://www.euspa.europa.eu

19. Ranganathan, N. (2019). “Jamming and Anti-Jamming Techniques in GNSS: A Survey.” International Journal of Electronics and Communication Engineering, 13(6), 181–190.

20. National Academies of Sciences, Engineering, and Medicine. (2017). Position, Navigation, and Timing Technologies in the 21st Century. The National Academies Press.

21. U.S. Department of Defense. (2020). Global Positioning System Standard Positioning Service Performance Standard.

22. ICAO (International Civil Aviation Organization). (2021). Global Navigation Satellite System (GNSS) Manual (Doc 9849).

23. ITU-R. (2019). Technical Characteristics and Protection Criteria for Radio Navigation Systems. Recommendation ITU-R M.1461-2.

24. Васильєв В. М. Радіонавігаційні системи: підручник / В. М. Васильєв. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2023. – 338 с.

25. Зубков В. П. Навігаційне забезпечення як складова інформаційного забезпечення сил оборони України. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2021. № 3(73). С. 109–115. https://doi.org/10.33099/2304-2745/2021-3-73/109-115.

26. Карлов Д.В., Коробецький О.В., Рєзніков Ю.В. Рекомендації щодо розробки захищеного від завад приймача глобальних навігаційних супутникових систем для вирішення завдань Збройних Сил України. Системи озброєння і військова техніка. 2020. № 4. С. 60–66.

27. Шолохов С.М., Самборський І.І., Вакуленко О.В., Ніколаєнко Б.А. Завадозахист радіоелектронних засобів. Частина 1. Основи завадозахисту систем зв'язку: навчальний посібник. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 210 с.

28. Петровський А. Алгоритм виявлення впливу спуфінгу під час виконавчої прокладки програмними засобами електронної картографічної навігаційно-інформаційної системи. Проблеми інформаційних технологій. Херсон, 2019

29. Опірський І., Бибик Р. Дослідження сучасних методів РЕБ та методів і засобів її протидії. Український науковий журнал інформаційної безпеки. 2023. Т. 29, № 2. С. 88–97.

30. Крючкова Л.П. Сигнали GPS як об'єкти радіоподавлення в задачах об'єктово-територіального захисту / Крючкова Л.П., Пшоннік В.О., Зозуля С.А // Сучасний захист інформації. – 2019. – №1. – С. 53–58.

31. Ярош, С. П., Гур'єв, Д. О. Впровадження специфічних способів і засобів протидії безпілотним літальним апаратам в угрупованні зенітних ракетних військ. Наука і техніка Повітряних Сил Збройних Сил України, 2 (47), 2022.

32. Yang Ch., Soloviev A. In-Situ Calibration of GPS Antenna Array with Ambient Signals. Proceedings of the 2023 International Technical Meeting of The Institute of Navigation. Long Beach, California, January 2023. P. 751–769.

33. C. Anderson Givhan, Scott M. Martin Comparison of CRPA Direction of Arrival Methods on Post Correlated GNSS Signals for Solution Authentication and Spoofing Detection. Proceedings of the 2023 International Technical Meeting of The Institute of Navigation. Long Beach, California, January 2023. P. 303–314.

34. Arribas J., Gómez M. A., Fernández-Prades C., Martín D. L., García-Tuñón J. M., Rioja T. G. A Receiver-Independent GNSS Smart Antenna for Simultaneous Jamming and Spoofing Protection. 2023 IEEE Aerospace Conference. Big Sky, MT, USA, 2023. P. 1–13.

35. Esswein M. C. GNSS Signal Processing Techniques for Spoofing Resiliency. Doctoral Dissertations. 2023.

36. Wiggins G. Improving CRPA Anti-Jamming Performance with Virtual Array Integration: Master's Thesis. 2023.

37. Pérez-Marcos E., Cuntz M., Konovaltsev A., Kurz L., Caizzone S., Meurer M. CRPA and Array Receivers for Civil GNSS Applications. 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS). Monterey, CA, USA, 2023. P. 318–328.

38. Yang C., Soloviev A. Self-Contained Implementation of Nullsteering and Beamforming with a Standalone Antenna Array for GNSS Signals under Interference. 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS). Monterey, CA, USA, 2023. P. 917–934.

39. Liu J., Chen F., Xie Y., Ge B., Lu Z., Sun G. Robust Spoofing Detection for GNSS Array Instrumentation Based on C/N0 Difference Measurements. IEEE Transactions on Instrumentation and Measurement. 2023. Vol. 72. P. 1–11. Art No. 8507211.

40. Madni A., Khan W. T. Design of a Compact 4-Element GNSS Antenna Array With High Isolation Using a Defected Ground Structure (DGS) and a Microwave Absorber. IEEE Open Journal of Antennas and Propagation. 2023. Vol. 4. P. 779–791.

41. Santarelli K. P., Lan W. D. Coherent Global Positioning System Signal Interference Detection and Mitigation: Master's Thesis. 2023.

42. BniLam N., Principe F., Crosta P. Large Array Antenna Aperture for GNSS Applications. IEEE Transactions on Aerospace and Electronic Systems

43. Z. Zhang, X. Zhan, and Y. Zhang, “GNSS spoofing localization based on differential code phase,” in *Proc. Forum Cooperat. Positioning Service (CPGPS)*, Harbin, China, May 2017, pp. 338–344.

44. What Is Spread Spectrum and Its Impact on GNSS/GPS Antennas? Режим доступу: https://novotech.com/pages/spread-spectrum (дата звернення 08.06.25)

45. Мовчан К.О. Сучасні стратегії навігації дронів у випадках відсутності GPS сигналу. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. Том 35 (74) № 5, 2024.

46. Magiera J., Katulski R. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *Journal of Applied Research and Technology, 13*(1), 45-57. Elsevier Ltd. Retrieved April 15, 2019. Available at https://www.learntechlib.org/p/198163/.

47. Renbiao Wu, Wenyi Wang, Dan Lu, Lu Wang, Qionggiong Jia. Adaptive Interference Mitigation of GNSS. Navigation: Science and Technology. DOI https://doi.org/10.1007/978-981-10-5571-3.

48. Semanjski S., Semanjski I., Wilde W.D., Gautama S. Use of supervised machine learning for GNSS signal spoofing detection with validation on realworld meaconing and spoofing data – Part II. Sensors. 2020. № 20(7):1806. pp. 1-15.

49. Крючкова, Л., & Ворохоб, Н. (2025). Адаптивні методи протидії активним шумовим завадам. Кібербезпека: освіта, наука, техніка, 2(30), 455–472. https://doi.org/10.28925/2663-4023.2025.30.987

50. Guo Y, Miao L, Zhang X. Spoofing Detection and Mitigation in a Multi-correlator GPS Receiver Based on the Maximum Likelihood Principle. Sensors (Basel). 2018 Dec 22;19(1):37. doi: 10.3390/s19010037. PMID: 30583497; PMCID: PMC6339142.

51. Крючкова, Л., & Шандрук, М. (2025). Методи протидії в радіонавігаційних конфліктах. Кібербезпека: освіта, наука, техніка, 4(28), 766–780. https://doi.org/10.28925/2663-4023.2025.28.863

52. V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.

53. S. Shevchenko, et al., Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 333–342.

54. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915

55. Соколов, В. (2025). Забезпечення стійкості безпроводових систем до атак глушіння. Телекомунікаційні та інформаційні технології, 1(86), 50–60. https://doi.org/10.31673/2412-4338.2025.013623

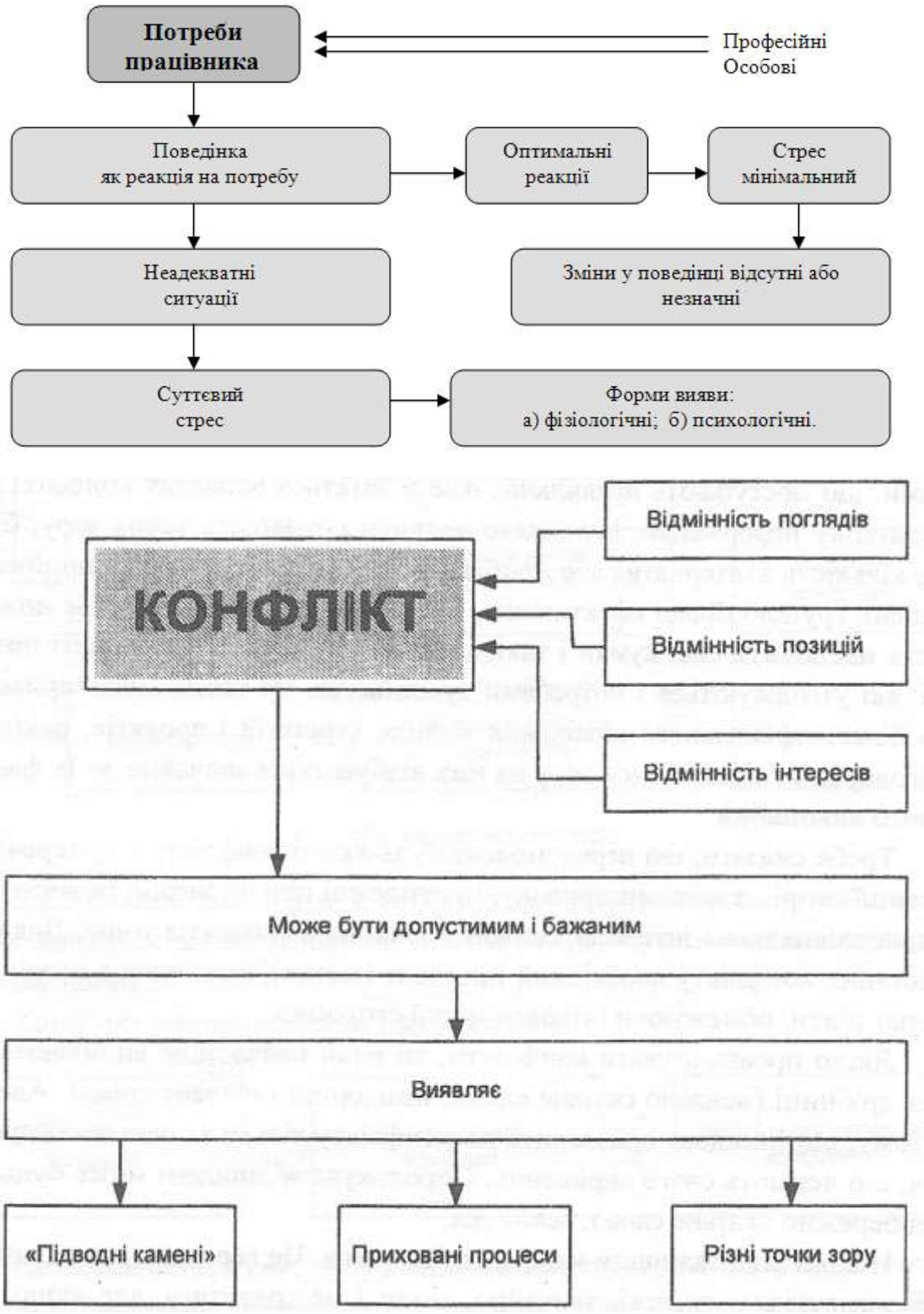
56. V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.

57. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf

ДОДАТКИ

Додаток А

Види загроз у радіонавігайцих конфліктах



Додаток Б.

Додаток В

Лістинг коду формування корисного сигналу

```
# ==========================================
# 2. КОРИСНІ СИГНАЛИ (5 видів)
# ==========================================

useful_signals = []

# 1. Вузькосмуговий гармонічний сигнал (GPS L1 C/A)
f_c = 50  # Несуча, Гц (для наочності)
u1 = np.cos(2 * np.pi * f_c * t) * signal.sawtooth(2 * np.pi * 1.023e6 * t / 50, width=0.5)[:len(t)]
useful_signals.append(('Вузькосмуговий BPSK\n(GPS-подібний)', u1))

# 2. Широкосмуговий шумовий сигнал (DSSS)
np.random.seed(42)
prn = np.sign(np.random.randn(len(t)))
u2 = signal.convolve(prn, np.ones(50), mode='same') / 50 * np.cos(2 * np.pi * f_c * t)
useful_signals.append(('Широкосмуговий DSSS', u2))

# 3. Частотно-модульований сигнал (ЧМ)
f_dev = 20
u3 = np.sin(2 * np.pi * 30 * t + f_dev * np.cumsum(np.sin(2 * np.pi * 2 * t)))
useful_signals.append(('Частотно-модульований', u3))

# 4. ЛЧМ-сигнал (лінійна частотна модуляція)
k = 40 / T  # швидкість зміни частоти
u4 = np.sin(2 * np.pi * (30 * t + 0.5 * k * t**2))
useful_signals.append(('ЛЧМ-сигнал (чирп)', u4))

# 5. Импульсний сигнал з високою шпаруватістю
u5 = np.zeros_like(t)
u5[200:300] = 1
u5[700:800] = 1
u5[1200:1300] = 1
u5 = signal.convolve(u5, signal.windows.gaussian(100, 15), mode='same') * np.cos(2 * np.pi * 60 * t)
useful_signals.append(('Імпульсний сигнал', u5))
```

Додаток В

Лістинг коду формування завадового сигналу

```
# ==========================================
# 3. ЗАВАДОВІ СИГНАЛИ (5 видів)
# ==========================================

jam_signals = []

# 1. Гармонічна завада (тональна)
j1 = 2.5 * np.cos(2 * np.pi * 50 * t + 0.3)
jam_signals.append(('Тональна завада 50 Гц', j1))

# 2. Широкосмуговий шум
j2 = 3.0 * np.random.randn(len(t))
jam_signals.append(('Білий гаусів шум', j2))

# 3. Імпульсна завада
j3 = np.zeros_like(t)
j3[::100] = 10 * (np.random.rand(len(t)//100) - 0.5)
j3 = signal.convolve(j3, signal.windows.gaussian(50, 10), mode='same')
jam_signals.append(('Імпульсна завада', j3))

# 4. ЧМ-завада з великим відхиленням
j4 = 4.0 * np.sin(2 * np.pi * 48 * t + 50 * np.sin(2 * np.pi * 3 * t))
jam_signals.append(('Широкосмугова ЧМ-завада', j4))

# 5. Прицільна завада по несучій корисного сигналу
j5 = 3.0 * np.cos(2 * np.pi * 50 * t + np.pi/4)
jam_signals.append(('Прицільна завада по несучій', j5))
```

Додаток В

Лістинг коду формування конфліктної взаємодії корисного та завадового сигналів.

```
# ============================================
# 4. ВІДОБРАЖЕННЯ СИГНАЛІВ
# ============================================

def plot_signals(signals, title_prefix, filename, cols=3):
    rows = (len(signals) + cols - 1) // cols
    fig, axes = plt.subplots(rows, cols, figsize=(15, 3*rows))
    if rows == 1:
        axes = axes.reshape(1, -1)
    for i, (name, sig) in enumerate(signals):
        ax = axes[i // cols, i % cols] if rows > 1 else axes[i]
        ax.plot(t, sig, color='tab:blue')
        ax.grid(True, alpha=0.3)
        ax.set_title(name, fontsize=12, weight='bold')
        ax.set_xlabel('Час, с')
        ax.set_xlim(0, T)
    for j in range(i+1, rows*cols):
        axes[j // cols, j % cols].axis('off') if rows > 1 else axes[j].axis('off')
    fig.suptitle(title_prefix, fontsize=16, weight='bold', y=0.98)
    plt.tight_layout()
    plt.savefig(filename, dpi=300, bbox_inches='tight')
    plt.show()

# Корисні сигнали
plot_signals(useful_signals, 'КОРИСНІ СИГНАЛИ', 'useful_signals.png')

# Завадові сигнали
plot_signals(jam_signals, 'ЗАВАДОВІ СИГНАЛИ', 'jam_signals.png')
# ============================================
# 5. ВЗАЄМОДІЯ (5 прикладів)
# ============================================

interactions = [
    (useful_signals[0], jam_signals[0], "Вузькосмуговий + тональна завада"),
    (useful_signals[1], jam_signals[1], "DSSS + білий шум"),
    (useful_signals[2], jam_signals[3], "ЧМ + широкосмугова ЧМ-завада"),
    (useful_signals[3], jam_signals[2], "ЛЧМ + імпульсна завада"),
    (useful_signals[4], jam_signals[4], "Імпульсний + прицільна завада по несучій")
]

fig, axes = plt.subplots(5, 3, figsize=(18, 20))
```

```
    for idx, (u, j, title) in enumerate(interactions):
        s = u[1] + j[1]
        # Корисний
        axes[idx, 0].plot(t, u[1], color='green')
        axes[idx, 0].set_title(f'{title}\nКорисний сигнал', color='green', weight='bold')
        axes[idx, 0].grid(True, alpha=0.3)
        axes[idx, 0].set_ylabel('Амплітуда')
        # Завада
        axes[idx, 1].plot(t, j[1], color='red')
        axes[idx, 1].set_title('Завада', color='red', weight='bold')
        axes[idx, 1].grid(True, alpha=0.3)
        # Сумарний
        axes[idx, 2].plot(t, s, color='black')
        axes[idx, 2].set_title('Результат взаємодії\n(u(t) + j(t))', weight='bold')
        axes[idx, 2].grid(True, alpha=0.3)

    axes[4, 0].set_xlabel('Час, с')
    axes[4, 1].set_xlabel('Час, с')
    axes[4, 2].set_xlabel('Час, с')

    #--plt.suptitle('ПРИКЛАДИ ВЗАЄМОДІЇ КОРИСНОГО ТА ЗАВАДОВОГО СИГНАЛІВ', fontsize=18,
weight='bold', y=0.95)--#
    plt.tight_layout()
    plt.savefig('interactions.png', dpi=300, bbox_inches='tight')
    plt.show()

    print("Згенеровано файли:")
    print("  - scheme.png         – схема дослідження")
    print("  - useful_signals.png – 5 корисних сигналів")
    print("  - jam_signals.png    – 5 завадових сигналів")
    print("  - interactions.png   – 5 прикладів взаємодії")
```