



DOI 10.28925/2663-4023.2025.28.863

УДК 621.396

Крючкова Лариса Петрівна

доктор технічних наук, професор

професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID 0000-0002-8509-6659

l.kriuchkova@kubg.edu.ua**Шандрук Максим Сергійович**

магістр

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID 0009-0001-0431-9735

mshandruk99@gmail.com**МЕТОДИ ПРОТИДІЇ В РАДІОНАВІГАЦІЙНИХ КОНФЛІКТАХ**

Анотація. Сучасні радіонавігаційні системи відіграють критично важливу роль у функціонуванні глобальної економіки, транспорту, оборони та повсякденному житті. Разом з тим зростання залежності від цих систем створює нові виклики, пов'язані з їх уразливістю до глушіння навігаційних сигналів (jamming), формування фальшивих сигналів радіонавігаційної системи (spoofing) та інших видів деструктивного радіоелектронного впливу. Висока динаміка сучасних бойових дій, розвиток високоточних ударних комплексів і систем, впровадження мережецентричних автоматизованих систем управління, підвищення вимог до оперативності, точності та надійності навігаційної інформації обумовлюють необхідність удосконалення як методів навігаційного забезпечення, так і методів шкідливих радіоелектронних впливів. В зазначених умовах радіонавігаційні конфлікти є однією з найактуальніших загроз для сучасних глобальних навігаційних супутникових систем, а завдання дослідження методів протидії в радіонавігаційних конфліктах є актуальним і необхідним для підвищення стійкості радіонавігаційних систем та національної безпеки. Мета публікації – систематизація і аналітичний огляд методів протидії в радіонавігаційних конфліктах для виявлення перспективних напрямків їх розвитку. Розглянуто основні види навмисних завад, що спрямовуються на апаратуру споживачів супутникових радіонавігаційних систем, зокрема принципи формування spoofing-завад; методи виявлення хибних навігаційних сигналів, створюваних постановниками імітаційних завад; методи захисту від маскувальних і імітаційних завад. Зазначено, що завдання забезпечення ефективної протидії в радіонавігаційних конфліктах потребує постійного вдосконалення відповідних технологій і стратегій, що охоплюють як технічні, так і організаційні аспекти.

Ключові слова: супутникові радіонавігаційні системи; навігаційний сигнал; точність позиціонування; навігаційна апаратура споживача; завадозахищеність; радіонавігаційний конфлікт; радіоподавлення; spoofing; jamming; радіоелектронна боротьба, методи протидії; методи захисту; системи CRPA.

ВСТУП

Супутникові радіонавігаційні системи (СРНС) призначені для позиціонування, точного визначення тривимірних координат (широти, довготи, висоти над рівнем моря) об'єкта, оснащеного спеціальним навігаційним приймачем, а також його швидкості, напрямку руху і поточного часу [1]. Важливою перевагою СРНС є відсутність обмежень на кількість користувачів.



Принцип визначення місця перебування об'єкта на земній поверхні в глобальній системі позиціонування полягає в одночасному вимірі відстані до декількох навігаційних супутників (не менше чотирьох) з відомими параметрами їх орбіт на кожний момент часу і обчисленні за вимірними відстанями власних координат за допомогою навігаційної апаратури споживача. Навігаційна апаратура споживача складається з навігаційних приймачів і пристроїв обробки сигналів, що дозволяють забезпечити обчислення власних координат, швидкості і часу.

Початком масштабного застосування GPS можна вважати операції США (НАТО) на Близькому сході на початку 90-х років, коли супутникова навігація стала базисом для високоточної зброї.

В інтересах оборони поряд з розвитком власних СРНС актуальним є створення ідеології техніки протидії СРНС супротивної сторони [2]. Протидія реалізується засобами радіоподавлення в інтересах захисту цивільних об'єктів (населених пунктів, промислових підприємств, електростанцій, мостів, аеродромів тощо), а також військових об'єктів від засобів розвідки і ураження, які вирішують завдання свого місцезнаходження і наведення зброї з використанням засобів супутникової навігації [3]. Мета протидії – ускладнення вирішення завдань визначення власних координат і параметрів руху небезпечними об'єктами супротивної сторони.

Про протидію високоточної зброї шляхом постановки завад приймачам супутникової навігації стало відомо з конфлікту на Балканах, коли вперше було масово застосовано високоточні авіаційні бомби JDAM (Joint direct attack munition) з GPS-наведенням. Таке озброєння залежить як від точності системи вимірювання, що використовується для визначення місцезнаходження, так і від точності визначення координат цілі, яка критично залежить від розвідувальної інформації. В другій половині 90-х років вводиться концепція «навігаційної війни» (NAVWAR – Navigation War), розробляються технічні вимоги до модулів GPS (GRAM), впроваджується модернізований криптистійкий сигнал P(Y)-код, створюються перші цифрові адаптивні антенні решітки з підвищеною завадостійкістю для захисту сигналів GPS.

Наразі експлуатуються глобальні СРНС – американська NAVSTAR GPS, європейська Galileo, китайська BeiDou/Compass, російська ГЛОНАСС. Всі вони, в тій чи іншій мірі використовуються військовими. Принципи побудови і функціонування підсистем, що входять до складу зазначених СРНС, багато в чому аналогічні, що відкриває можливість їх спільного використання.

В сучасних умовах, коли в складі навігаційної апаратури споживачів СРНС застосовуються ефективні засоби завадозахищеності, актуальною задачею є вдосконалення методів радіоподавлення сигналів GPS і навігаційної апаратури споживачів [4]. В рамках даної публікації в якості об'єкта радіоподавлення і вирішення задач захисту розглядаються сигнали супутникової радіонавігаційної системи NAVSTAR GPS.

Основними завданнями протидії навігаційній апаратурі споживачів СРНС є:

- протидія супутниковій навігації небезпечних об'єктів (терористів, розвідувальних і ударних безпілотних літальних апаратів тощо);
- захист об'єктів від засобів розвідки і ураження, які використовують навігаційні засоби СРНС (об'єктовий захист);
- захист території (створення протяжних суцільних зон радіоподавлення з метою захисту певної кількості об'єктів).

Постановка проблеми. Залежність сучасної цивілізації від точного позиціонування, навігації та синхронізації часу, що надаються глобальними



навігаційними супутниковими системами, продовжує зростати експоненційно. Від функціонування СРНС залежать не лише військові операції та спеціальні місії, але й критично важливі цивільні сектори: авіація, морський транспорт, логістика, телекомунікації, енергетика, фінансові операції, сільське господарство, повсякденне використання смартфонів тощо. Зазначене робить СРНС життєво важливою інфраструктурою, а будь-які збої в їх роботі можуть мати катастрофічні наслідки. Проте, саме ця критична важливість робить СРНС привабливою мішенню для навмисних ворожих впливів у контексті радіонавігаційних конфліктів. З появою доступного та потужного обладнання для створення електромагнітних завад, таких як джаммери та спуфери, загроза для якісного функціонування СРНС значно зросла. Джаммери перешкоджають прийому супутникових сигналів, створюючи шумові завади, що призводить до повного або часткового подавлення сигналу. Спуфери ж генерують імітаційні сигнали, що обманюють приймач, призводячи до неправильного місцезнаходження, що є особливо небезпечним, оскільки споживач навігаційної інформації може не усвідомлювати факту атаки. Крім того, існують загрози, пов'язані з кібератаками на наземну інфраструктуру СРНС, що може призвести до маніпуляцій з даними або повного вимкнення систем [5]. Зазначені радіонавігаційні конфлікти створюють численні виклики. Для військових це може означати втрату точності наведення, дезорієнтацію військ та зрив операцій. У цивільному секторі – аварії на транспорті, збої в роботі мереж зв'язку, фінансові втрати та порушення логістичних ланцюгів. Актуальність проблеми підсилюється геополітичною напруженістю та зростанням використання засобів радіоелектронної боротьби (РЕБ) у сучасних конфліктах.

Основними принципами РЕБ в операціях (бойових діях) є: відповідність; цілеспрямованість; активність; раптовість; випередження; масоване і комплексне застосування сил і засобів радіоелектронного подавлення в тісному поєднанні з вогневим ураженням і знищенням основних об'єктів систем і засобів управління військами і зброєю; неперервність і комплексність здійснення заходів з радіоелектронного захисту систем і засобів управління своїми військами і зброєю [6]. Існує гостра потреба у розробці та впровадженні ефективних методів протидії цим загрозам, що забезпечить стійкість та надійність функціонування СРНС. Це вимагає комплексного підходу, що включає вдосконалення існуючих технологій та розробку нових, інтеграцію різних систем та методів захисту. Недостатня увага до цих аспектів може призвести до серйозних наслідків для національної безпеки, економіки та суспільства в цілому.

Аналіз останніх досліджень і публікацій. Проблема вразливості радіонавігаційних систем та методи протидії загрозам привернули значну увагу наукової спільноти та військових фахівців у всьому світі. Існує велика кількість публікацій, присвячених цій тематиці, що охоплюють широкий спектр досліджень – від фундаментальних до прикладних.

В [7] авторами розглянуто навігаційні сигнали GPS в якості об'єкта радіоподавлення, яке здійснюється для вирішення задач об'єктово-територіального захисту, алгоритми пошуку і захвату навігаційного сигналу.

Аналіз засобів радіоелектронної боротьби (РЕБ) та засобів інженерної підтримки здійснено в [8]. У статті проаналізовано особливості озброєння для протидії безпілотним літальним апаратам (БПЛА), що використовуються в підсистемах управління силами та засобами боротьби з БПЛА, безпілотного прикриття, інженерного забезпечення, маскування та введення в оману.



В [9] описано двоетапну процедуру калібрування антени з керованою спрямованістю прийому (англ. Controlled Reception Pattern Antenna, CRPA), призначеної для протидії спуфінгу і радіоглушінню навігаційного сигналу. Перший етап полягає в оцінці невідповідності каналу, що дозволяє компенсувати помилки підсилення та фазові спотворення сигналів. Другий етап охоплює оцінювання взаємозв'язку між елементами антенної решітки з метою точного визначення коефіцієнтів взаємного впливу, що критично важливо для формування точної діаграми направленості.

В [10] викладено порівняльний аналіз трьох методів визначення напрямку джерела завад у CRPA. Метод класифікації множинних сигналів показав найвищу точність, однак потребує значних обчислювальних ресурсів і тривалого часу роботи. Метод різниць фаз продемонстрував нижчу точність, проте його основною перевагою є висока ефективність з точки зору обчислювального навантаження. Найменш точним виявився метод, заснований на принципі інваріантності до обертання, хоча його перевагою є найменший час обробки.

Публікація [11] присвячена розробці прототипу системи CRPA із використанням комерційно доступних комплектуючих. У роботі надано детальний опис архітектури, апаратної реалізації та аналіз функціональних характеристик створеної системи, що свідчить про її потенціал для практичного застосування в умовах реальних загроз.

В [12] запропоновано удосконалений підхід застосування методу Chimera з метою підвищення стійкості GNSS-приймачів до атак та спуфінгу. Запропонована концепція базується на поєднанні CRPA, механізмів автентифікації навігаційних сигналів, використанні даних від інерційних систем безпілотних літальних апаратів, цифрових підписів у повідомленнях та детекції аномалій у кодах навігаційних сигналів.

У науковій роботі [13] розглянуто можливості інтеграції віртуальної антенної решітки до існуючих CRPA-систем із керованою діаграмою спрямованості. Такий підхід дозволяє значно розширити функціональність антенної системи та підвищити її адаптивність до змін навколишнього середовища.

В [14] представлено результати застосування алгоритмів CRPA для виявлення спуфінгових атак. Показано, що дані алгоритми здатні ефективно виявляти навмисні спроби обману навігаційної системи шляхом імітації справжніх сигналів супутників.

Документ [15] описує автономну версію CRPA, яка самостійно формує діаграму спрямованості, використовуючи спеціальний механізм перевірки та оптимізації вагових коефіцієнтів. Така система мінімізує потребу в зовнішньому керуванні та здатна адаптуватися до зміни ситуації в реальному часі.

В [16] запропоновано новий метод виявлення спуфінгу та захисту від активних радіозавад, який базується на використанні властивостей CRPA. Розроблений підхід дозволяє підвищити стійкість до складних електромагнітних атак, забезпечуючи високу надійність позиціонування.

У дослідженні [17] розроблено широкосмугову 4-елементну антенну решітку, яка складається з чотирьох прямокутних антен із правосторонньою круговою поляризацією (RHCP). Така конструкція забезпечує широке частотне покриття й високу ефективність у прийомі супутникових сигналів.

Робота [18] акцентує увагу на методах протидії імітаційним перешкодам у GNSS-системах. У ній розглядаються різноманітні технічні та алгоритмічні рішення, спрямовані на підвищення надійності роботи приймачів у складних умовах електронного впливу.



В [19] обґрунтовано концепцію великої віртуальної антенної решітки, створеної на базі існуючих антенних модулів, що дозволяє досягти високих показників посилення та просторової роздільної здатності.

Як видно з розглянутих досліджень і публікацій, радіонавігаційні конфлікти є однією з найактуальніших загроз для сучасних глобальних навігаційних супутникових систем, а завдання дослідження методів протидії в радіонавігаційних конфліктах є актуальним і необхідним для підвищення стійкості радіонавігаційних систем та національної безпеки. Метою публікації є систематизація і аналітичний огляд методів протидії в радіонавігаційних конфліктах для виявлення перспективних напрямків їх розвитку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Основні методи постановки завд.

Навмисні радіозавади за принципом їх впливу на навігаційну апаратуру споживачів можна поділити на чотири основні групи: *маскувальні, дезінформуючі, спотворюючі та засліплюючі*.

Маскувальна завада (енергетична) створює на вході приймача навігаційної апаратури безладний шумовий електромагнітний фон, який ускладнює виявлення навігаційних сигналів та вимірювання їх інформативних параметрів. До основних типів активних маскувальних радіозавад, які можуть бути використані для подавлення приймачів навігаційної апаратури, належать:

- прицільні шумові завади, налаштовані на фіксовану частоту навігаційного сигналу;
- гармонійні завади з фіксованою або змінною частотою у межах смуги пропускання приймачів навігаційної апаратури;
- фазоманіпульовані завади на частотах навігаційного сигналу, які поділяються на загороджувальні сигналоподібні завади, сформовані генераторами, та завади внутрішньо-системного походження, створені шляхом ретрансляції навігаційних сигналів.

До так званих "енергетичних" завд відносяться jamming [13], спрямований на порушення функціонування навігаційної апаратури споживача СРНС шляхом подавлення корисного інформаційного сигналу, а також будь-які дії, спрямовані на порушення функціонування самої СРНС, включаючи атаку на супутники та наземну інфраструктуру управління.

Дезінформуюча (імітаційна) завада [20] являє собою хибні навігаційні сигнали, призначені для передачі на навігаційну апаратуру споживача СРНС неправдивої інформації шляхом формування спеціальними джерелами сигналів, автентичних сигналів СРНС. Головна вимога до імітаційних завд – достатня наближеність сукупності параметрів створюваних хибних навігаційних сигналів до справжніх, на основі яких навігаційна апаратура споживача СРНС вирішує завдання ідентифікації навігаційних сигналів.

Для формування spoofing-завади застосовуються два основні методи: генераторний і ретрансляційний.

Принцип формування spoofing-завади на основі генераторного методу пояснює рис.1.

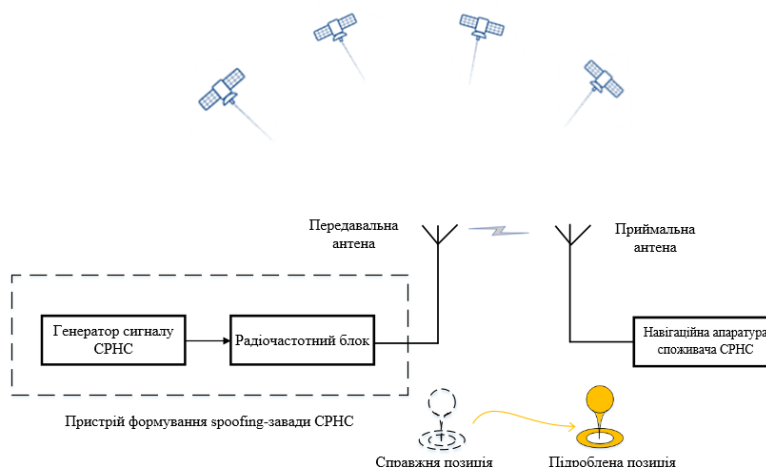


Рис. 1. Принцип формування spoofing-завади на основі генераторного методу

Генератор сигналу СРНС формує spoofing-заваду з параметрами, аналогічними параметрам навігаційних сигналів СРНС, яка випромінюється в напрямку навігаційної апаратури споживача СРНС.

Якщо хибні навігаційні сигнали не ідентифікуються навігаційною апаратурою споживача СРНС як "хибні навігаційні сигнали", то за певних умов вони можуть бути захоплені системою для відстеження. Вимірювання, виконані на основі таких хибних навігаційних сигналів, призводять до внесення аномальних помилок у результати навігаційного визначення об'єкта. Розмір помилок у загальному випадку залежить від кількості створених хибних навігаційних сигналів і від близькості їхніх параметрів до параметрів справжніх навігаційних сигналів. Можна стверджувати, що якщо навігаційна апаратура споживача СРНС не здатна ефективно виявляти хибні навігаційні сигнали, то в умовах впливу дезінформуючих завад вона з великою ймовірністю стане непрацездатною.

Для створення spoofing-завади системам військового призначення зазвичай використовується ретрансляційний метод (рис.2).

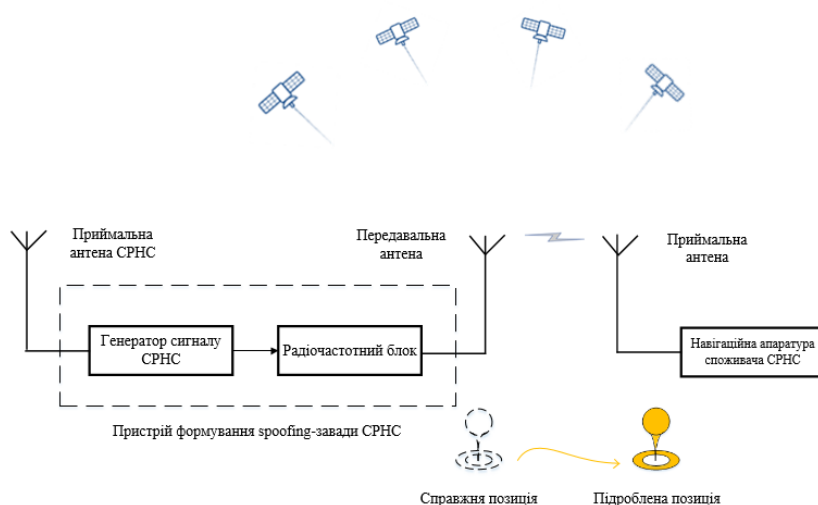


Рис. 2. Принцип формування spoofing-завади на основі ретрансляційного методу



При використанні ретрансляційного методу пристрій формування spoofing-завади спочатку отримує автентичний сигнал СРНС за допомогою приймальної антени, а потім після додавання до сигналу певної часової затримки та, інколи, додаткового зсуву частоти посилює його і спрямовує завадовий сигнал за допомогою передавальної антени на навігаційну апаратуру. Навігаційна апаратура СРНС після отримання завадового сигналу обчислює псевдодальність до відповідного уявного супутника, тому позиціонування об'єкта здійснюється з помилкою.

Спотворююча завада [21], на відміну від імітаційної, діє саме в тій смузі частот, де присутній справжній навігаційний сигнал. Дія спотворюючої завади спричиняє збільшення похибки фіксації моменту максимуму функції взаємної кореляції. Наслідком цього є зростання похибки вимірювання псевдодальності.

Основні види спотворювальних завад:

- прицільні за частотою та кодом сигналоподібні завади генераторного типу;
- слідкуючі сигналоподібні завади генераторного типу;
- хаотичні імпульсні завади у вигляді потоків коротких радіоімпульсів (тривалість імпульсів співмірна з тривалістю символу коду навігаційного сигналу) з досить великою імпульсною потужністю;
- пасивні завади у вигляді відбиттів, створених ділянками підстилаючої поверхні, місцевими предметами або спеціальними відбивачами, які на даний момент знаходяться поблизу носія навігаційної апаратури.

Досить часто спотворюючі завади (прицільні та слідкуючі) формуються із залученням зовнішніх цілевказівок від підсистеми радіомоніторингу індивідуально для кожного навігаційного сигналу в конкретні періоди часу. Варто зазначити, що отримання таких цілевказівок є непростим завданням, у зв'язку з чим використання прицільних і слідкуючих сигналоподібних завад для радіоподавлення не тільки захищених навігаційних сигналів а й цивільних наразі є проблематичним.

Засліплююча завада – це вузькосмугове випромінювання на частоті навігаційного сигналу, потужність якого на вході приймача навігаційної апаратури у межах його смуги пропускання є достатньою для перевантаження приймача. До можливих типів завад, які можуть мати засліплюючу дію, є вище вказані гармонійна, вузькосмугова шумова завада та хаотичні імпульсні завади [22].

Ефективність засліплюючої завади, як засобу радіоподавлення навігаційної апаратури залежить від відстані між постановником активних завад та носієм навігаційної апаратури, а також від величини динамічного діапазону приймача навігаційної апаратури. При невеликій відстані до навігаційної апаратури, на яку здійснюється вплив, дія цих завад може призводити до насичення приймальних пристроїв навіть за відносно невеликої потужності завадового сигналу.

Однією з найважливіших енергетичних характеристик завадового сигналу є коефіцієнт подавлення, тобто мінімальне відношення енергії даного завадового сигналу до енергії корисного сигналу на вході приймального пристрою, який подавляється, в смузі пропускання його лінійної частини, при якому має місце заданий інформаційний збиток. Інформаційний збиток, який виникає внаслідок впливу завад, проявляється в маскуванні, імітації, затримці у надходженні інформації тощо. Характер інформаційної шкоди залежить від виду завадового сигналу і подавляючого засобу.

Методи захисту від маскувальних завад.

Відомі способи захисту від активних маскувальних завад ґрунтуються на просторово-часовій, частотно-часовій та кореляційній обробці сигналів, що надходять на вхід приймача навігаційної апаратури споживачів, а також на спеціальних заходах, які



дозволяють підвищити потужність корисних навігаційних сигналів у зоні розташування носіїв навігаційної апаратури. Метою захисту від активних маскувальних завад є збільшення співвідношення сигнал/завада на виході пристрою захисту та корелятора навігаційної апаратури.

Просторово-часова обробка дозволяє реалізувати просторове подавлення завад та просторову селекцію корисних навігаційних сигналів. Просторове подавлення завад досягається шляхом формування «нулів» у діаграмі направленості антенної решітки у напрямках на джерела завад. Просторова селекція передбачає формування такої діаграми направленості антенної решітки навігаційної апаратури, при якій її максимуми орієнтовані на корисні навігаційні супутники.

Більшість типів навігаційної апаратури, які працюють у системах СРНС, використовують одноелементні антени з фіксованою діаграмою направленості, головна пелюстка якої спрямована у верхню півсферу й покриває всю область «вище лінії горизонту», де розміщені корисні навігаційні супутники. Постановники активних завад можуть діяти з будь-якого кутового напрямку в межах цієї області. Для захисту від таких загроз навігаційна апаратура може використовувати багатоелементні антенні решітки, які дозволяють формувати «нулі» в діаграмі направленості антенної решітки в напрямку джерел завад і максимуми – у напрямку корисних навігаційних супутників. Кількість можливих «нулів» у діаграмі направленості дорівнює кількості елементів антенної решітки мінус один. На сьогодні розроблено багатоелементні антенні решітки із 4 та 7 антенними елементами, які дозволяють формувати «точкові» провали в напрямку трьох і п'яти джерел завад відповідно [23]. При цьому коефіцієнт покращення співвідношення сигнал/завада на виході такої багатоелементної антенної решітки може досягати 56 дБ і більше.

Частотно-часова обробка дозволяє реалізувати компенсацію і частотну режекцію завад. Компенсація полягає у відніманні сформованої копії (оцінки) завадового сигналу від вхідного спостереження. Різноманітність варіантів побудови компенсаторів завад визначається способами формування оцінки завадового сигналу, при цьому суттєву роль відіграє апріорна інформація про структуру і параметри завадового сигналу. Режекція в частотній області передбачає формування амплітудно-частотної характеристики лінійного фільтра з «провалами» в зонах, де зосереджені спектральні складові завад.

Кореляційна обробка сигналів, що діють на вході приймача навігаційної апаратури, реалізується на базі кореляторів, наявних у складі навігаційної апаратури всіх типів, на етапі первинної обробки навігаційних сигналів. Кореляційна обробка, разом зі своїм прямим призначенням – забезпеченням кодового доступу навігаційної апаратури до навігаційних сигналів СРНС, реалізує накопичення енергії оброблюваних фрагментів навігаційних сигналів. Завдяки цьому відбувається різке підвищення співвідношення сигнал/завада на виході корелятора. Таким чином, корелятори, наявні у складі навігаційної апаратури всіх типів, є потужним засобом захисту від активних маскувальних завад.

Варто зазначити, що корелятор ефективно пригнічує також завади внутрішньо-системного походження, а також навмисні завади «внутрішньо-системного типу», сформовані на їхній основі.

Підвищення потужності навігаційних сигналів у зоні розташування носіїв навігаційної апаратури спрямоване на збільшення співвідношення сигнал/завада на вході приймачів навігаційної апаратури. Підвищення енергетичного потенціалу випромінюваних навігаційних сигналів досягається шляхом застосування у супутниках нового покоління вузькоспрямованих антен. Застосування вузькоспрямованих антен є



перспективним для формування поля навігаційних сигналів у відносно невеликих зонах, наприклад, у районах локальних збройних конфліктів.

Інший підхід до підвищення потужності навігаційних сигналів на вході навігаційної апаратури полягає у розгортанні локальних радіонавігаційних систем на основі псевдосупутників – приймально-передавальних пристроїв, розташованих на поверхні Землі, які здійснюють приймання навігаційних сигналів справжніх навігаційних супутників, синхронізацію з радіонавігаційною системою, обробку, підсилення та випромінювання сигналів, схожих за структурою до справжніх навігаційних сигналів. Такий підхід дозволяє збільшити потужність навігаційних сигналів на вході навігаційної апаратури і забезпечити високоточне визначення координат (похибка до 5...10 см) відносно псевдосупутників. Це досягається завдяки відсутності ефемеридних та іоносферних похибок у наземних станціях та їх оптимальному геометричному розташуванню. Підвищена потужність наземних передавачів (1...10 Вт) і можливість переналаштування робочої частоти навігаційних сигналів псевдосупутників підвищує рівень захищеності навігаційної апаратури в умовах створення супротивником навмисних завад у зоні бойових дій. В перспективі розглядається варіант розміщення псевдосупутників на безпілотних літальних апаратах.

Методи захисту від імітаційних завад.

Методи захисту від імітаційних завад базуються на виявленні факту впливу хибних навігаційних сигналів, що створюються постановниками імітаційних завад, і послабленні їх впливу на результати розв'язання навігаційної задачі. До відомих методів виявлення імітаційних завад належать наступні:

1. Методи, засновані на моніторингу величини співвідношення сигнал/шум на вході приймача навігаційної апаратури. Діапазон зміни потужності навігаційного сигналу на вході приймача навігаційної апаратури приблизно відомий, тому будь-яке аномальне відхилення цієї величини може бути використане для виявлення імітаційної завади. Присутність хибних навігаційних сигналів збільшує сумарну потужність у смузі пропускання приймача навігаційної апаратури, що призводить до зміни рівня керуючої напруги при автоматичному регулюванні підсилення. Аналіз змін цієї напруги дозволяє виявити наявність аномального зростання вхідного співвідношення сигнал/шум.

2. Методи, засновані на моніторингу відносної потужності навігаційних сигналів різних частотних діапазонів. Сучасна навігаційна апаратура може працювати одночасно на кількох частотах (наприклад, L1 і L2 — у системі GPS), тому аналіз відносної потужності істинних навігаційних сигналів між різними діапазонами частот можна використовувати для виявлення імітаційної завади. Аномальна різниця між потужностями навігаційних сигналів або відсутність одного з сигналів (наприклад, на частоті L2) під час спроби створення імітаційної завади може слугувати маркером для її виявлення в навігаційній апаратурі.

3. Методи, засновані на моніторингу співвідношення сигнал/шум на виходах різноспрямованих антен [24]. Передбачається використання у складі навігаційної апаратури гібридної антени, що складається з несиметричного вібратора і так званої «патч-антени», підключеної до двох незалежних блоків обробки навігаційного сигналу. «Патч-антена» має максимум діаграми направленості в напрямку зеніту, у той час як несиметричний вібратор має у цьому напрямку мінімум. Різниця у величині співвідношення сигнал/шум, отримана на виходах різноспрямованих антен, може бути використана для виявлення присутності імітаційної завади.

4. Методи, засновані на аналізі просторових характеристик навігаційних сигналів. Пристрої формування spoofing-завад зазвичай передають хибні навігаційні сигнали з



однієї й тієї ж антени, тоді як справжні сигнали від навігаційних супутників надходять з різних напрямків. В результаті відбувається просторова кореляція сигналів, що надає можливість виявляти імітаційні завади шляхом виявлення просторової кореляції прийнятих навігаційних сигналів з використанням технологій просторово-часової обробки сигналів.

Відомий метод [25] передбачає використання двох антен з фіксованим взаємним розташуванням. Оцінюється різниця фаз сигналів, прийнятих цими антенами, яка порівнюється з розрахунковою різницею фаз, що залежить від взаємного переміщення супутника та приймача навігаційної апаратури. Порівнюючи отриману різницю фаз з розрахунковою, можна, за наявності суттєвої неузгодженості між цими значеннями, припустити загрозу спуфінгу. Основний недолік зазначеного методу полягає в тому, що він потребує тривалого часу для проведення спостережень. Збільшення числа антен підвищує надійність цього методу виявлення імітаційних завад.

5. *Методи, засновані на порівнянні результатів розв'язання навігаційної задачі декількома навігаційними пристроями.* Рішення про наявність імітаційної завади приймається, якщо отримані результати занадто схожі між собою для кожного навігаційного пристрою. Для перевірки істинності розв'язання навігаційної задачі також можуть використовуватись приймачі, що одночасно працюють з кількома СРНС.

6. *Методи, засновані на моніторингу затримки навігаційного сигналу і меж навігаційного повідомлення.* Як відомо, супутники випромінюють навігаційні сигнали одночасно на кількох несних частотах. Наприклад, приймачі системи GPS можуть приймати сигнали на двох частотах – L1 і L2. Крос-кореляція між однаковими сигналами на частотах L1 і L2 (наприклад, $P(Y)$) викликає щонайменше один кореляційний пік. Оскільки сигнали на частоті L2 мають більшу затримку порівняно з сигналами на частоті L1 через іоносферний ефект, взаємна затримка навігаційних сигналів, прийнятих на частотах L1 і L2, є відомою. Наявність додаткових крос-кореляційних піків з аномальною затримкою дозволяє виявляти імітаційні завади.

7. *Методи, засновані на автентифікації шифрованих сигналів.* Сучасні зразки навігаційної апаратури споживача СРНС оснащені засобами автентифікації користувачів. Методи шифрування активно використовуються у військових застосуваннях (GPS, ГЛОНАСС), таким чином обмежується доступ неавторизованих користувачів до структури навігаційного повідомлення. Враховуючи високу ефективність захисту, для формування імітаційних завад використовують ретранслятори навігаційних сигналів. Зразки навігаційної апаратури, що працюють із цивільними навігаційними сигналами, вразливі до імітаційних завад, оскільки інформація про цивільні навігаційні сигнали є відкритою і міститься в інтерфейсній документації СРНС.

8. *Метод, заснований на моніторингу зміни затримки та доплерівського зміщення частоти навігаційного сигналу* [26]. Для створення ефективної імітаційної завади для рухомого об'єкту необхідно, щоб швидкість зміни затримки хибного навігаційного сигналу, створеного імітатором, не перевищувала певного заданого порогу, інакше вона може бути виявлена завдяки аналізу вихідної інформації з контурів стеження за затримкою. Якщо відносна швидкість і координати навігаційної апаратури споживача відносно кожного супутника можуть бути визначені, то можна виявити аномальне значення доплерівського зміщення частоти імітаційної завади. Таким чином, інформація, отримана з виходів контурів стеження за затримкою та частотою, може бути використана для виявлення імітаційної завади.

9. *Метод, заснований на контролі нев'язок вимірювань.* Спосіб використовує надлишковість навігаційної інформації, отриманої від навігаційного супутника.



Розв'язання навігаційної задачі здійснюється з використанням методу найменших квадратів [27]:

$$\sum_{i=1}^N \{\tilde{p}_i(x, y, z, \Delta\tau) - p_i\}^2 \xrightarrow{x, y, z, \Delta\tau} \min,$$

де величини $\{\tilde{p}_i(x, y, z, \Delta\tau) - p_i\}^2$ називають нев'язками вимірювань. Якщо яка-небудь із знайдених псевдовідстаней містить аномальну похибку, нев'язки вимірювань різко зростають. При цьому, якщо

$$\tilde{p}_i(x, y, z, \Delta\tau) - p_i \geq \Delta p_{\max},$$

де $\Delta p_{\max}$ – деяке порогове значення, то здійснюється виявлення спотвореного вимірювання з заданою ймовірністю хибної тривоги. При виключенні спотворених вимірювань нев'язки різко зменшуються. Поріг виявлення для заданої ймовірності хибної тривоги може бути визначений з урахуванням нормалізації статистики нев'язок. Зазначається [27], що надійність виявлення та виключення нев'язок вимірювань (за псевдовідстанню або доплерівською частотою) залежить від кількості отриманих вимірювань навігаційних сигналів від різних навігаційних супутників. При дії імітаційних завад з невеликими розбіжностями за псевдовідстанню і доплерівською частотою можливі помилкові рішення, коли справжні вимірювання від навігаційних супутників будуть прийняті за хибні.

Варто зазначити, що окрім технічних рішень, невід'ємною частиною ефективної протидії в радіонавігаційних конфліктах є організаційні методи. До них належить навчання та тренування персоналу, щоб оператори були обізнані із загрозами і ризиками в радіонавігаційних конфліктах та знали, як діяти у зазначених ситуаціях. Резервування та дублювання систем, включаючи використання альтернативних навігаційних систем (VOR/DME, LORAN) або повністю автономних систем, є ключовим для забезпечення безперебійної навігації. Регулярне оновлення програмного забезпечення приймачів і навігаційного обладнання дозволяє впроваджувати нові алгоритми протидії та виправляти виявлені вразливості. Нарешті, міжнародна співпраця та обмін інформацією про радіонавігаційні інциденти та розробки у сфері протидії між країнами та організаціями є життєво важливими при вирішенні задач протидії у радіонавігаційних конфліктах. Загалом, ефективна протидія радіонавігаційним конфліктам потребує постійного вдосконалення технологій, інтеграції різноманітних сенсорів та алгоритмів, а також розвитку комплексних стратегій захисту, що охоплюють як технічні, так і організаційні аспекти.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

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 СРПА, 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.

Майбутні зусилля мають бути спрямовані на створення більш універсальних та адаптивних систем протидії, здатних ефективно працювати в складних електромагнітних умовах. Окрім технічних рішень, важливими є організаційні заходи, такі як навчання персоналу, регулярне оновлення програмного забезпечення та міжнародна співпраця.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Васильєв В. М. Радіонавігаційні системи: підручник / В. М. Васильєв. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2023. – 338 с.
2. 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>.
3. 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.
4. 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: ІСЗІ КПІ ім. Ігоря Сікорського, 2021. 210 с.
5. Петровський А. Алгоритм виявлення впливу спуфінгу під час виконавчої прокладки програмними засобами електронної картографічної навігаційно-інформаційної системи. Проблеми інформаційних технологій. Херсон, 2019
6. Опіський 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.
7. 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.



8. 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.
9. 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.
10. 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.
11. 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.
12. Esswein M. C. GNSS Signal Processing Techniques for Spoofing Resiliency. *Doctoral Dissertations*. 2023.
13. Wiggins G. Improving CRPA Anti-Jamming Performance with Virtual Array Integration: Master's Thesis. 2023.
14. Pérez-Marcos E., Cuntz M., Konovaltsev A., Kurz L., Caizzzone 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.
15. 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.
16. 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.
17. 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.
18. Santarelli K. P., Lan W. D. Coherent Global Positioning System Signal Interference Detection and Mitigation: Master's Thesis. 2023.
19. BniLam N., Principe F., Crosta P. Large Array Antenna Aperture for GNSS Applications. *IEEE Transactions on Aerospace and Electronic Systems*.
20. 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.
21. What Is Spread Spectrum and Its Impact on GNSS/GPS Antennas? Режим доступу: <https://novotech.com/pages/spread-spectrum> (дата звернення 08.06.25)
22. 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.
23. 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/>.
24. 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>.
25. 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.
26. Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gerard Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation*, Volume 2012, Article ID 127072, 15 pages. DOI <http://dx.doi.org/10.1155/2012/127072>.
27. 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.

**Kriuchkova Larysa Petrivna**

Doctor of technical sciences, professor

Professor of the Volodymyr Buriachok Department of Information and Cyber Security

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID ID 0000-0002-8509-6659

l.kriuchkova@kubg.edu.ua**Shandruk Maksim Serhiyovych**

master

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID ID 0009-0001-0431-9735

mshandruk99@gmail.com**METHODS OF COUNTERACTION IN RADIO NAVIGATION CONFLICTS**

Abstract. Modern radionavigation systems play a critically important role in the functioning of the global economy, transportation, defense, and everyday life. At the same time, the growing dependence on these systems creates new challenges related to their vulnerability to navigation signal jamming, spoofing of radionavigation system signals, and other types of destructive radio-electronic interference. The high dynamics of modern warfare, the development of high-precision strike complexes and systems, the implementation of network-centric automated control systems, and the increasing requirements for the timeliness, accuracy, and reliability of navigation information necessitate the improvement of both navigation support methods and hostile radio-electronic interference techniques. Under these conditions, radionavigation conflicts are among the most pressing threats to modern global navigation satellite systems, and the task of researching counteraction methods in radionavigation conflicts is relevant and necessary for enhancing the resilience of radionavigation systems and national security. The purpose of this publication is to systematize and provide an analytical overview of counteraction methods in radionavigation conflicts to identify promising directions for their development. The main types of intentional interference targeting the equipment of global navigation satellite system users are considered, in particular, the principles of spoofing interference formation; methods for detecting false navigation signals generated by spoofing devices; and protection methods against masking and spoofing interference. It is noted that ensuring effective counteraction in radionavigation conflicts requires continuous improvement of appropriate technologies and strategies, encompassing both technical and organizational aspects.

Keywords: global navigation satellite systems (GNSS); navigation signal; positioning accuracy; user navigation equipment; interference resistance; radionavigation conflict; spoofing; jamming; radio-electronic warfare; counteraction methods; protection methods; CRPA systems.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Vasyliiev, V. (2023). *Radionavhatsiini systemy: Pidruchnyk*. KPI im. Ihoria Sikorskoho, Vyd-vo «Politekhnik».
2. Zubkov, V. (2021). Navihatsiine zabezpechennia yak skladova informatsiinoho zabezpechennia syl oborony Ukrainy. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho, 3(73), 109–115. <https://doi.org/10.33099/2304-2745/2021-3-73/109-115>
3. Karlov, D., Korobetskyi, O., & Rieznikov, Yu. (2020). Rekomendatsii shchodo rozrobky zakhyshchenoho vid zavad pryimacha hlobalnykh navihatsiinykh suputnykovykh system dlia vyrishennia zavdan Zbroinykh Syl Ukrainy. *Systemy ozbroiennia i viiskova tekhnika*, (4), 60–66.
4. Sholokhov, S., Samborskyi, I., Vakulenko, O., & Nikolaienko, B. (2021). *Zavadozakhyst radioelektronnykh zasobiv. Chastyna 1. Osnovy zavadozakhystu system zviazku: Navchalnyi posibnyk*. ISZZI KPI im. Ihoria Sikorskoho.



5. Petrovskiy, A. (2019). Alhorytm vyivlennia vplyvu spufinhu pid chas vykonavchoi prokladky programnykh zasobamy elektronnoi kartohrafichnoi navihatsiino-informatsiinoi systemy. *Problemy informatsiinykh tekhnolohii*.
6. Opirskiy, I., & Bybyk, R. (2023). Doslidzhennia suchasnykh metodiv REB ta metodiv i zasobiv yii protydii. *Ukrainskyi naukovi zhurnal informatsiinoi bezpeky*, 29(2), 88–97.
7. Kriuchkova, L., Pshonnik, V., & Zozulia, S. (2019). Syhnaly GPS yak obiekty radiopodavleniia v zadachakh obiektovo-terytorialnoho zakhystu. *Suchasnyi zakhyst informatsii*, (1), 53–58.
8. Yarosh, S., & Huriev, D. (2022). Vprovadzhennia spetsyfichnykh sposobiv i zasobiv protydii bezpilotnym litalnym aparatam v uhrupovanni zenitnykh raketnykh viisk. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*, (2 (47)).
9. Yang, C., & Soloviev, A. (2023). In-Situ calibration of GPS antenna array with ambient signals. *U Proceedings of the 2023 international technical meeting of the institute of navigation* (s. 751–769).
10. Givhan, C. A., & Martin, S. M. (2023). Comparison of CRPA direction of arrival methods on post correlated GNSS signals for solution authentication and spoofing detection. *U Proceedings of the 2023 international technical meeting of the institute of navigation* (s. 303–314).
11. Arribas, J., Gómez, M., Fernández-Prades, C., Martín, D., García-Tuñón, J., & Rioja, T. (2023). A receiver-independent GNSS smart antenna for simultaneous jamming and spoofing protection. *U 2023 IEEE aerospace conference* (s. 1–13).
12. Esswein, M. (2023). *GNSS signal processing techniques for spoofing resiliency* [Neopubl. Doctoral dissertation]. Unknown.
13. Wiggins, G. (2023). *Improving CRPA anti-jamming performance with virtual array integration* [Neopubl. Master's Thesis]. Unknown.
14. Pérez-Marcos, E., Cuntz, M., Konovaltsev, A., Kurz, L., Caizzone, S., & Meurer, M. (2023). CRPA and array receivers for civil GNSS applications. *U 2023 IEEE/ION position, location and navigation symposium (PLANS)* (s. 318–328).
15. Yang, C., & Soloviev, A. (2023). Self-Contained implementation of nullsteering and beamforming with a standalone antenna array for GNSS signals under interference. *U 2023 IEEE/ION position, location and navigation symposium (PLANS)* (s. 917–934).
16. Liu, J., Chen, F., Xie, Y., Ge, B., Lu, Z., & Sun, G. (2023). Robust spoofing detection for GNSS array instrumentation based on C/N0 difference measurements. *IEEE Transactions on Instrumentation and Measurement*, 72, 1–11.
17. Madni, A., & Khan, W. (2023). 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*, 4, 779–791.
18. Santarelli, K., & Lan, W. (2023). *Coherent global positioning system signal interference detection and mitigation* [Neopubl. Master's Thesis].
19. BniLam, N., Principe, F., & Crosta, P. (2023). Large array antenna aperture for GNSS applications. *IEEE Transactions on Aerospace and Electronic Systems*.
20. Zhang, Z., Zhan, X., & Zhang, Y. (2017). GNSS spoofing localization based on differential code phase. *U Proc. Forum Cooperat. Positioning Service (CPGPS)* (s. 338–344).
21. *What is spread spectrum and its impact on GNSS/GPS antennas?* . (date of acceses 08.06.2025)
22. Movchan, K. (2024). Suchasni stratehii navihatsii droniv u vypadkakh vidsutnosti GPS syhnalu. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Serii: Tekhnichni nauky*, 35 (74)(5).
23. Magiera, J., & Katulski, R. (2019). Detection and mitigation of GPS spoofing based on antenna array processing. *Journal of Applied Research and Technology*, 13(1), 45–57.
24. Wu, R., Wang, W., Lu, D., Wang, L., & Jia, Q. (2017). Adaptive interference mitigation of GNSS. *Navigation: Science and Technology*.
25. Semanjski, S., Semanjski, I., Wilde, W., & Gautama, S. (2020). Use of supervised machine learning for GNSS signal spoofing detection with validation on realworld meaoning and spoofing data – Part II. *Sensors*, 20(7), 1806.
26. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*.
27. Guo, Y., Miao, L., & Zhang, X. (2018). Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle. *Sensors (basel)*, 19(1), 37.
<https://doi.org/10.3390/s19010037>

