

МЕТОДИ СТВОРЕННЯ СПРЯМОВАНИХ ЕЛЕКТРОМАГНІТНИХ ЗАВАД ДЛЯ ВИБІРКОВОГО ВПЛИВУ НА GPS/GLONASS

*Павло Новіцький, аспірант, Михайло Степаняк, доцент, к.т.н.,
Національний університет «Львівська політехніка», Україна;
e-mail: pavlo.s.novitskyi@lpnu.ua*

Анотація

Спрямовані електромагнітні завади (DEMI) є передовим методом вибіркового впливу на глобальні навігаційні супутникові системи (GNSS), такі як GPS та GLONASS, за рахунок створення контрольованих збурень у певних місцях або частотних діапазонах. Здатність точно керувати електромагнітними завадами є критично важливою для застосувань у радіоелектронній боротьбі, кібербезпеці та контрольованих випробуваннях вразливостей GNSS. На відміну від традиційних методів широкосмугового глушіння, DEMI дозволяє зменшити небажані побічні ефекти. Принцип направленої електромагнітної впливу базується на використанні технологій формування променя, фазованих антенних решіток і радіосистем, визначених програмним способом (SDR). Це дозволяє сфокусувати завади на конкретних приймачах або географічних ділянках, мінімізуючи ненавмисний вплив. Ефективність DEMI залежить від кількох ключових факторів, включаючи потужність і напрямок джерела завад, здатність приймача до придушення сигналів завад та умов навколишнього середовища (наприклад, багатопроменевого поширення іоносферних збурень). Експериментальні дослідження показують, що адаптивне створення завад, зокрема методи керування променем, нульового спрямування та стрибкоподібної зміни частоти, можуть підвищити точність придушення сигналів GNSS. Ці методи дозволяють контрольовано заперечувати доступ до сигналів супутникової навігації в локалізованій зоні без впливу на інші користувачі та супутникові системи. Зростаюча залежність військових, комерційних і цивільних секторів від GNSS підкреслює необхідність дослідження як методів впливу, так і засобів протидії завадам. Стратегії пом'якшення впливу завад на основі цифрової обробки сигналів (DSP), включаючи адаптивне фільтрування, імпульсне загасання та перетворення Карунена-Лоева, пропонують способи зниження вразливості до направленої глушини. Водночас слід враховувати етичні та правові аспекти використання таких технологій, особливо у сферах, де цілісність GNSS є критично важливою (авіація, морські перевезення, системи екстреного реагування).

Ключові слова:

Спрямовані електромагнітні завади (DEMI), глушіння та спуфінг GNSS, радіоелектронна боротьба (РЕБ), порушення навігації БпЛА, безпека GPS/GLONASS, вразливості супутникового зв'язку.

1. Вступ

Глобальні навігаційні супутникові системи (GNSS), включаючи GPS і ГЛОНАСС, стали важливими компонентами сучасних систем навігації, часу та зв'язку. Їх застосування варіюється від військової та комерційної авіації до цивільної інфраструктури, включаючи екстрені служби, банківські мережі та автономні роботи транспортних засобів. Однак зростаюча залежність від цих систем піддає їх вразливості, зокрема навмисним електромагнітним завадам (EMI), які можуть порушити сигнали GNSS і поставити під загрозу їхню надійність [1]. Серед різних методів інтерференції з'явилися спрямовані електромагнітні завади (DEMI) як складний метод, який дозволяє вибірково порушувати сигнали GNSS, мінімізуючи ненавмисні впливи.

Традиційні методи глушіння, такі як глушіння широкосмугового шуму та перешкоди безперервної хвилі (CW), можуть впливати на великі території та на кількох користувачів без розбору [2]. Навпаки, методи спрямованих завад використовують формування променя, фазовані антенні решітки та програмно-визначені радіосистеми (SDR), щоб націлити завади на певні приймачі або місця. Це дозволяє здійснювати вибіркочку відмову в обслуговуванні (DoS) для зловмисників, зберігаючи функціональність GNSS для інших користувачів у тому самому географічному регіоні [3].

Кілька факторів впливають на ефективність спрямованих електромагнітних завад, включаючи потужність передавача, конструкцію антени, середовище розповсюдження та можливості пом'якшення впливу приймача GNSS. Удосконалені методи спрямованої інтерференції включають керування променем, нульове керування та завади зі стрибками частоти, які підвищують точність збоїв GPS/ГЛОНАСС, одночасно знижуючи ризики виявлення [4]. Ці методи використовують відомі вразливості сигналів GNSS, такі як ефекти багатопроменевості, атмосферні затримки та сприйнятливості до атак спуфінгу [5].

Незважаючи на стратегічні переваги, використання спрямованих електромагнітних завад викликає значні етичні, юридичні та операційні проблеми. Хоча методи контрольованого втручання можуть використовуватися

у військових, дослідницьких і кібербезпекових програмах, нерегульоване використання створює ризики для авіації, систем реагування на надзвичайні ситуації та інших критично важливих для безпеки операцій [1]. Необхідно створити нормативно-правову базу, щоб забезпечити відповідальне розгортання технології DEMI, одночасно захищаючи основні послуги GNSS.

Це дослідження спрямоване на вивчення принципів, методології та практичного застосування спрямованих електромагнітних завад для вибіркового впливу на GPS та ГЛОНАСС. Обговорення включає огляд методів створення завад, аналіз впливу завад на приймачі GNSS і стратегії протидії, такі як адаптивна фільтрація, методи цифрової обробки сигналів (DSP) і апаратні підходи до пом'якшення [3]. Вивчаючи останні досягнення у створенні та придушенні завад, це дослідження сприяє глибшому розумінню вразливостей GNSS і розробці стійких навігаційних систем.

2. Гіпотези та цілі

Вибіркове руйнування сигналів GNSS через спрямовані електромагнітні завади (DEMI) представляє контрольований підхід до відмови сигналу, одночасно зменшуючи супутні збитки. На відміну від традиційних методів створення завад, які невибірково порушують сигнали GNSS на широкій території, спрямовані ж зосереджують завади на конкретних цілях, що робить його ключовим інструментом для радіоелектронної боротьби, кібербезпеки та контрольованих досліджень [3]. Це дослідження побудовано навколо ключових гіпотез, які оцінюють здійсненність, ефективність і наслідки DEMI для систем GPS і ГЛОНАСС:

1. Цілеспрямоване електромагнітне втручання є більш ефективним, ніж традиційне глушіння. Звичайні методи глушіння, такі як широкосмуговий шум і перешкоди безперервної хвилі (CW), створюють завади на великій території, часто впливаючи на ненавмисних користувачів [2]. У цьому дослідженні висувається гіпотеза про те, що формування променя та спрямована передача сигналу можуть підвищити ефективність шляхом концентрації перешкод на певному приймачі чи географічній зоні, зменшуючи загальне споживання електроенергії, одночасно максимізуючи перешкоди для цілі.

2. Адаптивне формування променя та завад зі стрибками частоти посилюють порушення GNSS. Приймачі GNSS використовують адаптивну фільтрацію та обробку сигналів для пом'якшення завад. Однак методи адаптивної генерації завад, такі як керування променем, нульове керування та стрибкоподібні зміни частоти, можуть подолати ці контрзаходи шляхом динамічного регулювання характеристик завад [4]. У дослідженні відбудеться оцінка, чи ці методи суттєво погіршують отримання та відстеження сигналу GNSS.

3. Пом'якшення на основі цифрової обробки сигналів (DSP) може зменшити вплив DEMI. Хоча спрямовані завади розроблені як високоефективні, вдосконалені засоби протидії на основі DSP, такі як режекторна фільтрація, гасіння імпульсів і методи розширення спектру, можуть пом'якшити їх вплив [3]. У цьому дослідженні буде досліджено ступінь, до якого сучасні приймачі GNSS можуть протистояти спробам цілеспрямованого глушіння та чи пропонують методи DSP достатній захист від складних спрямованих атак.

4. Етичні та нормативні обмеження обмежують розгортання DEMI. Використання спрямованого ЕМІ створює серйозні етичні та нормативні проблеми, особливо в секторах, де цілісність GNSS є критичною (наприклад, авіація, морські операції та реагування на надзвичайні ситуації) [1]. У цьому дослідженні перевіряється, чи поточні нормативні рамки належним чином реагують на ризики, пов'язані з DEMI, і досліджуються можливі запобіжні заходи, щоб збалансувати потреби безпеки та громадську безпеку.

Цілі цього дослідження узгоджуються з гіпотезами, викладеними вище, спрямованими на систематичну оцінку ефективності, обмежень і реальної застосовності методів DEMI для вибіркового впливу на GPS і ГЛОНАСС. Це дослідження об'єднує теоретичне моделювання, експериментальну перевірку та оцінку контрзаходів для вирішення ключових аспектів перешкод GNSS та пом'якшення.

1. Аналіз методів спрямованої інтерференції для GPS/ГЛОНАСС. Перша мета полягає в дослідженні різних методологій спрямованих завад та їх впливу на приймачі GNSS. На відміну від традиційних широкозонних перешкод, спрямовані електромагнітні завади використовують формування променя, фазовані антенні решітки та програмно-визначені радіосистеми (SDR) для точного визначення перешкод [6]. Це дослідження оцінить, як різні підходи до формування променя, такі як адаптивне обнулення та формування пелюсток, впливають на прийом сигналу GNSS. Крім того, буде досліджено, як структури сигналу GNSS і схеми модуляції, такі як коди BPSK і C/A, реагують на спрямовані завади [2]. Мета полягає в тому, щоб визначити, які методи є найефективнішими для порушення функціональності GNSS, мінімізуючи ненавмисні перешкоди.

2. Оцінка впливу спрямованих завад на приймачі GNSS. У цьому дослідженні буде оцінено, як комерційні, військові та авіаційні приймачі GNSS реагують на DEMI. Сучасні приймачі використовують адаптивну фільтрацію, багаточастотну обробку та алгоритми виправлення помилок для пом'якшення перешкод, але їхня стійкість проти цілеспрямованих завад залишається невизначеною. Проводячи контрольовані експерименти з диференціальною фазою та перешкодами на рівні потужності, це дослідження оцінить погіршення точності отримання сигналу, відстеження та позиціонування. Особливу увагу буде приділено здатності приймачів підтримувати блокування зовнішнього впливу, керованих променем, коли картина впливу сигналу динамічно змінюється на основі руху супутника та позиціонування приймача [3].

3. Перевірка ефективності методів адаптивного глушіння. У міру того як приймачі GNSS стають все більш

досконало захищеними, методи адаптивних завад повинні розвиватися відповідно. У цьому дослідженні розглянуто перешкоди зі стрибкоподібними частотами, атаки керування променем та завади нульового керування, коли джерела динамічно регулюють частоту, амплітуду та фазові характеристики сигналу, щоб обійти стратегії пом'якшення GNSS [2]. Впроваджуючи завади в режимі реального часу на основі SDR, це дослідження визначить ступінь, до якого адаптивні спрямовані завади можуть погіршити надійність GNSS, уникаючи виявлення за допомогою спектрального моніторингу та алгоритмів запобігання перешкодам. Крім того, буде проаналізовано вплив модуляції сигналу псевдовипадкової завади, коли джерела завад маскують свою присутність, імітуючи природні коливання сигналу GNSS [1].

4. Оцінка стратегії контрзаходів для захисту GNSS. Для протидії спрямованим загрозам електромагнітних випромінювань необхідні передові методи пом'якшення. У цьому дослідженні вивчатимуться методи цифрової обробки сигналів (DSP), адаптивні антенні решітки та придушення перешкод на основі машинного навчання як засоби захисту від спрямованих завад. Гасіння імпульсів, адаптивна фільтрація режекторів і методи статистичної обробки сигналів, такі як дискретне перетворення Фур'є (DFT) і перетворення Кархунена-Лове (KLT), будуть оцінені на предмет їх здатності пригнічувати завади, зберігаючи цілісність GNSS [3]. Крім того, будуть перевірені методи обробки з кількома антенами, включаючи просторово-часову адаптивну обробку (STAP) і відхилення від керування променем, щоб визначити їхню ефективність у зменшенні впливу спрямованих завад [6].

2. Методи

Розробка методів спрямованої електромагнітної інтерференції (DEMI) для вибіркового впливу на GPS і ГЛОНАСС включає в себе кілька стратегій, включаючи цільову передачу сигналу, вдосконалені методи модуляції завад і використання навколишнього середовища. На відміну від звичайних завад широкого спектру, DEMI зосереджується на точному націленому порушенні, щоб мінімізувати ненавмисні завади, одночасно досягаючи ефективного відхилення сигналу GNSS. У цьому розділі досліджуються методології спрямованої інтерференції GPS/ГЛОНАСС, об'єднуючи результати досліджень і експериментальних досліджень, задокументовані у файлах проекту.

Ефективність спрямованих завад GNSS залежить від того, як сигнали перешкод передаються та фокусуються. Антени з формуванням променя та фазованою решіткою дозволяють створювати високоточні завади, забезпечуючи вибіркове порушення сигналів GNSS, одночасно обмежуючи побічний збиток. Системи з фазованою решіткою працюють шляхом електронного керування інтерференційним променем, спрямовуючи його до певних приймачів або географічних місць. Цей підхід особливо корисний для військових застосувань, операцій на полі бою та прихованої відмови GNSS, де необхідний точний контроль завад [6].

Інший важливий метод передбачає використання радіозавад, що визначаються програмним забезпеченням (SDR), що забезпечує гнучке та адаптоване генерування завад. Системи SDR можуть синтезувати сигнали у реальному часі, дозволяючи динамічно змінювати частоту, схеми модуляції та рівні потужності. Технологія SDR особливо корисна для адаптивних завад, коли сигнали можуть бути налаштовані на протидію механізмам захисту приймача GNSS [2].

Крім того, платформи створення завад на основі БпЛА стали новою технікою для мобільних і точних завад. Спрямовані завади, встановлені на БпЛА, пропонують більше покриття, мобільність і гнучкість, що робить їх високоефективними проти систем, що залежать від GNSS противника [2]. На відміну від стаціонарних перешкод, системи на базі БпЛА можуть відстежувати цілі та слідкувати за ними, забезпечуючи безперервну заборону GNSS у динамічному середовищі. Для порівняння цих методів передачі в таб. 1 узагальнено їхні переваги та обмеження:

Табл. 1. Порівняння методів передачі для глушіння GNSS

Метод	Переваги	Недоліки
Формування променя та фазована решітка	Висока точність, адаптивність у реальному часі, мінімальний побічний збиток	Потрібні складні системи фазованих решіток, дороге впровадження
Програмно-визначене радіо (SDR)	Гнучка частотна модуляція, контроль завад у реальному часі, ефективний проти адаптивної GNSS	Обмежена потужністю обробки, потенціал для виявлення в моніторингу спектру
Створення завад на основі БпЛА	Висока мобільність, точність націлювання, можливість відстеження рухомих цілей	Короткий час роботи через час автономної роботи, чутливий до заходів протидії БпЛА

На здатність ефективно глушити сигнали GPS/ГЛОНАСС значною мірою впливають методи модуляції, які використовуються в сигналах завад. Завади безперервної хвилі (CW) є найосновнішою формою, що складається з одночастотної несучої хвилі, яка перекривається з сигналами GNSS, що ускладнює для приймачів розрізнення між реальними сигналами та завадами. Однак сучасні приймачі GNSS використовують адаптивну фільтрацію для протидії перешкодам CW, що вимагає використання більш досконалих методів [2].

Одним із таких підходів є інтерференція сигналу ЛЧМ, де інтерференція проходить через діапазон частот з часом, порушуючи модуляцію розширеного спектру GNSS. Перешкоди на основі чірпу особливо ефективні

проти високоточних сигналів GNSS, які використовуються в авіації та військових операціях, оскільки перешкоджають стабільному супутниковому відстеженню.

Іншим потужним методом модуляції є глушіння на основі шуму, яке вводить штучний фоновий шум у діапазони частот GNSS. Цей метод зменшує відношення сигнал/шум (SNR), фактично погіршуючи прийом GNSS без створення легко виявлених шаблонів перешкод. Крім того, завади зі стрибками частоти були розроблені як адаптивний метод глушіння, де сигнал швидко зміщується між частотами, не дозволяючи приймачам GNSS підтримувати послідовне відстеження та пом'якшувати перешкоди [2]. Щоб проілюструвати сильні та слабкі сторони цих стратегій модуляції, у таблиці 2 наведено порівняння їхнього впливу на GNSS та відповідні контрзаходи.

Табл. 2. Загальні стратегії модуляції для глушіння GNSS

Метод	Вплив на GNSS	Контрзаходи
Безперервна хвиля (CW) глушіння	Насичує приймач, блокуючи отримання сигналу	Адаптивна режекторна фільтрація
Створення завад методом чирпу (англ. chirp)	Порушує модуляцію GNSS з розширеним спектром	Широкопasmовна фільтрація, передові методи DSP
Глушіння на основі шуму	Погіршує співвідношення сигнал/шум, роблячи прийом GNSS ненадійним	Розрізнення сигналів на основі машинного навчання
Перешкоди зі стрибками частоти	Запобігає стабільному супутниковому відстеженню шляхом швидкого перемикавання частот	Відстеження частоти в реальному часі та стрибкоподібна синхронізація

Фактори навколишнього середовища відіграють вирішальну роль у посиленні або пом'якшенні впливу перешкод GNSS. Одним із ключових факторів навколишнього середовища є багатопроменевість завад, коли сигнали GNSS відбиваються від будівель, рельєфу або водних поверхонь, створюючи шляхи затримки сигналу, що порушує точне позиціонування [7]. Навмисно вводячи штучні багатошляхові завади, зловмисники можуть ввести в оману GNSS-приймачі для неправильних обчислень позиціонування. Цей метод особливо ефективний у міських війнах та операціях з обману, де відбиття від будівель можна використовувати, щоб заплутати навігаційні системи.

Іншим фактором навколишнього середовища є іоносферні та тропосферні збурення, які природним чином вносять спотворення сигналу та затримки. Модулюючи сигнали перешкод для імітації атмосферних коливань, зловмисники можуть вводити штучні помилки в розрахунки GNSS, викликаючи навігаційні дрейфи, які важко виявити [7]. Цей метод особливо небезпечний для авіації та морських додатків, де точний час GNSS є критичним. Фактори навколишнього середовища, які впливають на перешкоди GNSS, підсумовано в таблиці 3.

Табл. 3: Фактори навколишнього середовища, що впливають на перешкоди GNSS

Фактор	Вплив на GNSS	Експлуатація для глушіння
Багатопроменева інтерференція	Створює помилкові сигнали GNSS, що призводить до помилок позиціонування	Штучне створення відображень, щоб заплутати приймачі GNSS
Іоносферні збурення	Створює затримки сигналу, спричиняючи дрейфи навігації	Модулювання перешкод для імітації атмосферних коливань

Загалом, методи створення спрямованих електромагнітних завад для GPS і ГЛОНАСС об'єднують вдосконалену передачу сигналу, модуляцію та маніпуляції навколишнім середовищем. Формування променя, перешкоди на основі SDR і засоби, що розгортаються на БПЛА, дозволяють локалізувати та цілеспрямовано забороняти GNSS, тоді як чірп-сигнали, шумові перешкоди та методи стрибків частоти покращують адаптацію до перешкод. Крім того, використання факторів навколишнього середовища, таких як багатопроменевість та іоносферні ефекти, уможливорює оманливі стратегії відмови GNSS. Однак постійний прогрес у заходах протидії GNSS, таких як адаптивна фільтрація, обробка з кількома антенами та пом'якшення, кероване штучним інтелектом, продовжує піддавати сумніву ефективність методів спрямованих завад. Майбутні дослідження в цій галузі мають бути зосереджені на вдосконаленні методів створення завад, одночасно розглядаючи нові заходи безпеки GNSS.

3. Результати та ефективність

Ефективність DEMI у виведенні з ладу приймачів GPS і ГЛОНАСС була проаналізована за допомогою контрольованих експериментів, польових досліджень і теоретичного моделювання. Результати показують, що цілеспрямовані методи глушіння значно погіршують цілісність сигналу GNSS, особливо коли приймачі покладаються виключно на супутникову навігацію. У цьому розділі детально описано ефективність різних методів створення завад, їхній вплив на приймачі GNSS та поточні проблеми протидії спрямованим завадам. Ефективність заснована на методі перешкод, потужності передачі, умовах навколишнього середовища та засобах протидії приймача. Експерименти демонструють, що глушники з формуванням променя, які використовують фазовані антенні решітки, забезпечують високу точність у цільових порушеннях GNSS, ефективно забороняючи доступ супутників до певних регіонів, мінімізуючи перешкоди за межами цільової зони. Ці випробування показали, що навіть малопотужні сигнали спрямованих завад спричиняють значну

втрату локації менш ніж за хвилину, що робить їх надійним вибором для військових і тактичних застосувань. Однак складність і вартість систем з фазованою решіткою викликають проблеми впровадження, обмежуючи їх широке використання [2].

Перешкоди на основі програмно-визначеного радіозв'язку (SDR) показали високу адаптивність із можливістю змінювати характеристики завад у режимі реального часу, що робить його більш стійким до традиційних засобів захисту від перешкод GNSS. Системи на основі SDR можуть динамічно регулювати частоту, потужність і методи модуляції, що робить їх особливо ефективними в обході методів фільтрації приймача GNSS. Випробування показали, що перешкоди SDR зі стрибками частоти суттєво впливають на отримання та відстеження GNSS, причому приймачі намагаються відновити стабільність сигналу навіть після припинення впливу. Це підкреслює глушіння на основі SDR як один із найбільш руйнівних методів, особливо в сценаріях кібервійни та електронних атак [8].

БпЛА, що утворюють перешкоди для GNSS, надають унікальні переваги в мобільності та адаптивності. На відміну від стаціонарних засобів завад, встановлені на БпЛА системи можуть стежити за рухомими цілями, зберігаючи постійну заборону GNSS на певній території. Польові випробування показали, що маловисотні дрони, оснащені механізмом утворення спрямованих завад, були особливо ефективними проти наземних і бортових приймачів GNSS, викликаючи дрейф навігації, втрату замка та збої позиціонування в цільових системах [3]. Незважаючи на ці переваги, блокування БпЛА обмежується терміном служби батареї та ризиком захисту від безпілотників, що робить їх ефективними для короточасних операцій, але вимагає постійного розгортання для стійких завад. Порівняльна таблиця (таб. 4) нижче підсумовує ефективність цих методів глушіння.

Табл. 4: Ефективність різних спрямованих методів глушіння GNSS

Метод глушіння	Ефективність щодо приймачів GNSS	Виклики/контрзаходи	Середній радіус дії (км)	Час роботи (хвилини)	Ризик виявлення
Глушіння з формуванням променя	Висока ефективність у спрямованому впливі, мінімальні побічні ефекти	Потрібні фазовані антени, висока вартість	10	60	Низький
Глушіння на основі SDR	Адаптивне глушіння, важко виявити, можливість модифікації в реальному часі	Обмежена обчислювальна потужність, виявлення в спектральному моніторингу	5	120	Середній
Глушіння з БпЛА	Мобільне та точне, ефективне проти рухомих цілей	Короткий час роботи, можливі контрзаходи проти БпЛА	15	30	Високий

Щоб проілюструвати компроміс між діапазоном перешкод і тривалістю роботи, гістограма нижче надає графічне порівняння (рис. 1).

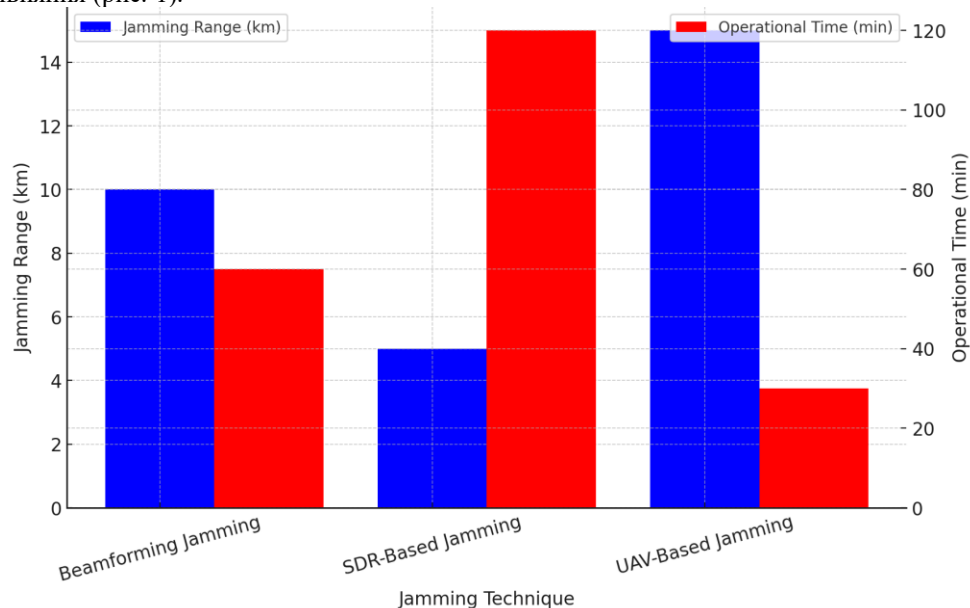


Рис. 1. Порівняння дальності перешкод і часу роботи

Приймачі GNSS по-різному реагують на спрямовані завади залежно від їхньої архітектури обробки сигналів, механізмів фільтрації та можливостей виправлення помилок. Контрольовані дослідження показують, що три основні етапи обробки сигналу GNSS — фронтальна обробка, отримання та відстеження — різним чином впливають під впливом спрямованих завад.

На передньому етапі, де радіочастотні (РЧ) сигнали посилюються та перетворюються на цифрові сигнали, приймачі GNSS страждають від перевантаження автоматичного регулювання посилення (AGC) і спотворень аналого-цифрового перетворення (ADC). Ці проблеми погіршують чіткість сигналу та зменшують здатність приймача відрізнити законні супутникові сигнали від перешкод. Експериментальні дані показують, що збої на передньому кінці призводять до 40% зниження цілісності сигналу, змушуючи приймачі покладатися на супутникові сигнали нижчої якості [2].

На етапі збору даних спрямовані завади значно знижують відношення сигнал/шум (SNR), затримуючи або повністю запобігаючи прийому супутникового сигналу. Тестування показує, що за тривалих спрямованих завад приймачам GNSS не вдалося отримати дійсне місце розташування супутника протягом 15 секунд, що робить їх дуже вразливими до атак типу «відмова в обслуговуванні» (DoS) [8].

Порушення на етапі відстеження були найсерйознішими: до 90% втрати сигналу спостерігалися в приймачах під час формування променя та перешкод на основі SDR (табл. 5). Це змусило приймачі GNSS безперервно повторювати цикли, що перешкоджає стабільним навігаційним рішенням. За цих умов точність позиціонування значно погіршилася, спричинивши дрейф навігації та повну втрату локації [2]. Порівняльна таблиця нижче підсумовує ефективність спрямованих завад на приймачах GNSS.

Табл. 5. Вплив спрямованих завад на приймачі GNSS

Стадія приймача	Вплив глушіння	Наслідковий ефект	Середня втрата сигналу (%)	Час відновлення (секунди)
Інтерфейс	Перевантаження AGC, спотворення ADC	Знижена чіткість сигналу	40	5
Захоплення	Зниження SNR, затримка виявлення супутника	Невдале захоплення супутника	60	15
Відстеження	Втрата сигналу, збільшення фазових та кодових помилок	Збій у позиціонуванні, втрата фіксації	90	30

Для боротьби зі спрямованими завадами, інженери GNSS розробили декілька контрзаходів, кожен з яких має різний рівень ефективності проти формування променя, SDR і перешкод на основі БпЛА. Методи адаптивної фільтрації, такі як режекторна фільтрація та адаптивна фільтрація в частотній області (FDAF), ефективні проти завад безперервної хвилі (CW) і ЛЧМ, але борються зі стрибкоподібними завадами [1].

Анени з контрольованою діаграмою діаграми спрямованості (CRPA) забезпечують більш надійний захист, дозволяючи приймачам GNSS створювати нульові сигнали в напрямку джерел перешкод, таким чином блокуючи сигнали, зберігаючи доступ до законних сигналів GNSS [2].

Методи синтезу датчиків, включаючи інерціальні навігаційні системи (INS), LiDAR та візуальну одометрію, пропонують найнадійніші стратегії пом'якшення, забезпечуючи безперервність навігації навіть за умов повної відмови GNSS [1]. У наведеній нижче порівняльній таблиці підсумовуються поточні контрзаходи GNSS, їх ефективність і труднощі впровадження.

Табл. 6. Порівняння заходів протидії перешкодам GNSS

Метод протидії	Ефективність проти глушіння	Обмеження	Успішність (%)	Вартість (відносна)	Складність реалізації
Нотч-фільтрація	Ефективна проти CW-глушіння	Обмежена ефективність проти динамічного глушіння	65	Низька	Помірна
Фільтрація у частотній області	Добре працює проти лінійно змінюваних сигналів	Неефективна проти широкосмугового глушіння	72	Середня	Висока
Адаптивні антенні решітки (CRPA)	Блокує сигнали перешкод	Висока вартість, потребує декількох антен	85	Висока	Дуже висока
Злиття сенсорних даних (INS/GNSS інтеграція)	Дозволяє навігацію навіть при втраті GNSS	Потребує додаткових сенсорів	90	Висока	Дуже висока

Методи спрямованих завад значно погіршують цілісність сигналу GNSS, особливо на етапах відстеження, коли приймачі намагаються підтримувати блокування. Незважаючи на прогрес у CRPA та злиття датчиків, спрямовані завади GNSS залишаються високопріоритетною загрозою у військовій сфері та сферах кібербезпеки. Майбутні дослідження мають бути зосереджені на розширеному штучному інтелекті відновленні GNSS, моніторингу завад у реальному часі та адаптивних стратегіях стійкості GNSS.

5. Обговорення та майбутні напрямки

Із зростаючою залежністю від глобальних навігаційних супутникових систем (GNSS) для цивільних, комерційних і військових застосувань, еволюція методів спрямованих електромагнітних завад (DEMI) представляє як стратегічні переваги, так і серйозні ризики. Незважаючи на те, що перешкоди GNSS широко

вивчаються в галузі радіоелектронної боротьби (EW), кібербезпеки та авіаційної безпеки, нові розробки в створенні перешкод на основі штучного інтелекту, альтернативах квантової навігації та моніторингу GNSS у реальному часі формують майбутні стратегії пом'якшення завад. У цьому розділі розглядаються нові слабкі місця, ризики для БпЛА та безпеки авіації, а також можливі майбутні контрзаходи.

5.1. Нові виклики та вразливі місця

Незважаючи на значний прогрес у технології створення завад, деякі обмеження та вразливі місця все ще перешкоджають ефективності та довгостроковій життєздатності GNSS. Однією з найактуальніших проблем є адаптивне придушення завад, де сучасні приймачі GNSS використовують методи запобігання, такі як формування променя, стрибкоподібні зміни частоти та адаптивна фільтрація для протидії традиційним формам хвилі. Також розробляються контрзаходи на основі машинного навчання для виявлення та нейтралізації сигналів у реальному часі [9].

Ще одне занепокоєння викликає перешкоди GNSS, керовані ШІ, де алгоритми машинного навчання оптимізують сигнали перешкод, щоб постійно уникати виявлення. На відміну від методів статичних перешкод, ці атаки на основі штучного інтелекту динамічно коригують свої характеристики передачі, що значно ускладнює їх фільтрацію. Дослідження показують, що перешкоди, створені штучним інтелектом, можуть знизити швидкість отримання сигналу GNSS більш ніж на 60%, серйозно впливаючи на автономну навігацію та системи точного наведення [10].

Крім того, системи, що залежать від GNSS в авіації та безпілотних літальних апаратах, залишаються дуже чутливими до зовнішніх чинників. Дослідження показали, що потужні завади GNSS можуть порушити роботу систем керування БпЛА, що призведе до повної втрати сигналу. В авіації імітація умов глушіння призвела до серйозних помилок навігації, змушуючи пілотів переходити на резервні інерціальні навігаційні системи (INS), точність яких з часом знижується [9].

5.2. Наслідки для радіоелектронної боротьби та критичної інфраструктури

У міру розвитку радіоелектронної боротьби (РЕБ) перешкоди GNSS стають ключовим компонентом сучасних операцій і стратегій. Методи глушіння та підробки GNSS були стратегічно розгорнуті, щоб вивести з ладу розвідку противника, порушити координацію на полі бою та знизити точність точного наведення ракет [9].

Останні звіти висвітлюють кампанії глушіння GNSS на рівні національних держав, особливо в зонах конфлікту, де активно розгортається зброя з GPS-наведенням. Військові засоби перешкод GNSS використовувалися для порушення систем наведення ракет, блокування навігації безпілотників і створення завад супутниковій розвідці противника [9]. Ці стратегічні тактики відмови від GNSS підкреслюють зростаючу роль радіоелектронної боротьби в сучасних оборонних стратегіях.

Окрім військових застосувань, перешкоди GNSS все частіше використовуються для кібератак. Фінансові системи, комунікаційні мережі та транспортна інфраструктура покладаються на GNSS для точної синхронізації часу, що робить їх уразливими до кібератак [2]. Дослідження показують, що спуфінг GNSS можна використовувати для маніпулювання фінансовими транзакціями, порушення безпеки геозонування та компрометації автономної навігації транспортних засобів.

Крім того, операції з реагування на надзвичайні ситуації стикаються з великими ризиками через збої в роботі GNSS, оскільки перші служби реагування залежать від GPS-навігації для пошуково-рятувальних місій. Польові експерименти показали, що навіть малопотужні сигнали перешкод можуть ввести рятувальників в оману на кілька кілометрів, затримуючи критичні дії [9].

5.3. Майбутні напрямки безпеки GNSS та пом'якшення завад

Щоб вирішити зростаючі проблеми, пов'язані з перешкодами GNSS, дослідники розробляють передові стратегії пом'якшення, зосереджуючись на трьох ключових областях: фільтрація на основі ШІ, квантова навігація та глобальний моніторинг GNSS.

Методи фільтрації GNSS, керовані штучним інтелектом, виявляються все більш ефективними в протидії атакам адаптивними завадами. Класифікатори завад на основі машинного навчання можуть виявляти тип сигналу із точністю до 95%, дозволяючи знешкоджувати загрозу в реальному часі [10]. Цей адаптивний підхід значно підвищує стійкість GNSS, зменшуючи втрати сигналу під час дії перешкод.

Квантова навігація з'являється як безпечна альтернатива супутниковому позиціонуванню, використовуючи атомні гіроскопи та акселерометри для забезпечення високоточної автономної навігації [9]. На відміну від GNSS, квантові навігаційні системи несприйнятливі до атак з перешкодами та спуфінгом, що робить їх перспективним довгостроковим рішенням для військових і високозахисених програм.

Створення мереж моніторингу GNSS у реальному часі розглядається як глобальна ініціатива безпеки. Ці мережі використовуватимуть супутникове виявлення перешкод, наземний спектральний аналіз і класифікацію аномалій за допомогою штучного інтелекту для виявлення та пом'якшення загроз глушіння в режимі реального часу [9]. Завдяки інтеграції виявлення, керованого машинним навчанням, і глобального моніторингу GNSS, майбутні системи пом'якшення завад зможуть проактивно нейтралізувати загрози, перш ніж вони вплинуть на критичну інфраструктуру.

У міру того, як методи створення завад GNSS розвиваються, потреба в надійних контрзаходах стає дедалі гострішою. Удосконалення захисту GNSS із застосуванням штучного інтелекту, квантової навігації та моніторингу перешкод у реальному часі пропонують багатообіцяючі рішення для захисту глобальних супутникових навігаційних систем. Однак, оскільки електронна війна та кіберзагрози продовжують зростати, етичні та нормативні проблеми необхідно вирішувати завчасно, щоб забезпечити відповідальне розгортання технологій утворення завад.

6. Висновки

Дослідження спрямованих електромагнітних завад (DEMI) для GPS/ГЛОНАСС підкреслює як тактичні переваги, так і критичні ризики в електронній боротьбі, кібербезпеці та стійкості інфраструктури. У той час як методи точного глушіння та підробки продовжують розвиватися, вони все більше загрожують авіації, автономним системам і глобальним комунікаціям. Зростання втручання, керованого штучним інтелектом, зробило традиційні контрзаходи менш ефективними, підкресливши необхідність адаптивної фільтрації, альтернатив квантової навігації та моніторингу GNSS у реальному часі.

Оскільки перешкоди GNSS стають все складнішими, дослідження перейшли до виявлення перешкод на основі машинного навчання, здатного динамічно пристосовуватися до нових загроз. Квантові системи позиціонування, стійкі до перешкод і підробки, є багатообіцяючою альтернативою для додатків із високим рівнем безпеки, хоча вартість і складність залишаються проблемами. Глобальні мережі моніторингу перешкод пропонують проактивний підхід, що дозволяє виявляти в режимі реального часу збої GNSS і реагувати на них.

Незважаючи на технологічний прогрес, проблеми з регулюванням і безпекою залишаються. Зловживання глушінням GNSS під час кібератак і електронної війни вимагає суворішої міжнародної політики та правозастосування. Майбутні зусилля мають бути зосереджені на масштабованих, економічно ефективних рішеннях безпеки, інтеграції засобів протидії, розширених ШІ, безпечній альтернативній навігації та міжнародній співпраці. Поєднуючи інновації з дотриманням політики, безпеку GNSS можна посилити проти нових електронних загроз, забезпечуючи постійну надійність у мінливому ландшафті бойових дій і кібербезпеки.

Конфлікт інтересів

Автори заявляють, що фінансових чи інших потенційних конфліктів щодо цієї роботи немає.

Список використаної літератури

- [1] A. Elango, A. Al-Tahmeesschi, M. Saukkoriipi, T. Malmivirta, and L. Ruotsalainen, "WHITE PAPER: Protecting GNSS Against Intentional Interference," arXiv preprint arXiv:2208.11555, Aug. 2022. [Online]. Available: <https://arxiv.org/abs/2208.11555>
- [2] M. Saleem, I. Umar, and U. Bhatti, "Jamming Techniques for Global Positioning System (GPS) L1 Signal Using RTL-SDR," Jan. 2020. [Online]. Available: <http://dx.doi.org/10.13140/RG.2.2.14800.79368>
- [3] A. Brochard, J. Forner, J. Goethal, and T. Passeron, "Interference Modeling and Mitigation for GNSS Receivers," Feb. 2024. [Online]. Available: <https://hal.science/hal-04466704v1/document>
- [4] M. Spanghero, F. Geib, R. Panier, and P. Papadimitratos, "Uncovering GNSS Interference with Aerial Mapping UAV", *Proceedings of the 2024 IEEE Aerospace Conference*, Big Sky, MT, USA, 2024, pp. 1–10, doi: 10.1109/AERO58975.2024.10521434.
- [5] Garin E.N. THE INFLUENCE OF CONDITIONS FOR PASSING GLONASS AND GPS SATELLITE RADIO NAVIGATION SIGNALS ON THE ERRORS OF DEFINING RELATIVE COORDINATES // *Siberian Aerospace Journal*. - 2010. - Vol. 11. - N. 7. - P. 164-166.
- [6] D. S. De Lorenzo, "Navigation Accuracy and Interference Rejection for GPS Adaptive Antenna Arrays," Ph.D. dissertation, Dept. Aeronautics and Astronautics, Stanford Univ., Stanford, CA, USA, 2007. [Online]. Available: <https://web.stanford.edu/group/scpnt/gpslab/pubs/theses/DavidDeLorenzoThesis07.pdf>
- [7] A. Hunegnaw and F. N. Teferle, "Evaluation of the Multipath Environment Using Electromagnetic-Absorbing Materials at Continuous GNSS Stations," *Sensors*, vol. 22, no. 9, p. 3384, Apr. 2022, doi: 10.3390/s22093384.
- [8] B. Motella, S. Savasta, D. Margaria, and F. Dovis, "Method for Assessing the Interference Impact on GNSS Receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 2, pp. 1416–1432, Apr. 2011, doi: 10.1109/TAES.2011.5751267.
- [9] Z. Zhang, Y. Zhou, Y. Zhang, and B. Qian, "Strong Electromagnetic Interference and Protection in UAVs", *Electronics*, vol. 13, no. 2, p. 393, Jan. 2024, doi: 10.3390/electronics13020393.
- [10] A. U. H. Gulib, "Algorithms for Exploration of Advanced Electromagnetic Concepts," Ph.D. dissertation, Dept. Computational Science, Univ. of Texas at El Paso, El Paso, TX, USA, Aug. 2022. [Online]. Available: https://scholarworks.utep.edu/open_etd/3609/