ЗАГРОЗИ ІНФОРМАЦІЇ ГЛОБАЛЬНОЇ НАВІГАЦІЙНОЇ СУПУТНИКОВОЇ СИСТЕМІ ТА СПОСОБИ ЇХ УСУНЕННЯ

Швець В.А.
кандидат технічних наук, доцент
Національний авіаційний університет, м. Київ, Україна

INFORMATION THREATS TO THE GLOBAL NAVIGATION SATELLITE SYSTEM AND HOW TO ELIMINATE THEM

Shvets V.A.
Candidate of Technical Sciences, Associate professor
National Aviation University, Kyiv, Ukraine

АНОТАЦІЯ

Рассматривается проблема ограничения доступности и целостности к информации в глобальной спутниковой навигационной системе, что ставит под угрозу эффективное функционирование объектов критической инфраструктуры. На основе исследований Национального авиационного университета предлагаются к реализации организационные способы в виде мониторинга и оценки доступности радионавигационного поля, а также технические решения по обеспечению целостности информации ГНСС – адаптивное управление диаграммой направленности, которое является наиболее эффективным решением по обеспечению доступности и целостности навигационной информации для потребителей.

ABSTRACT

The problem of limiting the availability and integrity of information in the global satellite navigation system is considered, which jeopardizes the effective functioning of objects of critical infrastructure. Based on the research of the National Aviation University, organizational methods are proposed for implementation in the form of monitoring and accessibility of the radio navigation field, as well as technical solutions for ensuring the integrity of GNSS information — adaptive control of the radiation pattern, which is the most effective solution to ensure the availability and integrity of navigation information for consumers.

Ключові слова: глобальна навігаційна супутникова система, загроза інформації, критична інфраструктура, jamming, адаптивна антенна, діаграма спрямованості, beamformer, nulling-антена, кореляційна матриця.

Keywords: global navigation satellite system, information threat, critical infrastructure, jamming, adaptive antenna, pattern, beamformer, nulling-antenna, correlation matrix.

Проблема експлуатації ГНСС. Сучасний етап розвитку суспільства характеризується все більш широким використанням координатно-часового забезпечення (КЧЗ), що становить основу ефективного функціонування багатьох галузей економіки і є найважливішою частиною сучасних транспортних систем, цифрових систем телекомунікації, енергетики, фінансової і банківській сфері, систем управління військами і високоточною зброєю, які відносяться до об'єктів критичної інфраструктури [1].

Однак при експлуатації глобальної навігаційної супутникової системи (ГНСС) виявилися факти їх низької завадостійкості, що позначається на доступності і цілісності навігаційних даних [2-8]. Таким чином, уразливість ГНСС є в даний час загальновизнаним фактом.

Аналіз досліджень і публікацій. Експлуатація ГНСС виявила можливість вразливості. Про вразливості цивільних приймачів ГНСС було відомо давно [3–11], але її рідко беруть до уваги виробники приймачів та їх користувачі.

Було проведено кілька аналізів вразливості транспортних систем, заснованих на використанні сигналів GPS [10 – 18]. Одним з найбільш важливих і своєчасних звітів про дослідження в цій області був звіт Центру Волпе [8] про вразливості GPS, у висновках якого зазначалося, що система GPS, як і інші радіонавігаційні системи, вразлива при впливі ненавмисних і навмисних завад і що такі завади несуть загрозу безпеці і можуть мати серйозні наслідки для економіки і навколишнього середовища. У звіті зроблено висновок про те, що зростаюче використання GPS в цивільній інфраструктурі робить її усе більш привабливою мішенню для ворожих дій окремих особистостей і груп. В той же час виявлена комерційна доступність обладнання для постановки перешкод. Можна сказати що в наявності є сумний факт поширення принципів радіоелектронної боротьби на сферу високої технології супутникової навігації, у тому числі й для цивільних застосувань [15-21].

Таким чином, вразливість ГНСС при впливі ненавмисних і навмисних завад є в даний час загальновизнаним фактом. Ця вразливість в рівній мірі відноситься як до GPS, ГЛОНАСС і ГАЛІЛЕО, оскільки принципи їх побудови і діапазони частот досить близькі.

В Національному авіаційному університеті були проведені власні дослідження впливу сигналів завад на якість роботи приймача ГНСС в залежності від статистичних характеристик завади. Результати випробувань повністю описані роботах співробітників університету [22-24].

Мета. На основі аналізу інформаційних потоків в ГНСС виявити найменш захищені місця в

структурі ГНСС та запропонувати способи їх усунення.

Викладення основного матеріалу. Об'єкти критичної інфраструктури цивільного сектору отримують наступну інформацію від ГНСС (рис. 1):

- *енергетика* – інформація від ГНСС про час;
- *телекомунікації* – інформація від ГНСС про час та позицію;
- *транспорт* – інформація від ГНСС про час та позицію;
- *фінанси і банківська сфера* – інформація від ГНСС про час.

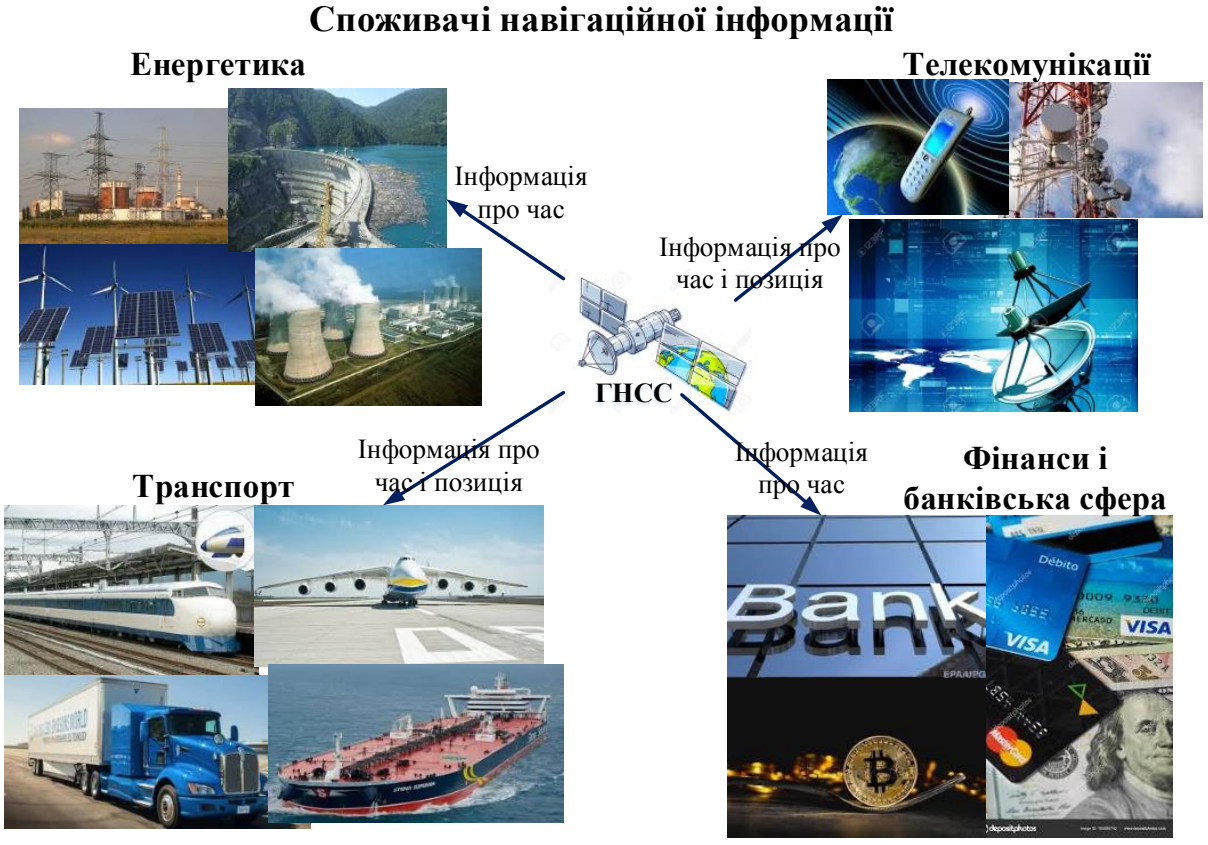

Рис. 1. Об'єкти критичної інфраструктури, споживачі навігаційної інформації

Основу КЧЗ складають ГНСС, які представлені в даний час СРНС ГЛОНАСС (Росія) і GPS (США). Європейське співтовариство створює для цих цілей свою СРНС GALILEO (*далі в роботі будуть розглядатися тільки ГНСС GPS і ГЛОНАСС, тому що вони офіційно введені в експлуатацію і мають нормативні міжнародні рекомендації до використання в навігації*).

Для оцінки загроз цілісності і доступності інформації ГНСС розглянемо загальні принципи побудови системи.

Супутникова радіонавігаційна система складається з п'яти основних сегментів [2]:

- *наземний керуючий сегмент*;
- *космічний сегмент*;
- *сегмент користувачів* – приймачі ГНСС;
- *сегменти наземних (GBAS) і космічних (SBAS) функціональних доповнень*.

Доповнення GBAS і SBAS включені ICAO і забезпечують режим диференціальної супутникової навігації, вирішують завдання контролю цілісності і доступності навігаційної інформації [2].

На основі повного опису ГНСС представленому в [2], зобразимо ГНСС у вигляді узагальненої схеми (рис. 2), щоб простежити інформаційні потоки і пристрої найбільш вразливі в плані захисту інформації (вразливість цілісності та доступності інформації).

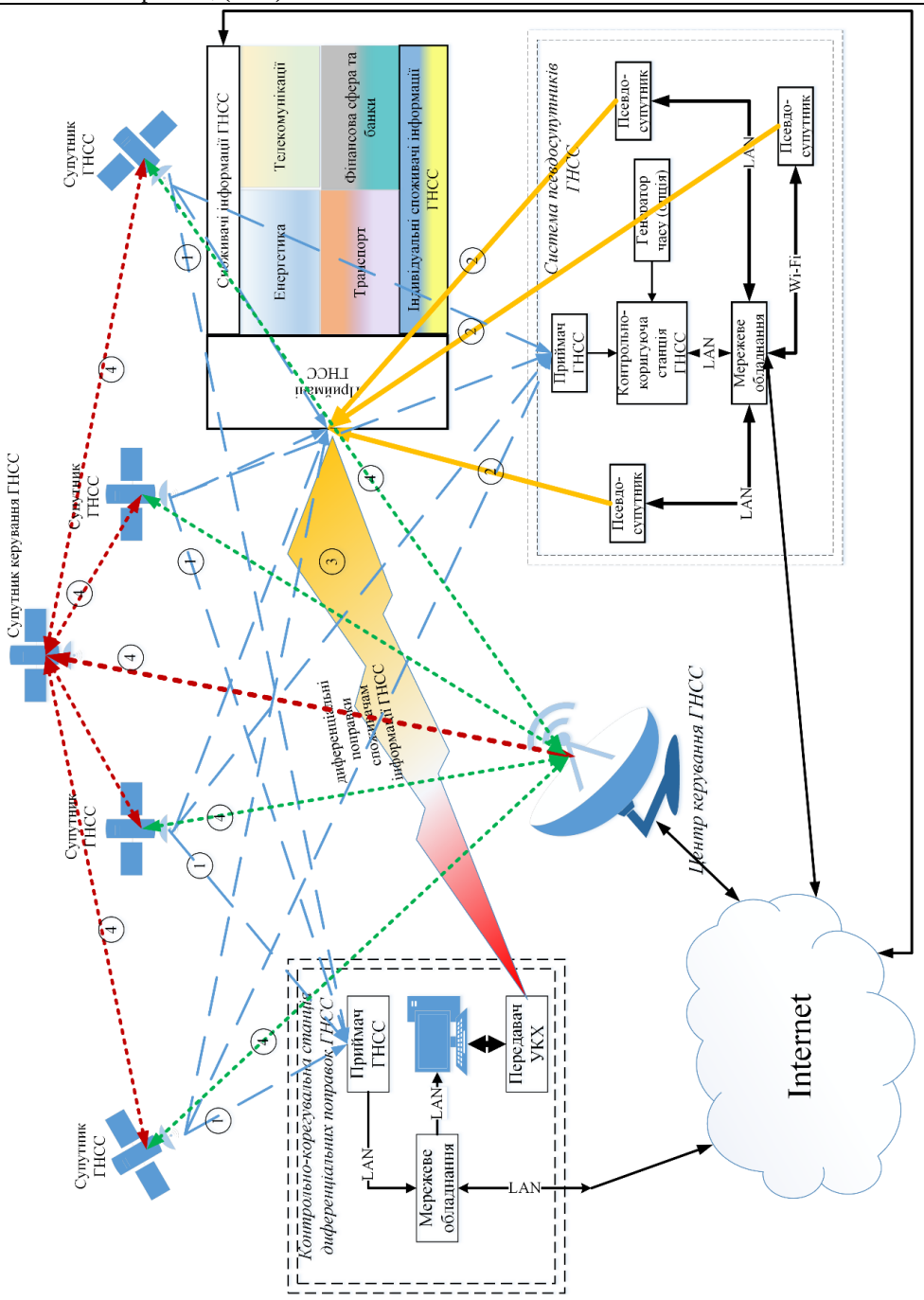

Рис. 2. Узагальнена схема інформаційних потоків в системі ГНСС
1 – навігаційна інформація від супутників ГНСС, 2 – навігаційна інформація від псевдосупутників ГНСС, 3 – диференціальні поправки споживачам, 4 – інформація керування космічним сегментом.

Наземний керуючий сегмент і космічний сегмент – об'єкти інформаційної діяльності (ОІД), на яких заходи щодо захисту інформації покладено на державні та військові органи. Передача інформації здійснюється по захищеним каналами зв'язку, тому можна сказати, що порушення цілісності та доступності інформації в мирний час не існує.

Сегмент користувачів складається з приймачів ГНСС і приймачів ГНСС з доповненнями GBAS, рівень сигналу від навігаційного супутника ГНСС на антені приймача становить від -157дБ до -163дБ [2]

Доповнення GBAS – це контрольно-коригувальна станція диференціальних поправок в складі якої є наземний приймач ГНСС, програмно-апаратна підсистема обробки даних і формування повідомлень GBAS, передавач УКХ діапазону, комп'ютерна мережа підключена до Internet, а також система псевдосупутників для поліпшення навігаційного поля в важко доступної місцевості і в місцях з високим інтерферентним рівнем сигналів, передача інформації через інтернет здійснюється стійкими криптографічними алгоритмами [2-11]. Доповнення GBAS це автономні малогабаритні системи, які розташовуються на поверхні Землі і не мають ніякого захищеного периметра, тобто до цього об'єкта ОІД є якщо не вільний доступ, то можна отримати доступ за підробленими документами.

Наприклад: в даний час ведуться переговори про розміщення доповнення GBAS в Міжнародному аеропорту «Київ» імені Ігоря Сікорського. Це доповнення буде покривати зону точної навігації радіусом 300 км (рис. 3). Аеропорт "Бориспіль", "Київ", злітні смуги концерну "Антонов" в Києві і

Гостомелі, злітна смуга в Василькові, Білій Церкві, Узині, Кропивницькому, Кременчукі, Хмельницькому, Вінниці.

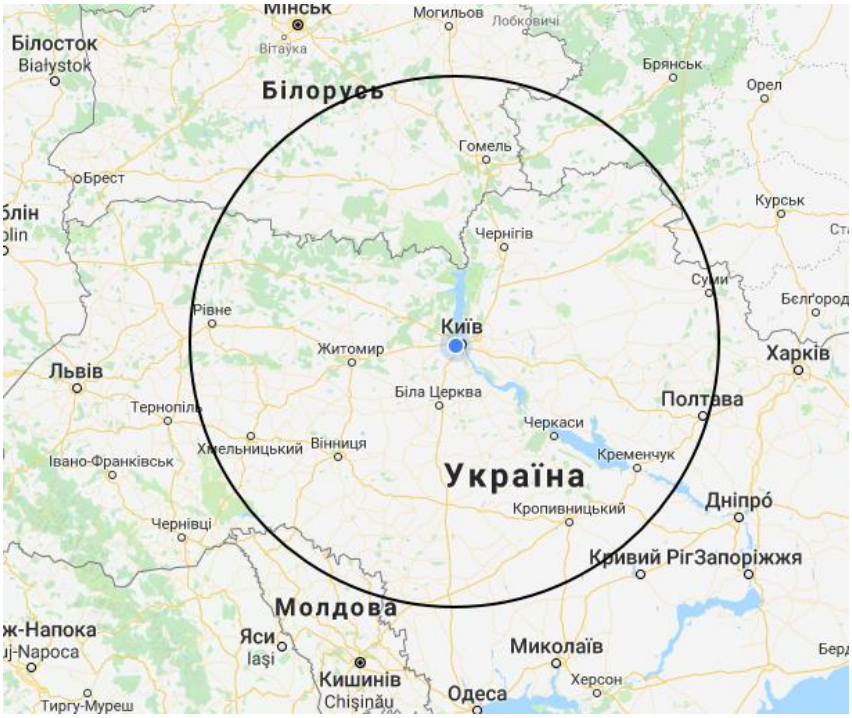

Рис. 3. Зона покриття доповнення GBAS, яке буде розташовано у аеропорту "Київ"

Як що на цей об'єкт буде скоєна навить терористична кібератака використання точної навігації буде неможливо в зоні дії GBAS.

Доповнення SBAS крім космічної складової має наземну мережу станцій моніторингу і збору даних ГНСС, які отримують інформацію від приймача ГНСС [2-11].

Вимоги до експлуатаційних характеристик ГНСС стосовно застосування на об'єктах критичної інфраструктури наведені в [2,8,25–30].

Найважливішою особливістю сигналів ГНСС є їх низький рівень потужності на антені приймача ГНСС яка становить приблизно 10^{-16} Вт. Тому ненавмисні та навмисні завади знижують продуктивність приймача ГНСС. Захист від ненавмисних завад проводиться на етапі розробки ГНСС її впровадження і організації експлуатації.

Зі сказаного вище можна зробити висновок, що приймач ГНСС – пристрій найбільш вразливий в плані доступності і цілісності навігаційної інформації, тому що слабкий сигнал від супутника ГНСС можна приховати в більш сильному сигналі від генератора з частотним діапазоном ГНСС, така загроза отримала назву *jamming*-атака [2-11]. У той же час технологію псевдоспутніков можна використовувати для порушення цілісності інформації від реальних супутників ГНСС шляхом підміни їх сигналів, так звана інтелектуальна перешкода. Така загроза отримала назву *spoofing*-атака [3-11].

Важливою науковою проблемою є захист від навмисних завад. Захист від навмисних завад поділяється на два напрямки [21,31,32]:

– анті-*jamming* – захист від силового придушення (порушення доступності та цілісності інформації ГНСС) ;

– анті-*spoofing* – захист від інтелектуального придушення (порушення цілісності інформації ГНСС).

Ці два напрямки являють собою незалежні наукові проблеми, які вимагають різних напрямків наукових досліджень.

В роботі пропонуються способи захисту від анті-*jamming*, тобто забезпечення доступності та цілісності інформації ГНСС апаратури споживачів.

Напрямки по компенсації перешкод даються в документах ІСАО [26,27] і діляться на організаційні заходи та технічні заходи.

В даний час світова навігаційна спільнота вже чітко сформулювала напрями анті-*jamming* [7,8,10,11,20,21,31-36] (рис. 4).

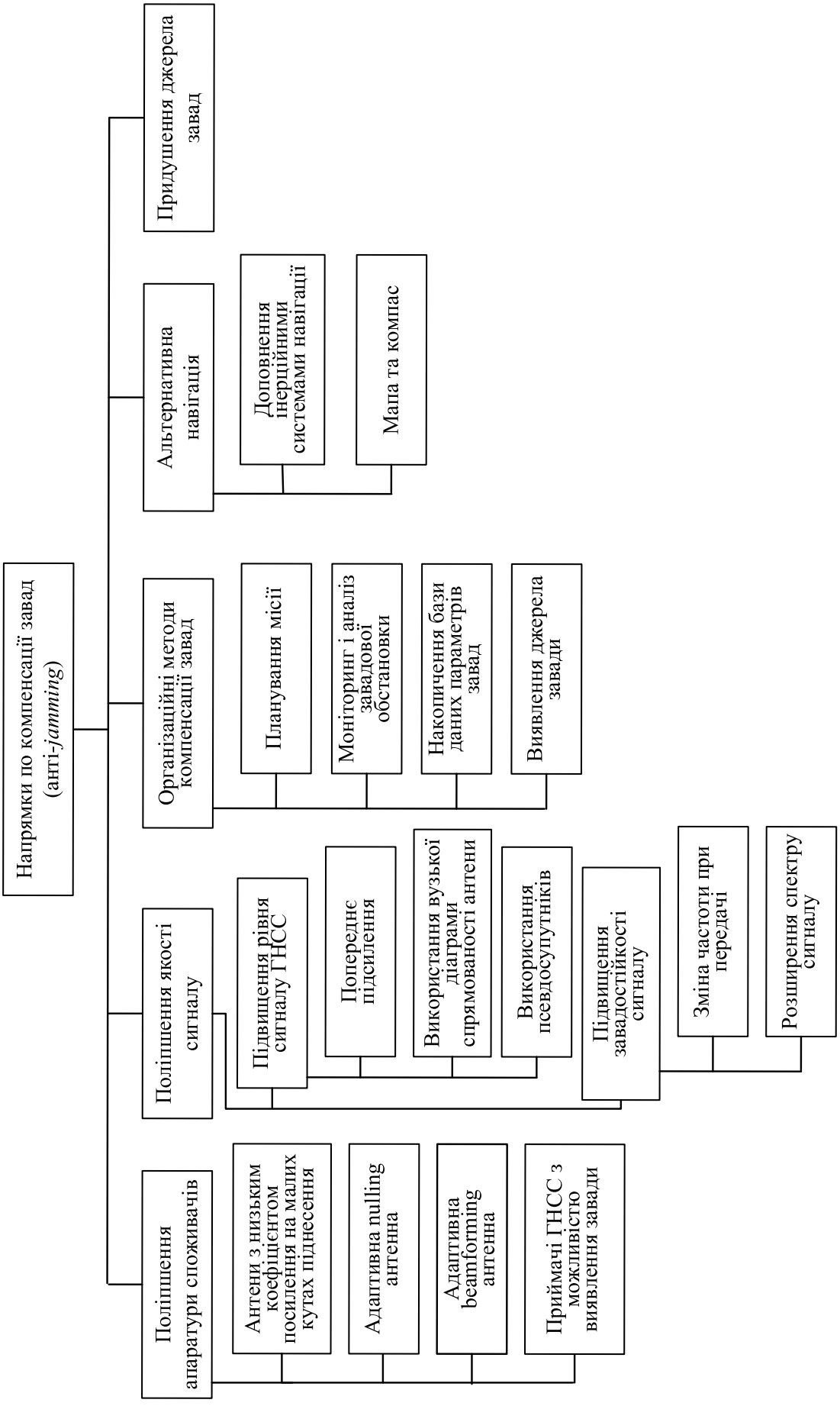

Рис. 4. Напрямки компенсації завад ГНСС

Відповідно до рис. 4 в [48] наведено можливий виграш в завадостійкості заходів (табл. 1).

Таблиця 1

Заходи поліпшення апаратури споживача ГНСС до завад

№ п/п	Заходи завадостійкості	Можливий виграш по відношенню до стандартних приймачів ГНСС, дБ	Можливий приріст вартості по відношенню до стандартних приймачів ГНСС, %	Примітки
1	Поліпшення діаграми спрямованості антени (ДСА) приймальних антен на малих кутах піднесення	10 − 15	30	Реально, у всіх системах споживачів
2	Управління ДСА, зменшує чутливість в напрямку джерела перешкод (*beamforming*- антенна)	20 − 25	До 100	Практично ефективний по одному постановнику завади, потрібно знання направлення на постановник завад
3	Управління ДСА, зменшує чутливість в напрямку джерела перешкод (*nullingng*-антенна)	до 80	До 100	Практично ефективний по де кільком постановників завади, не потрібно знання направлення на постановник завад
4	Антенна решітка з поляризацією сигналу	10 − 15	До 50	Діє не в усіх умовах застосування
5	Поліпшення обробки сигналів у приймачі	до 20	5 − 10	Потрібні дослідження з можливими методами реалізації. Не можливо реалізувати в діючих приймачах ГНСС
6	Комбінування приймача ГНСС з ІНС	10 − 15	10 − 300	Вартість визначається рівнем ІНС і має тенденції до зниження
7	Використання двочастотних приймачів L1, L2	5	20 − 30	
8	Використання багато частотних приймачів	8	40 − 50	

Інформація в табл. 1 розкриває напрям по анти-*jamming* при поліпшенні апаратури споживачів достоїнства і недоліки перераховані в примітках.

Поліпшення якості сигналу (рис. 4):

– *підвищення* рівня сигналу ГНСС, як недолік цього напряму потреба в додатковому зовнішньому обладнанні яке буде неефективно при значному великому енергетичному рівні завади;

– *підвищення* завадостійкості сигналу, ці заходи проводяться на передавальній стороні і як недолік це довга і дорога модернізація космічного сегменту ГНСС або введення нової системи ГНСС (наприклад ГНСС GALIEO).

Організаційні методи компенсації завад (рис. 4). Проведення організаційних заходів по забезпеченню цілісності та доступності інформації ГНСС це вимоги ICAO та IMO, які необхідно виконувати. Для цього необхідно створювати комплекси моніторингу радіонавігаційного поля ГНСС і аналізу завадової обстановки (система радіоконтролю) в зоні роботи апаратури споживача інформації ГНСС, моніторинг радіонавігаційного поля ГНСС необхідно одночасно виконувати в де кількох місцях від приймача ГНСС (рекомендована зона радіусом 5 – 10 км). В [37] надані рекомендації по складу системи радіоконтролю. Системи радіоконтролю повинні бути, по можливості, автоматизовані [38] із застосуванням ЕОМ, сучасної архітектури клієнт/сервер і засобів телекомунікації. Система радіоконтролю має антени, приймач (і), пристрій обробки/управління і технічну базу даних з результатами вимірів, що включає вимірювальний сервер. Вимірювальний сервер – це зазвичай компактний пристрій з шиною високої швидкості, що містить процесори (міні ЕОМ), приймачі та інші електронні пристрої. Для забезпечення необхідної чутливості вимірювань необхідно використовувати належний попередній підсилювач і забезпечити дозвіл по ширині смуги в 10 кГц або менше. Бажано проводити аналіз діапазонів частот GPS (1575 ± 20 МГц) і ГЛОНАСС (1598 ÷ 1604,25 ± 20 МГц). Рекомендується використовувати приймач з цифровою обробкою сигналів (DSP), а не аналізатор спектру, оскільки тільки DSP-приймачі забезпечують задовільну частоту розгортки [39,40].

В даний час використовуються дорогі за ціною (де кілька десятків тисяч доларів) стаціонарні комплекси радіоконтролю в районі аеропорту або морського порту (не всі адміністрації портів приймуть рішення про створення таких комплексів радіоконтролю) і це є недоліком. Можна проводити радіо-

контроль в точці розташування апаратури споживача ГНСС з математичним перерахунком в де яку точку простору, але недолік такого методу те що не має сертифікованих методик математичного перерахунку значення напруженості електричного поля в довільну точку простору яка б враховувала всі умови. Для усунення недоліків необхідно створювати мобільні (недорогі тактичні) комплекси радіоконтролю які можна застосовувати в зоні роботи апаратури споживача інформації ГНСС [41-43], тому розробка тактичних комплексів радіоконтролю радіонавігаційного поля ГНСС є актуальною науковою задачею.

В Національному авіаційному університеті розроблено радіоприймач для вимірювання напруженості електричного поля та методику оцінки доступності радіонавігаційного поля [44-48]. В результаті застосування методики отримуються графіки (рис. 5, 6). Розраховується граничне значення потужності завади в залежності від відстані до постановника завади (рис. 5). На підставі вимірюваної потужністю електричного поля отримується оцінка потужності завади. Як що оцінка потужності знаходиться нижче граничного значення то робиться висновок що приймач ГНСС знаходиться в області припустимих завад та радіонавігаційне поле ГНСС доступне для виконання навігаційної задачі.

На рис. 6 розраховано і побудовано графік залежності щільності потужності електричного поля від відстані прі постійній потужності джерела завади та цілісності даних ГНСС GPS [47,48], побудовано лінію розрахованої граничної щільності потоку потужності електричного поля завади на антені приймача ГНСС яка дорівнює $1{,}5148\times10^{-8}$ мВт/см^2 та лінію виміряної щільності потоку потужності електричного поля яка дорівнює $3{,}5\times10^{-11}$ мВт/см^2. У точках перетину ліній з кривими щільності потоку потужності опустимо перпендикуляри на вісь відстані (рис. 6). Область праворуч від перпендикуляра на вісь відстані і нижче кривої потужності завади – область в якій приймач ГНСС буде виконувати навігаційну задачу з ймовірністю не гірше заданої. Також з графіка можна визначити можливу відстань до джерела завади

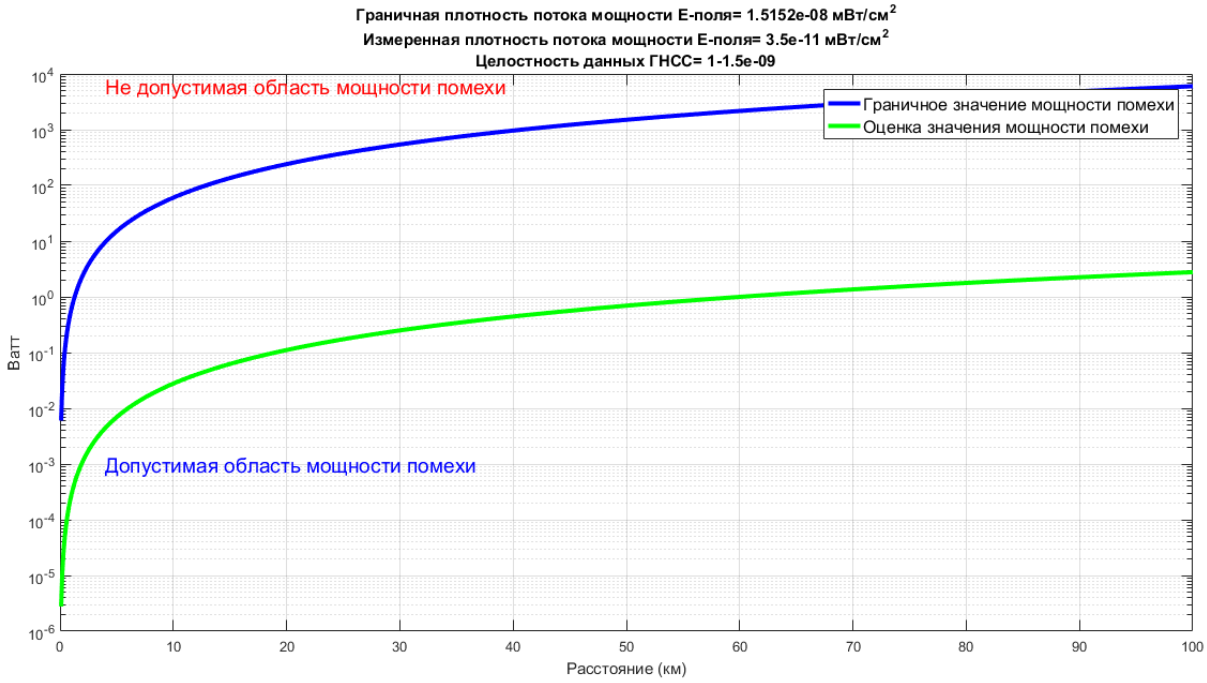

Рис. 5. Межа області потужності припустимих і не припустимих завад для необхідного відношення J/S (лінія синього кольору)

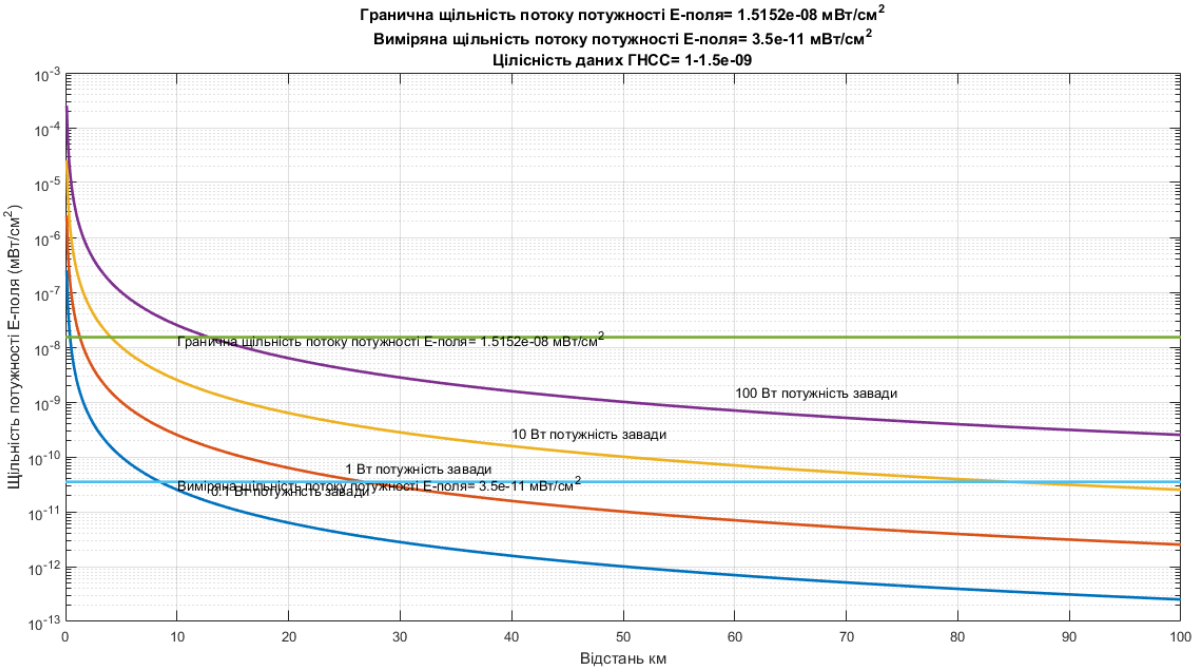

Рис. 6. Залежність щільності потужності електричного поля від відстані прі постійній потужності джерела завади та цілісності даних ГНСС GPS

Оцінюючи можливий виграш у стійкості апаратури споживачів ГНСС (табл. 1 п/п 2 та 3) до завад, найбільш перспективним методом є управління ДС приймальної антени (зменшення чутливості або встановлення "0" ДС в напрямку джерела завад) [2,20,21,36,52-54], тобто просторова часова обробка сигналів (ПЧОС), яка реалізується в антенних адаптивних компенсаторах завад (ААКЗ). Перевага ПЧОС в наступному:

− виграш в завадостійкості може бути вельми істотним;

− не потрібне коригування самого приймача супутникової навігації.

Адаптивні компенсатори завад будуються на основі антенних решіток і адаптивних методах управління ДС.

Основні напрямки розробки ААКЗ це радіолокаційні системи та системи радіозв'язку, т. к. в основному вирішувалися завдання підвищення завадостійкого прийому по боковим пелюсткам [53,54,6-62].

За останні роки опубліковано велика кількість робіт, присвячених використанню адаптивних методів компенсації завад, що належать переважно до систем радіолокації та систем радіозв'язку (перелік публікацій у [52-54]). У них найбільшу увагу приділено питанням обробки (в першу чергу ПЧОС) радіолокаційної інформації на тлі корельованих завад, що передбачає не тільки накопичення корисних сигналів, але і компенсацію сигналів які заважають [52-54].

У відкритій пресі з'являються роботи, присвячені забезпеченню цілісності та доступності до інформації ГНСС [2,3,15-17,49-62]. За структурою сигналів ГНСС відрізняються від радіолокаційних систем і систем радіозв'язку [2,33,62]. Тому при використанні адаптивних методів компенсації завад у каналах ГНСС слід враховувати ряд важливих особливостей, які часто ускладнюють реалізацію ААКЗ. Так, на відміну від радіолокаційних і систем радіозв'язку у ГНСС заздалегідь не відома частотно-часова структура корисного сигналу, що виключає можливість застосування ряду широко використовуваних методів адаптивної компенсації завад із застосуванням опорного сигналу [52-54,60,61]. Безперервний характер часової структури сигналу ГНСС істотно ускладнює можливість виділення компенсуючої напруги перешкоди і виключення впливу корисного сигналу на ланцюгу адаптації. Це значною мірою обмежує можливості використання у ГНСС багатоканальних пристроїв просторово-часової обробки з адаптивною компенсацією корельованих завад.

В основному всі розробки ААКЗ ГНСС проводяться з використанням рішень, які застосовувалися в радіолокації і радіозв'язку так звані *beamformer*-антені [52-54,62]. У *beamformer*-антенах в результаті когерентного вагового підсумовування корисного сигналу формується основний канал з вузькою діаграмою, спрямованої максимумом на джерело корисного сигналу. Крім того, у (N+1)-канальної ААР формується N слабкоспрямованих (перекривають бічні пелюстки ДС основної антени) адаптивно керованих компенсаційних каналів. Напруга компенсаційних каналів з урахуванням вагових коефіцієнтів додається до напруги основного каналу. При цьому здійснюється когерентна компенсація перешкод, прийнятих по боковим пелюсткам основної антени. Це рівносильне формуванню результуючої ДС з провалами на джерела перешкод (рис. 7). Компенсаційний канал в *beamformer*-антени використовує *LMS* або *RLS* адаптивний алгоритм за критерієм найменших квадратів, що базуються на леми про звернення матриці та *QR* розкладів [54].

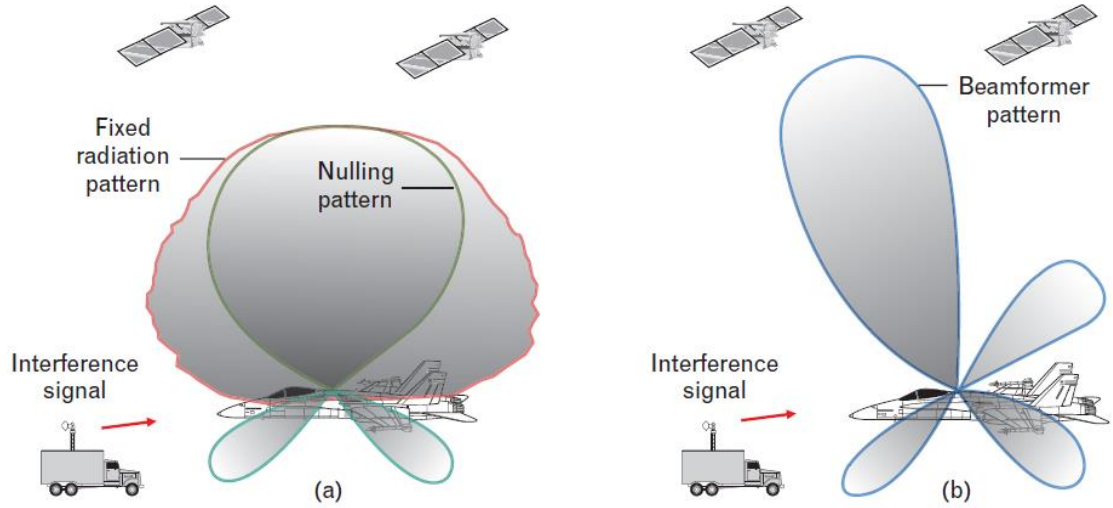

Рис. 7. Принцип роботи nulling-антени і beamformer-антени [46]. АР адаптивно формують ДС і утворюють нуль у напрямку джерел перешкод. (а) nulling-антена зменшує коефіцієнт посилення в напрямку сигналу перешкод, але без додаткового посилення сигналу супутникового зв'язку ГНСС. (б) beamformer-антена зменшує коефіцієнт посилення сигналу перешкод і збільшує коефіцієнт посилення сигналу супутникового зв'язку ГНСС.

До недоліків *beamformer*-антени можна віднести повільну збіжність *LMS* або *RLS* адаптивних алгоритмів [52,53], повільний перехідний процес, значне звуження основного пелюстка ДС і можлива втрата сигналу від де яких супутників, а також необхідність апріорних даних про направлення на заваду і прийнятому сигналі [52-54,60-62], тому *beamformer*-антени працюють в два етапи:

− оцінка напрямку (кута) на джерело завади, з використанням алгоритмів високого дозволу *MUSIC* або *ESPRIT*;

− за вимірюваним кутом обчислення вагових коефіцієнтів і формування ДС.

На жаль, максимальний коефіцієнт придушення завади у таких системах не перевищує 25 − 30 дБ (табл. 1). Однак розробка *beamformer*-антен ведеться в наш час з-за їх основної переваги – простота реалізації, можливість використання АР з великою апертурою, кроком між поодинокими елементами АР від λ/2 до 3λ/4 (збільшується коефіцієнт підсилення АР і підвищується роздільна здатність по куту) і лінійними розмірами одиничного елемента АР від λ/2 та невисокою обчислювальною складністю.

У теж час *beamformer*-антени не використовують можливості розв'язання рівняння Вінера-Хопфа (1) [53], та переваги адаптивної обробки сигналів, яке передбачає, що вся інформація про джерела завад, а саме його кутове положення в просторі знаходиться в кореляційній матриці завади:

$$\mathbf{W} = \mathbf{R}^{-1}\mathbf{S}, \qquad (1)$$

де **W** – вектор вагових коефіцієнтів (розмірністю N), $\mathbf{R}^{-1}$ – обернена кореляційна матриця завади (розмірністю $N \times N$), **S** – вектор комплексних амплітуд корисного сигналу (розмірністю N).

Для обчислення вагового вектору за виразом (1) необхідно провести операцію безпосереднього звернення кореляційної матриці. Однак на практиці кореляційна матриця невідома. Тому обчислюють максимально правдоподібну оцінку кореляційної матриці L часовими вибірками випадкових амплітуд вхідного процесу. Якщо ваговий вектор оцінюється за формулою (1), виникають дві проблеми. По-перше при $L<N$ (коротка вибірка) кореляційна матриця є виродженою і, отже, не має зворотної матриці, а при $L \geq N$ є погано обумовленої [60,61], де N – кількість елементів в АР, L – об'єм вибірки.

На основі рівняння (1) працює *nulling*-антенна, в якої формується нуль в ДС на джерело завади (рис. 7).

Використовуючи вираз 1 надається можливість в отриманні простий реалізації обчислення вагового вектору, необхідно тільки обчислити оцінку оберненої кореляційної матриці завади $\mathbf{R}^{-1}$ тобто використовувати прямий метод обчислення оберненої кореляційної матриці завади $\mathbf{R}^{-1}$ і знаходження оцінки вагового вектору **W** [60].

Прямі методи обчислення оберненої кореляційної матриці завади $\mathbf{R}^{-1}$ дають ряд важливих переваг:

- малий час для отримання оцінки вагового вектору;
- високий коефіцієнт придушення завади;
- відпадає необхідність у апріорних даних про параметри завади і сигналу, що на практиці є важливим.

В табл. 2 наведено порівняння за основними параметрами *beamformer* і *nulling* антен.

Таблиця 2

Порівняння за основними параметрами *beamformer* і *nulling* антен в ААКЗ

Параметри ААКЗ	*beamformer*-антена	*nulling*-антена
коефіцієнт придушення завади	до 35 дБ	до 90 дБ
апріорні данні про просторове розташування джерела корисного сигналу	+	–
апріорні данні про просторове розташування джерела завади	+	–
апріорна інформація про корисний сигнал	+	–
аналогова реалізація	+	–
цифрова реалізація	+	+
крок АР	від λ/4 до λ	від λ/4 до λ/2
тип АР:		
лінійна	+	+
пласка	+	+
перехідний процес	+	–
рівень бічних пелюсток	-40 ÷ -20 дБ	-100 ÷ - 80 дБ
звуження основного пелюстка	+	–
підвищення коефіцієнта підсилення в напряму корисного сигналу	+	–

Проведений аналіз дав підстави виділити найбільш дієві методи забезпечення цілісності і доступності інформації ГНСС при дії організованих завад серед котрих є застосування ААКЗ з використанням *beamformer* і *nulling* антен (рис. 4, табл. 1).

Серед *beamformer* і *nulling* антен найкращим є ААКЗ з *nulling*-антеною (табл. 2). Тому актуальним на даний час є дослідження розробка і впровадження ААКЗ на базі *nulling*-антен.

В результаті науково-дослідних робот в Національному авіаційному університеті розроблені методи керування ДС в ААКЗ на базі *nulling*-антен. Результати застосування цих методів наведені в роботах [63-74], а також створено ААКЗ [2].

Висновки. В роботі проведено огляд публікацій в яких розглядається проблема уразливості ГНСС до навмисним перешкод, розглядаються послідства впливу перешкод на ГНСС. Представлені інформаційні потоки в ГНСС для знаходження вразливих функціональних вузлів. На основі інформаційних потоків показано, що найбільш уразливим пристроєм в плані захисту інформації є приймач ГНСС. На основі розробок університету пропонуються як організаційні так і технічні заходи щодо забезпечення доступності радіонавігаційного поля, так і забезпечення цілісності інформації ГНСС. Запропоновані рішення можна використовувати на об'єктах критичної інфраструктури, а також користувачам навігаційної інформації.

Література

1. Суходоля, О. (2016). Зелена книга з питань захисту критичної інфраструктури в Україні. Упоряд. Д. Бірюков & С. Кондратов. за заг. ред. О. Суходолі К.:НІСД. Режим доступу: http://www.niss.gov.ua/public/File/2016_book/ Syxodolya_ost.pdf.

2. Конин, В. & Харченко, В. (2010). Системы спутниковой радионавигации. Киев: ХОЛТЕХ.

3. Ward, P. (1994). GPS Receiver RF Interference Monitoring, Mitigation, and Analysis Techniques, Navigation, 41(4), pp. 367–392. doi: 10.1002/j.2161-4296.1994.tb01886.x.

4. Parkinson, B. W. and Spilker, J. J. (1996). Progress In Astronautics and Aeronautics: Global Positioning System: Theory and Applications. American Institute of Aeronautics & Astronautics. Available at: http://books.google.com.ua/books?id=t0eGFpSwN0wC (Accessed: 3 February 2014).

5. Landry, R. and Renard, A. (1997). Analysis of potential interference sources and assessment of present solutions for GPS/GNSS receivers, 4th Saint-Petersburg on INS, pp. 1–13. Available at: http://scholar.google.com/scholar?hl =en&btnG=Search&q=intitle:ANALYSIS+OF+POTENTIAL+INTERFERENCE+SOURCES+AND+ASSESSMENT+OF+PRESENT+SOLUTIONS+FOR+GPS+/+GNSS+RECEIVERS #0 (Accessed 3 February 2014).

6. Littlepage, R. (1998). The Impact of Interference on Civil GPS. Proceedings ION GPS-98. pp. 821-828.

7. Corrigan, T. M. et al. (1999). GPS Risk Assessment Study. Final report. Washington. Available at: http://www.rvs.uni-bielefeld.de/publications/ Incidents/DOCS/Research/Other/Article/gps-risk-ass.pdf (Accessed 3 February 2014).

8. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System (2001). Final Report. Washington. Available at: https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf (Accessed 3 February 2014).

9. M. Powe, J. I. R. O. (1999). European Organisation for the Safety of Eurocontrol Experimental Centre GNSS Frequency Protection Requirements. Available at: https://www.eurocontrol.int/gnss-frequency-protection-requirements (Accessed 3 February 2014).

10. Corbell, P. M. (2000). Design and validation of an accurate gps signal and receiver truth model for comparing advanced receiver processing techniques, AIR FORCE INSTITUTE OF TECHNOLOGY. Available at:

http://www.dtic.mil/dtic/tr/fulltext/u2/a380760.pdf (Accessed 3 February 2014).

11. RTCA Inc. (2008). Assessment of Radio Frequency Interference Relevant to the GNSS L1 Frequency Band. Washington. Available at: http://books.google.com.ua/books/about/Assessment_of_Radio_Frequency_InterfeInt.html?id=w6NWewAACAAJ&redir_esc=y (Accessed 5 February 2014).

12. Wildemeersch, M. and Fortuny-Guasch, J. (2010). Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems. Ispra (VA), Italy. doi: 10.2788/6033.

13. Wildemeersch, M. et al. (2010). Impact Study of Unintentional Interference on GNSS Receivers, Tech. Rep. EUR-24742-EN, Publications Office of the European Union. Luxembourg. doi: 10.2788/57794.

14. Bauernfeind, R. et al. (2012) Analysis, detection and mitigation of incar gnss jammer interference in intelligent transport systems, Deutscher Luft- und Raumfahrtkongress, pp. 1–10. Available at: http://www.dglr.de/publikationen/ 2013/281260.pdf (Accessed: 17 July 2014).

15. Rügamer, A., Iis, F. and Kowalewski, D. (2015). Jamming and Spoofing of GNSS Signals-An Underestimated Risk?! Motivation Applications of GNSS Motivation Applications of GNSS Content Jamming and Spoofing of GNSS Signals-An Underestimated Risk?! Available at: https://www.fig.net/resources/proceedings/ fig_proceedings/fig2015/ppt/TS05G/TS05G_ruegamer_kowalewski_7486_ppt.pdf (Accessed: 19 July 2014).

16. Rügamer, A. and Kowalewski, D. (2015). Jamming and Spoofing of GNSS Signals-An Underestimated Risk?!, in From the Wisdom of the Ages to the Challenges of the Modern World. Sofia, Bulgaria,: International Federation of Surveyors, pp. 1–24. Available at: https://www.fig.net/resources/proceedings/fig_proceedings/ fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf (Accessed: 19 July 2014).

17. Curran, J. et al. (2017). A look at Threat of Systematic Jamming of GNSS, InsideGNSS, 5, pp. 46–53. Available at: http://insidegnss.com/auto/sepoct17-CURRAN.pdf (Accessed: 19 July 2014).

18. Boynton, F. (2014). GNSS INTERFERENCE / DENIALS, NEEDS AND CHALLENGES. Available at: https://gpsworld.com/wp-content/uploads/2014/05/Loctronix-2014-GNSS-Webinar-140521-final.pdf.

19. Landry, R. and Renard, A. (1997). Analysis of potential interference sources and assessment of present solutions for GPS/GNSS receivers, 4th Saint-Petersburg on INS, pp. 1–13. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:ANALYSIS+OF+POTENTIAL+INTERFERENCE+SOURCES+AND+ASSESSMENT+OF+PRESENT+SOLUTIONS+FOR+GPS+/+GNSS+RECEIVERS#0.

20. Dovis, F. (2015). GNSS Interference Threats and Countermeasures. Edited by F. Dovis. Boston|London: ARTECH HOUSE, INC.

21. Sklar, J. R. (2003). Interference Mitigation Approaches for the Global Positioning System, LINCOLN LABORATORY JOURNAL, 14(2), pp. 167–180. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.4732& rep=rep1&type=pdf (Accessed: 25 July 2018).

22. Сушич О. (2012). Експериментальна оцінка впливу навмисних завад на апаратуру споживача глобальної навігаційної супутникової системи, Вісник інженерної академії України, № 3-4, с. 32 – 36.

23. Швець В. (2012). Експериментальні дослідження завадостійкості систем GPS, Вісник інженерної академії України, № 3-4, с. 160 – 164.

24. Швець В. (2013). Аналіз загроз для транспортних систем, орієнтованих на використання глобальних навігаційних супутникових систем. Вісник інженерної академії України. № 3-4. с.82 – 86.

25. Global Navigation Satellite Systems Panel (GNSSP), Appendix A. Working papers of the Third meeting, (1999). Montreal: ICAO.

26. Циркуляр 267-AN/159 Рекомендации по внедрению и эксплуатационному использованию глобальной спутниковой навигационной системы (GNSS) (1996). М.: ИКАО.

27. International Civil Aviation Organization. (2014). Aeronautical Telecommunications Annex 10 to the Convention on International Civil Aviation, Volume I (Radio Navigation Aids), 6 ed.

28. IMO Resolution A915. Revised maritime policy and requirements for a future global navigation satellite system (GNSS) (2002). IMO. Available at: http://transport.mid.gov.kz/ru/kategorii/dokumenty-mezhdunarodnoy-morskoy-organizacii-imo?page=1&theme_version=mirm (Accessed: 19 July 2014).

29. Butterline, Ed, Frodge, Sally L., (1999). GPS: Synchronizing Our Telecommunications Networks, In: Proceedings of the 12th International Technical Meeting of the Satellite Division of The Institute of Navigation. Nashville, TN, September 1999, pp. 597-606.

30. RTCA, 2002. DO-242A Minimum aviation system performance standards for automatic dependent surveillance broadcast (ADS-B). Washington: RTCA, Inc.

31. SPIRENT (2015). Fundamentals of GPS Threats: White paper, EGNSSA, GNSS Market Report. Available at: https://www.spirent.com/Assets/WP/WP-Fundamentals-of-GPS-Threats.

32. Gao, G. X. et al. (2016) 'Protecting GNSS Receivers from Jamming and Interference', in Proceedings of the IEEE, pp. 1327–1338. doi: 10.1109/JPROC.2016.2525938.

33. Дятлов, А., Дятлов, П., & Кульбикаян, Б. (2004). Радиоэлектронная борьба со спутниковыми радионавигационными системами. М.: Радио и связь.

34. Psiaki, M. L. and Humphreys, T. E. (2016). GNSS Spoofing and Detection, Proceedings of the IEEE, 104(6), pp. 1258–1270. doi: 10.1109/JPROC.2016.2526658.

35. Huang, J. et al. (2016). GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky, ICT Express. Elsevier, 2(1), pp. 37–40. doi: 10.1016/J.ICTE.2016.02.006.

36. Коротоношко, А., Перунов, Ю., (2006). Устойчивость и радиотехническая защищенность транспортных систем, использующих точную спутниковую навигацию, Новости навигации, 3, с., 26 – 32.

37. Справочник по управлению использованием спектра на национальном уровне (2005). Женева: ITU. Available at: https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-21-2005-PDF-R.pdf.

38. МСЭ-R (2014) Автоматизация и интеграция систем радиоконтроля в автоматизированное управление использованием спектра. Женева. Available at: https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1537-1-201308-I!!PDF-R.pdf.

39. Manual on Testing of Radio Navigation Aids (2000). Montreal: ICAO. Available at: http://www.caa.lv/file/935/280.

40. Manual on Testing of Radio Navigation Aids (2007) Aviation. Montreal: ICAO. Available at: http://www.caa.lv/file/936/280.

41. Harris Corporation - Detect and Locate GPS Jamming with Signal Sentry™ 1000 - YouTube (no date). Available at: https://www.youtube.com/watch?v=XMpBxrNaV84 (Accessed: 27 August 2018).

42. GPS Jammer Detector and Locator | GNSS interference detection (no date). Available at: http://www.gps-world.biz/products/gnss-interference-detection/ products-solutions/ctl-3520#datasheets (Accessed: 27 August 2018).

43. Curry, C. (2011). Sentinel Project Report on GNSS Vulnerabilities. Lydbrook. Available at: http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf.

44. Швець В. (2015). Підходи щодо дослідження електромагнітної сумісності глобальних навігаційних супутникових систем в зоні аеропорту. Вісник інженерної академії України, №4. с. 61 – 64. http://er.nau.edu.ua:8080/handle/NAU/17700

45. Швець В. (2016). Способи оцінки енергетики електричного поля групи випромінювачів в зоні аеропорту які створюють завади глобальним навігаційним супутниковим системам. Вісник інженерної академії України, №1. с. 45 – 48. http://er.nau.edu.ua:8080/handle/NAU/20735

46. Швець В. (2016). Спрощена концепція математичного моделювання електромагнітної обстановки системам GPS, ГЛОНАСС, ГАЛИЛЕО. Вісник інженерної академії України, №2. с. 23 – 26. http://er.nau.edu.ua:8080/handle/NAU/22285

47. Shvets V. (2018). Method of evaluation of the electric field level of dangerous signals to GNSS receivers. Proceedings of the National Aviation University, №2 (75). pp. 7–12. http://er.nau.edu.ua:8080/handle/NAU/37401

48. Shvets V., Kondratiuk V., Ilnytska S., Kutsenko O. (2018). Radionavigation field monitoring in the landing area using software-defined radio receiver. Aviation in the XXI-st century 2018: World Congress. Kyiv: NAU. p 5.1.21 – 5.1.26. http://er.nau.edu.ua:8080/handle/NAU/36846

49. Borio, D. et al. (2016) 'Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers', Proceedings of the IEEE, 104(6), pp. 1233–1245. doi: 10.1109/JPROC.2016.2543266.

50. Thyagarajan, V. and Kaja Mohideen, S. (2014) 'GPS jamming: Strengthening anti jam GPS system with adaptive phase only nulling using cuckoo search', Research Journal of Applied Sciences, Engineering and Technology, 8(5), pp. 679–686. doi: 10.19026/rjaset.8.1022.

51. Senthilkumar, K. S. et al. (2016) 'Single Perceptron Model for Smart Beamforming in Array Antennas', International Journal of Electrical and Computer Engineering (IJECE), 6(5), pp. 2300–2309. doi: 10.11591/ijece.v6i5.10719.

52. Монзинго, Р., Миллер, Т. (1986). Адаптивные антенные решетки: Введение в теорию. Пер. с англ. В. Челпанова, В. Лоскаченко. М.: Радио и связь.

53. Уидроу, Б., Стринз, С. (1989). Адаптивная обработка сигналов. Пер. с англ. Ю. Скальникова. Под ред. В. Шахгильдяна. М.: Радио и связь.

54. Джиган, В. (2013). Адаптивная фильтрация сигналов: теория и алгоритмы. М.: Техносфера.

55. Williams, D. et al. (2000) 'Four-Element Adaptive Array Evaluation for United States Navy Airborne Applications', in ION GPS 2000, 19-22 September 2000. Salt Lyke City, pp. 2523–2532. Available at: https://pdfs.semanticscholar.org/aee5/aa45796a951171df421fed32d776b8dd1261.pdf.

56. Ward, K. D. (2006) Development of Smart Antenna Technology Final Report, Smart Antenna Technology. Kidlington. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0014/36014/smartpres1.pdf.

57. Prabhu, M. R. and Sasikala, U. T. (2014) 'Gps- 4 Arrays Smart Antenna for Anti-Jamming', International Journal of Engineering Science Invention, 3(4), pp. 29–41. Available at: http://www.ijesi.org/papers/Vol(3)4/Version-4/D0344029041.pdf.

58. Fernandez-Prades, C., Arribas, J. and Closas, P. (2016) 'Robust GNSS Receivers by Array Signal Processing: Theory and Implementation', Proceedings of the IEEE, 104(6), pp. 1207–1220. doi: 10.1109/JPROC.2016.2532963.

59. ВНИИР-Прогресс (2017). Малогабаритные адаптивные антенные решетки четырех элементные серии «Комета» — «ВНИИР-Прогресс», ВНИИР-Прогресс. Available at: http://www.vniir-progress.ru/production/malogabaritnye-adaptivnye-antennye-reshetki-chetyrexelementnye-serii-kometa/ (Accessed: 31 July 2018).

60. Ратынский, М., (2003). Адаптация и сверхразрешение в антенных решетках. М.: Радио и связь.

61. Лосев, Ю., Бердников, Э., Гойхман, Э., Сизов, Б. (1988). Адаптивная компенсация помех в каналах связи. М.: Радио и связь.

62. Перов, А. and Харисов, В. (2010) ГЛОНАСС. Принципы построения и функционирования. М.: Радио и связь.

63. Швець В. (2013). Формування вагових коефіцієнтів прямими методами в антенних решітках систем GPS. Вісник інженерної академії України №1. с. 92 – 94.

64. Швець В. (2013). Застосування трикутної схеми розташування випромінювачів в вимірювальних антенних решітках супутникових аеронавігаційних систем. Вимірювальна та обчислювальна техніка в технологічних процесах. №1. с. 255 – 261

65. Щвець В. А. (2013). Оптимізація антенних решіток глобальних навігаційних супутникових систем, XI Міжнародна науково-технічна конференції "ABIA-2013". К.:НАУ Том 2. с. 7.1–7.4. http://er.nau.edu.ua:8080/handle/NAU/11180

66. Швець В. (2013). Розрахунок антенної решітки супутникових аеронавігаційних систем. Радіотехніка. Вип. 173. Харків: ХНУРЕ. с. 38–41.

67. Швець В. (2013). Синтез пласкої антенної решітки супутникових еронавігаційних систем GPS, ГАЛІЛЕО, ГЛОНАСС. Вісник інженерної академії України. № 3-4. с.87 – 89.

68. Швець В. (2014). Структурна схема завадостійкої антенної решітки навігаційних систем GPS, ГАЛІЛЕО, ГЛОНАСС . Вісник інженерної академії України. № 1. с.149 – 151. http://er.nau.edu.ua:8080/handle/NAU/32873

69. Швец В. (2014). Необходимость защиты информации глобальных навигационных спутниковых систем GPS, ГЛОНАСС. Безпека інформації. №2, Том 20. с. 185 – 192. http://er.nau.edu.ua:8080/handle/NAU/35355

70. Щвец В. (2015). Моделирование радиоприемного тракта адаптивных антенных решеток в системах позиционирования GPS, ГЛОНАСС, ГАЛИЛЕО, XII Міжнародна науково-технічна конференції "ABIA-2015". К.:НАУ, с. 8.50 – 8.53. http://er.nau.edu.ua:8080/handle/NAU/32881

71. Щвец В. (2017). Импульсная характеристика пространственного фильтра как аналог корреляционной матрицы помехи в адаптивной антенной решетке навигационных систем GPS, ГЛОНАСС, GALILEO. XIII Міжнародна науково-технічна конференція "ABIA-2017". К.:НАУ. с. 12.53 – 12.55. http://er.nau.edu.ua:8080/handle/NAU/29804

72. Shvets V., Kharchenko V. (2017). Pulse characteristics of network satellite systems adaptive antenna for assessing correlation interference matrix Proceedings of the National Aviation University, №4 (73). pp. 30 – 35. http://er.nau.edu.ua:8080/handle/NAU/32567

73. Shvets V., Kharchenko V. (2017). Pulse characteristics of network satellite systems adaptive antenna for assessing correlation interference matrix Proceedings of the National Aviation University, №4 (73), pp. 30 – 35. http://er.nau.edu.ua:8080/handle/NAU/32567

74. Shvets V. Kharchenko V. (2018). Antenna array as a constructive element of increasing cybersecurity of network satellite system receivers. Proceedings of the National Aviation University, №1 (74), pp. 30 – 37. http://er.nau.edu.ua:8080/handle/NAU/34029