*TRANSPORT*

# НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ І ЦІЛІСНОСТІ ІНФОРМАЦІЇ ГЛОБАЛЬНИХ НАВІГАЦІЙНИХ СУПУТНИКОВИХ СИСТЕМ

***Швець В. А.,*** *к.т.н., доцент кафедри засобів захисту інформації*
***Мелешко Т. В.,*** *старший викладач кафедри засобів захисту інформації*
*Україна, м. Київ, Національний авіаційний університет*

***Abstract.*** *Based on the analysis of reports and literature on the vulnerability of global navigation satellite systems, the robot presents a developed threat model and an intruder model for navigation information. Using the developed models, organizational and technical measures to protect information are determined. Directions for improving consumer equipment to jamming are given. Organizational measures for protecting against jamming are described.*
***Keywords:*** *radio navigation field, global navigation satellite systems, critical infrastructure facilities, information security, jamming, violator model, nulling-antenna.*

**Вступ.** 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 (рис. 1), систем управління військами і високоточною зброєю, які відносяться до об'єктів критичної інфраструктури [1].

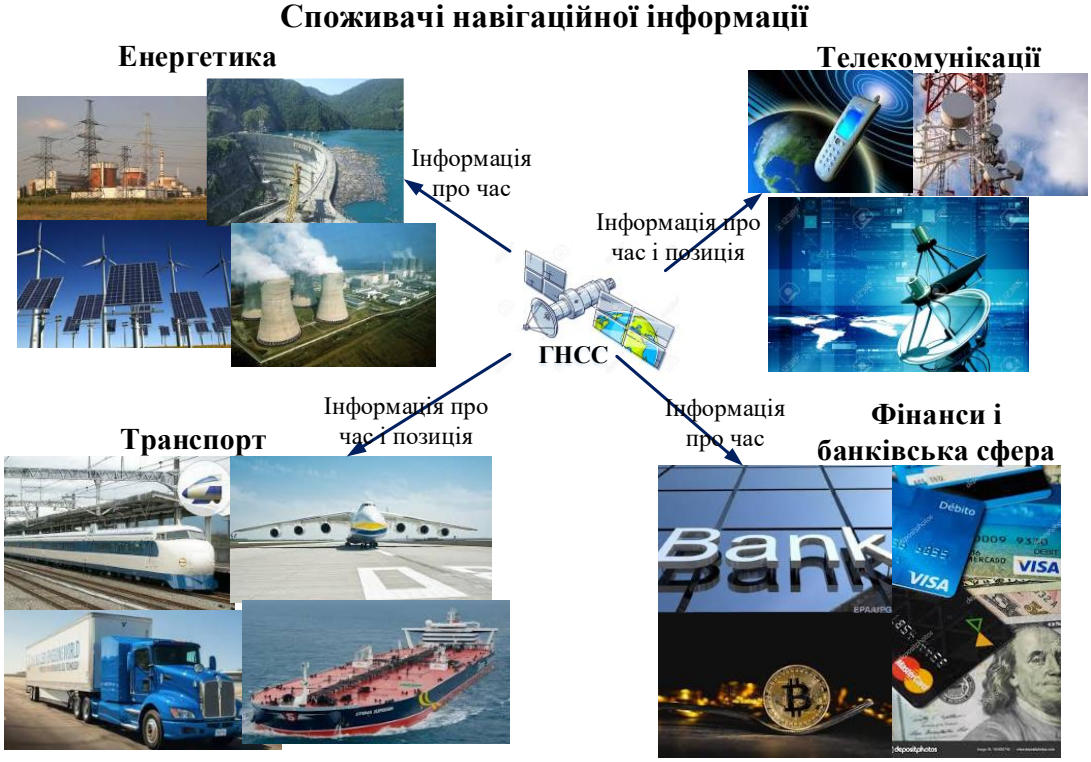


*Рис. 1. Об'єкти критичної інфраструктури, споживачі навігаційної інформації*

Зосередимося на об'єктах критичної інфраструктури цивільного сектора, які отримують від глобальних навігаційних супутникових систем (ГНСС) наступну інформацію:

- **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.

Основу КЧЗ складають ГНСС, які представлені в даний час СРНС ГЛОНАСС (Росія) і GPS (США). Європейське співтовариство створює для цих цілей свою СРНС GALILEO. Використання глобального координатно-часового поля, створюваного ГНСС, дозволяє визначити положення будь-якого користувача в просторі з точністю до одиниць метрів і час з точністю до десятків і одиниць наносекунд в будь-якій точці Земної кулі і навколоземного простору в будь-який момент часу і в будь-яку погоду (*далі будуть розглядатися тільки ГНСС GPS і ГЛОНАСС, тому що вони офіційно введені в експлуатацію і мають нормативні міжнародні рекомендації до використання в навігації*).

Після ейфорії перших років освоєння супутникових навігаційно-часових технологій, в даний час більш ретельно аналізується використання ГНСС в якості єдиного джерела КЧІ, починає поступатися місцем більш тверезого підходу до перспектив використання ГНСС. Насамперед, це обумовлено вразливістю ГНСС при впливі ненавмисних і навмисних завад. Про вразливості цивільних приймачів ГНСС було відомо давно [2 - 5], але її рідко беруть до уваги виробники приймачів та їх користувачі. Тільки тоді, коли Міністерство оборони США активізувало свою діяльність, пов'язану із застосуванням GPS у воєнних умовах (NAVWAR), стало очевидним, що навмисні завади для цивільних приймачів слід враховувати як важливий фактор.

Було проведено кілька аналізів вразливості транспортних систем, заснованих на використанні сигналів GPS [6]. Одним з найбільш важливих і своєчасних звітів про дослідження в цій області був звіт Центру Волпе [5] 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 завад [7].

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 [8 – 11].

**Обговорення.** В даний час радіонавігаційна спільнота активно обговорює проблему вразливості ГНСС і пошуку засобів і методів забезпечення доступності і цілісності радіонавігаційного поля ГНСС.

Засоби і методи забезпечення доступності і цілісності радіонавігаційного поля ГНСС можуть бути розроблені як що буде представлена модель загроз та модель порушника інформації ГНСС.

На підставі міжнародних звітів стосовно вразливості ГНСС та власних досліджень проведених в Національному авіаційному університеті була сформована модель загроз інформації ГНСС (табл. 1).

Таблиця 1. Модель загроз інформації ГНСС

| Джерело загрози | Тип загрози | Опис загрози | Можливість існування | Вплив на користувача |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| Сонячні бурі | Природні | Електромагнітні завади від сонячних спалахів та іншої сонячної активності «заглушають» супутникові сигнали в космосі. | Поширений у широких географічних районах у періоди інтенсивної сонячної активності | Втрата сигналу або помилки діапазону, що впливають на точність інформації про місцезнаходження та час. |
| Сцинтиляція | Природні | Супутниковий сигнал заломлюється або дифракція в просторі неправильною іоносферною активністю. | Ефекти сцинтиляції найбільш яскраво виражені в тропічних широтах і на великих широтах. | Вплив на приймач може включати неточну інформацію про місцезнаходження. |

Продовження таблиці 1.

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Затьмарення | Природні | Має недостатня кількість супутників, щоб можна було забезпечити точне положення - завдяки конструкціям, що затьмарюють антенний погляд на небо. | Зустрічається в основному в приміщенні, під землею, на забудованих територіях, в лісистих місцевостях, гірських ярах або глибоких рубок. | Втрата сигналу або помилки діапазону, що впливають на точність інформації про місцезнаходження та час. |
| Перевипромінювання | Природні | Сигнали від одного або декількох супутників відбиваються від сусідніх структур, фрагментуючи їх шлях до приймача. | Зазвичай зустрічається в "міських районах", де вулиці оточені високими скляними будівлями. | Помилки, що впливають на точність інформації про місцезнаходження. |
| Погана установка | штучний | Антена пристрою встановлюється в такому положенні, де він не може отримати чіткий вигляд неба або чисті сигнали із супутників, або неправильно узгоджена антена до приймача, що може призвести до витоку радіочастот, що виглядає як джерело завад. | Це може бути пов’язано з поганим дизайном продукту, або з нерухомими антенами, які закриваються новими високими будівлями, які будуються неподалік. | Неоптимальна супутникова геометрія може призвести до того, що приймач не може вирішити своє положення, неточності, що впливають на інформацію про місцезнаходження та час. Вплив поганої установки може призвести до повної втрати сигналу. |
| Jamming | штучний | Локально сформовані РЧ-завади використовуються для «заглушення» супутникових сигналів. | глушіння радіопередачі щоб запобігти відстеженню руху. Незаконне використання пристроїв значно збільшується. | Втрата сигналу (якщо глушитель блокує всі супутникові сигнали) або помилки діапазону, що впливають на точність інформації про місцеположення або синхронізацію (якщо приймач знаходиться на межі діапазону передавача завади). |
| Spoofing | штучний | Підроблені супутникові сигнали передаються на пристрій, щоб змусити його повірити, що це десь або в інший момент часу. | Spoofing колись було зробити надзвичайно важко, але останні демонстрації показали, що зараз легко створити генератор ГНСС з SDR передавача та недорогих компонентів | Неправильне зчитування місця та часу, що може мати сильний вплив на автоматизовані та автономні пристрої та пристрої, які залежать від точного GPS-часу. |
| Hacking | штучний | Маніпуляція програмним рівнем пристрою для зміни його інтерпретації даних супутникового сигналу. | Сьогодні широко використовується в персональних пристроях, таких як мобільні телефони і планшети. Операційна система перервана в джейлбрейк і користувач встановлює додаток, який дозволяє замінити інформацію GPS-приймача ручною редагованою інформацією в окремий додаток. Є дані, що це також є поширеним при маніпулюванні даними AIS у морському сегменті. | Неправильне зчитування місця та часу, що може мати сильний вплив на автоматизовані та автономні пристрої та пристрої, які залежать від точного GPS-часу. |

Продовження таблиці 1.

| | | | | |
|---|---|---|---|---|
| ВЧ-інтерференція | штучний | Шум від радіочастотних передавачів, що знаходяться поблизу (всередині або зовні пристрою) затьмарює супутникові сигнали. | Переважно в районах з підвищеним радіочастотним шумом (наприклад, біля стільникових веж) або в місці розташування, де приймач ГНСС не захищений належним чином від інших компонентів. | Втрата сигналу (якщо передавач блокує всі супутникові сигнали) або помилки діапазону, що впливають на точність зчитування місця (якщо приймач знаходиться на межі діапазону передавача). |
| Помилка користувача | штучний | Користувачі надмірно покладаються на дані ГНСС, які йому представлені, ігноруючи докази інших систем або те, що вони можуть бачити. | Поширений у будь-якому сценарії, коли користувач стає надто залежним від інформації своєї навігаційної системи. | Це може призвести до помилкового прийняття рішень у різних сценаріях (наприклад, вантажні автомобілі, що рухаються по занадто вузьких смугах, кораблі керують занадто близько до небезпечних об'єктів). |

**Модель порушника.** В якості порушника інформації ГНСС може виступати держава агресор або держава яка проводить таємні операції на території іншої країни, організація з терористичним напрямом діяльності, фізична особа яка незадоволена своїм суспільним становищем або схильним до психічних розладів [4,5,12 - 17].

Враховуючи модель порушника (табл. 1) проблемою забезпечення доступності та цілісності інформації ГНСС є захист від навмисних завад. Захист від навмисних завад поділяється на два напрямки [15 -17]:

– 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.

Напрямки по захисту від навмисних завад даються в документах ICAO [19,20] і діляться на організаційні заходи та технічні заходи. Як що в цих двох документах організаційні заходи що до анті-*jamming* прописані дуже чітко, то стосовно технічних заходів в документах наведено наступне [20]: "Применение адаптивных методов компенсации в приемниках дает возможность улучшить подавление помех в рабочем диапазоне приемника, данные методы должны исследоваться и разрабатываться в том случае, если они повышают безопасность и являются эффективными, надежными и приемлемыми в отношении стоимости". Тому в різних країнах дуже активно провадяться наукові дослідження в напряму анті-*jamming* апаратури споживачів.

В даний час світова навігаційна спільнота вже чітко сформулювала напрями анті-*jamming* [5,15,17 - 22] (рис. 2).

До технічних заходів забезпечення доступності та цілісності інформації ГНСС можна віднести: поліпшення апаратури споживачів, поліпшення якості сигналу.

Відповідно до рис. 2 в [23] наведено можливий виграш в завадостійкості, скорочення дальності придушення і ймовірності пропонованих заходів в плані поліпшення апаратури споживачів (табл. 3 та 4).

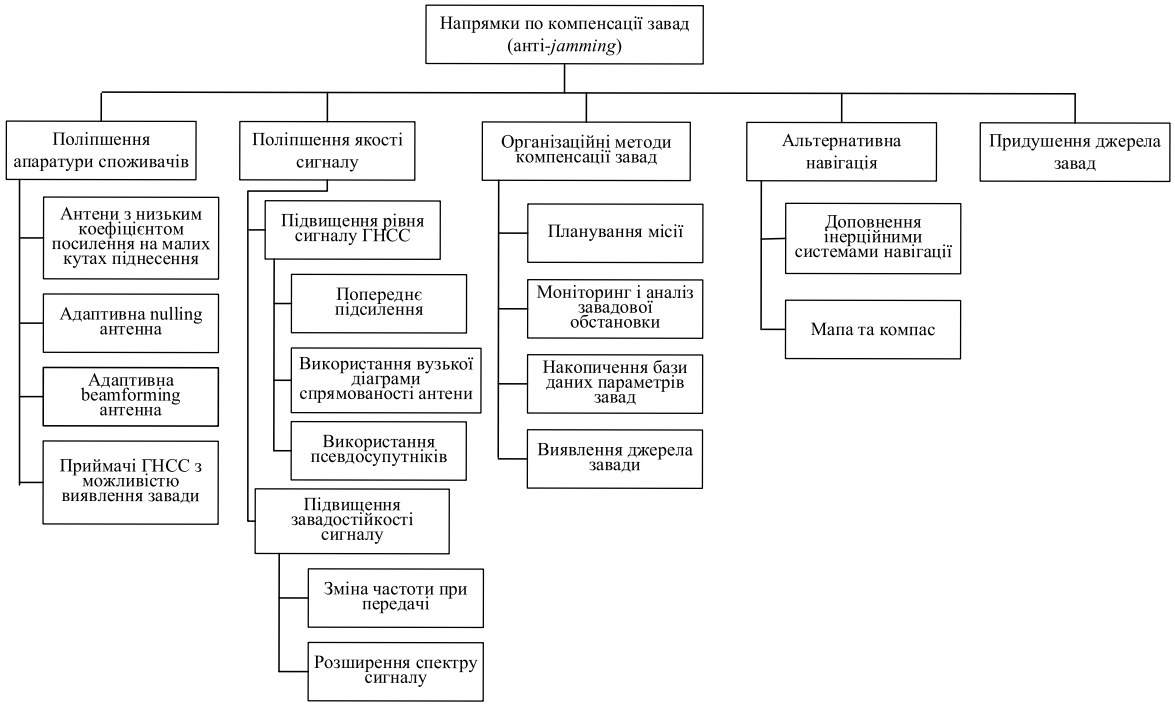


*Рис. 2 Напрямки компенсації завад ГНСС*

Таблиця 3. Заходи поліпшення апаратури споживача до завад

| № п/п | Заходи завадостійкості | Можливий виграш по відношенню до стандартних приймачів ГНСС, дБ | Можливий приріст вартості по відношенню до стандарт-них приймачів ГНСС, % | Примітки |
|---|---|---|---|---|
| 1 | Поліпшення ДСА приймальних антен на малих кутах піднесення | 10 − 15 | 30 | Реально, у всіх системах споживачів |
| 2 | Управління ДСА, зменшує чутливість в напрямку джерела завад (*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 завад (*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 | |

Таблиця 4. Оцінка ефективності заходів захисту при використанні ГНСС в локальній зоні при терористичному придушенні, що використовує 50 Вт ("базовий") передавач

| № п/п | Приймач | Приріст завадостійкості по відношенню до базового варіанту, дБ | Дальність придушення від "базового" передавача, км (антена передавача на висоті 1 м) |
|---|---|---|---|
| 1 | Стандартний приймач GPS L1 або ГЛОНАСС L1 | – | 57,0 |
| 2 | Приймач GPS L1 або ГЛОНАСС L1 з поліпшеною ДСА на малих кутах місця | 15 | 17,5 |
| 3 | Приймач з п. 2, комплексований з ІНС | 10 | 10,0 |
| 4 | Приймач з п. 3, введеної частотою L2 (двох частотний) | 5 | 6,0 |
| 5 | Приймач з п. 3, з введеними частотами L2, L3 (трьох частотний) | 8 | 4,1 |
| 6 | Приймач з п. 4 і комплексуванням GPS/ГЛОНАСС | 5 | 3,3 |
| 7 | Приймач з п. 5 і комплексуванням GPS/ГЛОНАСС | 5 | 2,2 |

Інформація в табл. 3 розкриває напрям по анті-*jamming* при поліпшенні апаратури споживачів достоїнства і недоліки перераховані нижче.

*Поліпшення* якості сигналу (рис. 2):

– *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).

Оцінюючи можливий виграш у стійкості апаратури споживачів ГНСС (табл. 3 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) [9,12,14,21,22]. Зменшення чутливості або встановлення "0" ДС в напрямку джерела завад це ПЧОС, яка реалізується в КЗАР. Перевага ПЧОС в наступному:

− виграш в завадостійкості може бути вельми істотним;

− не потрібне коригування самого приймача супутникової навігації.

Компенсатори завад будуються на основі антенних решіток і адаптивних методах управління діаграмою спрямованості, дуже часто компенсатори завад на антенної решітки (КЗАР) називають адаптивними антенними решітками (ААР). Серед *beamformer* і *nulling* антен найкращим є КЗАР з *nulling*-антеною (табл. 3). Тому актуальним на даний час є дослідження розробка і впровадження КЗАР на базі *nulling*-антен [21,22].

*Організаційні* методи компенсації завад (рис. 2). Проведення організаційних заходів по забезпеченню цілісності та доступності інформації ГНСС це вимоги ІСАО та ІМО, які необхідно виконувати. Для цього необхідно створювати комплекси моніторингу і аналізу стану ЕМО в зоні роботи апаратури споживача інформації ГНСС. Недоліки цих заходів – вимірювальна апаратура має дуже велику ціну та габарити, комплекси моніторингу ЕМО можна використовувати тільки в районі аеропорту або морського порту [54] (не всі адміністрації портів приймуть рішення про створення комплексів моніторингу). Можна проводити моніторинг ЕМО в точці розташування комплексу 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 недоліку необхідно створювати мобільні (недорогі тактичні) комплекси моніторингу ЕМО які можна застосовувати в зоні роботи апаратури споживача інформації ГНСС [25,27], тому розробка тактичних комплексів моніторингу ЕМО ГНСС є актуальною науковою задачею.

В даний час в Національному авіаційному університеті в рамках науково-дослідних робіт створено елементи комплексу моніторингу радіонавігаційного поля ГНСС [24 - 27] та експериментальний КЗАР [12,21,22].

**Висновки.** Об'єкти критичної інфраструктури які використовують інформацію ГНСС піддаються значному впливу навмисних завад що порушує цілісність і доступність інформації ГНСС в апаратурі споживачів, де найбільш вразливим елементом є приймач інформації ГНСС.

На сучасних електронних компонентах можливо створити генератори завад ГНСС та використовувати їх в терористичних атаках на ГНСС для порушення цілісності і доступності інформації ГНСС на об'єктах критичної інфраструктури.

Високі вимоги до інформації ГНСС потребують її захисту, забезпечення цілісності і доступності в умовах терористичних *jamming*-атак.

Створено модель загроз та модель порушника інформації ГНСС, виходячи з моделей було обрано заходи захисту інформації ГНСС.

На об'єктах критичної інфраструктури які використовують інформацію ГНСС необхідно проводити постійний моніторинг та оцінку рівня завади на можливість застосування ГНСС.

Найбільш дієвим методом забезпечення цілісності та доступності інформації ГНСС в умовах дії терористичних дій *jamming*-атак є керування ДС антени приймача ГНСС.

Актуальним є напрям дослідження та створення КЗАР на основі *nulling*-антен.

## ЛІТЕРАТУРА


1. Суходоля О. Зелена книга з питань захисту критичної інфраструктури в Україні / О. Суходоля, под ред. Д. Бірюков, С. Кондратов, К.: НІСД, 2016. 176 с.
2. Ward P. GPS Receiver RF Interference Monitoring, Mitigation, and Analysis Techniques // Navigation. 1994. № 4 (41). С. 367–392.
3. Landry R., Renard A. Analysis of potential interference sources and assessment of present solutions for GPS/GNSS receivers // 4th Saint-Petersburg on INS. 1997. С. 1–13.
4. Corrigan T.M. [и др.]. GPS Risk Assessment Study. Final report. Washington, 1999.
5. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. Final report. Washington, 2001.
6. Швець В. А. Експериментальні дослідження завадостійкості систем GPS [Текст] / В. А. Швець // Вісник інженерної академії України . – 2012. № 3-4. С. 160 – 164.
7. Rügamer A., Kowalewski D. Jamming and Spoofing of GNSS Signals-An Underestimated Risk?! Sofia, Bulgaria: International Federation of Surveyors, 2015. 1–24 с.
8. Швець В. А Аналіз загроз для транспортних систем, орієнтованих на використання глобальних навігаційних супутникових систем [Текст] / В. А. Швець, О. В. Швець // Вісник інженерної академії України . – 2013. № 3-4. С.82 – 86.
9. Швец В. А. Необходимость защиты информации глобальных навигационных спутниковых систем GPS, ГЛОНАСС, ГАЛИЛЕО [Текст] / В. А. Швец // Безпека інформації. – 2014. – №2, Том 20. – С. 185 – 192.
10. Швець В. А. Загрози навігаційному сегменту мережевих супутникових систем [Текст] / В. А. Швець // І Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем": наук.-практ. конф. 5 – 6 квітня 2018 р. : тези допов. – К. Київський національний університет – С. 493 – 497.
11. Швець В. А. Цілісність і доступність навігаційних даних в мережевих супутникових системах [Текст] / В. П. Харченко, В. А. Швець // Чотирнадцята наукова конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба "Новітні технології – для захисту повітряного простору": тези доповідей, 11 – 12 квітня 2018 року. – Х.: ХНУПС ім. І. Кожедуба, 2018. – С. 479 – 480.
12. Конин В., Харченко В. Системы спутниковой радионавигации / В. Конин, В. Харченко, Киев: ХОЛТЕХ, 2010. 521 с.
13. Уязвимость каналов управления штатовскими тактическими БПЛА: технологические моменты // Военное обозрение [Электронный ресурс]. URL: https://topwar.ru/106252-uyazvimost-kanalov-upravleniya-shtatovskimi-takticheskimi-bpla-tehnologicheskie-momenty.html (дата обращения: 26.07.2018).
14. Dovis F. GNSS Interference Threats and Countermeasures / F. Dovis, под ред. F. Dovis, Boston|London: ARTECH HOUSE, INC., 2015. 217 с.
15. Sklar J.R. Interference Mitigation Approaches for the Global Positioning System // LINCOLN LABORATORY JOURNAL. 2003. № 2 (14). С. 167–180.
16. SPIRENT Fundamentals of GPS Threats: White paper // EGNSSA, GNSS Market Report [Электронный ресурс]. URL: https://www.spirent.com/Assets/WP/WP-Fundamentals-of-GPS-Threats
17. Gao G.X. [и др.]. Protecting GNSS Receivers from Jamming and Interference 2016. 1327–1338 с.
18. RTCA Inc. Assessment of Radio Frequency Interference Relevant to the GNSS L1 Frequency Band / RTCA Inc., Washington: RTCA, Inc., 2008. 464 с.

19. International Civil Aviation Organization (ICAO) Aeronautical Telecommmunication. Volume II: Communication procedures including those with PANS status. Annex 10 to the Convention on International Civil Aviation / International Civil Aviation Organization (ICAO), Montreal: Printed in ICAO, 2001. 96 c.
20. Циркуляр 267-AN/159 Рекомендации по внедрению и эксплуатационному использованию глобальной спутниковой навигационной системы (GNSS) М.: ИКАО, 1996. 114 с.
21. Shvets V., Ilnytska S., Kutsenko O. Chapter 14. Application of Computer Modelling in Adaptive Compensation of Interferences on Global Navigation Satellite Systems // Cases on Modern Computer Systems in Aviation. IGI Global, 2019. – pp. 339 – 380.
22. Shvets V. A. Pulse characteristics of network satellite systems adaptive antenna for assessing correlation interference matrix [Текст] / V. A. Shvets, Kharchenko V. P. // Proceedings of the National Aviation University, N 4 (73), 2017. pp. 30 – 35.
23. Коротоношко А.Н. Устойчивость и радиотехническая защищенность транспортных систем, использующих точную спутниковую навигацию. / Коротоношко А.Н., Перунов Ю.М. // Новости навигации № 3, 2006 г. С. 26 – 32.
24. Shvets V. A. Method of evaluation of the electric field level of dangerous signals to gnss receivers [Текст] / V. A. Shvets, V. P. Kharchenko // Proceedings of the National Aviation University, N 2 (75), 2018. pp. 7–12.
25. Shvets V., Kondratiuk V., Ilnytska S., Kutsenko O. Radionavigation field monitoring in the landing area using software-defined radio receiver // Aviation in the XXI-st century 2018: World Congress. (National Aviation University, October 10 – 12, 2018). Kyiv: Publisher NAU, 2018. P 5.1.21 – 5.1.26
26. Shvets V. A. Information threats to the global navigation satellite system and how to eliminate them [Text] / V. A. Shvets // Sciences of Europe, Vol. 1, №35 (2019). – Praha, Czech Republic: Global Science Center LP, 2019. pp. 61 – 73.
27. Shvets V. A. Radio receiver for the monitoring of the radionavigation field of global navigating satellite systems [Text] / V. A. Shvets // Sciences of Europe, Vol. 1, №36 (2019). – Praha, Czech Republic: Global Science Center LP, 2019. pp. 54 – 64.