

Заходи захисту навігаційної інформації в мережевих супутникових системах

УДК 004.451.64(043.2)

Валеріян Швець¹, Тетяна Мелешко²Національний авіаційний університет, ¹*hvan@nau.edu.ua*,²*sorokunnet@ukr.net*

В мережевих супутникових системах (МСС) одним із сегментів є глобальні навігаційні супутникові системи (ГНСС) GPS, ГЛОНАСС, GALILEO. Однак при експлуатації приймальних пристроїв ГНСС апаратури споживачів виявилися факти їх схильності до кіберзагроз - *jamming* і *spoofing*, що позначається на доступності і цілісності навігаційних даних.

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.

Зосередимося на об'єктах критичної інфраструктури цивільного сектора, які отримують від 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 навколоремного простору в будь-який момент часу і в будь-яку погоду.

Принципово новою вимогою до ГНСС із боку транспортних споживачів є забезпечення цілісності, доступності і стійкості навігації, у першу чергу, забезпечення стійкості роботи систем безпеки руху в умовах *jamming*. Інші фактори забезпечення стійкості, а саме робота в умовах ненавмисних радіозавад, споконвічно враховані при розробці й розгортанні систем ГНСС і новизни не представляють. Стійкість роботи в умовах відмов супутників і наземних об'єктів систем ГНСС також представляє спеціальний предмет досліджень.

Приймачі споживачів навігаційної інформації ГНСС, які застосовуються на об'єктах критичної інфраструктури, потенційно піддані впливу *jamming* (організованих завад, котрі впливають на цілісність і доступність інформації ГНСС), тому що низька потужність сигналу від супутника, вона складає всього 10-16 Вт або мінус160 дБ/Вт, на поверхні Землі. *Jamming* приводить до

неможливості виявлення сигналу й до зриву його супроводу, до захватів неправильних сигналів і до помилок виміру навігаційних параметрів.

Важливою науковою проблемою є захист від навмисних завад. Захист від навмисних завад поділяється на два напрямки:

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

- анти-*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 компенсації перешкод даються в документах ICAO і діляться на організаційні заходи та технічні заходи.

В якості організаційних заходів що до забезпечення доступності до інформації ГНСС запропоновано проведення моніторингу доступності радіонавігаційного поля ГНСС в точці розташування радіоприймача сигналів ГНСС.

Для проведення моніторингу доступності радіонавігаційного поля ГНСС розроблено радіоприймач з використанням технології SDR-радіо, який є елементом дешевого, за ціною від 60\$ до 400\$, автономного автоматизованого комплексу радіомоніторингу та удосконалено імовірнісний метод оцінювання якості ЕМО в точці розташування радіоприймача сигналів ГНСС; удосконалено енергетичний метод оцінювання якості ЕМО в точці розташування радіоприймача сигналів ГНСС; на підставі удосконалених методів вперше розроблено метод оцінки рівня потужності електричного поля небезпечних сигналів в точці розташування радіоприймача сигналів ГНСС. Проведено експериментальні дослідження та порівняльний аналіз розробленого радіоприймача з використанням розробленого методу оцінки рівня потужності електричного поля небезпечних сигналів в точці розташування радіоприймача сигналів ГНСС.

В якості технічних заходів пропонується найбільш перспективним метод управління ДС приймальної антени (зменшення чутливості або встановлення "0" ДС в напрямку джерела перешкод). Зменшення чутливості або встановлення "0" ДС в напрямку джерела завад це просторова-часова обробка сигналів (ПЧОС), яка реалізується в адаптивних антенних 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 діаграмою спрямованості, дуже часто ААКЗ називають адаптивні антенні решітки (ААР).

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.

Серед *beamformer* і *nulling* антен найкращим є ААКЗ з *nulling*-антенною. Тому актуальним на даний час є дослідження розробка і впровадження ААКЗ на базі *nulling*-антен.