классификацию, мониторинг и управление конфиденциальными данными в сетях, базах данных и хранилищах, а также облачных приложениях вроде Office 365. Устройства DG Network Appliance основаны на технологии сопоставления данных по цифровым отпечаткам, которая лучше всего подходит для идентификации и контроля личной информации и позволяет минимизировать ложные срабатывания и пропущенные угрозы.

DG MANAGEMENT CONSOLE. Веб-консоль для настройки платформы, конфигурирования и развертывания агентов, а также управления политиками, предупреждениями и отчетами.

Инженер по технической поддержке проектов группы компаний БАКОТЕК, Гурбанов Мурад.

УДК 004.056.5:621.396.933:527.8

В. А. Швець[1]
[1]*Національний авіаційний університет*
hvan@nau.edu.ua

ЗАГРОЗИ НАВІГАЦІЙНОМУ СЕГМЕНТУ МЕРЕЖЕВИХ СУПУТНИКОВИХ СИСТЕМ

Інформаційні потоки в суспільстві викликали необхідність об'єднання раніше розрізнених супутникових систем в інформаційно-обчислювальну мережу, що в даний час визначається як мережеві супутникові системи (МСС) (рис. 1.).

Одним із сегментів МСС є глобальні навігаційні супутникові системи (ГНСС) GPS, ГЛОНАСС, GALILEO. Ці ГНСС створюють координатно-часове забезпечення, що становить основу ефективного функціонування багатьох галузей економіки і є найважливішою частиною сучасних транспортних систем, цифрових систем телекомунікації, систем управління військами та високоточною зброєю.

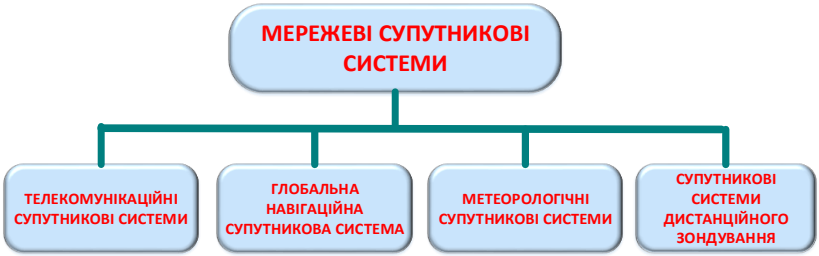

Рис. 1. Склад мережевих супутникових систем

Після ейфорії перших років освоєння супутникових навігаційно-часових технологій, в даний час більш скрупульозне аналізується використання ГНСС в якості єдиного джерела координатно-часової інформації (КЧІ), починає поступатися місцем більш тверезого підходу до перспектив використання ГНСС. Перш за все, це обумовлено вразливістю ГНСС при впливі випадкових і навмисних перешкод. Про уразливості цивільних приймачів ГНСС було відомо давно [1-6], але її рідко беруть до уваги виробники приймачів і їх користувачі. Було проведено кілька аналізів уразливості транспортних систем, заснованих на використанні сигналів GPS [1-6]. Одним з найбільш важливих і своєчасних звітів про дослідження в цій області був звіт Центру Волпе [3] про уразливість GPS, у висновках якого зазначалося, що система GPS, як і інші радіонавігаційні системи, уразливі при впливі випадкових і навмисних перешкод, і такі перешкоди несуть загрозу безпеці і можуть мати серйозні наслідки для економіки і навколишнього середовища.

Таким чином, уразливість ГНСС при впливі випадкових і навмисних перешкод є в даний час загальновизнаним фактом. Ця вразливість в рівній мірі відноситься як до GPS, ГЛОНАСС, GALILEO, оскільки принципи їх побудови і діапазони частот досить близькі. До числа критичних застосувань сигналів ГНСС можна віднести:

1) точні і грубі заходження на посадку літаків;

2) плавання морських і річкових суден в портах, на підходах до портів і на внутрішніх водних шляхах;

3) перевезення небезпечних вантажів наземним транспортом і реагування на надзвичайні ситуації;

4) синхронізації телекомунікаційних систем.

Проста реалізація комплексу придушення з незначною потужністю (шумова, гармонійна), можуть привести до створення зони придушення в сотні кілометрів (табл. 1).

Таблиця 1 Гранично небезпечні дальності джерела завад

Канал		GPS L1	GPS L1, L2C	ГЛОНАСС L1	ГЛОНАСС L1, L2	GPS+ ГЛОНАСС
Перешкода	Вт	Дальність джерела перешкод (км)				
Шумова прицільна	0.1	85	70	60	40	38
	1	280	230	200	132	125
	10	850	700	600	400	380
	100	2800	2300	2000	1320	1250
Гармонійна	0.1	280	230	87	49	46
	1	829	736	278	157	147
	10	2800	2300	870	490	460
	100	8290	7360	2780	1570	1740
Імітаційна генераторна	0.1	900	740	391	252	236
	1	2880	2368	1251	803	755
	10	9000	7400	3921	2520	2360
	100	28800	23680	12510	8030	7550

Виходячи, з вище викладеного можна запропонувати можливі заходи підвищення завадостійкості ГНСС від придушення:

1) поліпшення діаграми спрямованості прийомної антени на малих кутах піднесення;

2) управління діаграми спрямованості антени, що зменшує чутливість у напрямку джерела перешкод;

3) антенні решітки з поляризацією сигналу;

4) поліпшення обробки сигналів у приймачі;

5) комбінування приймачів ГНСС із ІНС;

6) використання двочастотних приймачів L1, L2;

7) використання тричастотних приймачів.

Аналіз джерел розробки апаратури компенсації завад, а також власний досвід, наукові теми НАУ показує, що можливе підвищення рівня просторового придушення перешкод (більше 30 дБ) із застосуванням ряду науково обґрунтованих технічних рішень (рис. 2).

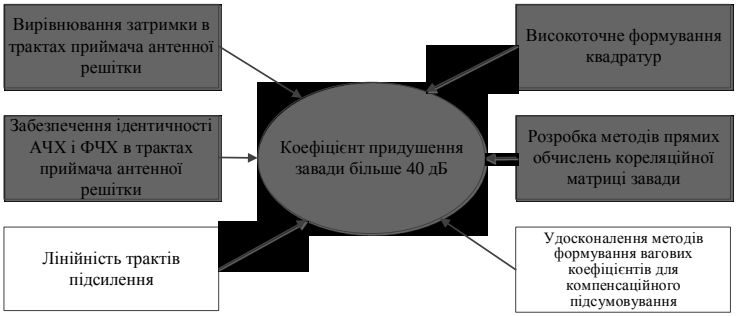

Рис. 2. Заходи по досягненню високої ефективності придушення завад

Зростаюче використання GPS в цивільній інфраструктурі робить її все більш привабливою мішенню для ворожих дій окремих особистостей і груп.

Література

1. Sushych O. P. (2012) Eksperymentalna otsinka vplyvu navmysnykh zavad na aparaturu spozhyvacha hlobalnoi navihatsiinoi suputnykovoi systemy [Experimental assessment of the effect of deliberate interference on the equipment of the consumer of the global navigation satellite system]. Visnyk inzhenernoyi akademiyi Ukrayiny, no. 3-4. pp. 32 – 35. (In Ukrainian).

2. Shvets V. A. (2012) Eksperymentalni doslidzhennya zavadostiykosti system GPS [Experimental studies of impedance of GPS systems]. Visnyk inzhenernoyi akademiyi Ukrayiny, no. 3-4. pp. 160 – 164. (In Ukrainian).

3. L. Bond. (1998) Overview of GPS Interference Issues. GPS Interference Symposium Volpe National Transportation System Center, Boston. pp. 341-352

4. John Hopkins University Applied Physics Laboratory // GPS Risk Assessment Study – Final Report, January 1999. Available at:

http://www.rvs.unibielefeld.de/publications/Incidents/DOCS/Research/Other/Article/gps-risk-ass.pdf (accessed 13.11.2017)

5. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. A John Volpe National Transportation System Center Final Report, August 29, 2001. Available at: https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf (accessed 13.11.2017)

6. Fundamentals of GPS Threats. European Global Navigation Satellite Systems Agency, GNSS Market Report Issue 4, March 2015 Available at: https://www.spirent.com/-/media/White-Papers/Positioning/Fundamentals-of-GPS-Threats.pdf (accessed 30.01.2018)

7. R. A. Monzingo, T. W. Miller. (2004) Introduction to adaptive arrays. SciTech Publishing, Inc. 2004. 552 p.