© Shvets V. The necessity of global navigation satellite systems GPS, GLONASS, GALILEO information security // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 185-192.

НЕОБХОДИМОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ ГЛОБАЛЬНЫХ НАВИГАЦИОННЫХ СПУТНИКОВЫХ СИСТЕМ GPS, ГЛОНАСС, ГАЛИЛЕО

Валериян Швец

Национальный авиационный университет, Украина

ШВЕЦ Валериян Анатольевич, к.т.н.

Год и место рождения: 1959 г., ст. Окница, Молдова.
Образование: Киевский институт инженеров гражданской авиации (с 2000 года – Национальный авиационный университет), 1986 год.
Должность: заведующий кафедрой систем защиты информации с 2004 года.
Научные интересы: цифровая обработка сигналов, биометрика, информационная безопасность.
Публикации: более 90 публикаций, среди которых монографии, учебники, учебные пособия, научные статьи, патенты.
E-mail: hvan@nau.edu.ua

Аннотация. *В статье рассматривается проблема функционирования глобальных навигационных спутниковых систем в условиях непреднамеренных и преднамеренных помех. Рассмотрены требования к эксплуатационным характеристикам глобальных навигационных спутниковых систем по видам транспортных систем. Рассмотрены основные угрозы глобальным навигационным спутниковым системам. Основываясь на требованиях к эксплуатационным характеристикам глобальных навигационных спутниковых систем, проведен анализ их уязвимости при воздействии преднамеренных и непреднамеренных помех. Выделены наиболее уязвимые эксплуатационные характеристики глобальных навигационных спутниковых систем (целостность и доступность) Предложен метод уменьшения уязвимости глобальных навигационных спутниковых систем при воздействии непреднамеренных и преднамеренных помех.*

Ключевые слова: *защита информации, GPS, ГЛОНАСС, ГАЛИЛЕО, целостность, доступность, угрозы, антенные решетки.*

Вступление

Современный этап развития общества характеризуется все более широким использованием координатно-временного обеспечения (КВО), составляющего основу эффективного функционирования многих отраслей экономики и являющегося важнейшей частью современных транспортных систем, цифровых систем телекоммуникации, систем управления войсками и высокоточным оружием. Основу КВО составляют глобальные навигационные спутниковые системы (ГНСС), которые представлены в настоящее время спутниковыми радионавигационными системами (СРНС) ГЛОНАСС (Россия) и GPS (США). Европейское сообщество создает для этих целей свою СРНС Галилео. Использование глобального координатно-временного поля, создаваемого ГНСС, позволяет определять положение любого пользователя в пространстве с точностью до единиц метров и время с точностью до десятков и единиц наносекунд в любой точке Земного шара и околоземного пространства в любой момент времени и в любую погоду.

После эйфории первых лет освоения спутниковых навигационно-временных технологий, в настоящее время более скрупулезно анализируется использования ГНСС в качестве единственного источника координатно-временной информации (КВИ), начинает уступать место более трезвому подходу к перспективам использования ГНСС. Прежде всего, это обусловлено уязвимостью ГНСС при воздействии непреднамеренных и преднамеренных помех. Об уязвимости гражданских приемников ГНСС было известно давно [1-7], но ее редко принимают во внимание изготовители приемников и их пользователи. Только тогда, когда Министерство обороны США активизировало свою деятельность, связанную с применением GPS в военных условиях (NAVWAR), стало очевидным, что преднамеренные помехи для гражданских приемников следует учитывать как важный фактор. Проведенные в США в интересах военных испытания в зоне Нью-Йорка [8] показали, что ряд приемников, установленных на борту самолетов гражданской авиации, утратил возможность слежения за сигналами GPS при заходе на посадку в международном аэропорту в Ньюарке.

Анализ проблемы

Было проведено несколько анализов уязвимости транспортных систем, основанных на использовании сигналов GPS [9-13]. Одним из наиболее важных и своевременных отчетов об исследованиях в этой области был отчет Центра

Волпе [14] об уязвимости GPS, в выводах которого отмечалось, что система GPS, как и другие радионавигационные системы, уязвима при воздействии непреднамеренных и преднамеренных помех и что такие помехи несут угрозу безопасности и могут иметь серьезные последствия для экономики и окружающей среды. В отчете также сделан вывод о том, что растущее использование GPS в гражданской инфраструктуре делает ее все более привлекательной мишенью для враждебных действий отдельных личностей и групп. В то же время выявлена коммерческая доступность оборудования для постановки помех [8, 15].

Таким образом, уязвимость ГНСС при воздействии непреднамеренных и преднамеренных помех является в настоящее время общепризнанным фактом. Эта уязвимость в равной мере относится как к GPS, так и к ГЛОНАСС и Галилео, поскольку принципы их построения и используемые диапазоны частот достаточно близки. В настоящее время радионавигационное сообщество активно обсуждает проблему уязвимости ГНСС и поиска запасных систем. В связи с этим необходимо анализировать на основе имеющихся данных основные источники непреднамеренных помех, возможные способы постановки преднамеренных помех аппаратуре потребителей ГНСС и перспективы повышения надежности координатно-временного обеспечения в условиях воздействия помех.

Проблема определения состава и способов применения навигационно-временных средств находится в сфере ответственности конкретного потребителя координатно-временной информации исходя из необходимости решения стоящей перед ним задачи. Вместе с тем, существует ряд критичных применений навигационно-временных технологий, где представляется необходимым комплексное использование максимально возможного количества доступных средств для повышения надежности координатно-временного обеспечения в условиях воздействия помех. В данном контексте критичность определяется теми рисками, которые могут иметь место для человеческой жизни, национальной безопасности, экономики и окружающей среды в случае ухудшения характеристик радионавигационных сигналов или их потери. В первую очередь это относится ко всем видам транспортных систем и систем телекоммуникаций, использующих сигналы ГНСС. Поэтому приведем краткий анализ, касающийся уязвимости этих применений.

Авиация. Требования к эксплуатационным характеристикам ГНСС применительно к гражданской авиации в соответствии с рекомендациями ICAO приведены в табл. 1 [16-18].

Таблица 1

Требования к эксплуатационным характеристикам ГНСС

Операция	Точность (95 %)	Целост-ность	Непрерыв-ность	Предель-ное расстояние для тревоги	Время трево-ги	Доступность
Полет над океаном	12,4 мор. миль	$1\cdot10^{-7}$/час	$1\cdot10^{-5}$/час	4,0 мор. миль	2 мин.	от 0,99 до 0,99999
На маршруте	2,0 мор. миль	$1\cdot10^{-7}$/час	$1\cdot10^{-5}$/час	2,0 мор. миль	1 мин.	от 0,99 до 0,99999
Зона аэропорта	0,4 мор. миль	$1\cdot10^{-7}$/час	$1\cdot10^{-5}$/час	1,0 мор. миль	30 с	от 0,99 до 0,99999
NPA	220 м	$1\cdot10^{-7}$/час	$1\cdot10^{-5}$/час	0,3 мор. миль	10 с	от 0,99 до 0,99999
APV I	220 м (H) 220 м (V)	$1\text{-}2\cdot10^{-7}$ /заход	$1\text{-}8\cdot10^{-6}$/15 с	0,3 мор. миль (H) 50 м (V)	10 с	от 0,99 до 0,99999
APV II	16 м (H) 8 м (V)	$1\text{-}2\cdot10^{-7}$ /заход	$1\text{-}8\cdot10^{-6}$/час 15 с	40 м (H) 20 м (V)	6 с	от 0,99 до 0,99999
Категория I	16 м (H) 4,0-6,0 м (V)	$1\text{-}2\cdot10^{-7}$ /заход	$1\text{-}8\cdot10^{-6}$/15 с	40 м (H) 10-15 м (V)	6 с	от 0,99 до 0,99999
Категория II	6,9 м (H) 2,0 м (V)	$1\text{-}1\cdot10^{-9}$ /заход 15 с	$1\text{-}4\cdot10^{-6}$/15 с	17,3 м (H) 5,3 м (V)	1 с	от 0,99 до 0,99999
Категория III	6,2 м (H) 2,0 м (V)	$1\text{-}1\cdot10^{-9}$ /заход 15 с	$1\text{-}2\cdot10^{-6}$/30 с (L) $1\text{-}2\cdot10^{-6}$/15 с (V)	15,5 м (H) 5,3 м (V)	1 с	от 0,99 до 0,99999

Анализ данных, приведенных в таблице 1, показывает, что высокие требования, предъявляемые авиацией к ГНСС, позволяют использовать спутниковые навигационные системы в качестве первичного средства для полетов над океаном и в качестве дополнительных систем для полетов в зоне аэропорта, включая грубый и точный заход на посадку (с использованием функциональных дополнений). Вместе с тем в качестве вспомогательного средства ГНСС не может быть единственной навигационной системой на борту самолета, учитывая возможность ухудшения характеристик сигналов ГНСС или их потери при воздействии помех.

Морской транспорт. К морским операциям, в ходе которых могут быть использованы GPS и GPS с функциональными дополнениями, относятся:

– навигация судов с учетом следующих фаз или зон: в океане; в прибрежной зоне; в портах или при подходе к портам; на внутренних водных путях и каналах;

– наблюдение (обзор) для служб управления движением судов;

– задачи поиска;

– разведка природных ресурсов;

– геодезическая съемка, инженерная съемка и строительство.

Требования к характеристикам ГНСС при морских операциях приведены в таблице 2.

Таблица 2

Требования к эксплуатационным характеристикам при морских операциях

Операция	Точность (2d, 1σ)		Рабочая зона	Доступность	Интервал между засечками	Кол-во засечек	Многозначность
	прогноз	воспроизведение					
Океанская, безопасность	1-2 мор. миль	--	Глобальная	99 % засечек каждые 12 час.	15 мин.	2	Разрешима с вероятностью 99,9 %
Океанская, - поиск природных ресурсов	10-100 м	10-100 м	Глобальная	99 %	1 мин.	2	_"_
Океанская, – операции поиска	0,1-0,25 мор. миль	0,25 мор. миль	Национальные зоны	99 %	1 мин.	2	_"_
Прибрежная, безопасность	0,25 -2 мор. миль		Прибрежные зоны	99,7 %	2 мин.	2	-"-
Прибрежная, поиск	0,25 мор. миль	800-600 футов	Прибрежные зоны	99,7 %	1 мин.	2	-
Прибрежная, природные ресурсы	1,0-100 м	1,0-100 м	Прибрежная зона	99 %	1 с	2	-
Порт-безопасность	8-20 м	8-20 м	вход в порт и подход к порту	99,7 -99,9 %	6-10 с	2	Разрешена с вероятностью 99,9 9 %
Порт-природные ресурсы	1-5 м	1-5 м	вход в порт и подход к порту	99 %	1 с	2	-"-
Порт- съемка/ консалтинг	5 м (план) 0,1 м (выс.)	5 м (план) 0,1 м (выс.)	вход в порт, канал и т.д.	99 %	1-2 с	2 или 3	-"-
Внутренний водный путь – безопасность	2-5 м	2-5 м	системы водных путей	99,9 %	1-2 с	2	-"-
Внутренний водный путь строительство	5 м (план) 0,1 м (выс)	5 м (план) 0,1 м (выс)	системы водных путей	99 %	1-2 с	2 или 3	-"-

В настоящее время в рамках международного стандарта, утвержденного Международной морской организацией (ИМО), регламентировано использование автоматизированных идентификационных систем (АИС) на всех судах водоизмещением 300 регистровых тонн и более, используемых для международных перевозок людей, на грузовых судах водоизмещением 500 тонн и более и на пассажирских судах независимо от их водоизмещения. Аппаратура АИС включает в свой состав приемник ГНСС, приемник морских радиомаяков для приема дифференциальных поправок и УКВ приемоответчик цифрового селективного доступа. Таким образом, эта система с точки зрения передачи на берег и другие суда информации о месте, скорости и времени ориентирована на использование сигналов ГНСС.

Как следует из данных, приведенных в табл. 2, ряд морских применений ГНСС являются критичными к ухудшению характеристик и потере сигналов ГНСС.

Наземный транспорт. Областями применения сигналов ГНСС в наземном транспорте являются системы позиционного управления поездами и интеллектуальные транспортные системы (ITS), используемы для повышения безопасности и эффективности использования железных и шоссейных дорог и транзитных систем. Требования к навигации и местоопределению на железных дорогах приведены в табл. 3, а аналогичные требования для интеллектуальных транспортных систем – в табл. 4.

Таблица 3

Требования к навигации и позиционированию на железных дорогах

Область применения	Точность (1d, 1σ)	Время до тревоги	Доступность	Рабочая зона
Слежение за местонахождением поездов	10-80 м	5 с	99,7 %	вся страна
Определение скорости	± 1 км/час для скоростей < 20 км/час ± 5 % для скоростей ≥ 20 км/час	5 с	99,7 %	вся страна
Управление поездами	1 м	< 5 с	100 %	вся страна
Автоматическое предупреждение автомобилей на пересечениях шоссейных и железных дорог	1 м	< 5 с	100 %	вся страна

Таблица 4

Требования к точности навигационной системы в составе ITS

Режим	Точность (м), 95 %
Шоссейные дороги	
Навигация и наведение на маршруте	5-20
Автоматический мониторинг автомобилей	30
Автоматическая идентификация автомобилей	30
Общественная безопасность	10
Управление ресурсами	30
Реагирование на чрезвычайные ситуации	30
Предотвращение столкновений	1
Геофизическая съемка	5
Геодезические сети	< 1
Командование и управление автомашинами	30-50
Автоматическое оповещение об остановке автобуса	5 (25-30 м до остановки)
Реагирование на чрезвычайную ситуацию	75-100
Сбор данных	5

Анализ использования ГНСС на наземном транспорте показывает, что ухудшение характеристик или потеря сигнала ГНСС скорее приведут к снижению эффективности, чем к прямому ущербу для безопасности. Исключения составляют те применения ITS, где уязвимость ГНСС может привести к задержкам в оказании медицинской помощи при несчастных случаях и к ущербу для окружающей среды или угрозе человеческой жизни в случае инцидентов при перевозке опасных грузов.

Телекоммуникационные системы. В настоящее время использование сигналов ГНСС в телекоммуникационных системах возросло до такой степени, что ГНСС стала играть критичную роль с точки зрения обеспечения временной синхронизации. В настоящее время это наиболее частый способ достижения высокоточной синхронизации дешевыми способами [19].

Требования к синхронизации сетей связи и к иерархии часов в телекоммуникационных системах приведены в таблицах 5 и 6 соответственно [14].

Таблица 5

Требования к синхронизации сетей связи

Синхронизация в сетях связи, связанных с ITS	
Воспроизводимая точность	$1 \cdot 10^{-10}$ (по частоте)
Доступность	99,7 %
Интервал засечки	непрерывный
Рабочая зона	вся страна
Емкость системы	не ограничена

Таблица 6

Требования к уровням иерархии часов для телекоммуникационных систем

Уровень	Точность	Стабильность хранения	Технология
1	$1{,}0 \cdot 10^{-11}$	-	GPS/Cs/Лоран-С
2	$1{,}6 \cdot 10^{-8}$	$1{,}0 \cdot 10^{-10}$ за сутки	Rb
3E	$4{,}6 \cdot 10^{-6}$	$1{,}0 \cdot 10^{-8}$ за сутки	Кварц
3	$4{,}6 \cdot 10^{-8}$	$3{,}7 \cdot 10^{-7}$ за сутки	Кварц
4E	$3{,}2 \cdot 10^{-5}$	не требуется	Кварц
4	$3{,}2 \cdot 10^{-5}$	не требуется	Кварц

Приведенные в этих таблицах данные свидетельствуют о том, что характеристики телекоммуникационных служб, опирающихся на ГНСС, могут быть существенно ухудшены или полностью утрачены в случае ухудшения или потери сигналов ГНСС.

Таким образом, к числу критичных применений сигналов ГНСС можно отнести:

– точные и грубые заходы на посадку самолетов;

– плавание морских и речных судов в портах, на подходах к портам и на внутренних водных путях;

– перевозку опасных грузов наземным транспортом и реагирование на чрезвычайные ситуации;

– синхронизацию телекоммуникационных систем.

Угрозы глобальным навигационным спутниковым системам

Непреднамеренные помехи. Для оценки методов уменьшения уязвимости ГНСС при воздействии помех рассмотрим вначале типы непреднамеренных помех. Основной причиной уязвимости ГНСС является низкая мощность сигнала, она составляет всего 10^{-16} Вт или – 160 дБ/Вт на поверхности Земли.

Непреднамеренные помехи можно подразделить на естественные помехи и помехи искусственного происхождения.

К непреднамеренным помехам искусственного происхождения относятся излучения радиопередатчиков, могущие создать сигналы с нежелательным уровнем мощности в L-диапазоне. Идентифицированные искусственные непреднамеренные помехи (Табл. 7 [20]), создаются радиолиниями, гармониками телевизионных каналов, сигналами запроса систем ближней навигации, гармониками существующих УКВ радиостанций, спутниковой связной системой GLOBALSTAR, радиолокационными станциями системы управления воздушным движением.

Таблица 7

Возможные источники непреднамеренных искусственных помех

Диапазон частот, МГц, мешающих сигналов (номер канала)	Источник мешающих сигналов	Частоты GPS:1227,6; 1575,42;1176,45 МГц	Частоты ГЛОНАСС:1246-1256,5; 1602-1615,5; после 2005:1242,94-1247,75;1598-1604,25 МГц	Частоты ГАЛИЛЕО E1:1587-1591 МГц; E2:1559-1563 МГц; E5:1164-1215 МГц; E6:1260-1300 МГц
1533	Радиолиния	+	–	-
~ 500	3-я гармоника	+	+	+
66 и 67 каналы ТВ	2-я гармоника	+	+	+
22 и 23 каналы ТВ	3-я гармоника	+	+	+
157 УКВ	10-я гармоника	+	+	-
131 и 121 УКВ	12-я и 13-я гармоники	+	+	-
Сигналы запроса дальности РСБН	2-я гармоника	+	+	-
525 частота кристалла DME	3-я гармоника	+	–	-
1575	Немодулированная несущая	+	–	-
> 1610	GLOBALSTAR	–	+	-
1240…1243.25	Передача цифровых данных (пакетное радио)	–	+	-
1242…1242.7	Любительские радиорелейные станции	–	+	-
1243…1260	Любительские ТВ передатчики	–	+	+
1250…1259	РЛС УВД	–	+	+
108…118	Помехи в полосах ЛПД ДПС	+	+	+

Преднамеренные помехи. Преднамеренная помеха (jamming) – радиопомеха, создаваемая специально сконструированным источником и предназначенная для нарушения функционирования аппаратуры потребителей ГНСС. К преднамеренным помехам следовало бы также отнести любые действия, направленные на нарушение функционирования СРНС, включая атаку на спутники и наземную инфраструктуру управления. Однако такие операции означали бы начало военных действий, поэтому анализ их последствий выходит за рамки настоящей работы.

По-видимому, преднамеренные помехи направлены в первую очередь против военных применений. В этой ситуации гражданские потребители в критичных областях применения, являясь невинно пострадавшей стороной, тем не менее, должны быть готовы к защите от подобных действий.

К числу преднамеренных помех следует отнести радиопротиводействие и радио-дезинформацию.

При радиопротиводействии могут использоваться следующие типы помех:

– некогерентный синусоидальный сигнал;

– синусоидальный сигнал с изменяющейся частотой;

– импульсы с синусоидальным заполнением;

– узкополосный шум;

– полосовой шум;

– импульсный шум.

Существуют постановщики помех ГНСС самых разных размеров, различной выходной мощности и различной стоимости. Небольшие легкие недолговечные постановщики помех мощностью от 1 до 100 Вт могут стоить менее 1000 долларов, и они могут быть изготовлены из коммерчески доступных компонентов людьми, имеющими минимально необходимые знания.

Другим типом преднамеренных помех является радиодезинформация – метод, направленный на то, чтобы заставить приемник ГНСС осуществить привязку к ложным сигналам.

В Национальном авиационном университете проводились экспериментальные исследования влияния различных типов помех на работу приемников ГНСС GPS [21, 22].

Метод решения проблемы

Исходя из вышесказанного, при использовании ГНСС наиболее жесткие требования выдвигаются к доступности 99.999% (табл. 1, 2, 3) и целостности 10^{-9} (табл. 1) данных в информации ГНСС (табл. 7).

Цели защиты информации – обеспечение конфиденциальности, целостности и доступности данных. Информация ГНСС в настоящее время подвергается угрозам, нуждается в защите и однозначно ее надо защищать. Однако специфика применения информации ГНСС требует не традиционных методов защиты. Ограничивать доступ к информации спутников нельзя, на данном этапе ГНСС открытая система для всех пользователей. Шифровать данные − переделывать

все оборудование ГНСС (космический и наземный сегмент, пользователей – миллионы), на такие затраты ни одна страна разработчик сейчас не пойдет.

Направление по которому идут работы по защите данных ГНСС − модернизация космического сегмента (повышение мощности спутниковых передатчиков, применение сигналов с расширенным спектром). Однако сроки окончания этих работ все время отодвигаются, так система GPS должна была быть модернизирована до 2016 года. Окончательный срок модернизации правительством США в настоящее время не определен. ГАЛИЛЕО − запланированный ввод в эксплуатацию 2014 год, перенесено на 2018-2020 года. ГЛОНАСС − на данном этапе работает не полная группировка спутников, вводятся новые, старые спутники не модернизируются.

Предлагается один из методов защиты информации ГНСС, не требующий ограничения доступа и дополнительного шифрования данных ГНСС, т.е. обеспечение целостности и доступности, а именно использование управляемой пространственной избирательности (пространственно-временная обработка сигналов) многоэлементных антенных систем, в том числе с «нулями» в направлении на помехи [23, 24, 25, 26], который в данное время является наиболее действенным средством. Пространственная обработка возможна при применении антенных решеток (АР). На базе антенных решеток с помощью адаптивных алгоритмов возможно построение адаптивных антенно-приемных систем (ААПС), анализируя сигналы, которые принимаются, автоматически формируют провалы диаграммы направленности в направлении прихода помех, используя весовые коэффициенты в каждом канале АР. В отличие от методов, предложенных в [24, 26] сформировать опорный канал в ААПС, предлагаемых для защиты информации GNSS нет возможности. Поэтому сигнал и помеха будут приниматься одними и теми же антеннами и обрабатываться в одном приемном тракте. В связи с этим возникнет взаимная корреляция сигнала и помехи, что в свою очередь внесет изменения в корреляционную матрицу помехи, а это вызовет изменения весового вектора.

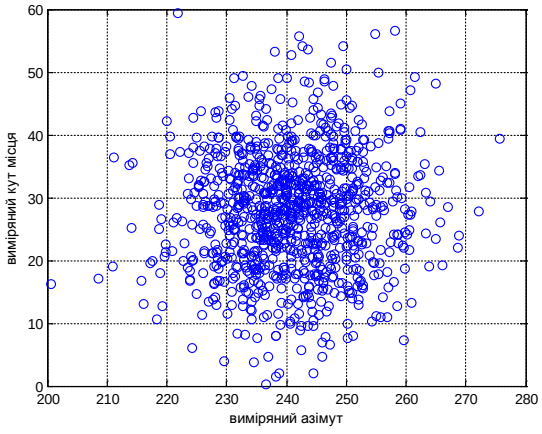

Рис. 1. Точность измерения координат помехового сигнала

Результаты экспериментальных исследований влияния сигнальной составляющей на точность измерения координат источника помех представлены на рис. 1.

Из рисунка видно, что при заданных угле места и азимута, присутствует значительная ошибка измерения. Результаты экспериментальных исследований доказывают, что для оптимизации весовых коэффициентов - необходимо исключение влияния сигнала при вычислении обратной матрицы помехи $\mathbf{R}^{-1}_{\text{сп}}$.

Также для уменьшения влияния неидентичности каналов ААПС (неидентичность частотных характеристик приемников, конструктивная неидентичность элементов ААПС, разброс квадратурных каналов по коэффициенту усиления и фазовому сдвигу и другие факторы), вычисляя весовые коэффициенты, необходимо исключать сигнальную составляющую при вычислении корреляционной матрицы помехи. Для этого рекомендуется удалять сигнал из смеси сигнал/помеха с помощью фильтрации, но проанализировав этот способ, было замечено внесение дополнительной корреляции в обрабатываемый сигнал. Корреляционная функция также сильно зависела от полосы пропускания фильтра.

Для устранения этой зависимости был разработан метод вычисления весовых коэффициентов без опорного сигнала, который объясняет следующая функциональная схема (рис. 2).

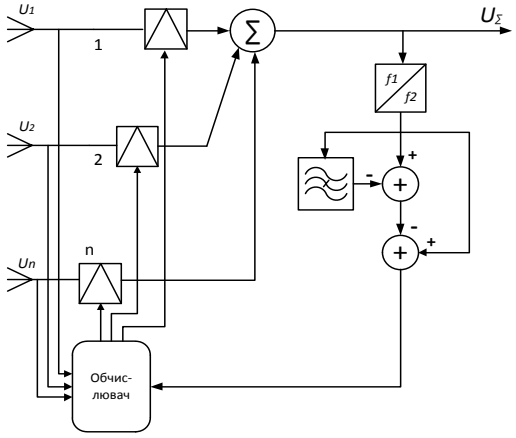

Рис. 2. Функциональная схема вычислителя

Преобразователь преобразует сигнал с частоты *f1* в сигнал с частотой *f2*, которая все время постоянная. Режекторный фильтр вырезает сигнальную составляющую и подает напряжение помехи с обратным знаком на сумматор, на выходе сумматора остается напряжение сигнала. Напряжение помехи получается вычитанием из смеси "сигнал/помеха" напряжения сигнала. Двойное вычитание предложено для того, чтобы не вносить изменений в корреляционные матрицы помехи.

Аналитически метод можно описать таким образом.

Сигнал ошибки формируется как разность

$$\varepsilon = \mathbf{w}^{\mathrm{T}}\mathbf{u}_{\text{сп}} - S\ . \qquad (1)$$

Квадрат ошибки

$$\varepsilon^2 = S^2 - 2S\mathbf{w}^{\mathrm{T}} + \mathbf{w}^{\mathrm{T}}\mathbf{u}^{*}_{\text{сп}}\mathbf{u}^{\mathrm{T}}_{\text{сп}}\mathbf{w} . \qquad (2)$$

Средний квадрат ошибки определяется как

$$E\left[\varepsilon^2\right] = S^2 + \mathbf{w}^{\mathrm{T}}\mathbf{R}_{\text{сп}}\mathbf{w} - 2\mathbf{w}^{\mathrm{T}}\mathbf{r}_{\text{сп,с}} , \qquad (3)$$

где $\mathbf{r}_{\text{сп,с}} = \overline{\mathbf{u}^{*}_{\text{сп}}S}$; E – среднее значение.

Корреляционная матрица $\mathbf{R}_{\text{сп}}$ равняется сумме корреляционной матрицы сигнала $\mathbf{R}_{\text{с}}$ и корреляционной матрицы помехи $\mathbf{R}_{\text{п}}$, $\mathbf{R}_{\text{сп}} = \mathbf{R}_{\text{п}} + \mathbf{R}_{\text{с}}$. Из рис. 2. видно, что при формировании сигнала ошибки корреляционная матрица вычисляется следующим образом $\mathbf{R}_{\text{сп}} = \mathbf{R}_{\text{п}} + \mathbf{R}_{\text{с}} - \mathbf{R}_{\text{с}} = \mathbf{R}_{\text{п}}$.

Так как сигнал от спутников ГНСС и сигнал помехи не коррелированы и сигнал спутников подавляется, то в выражении (3) $\mathbf{r}_{\text{сп,с}} = \mathbf{r}_{\text{п}}$.

Выражение (3) примет вид

$$E\left[\varepsilon^2\right] = \mathbf{w}^{\mathrm{T}}\mathbf{R}_{\text{п}}\mathbf{w} - 2\mathbf{w}^{\mathrm{T}}\mathbf{r}_{\text{п}} . \qquad (4)$$

Поскольку выражение (4) квадратичная функция, ее минимум может быть найден приравниванием к нулю производной

$$d(E\left[\varepsilon^2\right]) \Big/ d\mathbf{w} = d(\mathbf{w}^{\mathrm{T}}\mathbf{R}_{\text{п}}\mathbf{w} - 2\mathbf{w}^{\mathrm{T}}\mathbf{r}_{\text{п}}) / d\mathbf{w} .$$

В результате получим

$$2\mathbf{R}_{\text{п}}\mathbf{w} - 2\mathbf{r}_{\text{п}} = 0 .$$

Вектор весовых коэффициентов будет определятся выражением

$$\mathbf{w} = \mathbf{R}^{-1}_{\text{п}}\mathbf{r}_{\text{п}} . \qquad (5)$$

Выражение (5) полностью определяет уравнение Винера-Хопфа по вычислению весовых коэффициентов в ААПС.

На рис. 3 представлена диаграмма направленности ААПС, как видно в направлении источника помехи формируется провал.

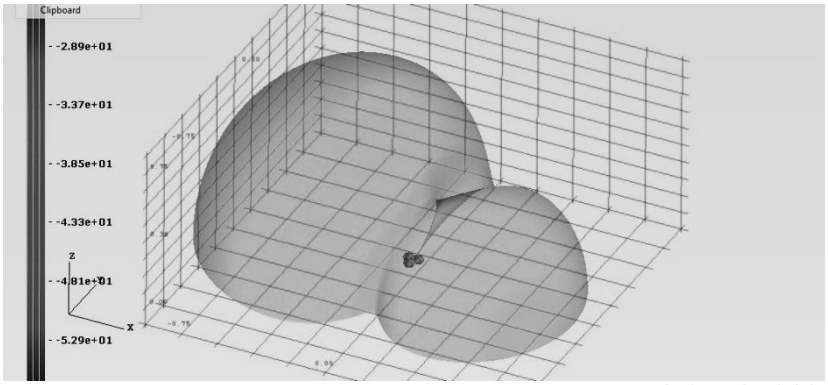

Рис. 3. Диаграмма направленности адаптивной антенно-приемной системы GPS, ГЛОНАСС, ГАЛИЛЕО

Выводы

Все радионавигационные системы подвержены воздействию непреднамеренных и преднамеренных помех. Однако влияние этих помех представляется наиболее важным в отношении ГНСС, используемых в настоящее время в качестве первичных источников координатно-временной информации.

Имеется ряд критичных применений КВО, в которых целесообразно использование методов защиты информации всех доступных средств КВО, для обеспечения человеческой и национальной безопасности, избегания больших экономических потерь и экологического ущерба.

Для обеспечения целостности и доступности данных систем ГНСС при воздействии непреднамеренных и преднамеренных помех предлагается повышение помехоустойчивости аппаратуры потребителей ГНСС, использованием дополнительных устройств – адаптивных антенно-приемных систем на базе антенных решеток, а также принятия соответствующих организационно-технических мероприятий для повышения надежности координатно-временного обеспечения критичных областей применения КВО.

Литература

[1] R.S. Littlepage. The Impact of Interference on Civil GPS // Proceedings ION GPS-98, - September 1998. – p. 821-828.

[2] Pinker, D. Walker, C.Smith. Jamming the GPS signal // Proceedings ION-98, - September 1998. – p. 829-837.

[3] S.V. Lyusin, L.B. Sazonov, I.G. Khazanov, A.S. Komarov. Combined GPS/GLONASS Receiver with High Antijamming Performance // Proceedings ION GPS-98. – September 1998. – p. 775-782.

[4] P. Ward. GPS Receiver RF Interference Monitoring, Mitigation and Analysis Technique // Journal of the Institute of Navigation, V. 41, № 4, 1994.

[5] S. Gilmore. The Impact of Jamming on GPS // Symposium on GPS Interference and Mitigation Technique held ay the Volpe National Transportation System Center, August 27, 1998.

[6] E.L. Key. Technique to Counter GPS Spoofing // International Memorandum, MITRE Corporation, February 17, 1995.

[7] L. Bond. Overview of GPS Interference Issues // GPS Interference Symposium – Volpe National Transportation System Center, Boston, August 27, 1998.

[8] B. Forssel, T.B. Olsen. Jamming Susceptibility of Some Civil GPS Receivers // GPS World, № 1, 2003, p. 54-58.

[9] B. Winer, et al., GPS Receiver Laboratory RFI Tests // Proceedings of the Institute of Navigation National Technical Meeting, Santa Monica, CA, January 22-24, 1996.

[10] S. Wallis. GPS Open Air Testing – Jamming at Woomera // Proceedings of 1999 Technical Meeting

& 19th Biennial Guidance Test Symposium, San Diego, January 25-27, 1999.

[11] G. Colby, et al. Test Results of the Joint FAA/DoD Investigation of GPS Interference // Proceedings of the 10th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-97, Kansas City, September, 1997.

[12] Report of the Commission to Address United States National Security Space Management and Organizations, January 11, 2001.

[13] John Hopkins University Applied Physics Laboratory // GPS Risk Assessment Study – Final Report, January 1999.

[14] Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System // A John Volpe National Transportation System Center Final Report, August 29, 2001.

[15] C. Rodgers. Development of a Low Cost PC Controlled GPS Satellite Signal Simulator // Proceedings of the 15th Biennial Guidance Test Symposium, Holloman AFB, New Mexico, 1991.

[16] US Department of Defense and US Department of Transportation, 1999 Federal Radio-navigation Plan, February 2000.

[17] Validated ICAO GNSS Standards and Recommended Practices (SARPS), November 2000.

[18] Minimum Aviation Performance Standards for the Automatic Dependent Surveillance Broadcast (ADS-B), RTCA DO-247, February 19, 1998.

[19] E. Batterline, S.L. Forge. GPS: Synchronizing Our Telecommunications Networks // Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-99, Nashville, September 14-17, 1999, pp. 597-605.

[20] Задорожный А.И., Соловьев Ю.А., Маркелов М.А., Гордиенко Д.Н. Авиационные применения спутниковых приемников в условиях помех, 3-я Международная конференция "Планирование глобальной радионавигации", Москва, 2000.

[21] Швець В.А. Експериментальні дослідження завадостійкості систем GPS [Текст] / В. А. Швець // Вісник інженерної академії України. – 2012. № 3-4. – С. 160 – 164.

[22] Сушіч О.П. Експериментальна оцінка впливу навмисних завад на апаратуру споживача глобальної навігаційної супутникової системи [Текст] / О.П. Сушіч// Вісник інженерної академії України . – 2012. № 3-4. С. 32 – 36.

[23] D. Gustafson, J. Dowdle, K. Flueckiger. A High Anti-Jam GPS-Based Navigator // Proceedings of the Institute of Navigation National Technical Meeting, Anaheim, CA, January 26-28, 2000, pp. 495-503

[24] S. Rounds. Jamming Protection of GPS Receivers // GPS World, February, 2004.

[25] Швець В.А Структурна схема завадостійкої антенної решітки навігаційних систем GPS, ГАЛІЛЕО, ГЛОНАСС [Текст] / В.А. Швець // Вісник інженерної академії України . – 2014. № 1. С.149 – 151.

[26] R. A. Monzingo, T. W. Miller. Introduction to adaptive arrays // SciTech Publishing, Inc. 2004.

УДК 004.056.5:629.056.8 (045)

Швець В. А. Необхідність захисту інформації глобальних навігаційних супутникових систем GPS, ГЛОНАСС, ГАЛІЛЕО

Анотація. *У статті розглядається проблема функціонування глобальних навігаційних супутникових систем в умовах ненавмисних і навмисних перешкод. Розглянуто вимоги до експлуатаційних характеристик глобальних навігаційних супутникових систем за видами транспортних систем. Розглянуто основні загрози глобальним навігаційним супутниковим системам. Ґрунтуючись на вимогах до експлуатаційних характеристик глобальних навігаційних супутникових систем, проведено аналіз їх вразливості при впливі навмисних і ненавмисних перешкод. Виділені найбільш вразливі експлуатаційні характеристики глобальних навігаційних супутникових систем (цілісність і доступність) Запропоновано метод зменшення вразливості глобальних навігаційних супутникових систем при впливі ненавмисних і навмисних перешкод.*

Ключові слова: *захист інформації, GPS, ГЛОНАСС, ГАЛІЛЕО, цілісність, доступність, загрози, антенні решітки.*

Shvets V. The necessity of global navigation satellite systems GPS, GLONASS, GALILEO information security

Abstract. *The paper considers the problem of the functioning of global navigation satellite systems in the conditions of unintentional and intentional interference. Considered the performance requirements of global navigation satellite systems by types of transport systems. The basic threat of global navigation satellite systems. Based on the performance requirements of global navigation satellite systems, the analysis of their vulnerability when exposed to intentional and unintentional interference. The most vulnerable operational performance of the global navigation satellite system (integrity, and availability). Proposed a method of reducing the vulnerability of global navigation satellite systems with impact unintentional and intentional interference.*

Keywords: *information security, GPS, GLONASS, GALILEO, integrity, availability, threats, antenna arrays.*

Отримано *07 травня 2014 року*, затверджено редколегією *28 травня 2014 року*