АНАЛИТИЧЕСКИЕ ИССЛЕДОВАНИЯ ЗАРУБЕЖНОГО ОПЫТА

УДК 623.764

АНАЛИЗ ТЕНДЕНЦИЙ УЯЗВИМОСТЕЙ GNSS И ОСНОВНЫЕ НАПРАВЛЕНИЯ СНИЖЕНИЯ УГРОЗ

© Авторы, 2019

Е.А. Лаврентьев *кандидат технических наук, доцент,*
зам. генерального директора – начальник ОКБ «ЛЭМЗ», ПАО «НПО «Алмаз», г. Москва
E-mail: srclav@rambler.ru
И.С. Вылегжанин *кандидат физико-математических наук,*
начальник СКБ, ПАО «НПО «Алмаз», г. Москва
E-mail: isv1980@yandex.ru
С.Ю. Нестеров *кандидат технических наук, доцент,*
зам. начальника ОКБ «ЛЭМЗ» – директор НПЦ-СПБ, ПАО «НПО «Алмаз», г. Санкт-Петербург
E-mail: nastserg@rambler.ru
Д.П. Шабанов
начальник отдела НПЦ-СПБ ОКБ «ЛЭМЗ», ПАО «НПО «Алмаз», г. Санкт-Петербург
Е.Н. Артемова
начальник бюро ОКБ «ЛЭМЗ», ПАО «НПО «Алмаз», г. Москва
E-mail: eartemova@lemz.ru

Рассматривается использование системы координатно-временного обеспечения как важной части функционирования многих современных систем. Определена роль глобальных навигационных спутниковых систем (GNSS) в транспортных и энергетических системах, в банковских технологиях, в системах телекоммуникаций, в средствах спасения, медицины и др. Проанализирована уязвимость GNSS от непреднамеренных и преднамеренных помех. Обозначены направления снижения уязвимости GNSS за счет применения систем ИФРНС в качестве дублирующих.

***Ключевые слова**: система координатно-временного обеспечения (КВО), глобальная навигационная спутниковая система (GNSS), ГЛОНАСС, GPS, непреднамеренная помеха, преднамеренная помеха, радиопротиводействие, радиодезинформация, импульсно-фазовая радионавигационная система (ИФРНС).*

The use of coordinate-time support system (CTS) is examined as an important part of many modern systems functioning. The role of global navigational satellite systems (GNSS) in transport and energy systems, banking technology, communications system, recovery aids, medicine etc. is determined. The GNSS vulnerability from unintended and intentional interference is analyzed. Directions for vulnerability reduction of GNSS are designated due to implementation of pulse-phase radio navigation system (PHRNS) as a redundant one.

***Keywords**: coordinate-time support system (CTS), Global Navigation Satellite System (GNSS), GLONASS, Global Positioning System (GPS), unintended interference, intentional interference (jamming), electronic countermeasures, spoofing, pulse-phase radio navigation system (PHRNS).*

Введение

Современный этап развития общества характеризуется всё более широким использованием систем координатно-временного обеспечения (КВО), составляющего основу эффективного

функционирования многих отраслей экономики и являющегося важнейшей частью современных систем управления войсками и высокоточным оружием.

Основу КВО составляют глобальные навигационные спутниковые системы (GNSS), которые представлены в настоящее время спутниковыми радионавигационными системами ГЛОНАСС (Россия) и GPS (США). Параллельно существующим, над совершенствованием собственных систем КВО работают Европейский Союз – GALILEO, Китай – проект региональной системы навигации BEIDOU, Индия – программа IRNSS, Япония – система QNSS и другие страны.

В 2006 году Индия приняла решение о создании собственной навигационной системы IRNSS. Все аппаратные средства системы разрабатываются только индийскими компаниями.

Использование глобального координатно-временного поля, создаваемого глобальной навигационной спутниковой системой (GNSS), 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.

Осуществляется широкомасштабное внедрение спутниковых навигационно-временных технологий в транспортные и энергетические системы, в банковские технологии, системы телекоммуникаций и различные типы систем управления, включая оборонные, а также средства спасения, медицины и других систем.

Вместе с тем, эйфория первых лет освоения спутниковых навигационно-временных технологий, нашедшая отражение в концепции использования GNSS в качестве единственного источника координатно-временной информации, начинает уступать место более трезвому подходу к перспективам использования GNSS [1].

Прежде всего, это обусловлено уязвимостью GNSS, при воздействии непреднамеренных и преднамеренных помех. Об уязвимости гражданских приёмников GNSS было известно давно, но её редко принимали во внимание их пользователи и изготовители.

В то же время, в «Руководстве по глобальной навигационной спутниковой системе (GNSS)» – издание 2013 года, в главе 5 «Уязвимость GNSS» отмечено, что предметом основной озабоченности является распространение устройств подавления, предназначенных для нарушения работы систем слежения за движущимися транспортными средствами.

«*Как отмечается в главе 7, в качестве составной части стратегии смягчения последствий при выходе из строя GNSS, рекомендуется использовать distance measuring equipmen (DME). Несмотря на то, что DME работает в той же полосе частот, что и GNSS, порог чувствительности DME к помехам значительно выше, чем у GNSS, так что помехи в совместно используемом диапазоне вряд ли окажут влияние на DME. Кроме того, маловероятно, что помеха в этой полосе частот сможет подавить все установки DME в пределах радиогоризонта воздушного судна*» [2–4].

«*Государства должны запрещать любые действия, приводящие к искажению сигналов GNSS. Ими должен быть разработан и соблюдаться свод жёстких нормативов, регламентирующих намеренное использование излучателей в пределах полосы частот, включая ретрансляторы сигналов GNSS, псевдоспутники, источники уводящих и подавляющих сигналов. Системы могут продолжать поддерживать режим работы в течение значительного периода времени, используя кварцевые часы, прежде чем потребуется новая коррекция времени GNSS, как это указано в п. 1.4.5 главы 1. В большинстве этих применений использование информации GNSS не является критическим фактором и приёмники сигналов времени используются вместе с другими системами предоставления временной информации, так что к ним не выдвигаются требования абсолютной точности. Самым серьёзным исключением является многопозиционный прием, который находится в критической зависимости от наличия времени GNSS*» [5].

Одним из наиболее важных и своевременных отчётов об исследованиях в области уязвимости GPS был отчёт Центра Волпе (*John A. Volpe National Transportation Systems Center*) – Национального центра транспортных систем и логистической экспертизы, работающего под управлением Министерства транспорта США [6].

В выводах центра 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 серьёзные последствия для экономики и окружающей среды. В отчёте также сделан вывод о том, что растущее использование GPS в гражданской

инфраструктуре делает её всё более привлекательной мишенью для враждебных действий отдельных личностей и групп. В то же время, в отчёте отмечается масштабная коммерческая доступность оборудования для постановки помех и активного вмешательства в процессы функционирования не только систем спутниковой навигации, но и всех систем, их использующих.

Только факты

Полная эксплуатационная готовность GPS была объявлена в 1993 году, и в ряде государств в этом же году были выданы разрешения на использование GPS. В 2001 году ИКАО приняла SARPs (*Standards and Recommended Practices*) для обеспечения полётов с применением GNSS и использованием дополнений к сигналам основных спутниковых созвездий для выполнения требований по безопасности и надёжности. Это отмечено в Руководстве по глобальной навигационной спутниковой системе [7].

Но уже в период бомбардировок Югославии в 1999 году, а также в период войн в Персидском заливе с 1991 по 2003 годы, Министерство обороны США осуществляло манипуляции с сигналами GPS, искусственно загрубляя «гражданский канал» для снижения точности позиционирования [8].

В августе 2008 года в ходе проведения операции в Южной Осетии артиллеристы группировки войск РФ столкнулись с фактом ошибок местоопределения целей с помощью навигационных приёмников на 100 и более километров от истинных координат.

В марте 2016 года власти Южной Кореи заявили о сбоях в работе GPS-систем в районах, прилегающих к КНДР. От этих действий пострадало значительное количество навигационных систем транспортных средств Южной Кореи, включая суда, автомобили и самолёты. В общей сложности сбои были зарегистрированы в течение шести дней. Воздействию подверглись около 1 700 самолётов и 700 судов [9].

Это был не первый случай подобных действий КНДР. Несколько лет назад Международный союз электросвязи, изучив ситуацию, признал правоту обвинений Южной Кореи в адрес Северной и вынес предупреждение КНДР.

Серия инцидентов со сбоями действия GPS-систем заставила южнокорейских инженеров задуматься над альтернативами американской сети. В итоге было создано устройство, которое принимает сигналы и от альтернативных систем, включая российские и китайские спутники, что позволяет обеспечить бесперебойное поступление сигнала [10, 11]. В публикациях тех лет практически отсутствуют сведения о причинах действий Северной Кореи по подавлению сигналов GPS. Ежегодно, как правило, весной проводятся совместные военные учения Соединённых Штатов и Южной Кореи у границ Северной Кореи. На учениях задействуется, в том числе, и стратегическая авиация.

Таким образом, в ряде случаев стремление отдельных стран к достижению локальных военно-политических целей приводит к искажению навигационных полей, что влечёт опасные последствия для полётов гражданской авиации, морского (речного) судовождения и использования наземных транспортных средств. Подобная тенденция разрушает Международное воздушное право и порождает массу опасных неопределённостей.

В этой связи случаи отключения GPS-навигации над зоной Черного моря и воздушного пространства Украины, начиная с весны 2014 года, ещё раз подтверждают целенаправленные действия США по блокированию определённой зоны для приёма сигналов навигационных спутников. Российские пилоты снова сообщают о сбоях GPS – теперь уже над территорией РФ.

Первое сообщение о сбое в работе системы GPS над Украиной поступило 24 апреля 2014 года от экипажа лайнера А321, следовавшего по маршруту Стамбул – Москва [12].

За 96 км от Днепропетровска они зафиксировали сбой в работе бортового GPS оборудования. Сразу после пересечения границы с Россией работа системы полностью восстановилась. Новые случаи были также зафиксированы пилотами «Аэрофлота» в ночь с 29 на 30 апреля.

29 апреля 2014 Росавиация предупредила авиакомпании о необходимости быть готовыми использовать «инерциальные системы, VOR/DME и другие». О полноценной эксплуатации ГЛОНАСС речь не шла, так как соответствующим оборудованием оснащены в основном российские самолёты *Sukhoi Superjet* 100. Росавиация также попросила фиксировать все случаи отказа систем и информировать её для выработки дальнейших действий [13].

В последнее время всё чаще приходят новости о том, что в том или ином месте перестал работать ГЛОНАСС. В российской спутниковой навигационной системе 2 апреля 2014 года

произошел сбой, из-за которого более чем 10 часов пользователи по всему миру получали неверные данные о своих координатах. Сбой был вызван так называемым «человеческим фактором» – ошибкой в передаче на спутники неверных эфемерид, то есть проблемой в математическом обеспечении деятельности группировки.

Как отмечал PC *World* со ссылкой на Дрю Дэвиеса (*Drew Davies*) из канадской компании *Rx Networks*, специализирующейся на навигационных сервисах, проблема с неверными данными ГЛОНАСС наблюдалась во всём мире.

Собеседник «Интерфакса» рассказал, что ошибка одновременно возникла почти на всех аппаратах, после чего на сайте Информационно-аналитического центра Роскосмоса спутники были обозначены как передающие неверные эфемериды.

В конце января 2016 года в системе GPS произошел сбой из-за отсутствия сигнала Всемирного координированного времени в течение 13 микросекунд. Возникли проблемы в навигационном оборудовании и системах связи по всему миру [14].

Инцидент произошел сразу после того, как Военно-воздушные силы США вывели из состава группировки самый старый спутник SVN 23 для его последующей замены на GPS *Block* IIF. В ходе процедуры в программном обеспечении, используемом в наземной инфраструктуре GPS, произошёл сбой, в результате которого на 13 микросекунд произошло отключение передаваемого GPS-спутниками сигнала Всемирного координированного времени (UTC).

Проблема не была ограничена устройствами одного конкретного производителя. «*Она коснулась всех GPS-устройств, вне зависимости, был ли это приёмник по последнему слову техники или аппаратура, функционирующая 25 лет*», – отметил Чарльз Карри (*Charles Curry*), управляющий директор британской компании *Chronos Technology*, выпускающей оборудование для синхронизации времени.

По словам Карри, сразу после задержки сигнала к ним на пульт с вопросом «*У нас проблема. Что произошло?*» позвонил каждый клиент, которого обслуживает *Chronos* – а это телекоммуникационные, энергетические компании и военные ведомства.

Дело в том, что все они используют данные о времени со спутников GPS в своей работе. Например, телекоммуникационные компании пользуются этой информацией для управления потоками трафика в своих сетях, поясняет BBC.

Временной сбой, приведший к проблемам оборудования, прошёл глобально по всему миру в разное время со смещением, соответствовавшим тому, как спутники GPS двигались вдоль своих орбит. «*Он как бы проехал по всему миру*, – сказал Карри. – *Но если вы находились в эпицентре, длительность сбоя составила около 12 часов*».

Карри не уточнил, как в результате сбоя повели себя потребительские устройства. Что же касается операторов связи, то их оборудование стало выдавать предупреждения обслуживающему персоналу, причём количество этих предупреждений увеличивалось по нарастающей. Во многих случаях избежать более серьёзных последствий помогли резервные системы синхронизации времени.

В декабре 2017 столичные автомобилисты вновь начали жаловаться на сбои в работе GPS в центре Москвы. По словам таксистов, им приходится использовать сразу несколько геолокационных сервисов, чтобы понять, где именно они находятся. Некоторые из них сообщили о некорректном расчёте длительности пути в *Uber* – они недополучают деньги из-за того, что система посчитала, что они проехали меньше фактического расстояния [26].

В данном разделе приведены лишь отдельные факты из обширной статистики уязвимостей GNSS в различных регионах мира на авиационном транспорте и в других областях человеческой деятельности.

Сама концепция создания системы и проблемы в её эксплуатации разными провайдерами подразумевает серьёзные, скоординированные вложения ресурсов, с учётом наземных и космических функциональных дополнений GNSS в интересах повышения надёжности системы, расширения её возможностей в предоставлении аэронавигационных услуг требуемого качества с установленной вероятностью.

В условиях стремительной трансформации мировой экономики, санкционных и экономических войн государств, а также снижения порогов военной эскалации, надеяться на согласованные совместные действия участников процесса в совершенствовании и развитии системы GNSS в обозримом будущем весьма проблематично.

Анализ уязвимостей GNSS

Таким образом, уязвимость GNSS при воздействии непреднамеренных и преднамеренных помех является в настоящее время общепризнанным фактом. Эта уязвимость в равной мере относится к GPS, ГЛОНАСС, GALILEO, и другим системам, поскольку принципы их построения и используемые диапазоны частот достаточно близки. В настоящее время радионавигационное сообщество активно обсуждает проблемы уязвимости GNSS и поиска путей противодействия непреднамеренным и умышленным воздействиям на систему. В связи с этим, представляется необходимым проанализировать на основе имеющихся данных основные источники непреднамеренных помех, возможные способы постановки преднамеренных помех аппаратуре потребителей GNSS и перспективы повышения надёжности координатно-временного обеспечения в условиях помехового воздействия.

Критичные применения GNSS-технологий, требующие принятия мер по защите от 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 надёжности 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. Это относится ко всем видам транспортных систем и систем телекоммуникаций, использующих сигналы GNSS и в первую очередь к авиации. Приведём краткий анализ, касающийся уязвимости этих применений 15, 27].

Авиация

Требования к эксплуатационным характеристикам GNSS применительно к гражданской авиации в соответствии с рекомендациями ICAO приведены в табл. 1.

Таблица 1

Требования к эксплуатационным характеристикам GNSS

Операция	Точность (95 %)	Целостность	Непрерывность	Предельное расстояние для тревоги	Время тревоги	Доступность
Полёт над океаном	12.4 мор. миль	$1–10^{-7}$/час	$1–10^{-5}$/час	4.0 мор. миль	2 мин.	от 0.99 до 0.9999
На маршруте	2.0 мор. миль	$1–10^{-7}$/час	$1–10^{-5}$/час	2.0 мор. миль	1 мин.	от 0.99 до 0.99999
Зона аэропорта	0.4 мор. миль	$1–10^{-7}$/час	$1–10^{-5}$/час	1.0 мор. миль	30 с	от 0.99 до 0,99999
NPA	220 м	$1–10^{-7}$/час	$1–10^{-5}$/час	0.3 мор. миль	10 с	от 0.99 до 0.99999
APV I	220 м (H) 220 м (V)	$1–2·10^{7}$/заход	$1–8·10^{-6}$/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)	$1–2·10^{7}$/заход	$1–8·10^{-6}$/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)	$1–2·10^{7}$/заход	$1–8·10^{-6}$/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)	$1–1·10^{9}$/заход 15 с	$1–4·10^{-6}$/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)	$1–1·10^{9}$/заход 15 с	$1–2·10^{-6}$/30 с (L) $1–2·10^{-6}$/15 с (V)	15.5 м (H) 5.3 м (V)	1 с	от 0.99 до 0.99999

Анализ данных, приведённых в табл. 1, показывает, что высокие требования, предъявляемые авиацией к GNSS, позволяют использовать спутниковые навигационные системы в качестве первичного средства для полётов над океаном и в качестве дополнительных систем для полётов в зоне аэропорта, включая грубый и точный заход на посадку (с использованием

функциональных дополнений). Вместе с тем в качестве вспомогательного средства GNSS не может быть единственной навигационной системой на борту самолёта, учитывая возможность ухудшения характеристик сигналов GNSS или их потери при воздействии помех [16].

Телекоммуникационные системы

В настоящее время использование сигналов GNSS в телекоммуникационных системах возросло до такой степени, что GNSS стала играть критичную роль с точки зрения обеспечения временной синхронизации. В настоящее время это наиболее частый способ достижения высокоточной синхронизации многочисленных систем и средств дешёвыми способами.

Требования к синхронизации сетей связи и к иерархии часов в телекоммуникационных системах приведены в табл. 2 и 3 соответственно.

Таблица 2

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 3

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

Приведённые в этих таблицах данные свидетельствуют о том, что характеристики телекоммуникационных служб, опирающихся на GNSS, могут быть существенно ухудшены или полностью утрачены в случае ухудшения или потери сигналов GNSS. Это может стать фатальным для чувствительных к временной синхронизации систем и средств, обеспечивающих безопасность при использовании воздушного пространства различными пользователями, в судовождении, в транспортировке опасных грузов и телекоммуникации.

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

– точные и грубые заходы на посадку воздушных судов;

– 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;

– системы энергетики и объекты Министерства обороны.

Непреднамеренные помехи

Основной причиной уязвимости GNSS является низкая мощность сигнала. Так, для GPS она составляет всего 10^{-16} Вт или 160 дБ/Вт на поверхности Земли для сигналов С/А-кода – гражданский дальномерный код (1 мс) в диапазоне L1. Непреднамеренные помехи можно подразделить на естественные помехи и помехи искусственного происхождения. Маломасштабные флуктуации электронной концентрации в ионосфере, воздействуя на сигнал GNSS, приводят к изменяющейся задержке распространения сигнала за счёт изменения диэлектрической проницаемости среды. Групповая задержка в первом приближении обратно пропорциональна квадрату частоты. Поэтому применение двухчастотного приёмника позволяет существенно снизить воздействие ионосферы. В периоды солнечной активности, например, при вспышках, погрешности по дальности у одночастотных приемников могут достигать 20 м, тогда как двухчастотные приёмники могут измерять и исключать эти погрешности [17].

К непреднамеренным помехам искусственного происхождения относятся излучения радиопередатчиков, могущие создать сигналы с нежелательным уровнем мощности в L-диапазоне. Идентифицированные искусственные непреднамеренные помехи (см. табл. 4) создаются радиолиниями, гармониками телевизионных каналов, сигналами запроса систем ближней навигации, гармониками существующих УКВ радиостанций, спутниковой связной системой GLOBALSTAR, радиолокационными станциями системы управления воздушным движением [18, 19].

Таблица 4

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**
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 GNSS. К преднамеренным помехам следовало бы также отнести любые действия, направленные на нарушение функционирования GNSS, включая атаку на спутники и наземную инфраструктуру управления [19]. По-видимому, преднамеренные помехи направлены в первую очередь против средств вооружённой борьбы. В этой ситуации гражданские потребители в критичных областях деятельности, являясь невинно пострадавшей стороной, тем не менее, должны быть готовы к защите от подобных действий [20].

К числу преднамеренных помех следует отнести радиопротиводействие и радиодезинформацию. Радиопротиводействие – это радиоизлучение сигналов достаточной мощности и с характеристиками, которые позволяют мешать приемникам GNSS отслеживать спутниковые сигналы в определённом регионе. При этом 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 GNSS самых разных размеров, различной выходной мощности и различной стоимости. Небольшие лёгкие недолговечные постановщики помех мощностью от 1 до 100 Вт могут стоить менее 1 000 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 приёмник GNSS осуществить привязку к ложным сигналам, похожим на штатные, и медленно сойти с заданного направления так, чтобы прошёл достаточно большой отрезок времени до обнаружения постороннего вмешательства. Одним из приёмов радиодезинформации является приём: задержка и переизлучение радионавигационных сигналов для введения в заблуждение потребителя.

Методы уменьшения уязвимости GNSS при воздействии непреднамеренных и преднамеренных помех

В «Руководстве по глобальной навигационной спутниковой системе (GNSS), Doc 9849 AN/457» [21] в статье 7.15.2 определено, что «Государства должны иметь планы действий в чрезвычайных обстоятельствах на случай международного конфликта или подавления сигналов GNSS соседним государством таким образом, что это приводит к нарушению обслуживания за пределами государства, являющегося источником помехи. Вопросы безопасности GNSS рассматриваются в некоторых государствах, и в результате этого могут появиться новые процедуры защиты безопасности и эффективности полётов воздушных судов».

Далее, в статье 7.16.2 отмечается: «Поставщики АНО и регулирующие органы должны взаимодействовать с эксплуатантами с целью определения технических решений и видов обслуживания, которые будут удовлетворять условиям безопасности и экономической целесообразности».

Исходя из анализа воздействия помех на функциональные свойства GNSS, а также следуя рекомендациям ICAO, преодоление уязвимости GNSS от помех может быть достигнуто следующими способами:

– разработкой требований к помехоустойчивости навигационной аппаратуры потребителей (НАП) и обязательной сертификацией этой аппаратуры на соответствие этим требованиям для критичных областей применения;

– организационными мероприятиями – обучением персонала критичных применений правилам обнаружения некорректного функционирования НАП и порядку использования резервных систем и эксплуатационных процедур;

– своевременным информированием оперативных служб о фактах обнаружения помех;

– жёстким регулированием со стороны государства соблюдения установленных норм на радиоизлучения, представляющие потенциальную помеховую опасность для сигналов GNSS, в соответствии с «Руководством по глобальной навигационной спутниковой системе (GNSS), Doc 9849 AN/457»;

– принятием специальных мер для повышения помехоустойчивости средств и систем GNSS при их проектировании;

– использованием дублирующих средств, систем и эксплуатационных процедур.

Достаточно эффективным способом уменьшения уязвимости GNSS при воздействии непреднамеренных помех является планируемое увеличение мощности сигналов, излучаемых спутниками, и введение новых гражданских сигналов в диапазонах L2 и L5 для GPS и F3 для ГЛОНАСС [22, 23].

Методы повышения помехоустойчивости наземных аппаратных средств достаточно хорошо изучены и могут быть следующими:

– создание специальных схем и алгоритмов подавления помех (оптимизация радиочастотной части, устройств преобразования «аналог-цифра» и канальных алгоритмов для вычисления отношения «сигнал/шум», адаптивной регулировки порога при вхождении в режим слежения, частотно-временная режекция);

– использование управляемой пространственной избирательности многоэлементных антенных систем;

– использование сигналов различных GNSS (ГЛОНАСС, GPS, GALILEO);

– использование информации автономных и других систем на борту подвижных средств для повышения помехоустойчивости следящих систем приёмников GNSS – снижения предельно допустимого отношения «сигнал/шум».

Вместе с тем, следует признать, что указанные методы ведут к довольно значительному удорожанию НАП, поэтому их использование является целесообразным в наиболее ответственных случаях и в специальной аппаратуре.

К числу наиболее эффективных дублирующих систем могут быть отнесены:

– автономная (инерциальная) система навигации подвижных объектов, комплексированная с аппаратурой потребителей GNSS;

– псевдоспутники, работающие на частотах, отличных от частот GNSS;

– радионавигационные системы дальнего действия «Лоран-С»/ «Чайка»;

– инструментальные системы посадки самолётов гражданской авиации ILS и системы посадки MLS, бортовые системы полёта по приборам VOR/DME.

Использование систем ILS, MLS, VOR/DME будет ещё в течение длительного периода времени целесообразным и необходимым для обеспечения грубого и точного захода на посадку воздушных судов до создания и развёртывания функциональных дополнений для этих целей в необходимых количествах. Системы радиолокационного обеспечения: ПРЛ, ВРЛ, средства госопознавания – будут выполнять главную функцию обеспечения безопасности полётов авиации в условиях военных угроз как элементы двойного назначения.

Использование псевдоспутников позволяет реализовать дополнительное преимущество, заключающееся в повышении надёжности навигационных определений в местах затруднённого приёма сигналов GNSS за счёт оптимального их расположения. С другой стороны, использование псевдоспутников имеет ряд недостатков:

– аппаратура потребителей в этом случае может быть более сложной;

– при широком использовании аппаратуры потребителей потребуется разнесение частот псевдоспутников с частотами навигационных спутников во избежание поражения обеих частот одновременно;

– потребуется решить ряд обычных проблем связанных с многолучевым приёмом и распространением.

Радионавигационные системы дальней навигации с наземным базированием передающих станций

Импульсно-фазовые радионавигационные системы (ИФРНС) «Лоран-С» и «Чайка» можно считать наиболее предпочтительными кандидатами на роль дублирующих систем по следующим причинам:

– сигналы этих систем имеют значительно более высокую мощность, чем сигналы GNSS, и могут быть использованы любыми типами потребителей при наличии интегрированного приёмника GNSS/ИФРНС;

– в интегрированном приёмнике осуществляется постоянная калибровка канала ИФРНС по сигналам GNSS. Поэтому при кратковременном отказе спутникового канала точность навигационных определений практически остаётся неизменной;

– имеется возможность надёжных навигационных определений в местах затруднённого приёма сигналов GNSS (в лесах, в горных ущельях, в городских условиях, в тоннелях и т.д.);

– системы «Лоран-С» и «Чайка» с использованием технологии Еврофикс или аналогичной могут осуществлять передачу дифференциальных поправок потребителям GNSS без нарушения основной навигационной функции, имея возможность при этом осуществлять мониторинг целостности GNSS [24].

Что касается уязвимости ИФРНС при воздействии естественных непреднамеренных помех, то эти системы уязвимы к ним в такой же степени, как и GNSS. Например, воздействие северных полярных сияний способно полностью блокировать работу ИФРНС. Ситуация несколько упрощается в отношении непреднамеренных помех искусственного происхождения. Имеется полный перечень жёстко регламентированных источников радиочастотных излучений в этом диапазоне, по крайней мере в Европе, что существенно упрощает принятие мер по преодолению их влияния при проектировании НАП ИФРНС. Представляется весьма маловероятным существование несанкционированных радиопередатчиков, работающих в диапазоне частот 50–150 кГц.

Как и в случае GNSS, использование преднамеренных помех ИФРНС можно определить как радиопротиводействие и радиодезинформацию. Наиболее опасными преднамеренными помехами следует признать синхронные синусоидальные помехи. Борьба с ними в случае ИФРНС значительно упрощается более эффективным построением режекторных фильтров, чем в случае GNSS. В настоящее время без особых затрат можно реализовать программным путём до 30 фильтров и более.

Самым изощрённым способом постановки помех ИФРНС является многокомпонентная спектральная помеха, содержащая все спектральные составляющие, излучаемые конкретной передающей станцией ИФРНС. Разработка такого постановщика помех доступна, по-видимому, только профессиональным разработчикам, и в настоящее время нет достоверных сведений о таких разработках. Вместе с тем, следует признать, что постановщики синхронных и многокомпонентных помех могут иметь мощность порядка десятков ватт для нарушения нормальной работы аппаратуры потребителей на расстояниях нескольких десятков километров, хотя такие действия представляются маловероятными.

В отношении радиодезинформации следует отметить, что для создания в рабочей зоне ИФРНС дезинформирующей помехи, способной нарушить нормальную работу приёмника, требуется обеспечить излучение сигнала с параметрами, идентичными сигналу одной из станций, которая подвергается атаке, то есть:

– пиковая мощность радиоимпульсов, излучаемых постановщиком помех, должна быть сравнима с пиковой мощностью сигналов поражаемой станции;

– формат сигнала (форма импульсов, структура фазового кода, период следования радиоимпульсов в пакете и период следования пакетов радиоимпульсов) должен совпадать с форматом сигнала, используемого в данной цепи ИФРНС;

– должна быть обеспечена высокая стабильность ложного излучаемого сигнала во времени.

Оценки показывают, что для создания эффективной помехи для станции ИФРНС с пиковой излучаемой мощностью 800 кВт в регионе с радиусом действия 100 км на удалении 500 км от передающей станции потребуется передатчик с мощностью 100…200 кВт. Конечно, такую операцию оперативно и скрытно провести практически невозможно.

Выводы

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

2. Имеется ряд критичных применений систем координатно-навигационного обеспечения, в которых целесообразно комплексное использование всех доступных средств для обеспечения безопасности воздушного движения и национальной безопасности страны.

3. Средства снижения уязвимости GNSS при воздействии непреднамеренных и преднамеренных помех предполагают повышение помехоустойчивости аппаратуры потребителей GNSS, использование дополнительных систем и резервных эксплуатационных процедур, а также принятие соответствующих организационно-технических мероприятий для повышения надёжности координатно-временного обеспечения.

4. Одной из наиболее перспективных дублирующих систем являются ИФРНС «Лоран-С»/ «Чайка». Система позволяет реализовать: дополнительные функции по передаче дифференциальных поправок потребителям GNSS, осуществить функции мониторинга целостности спутниковой группировки; обеспечить приём сигналов в труднодоступных местах из-за существенно большей устойчивости к воздействию преднамеренных помех [25].

5. В условиях опережающей динамики развития средств вмешательства в нормальную работу систем координатно-навигационного обеспечения, а также низкой эффективности пресечения фактов незаконного использования средств радиопротиводействия, представляется целесообразным создание и внедрение в систему ОрВД специальных средств контроля помехового фона с целью определения уровня угроз.

6. При составлении радиочастотного плана, особое внимание уделять взаимному влиянию радиосредств и использованию частотного ресурса во избежание воздействия преднамеренных помех. Перевод различных систем наблюдения, которые должны дополнять и дублировать друг друга на один частотный стандарт, недопустим.

Таким образом, успешное решение проблем уязвимости системы GNSS лежит в плоскости комплексного и системного использования всех видов оборудования обеспечения безопасности воздушного движения с эффективным использованием частотного ресурса и гибких процедурных технологий.

ЛИТЕРАТУРА

1. ***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.
2. *Guidance Material for Design of Terminal Procedures for Area Navigation* (DME/DME, B-GNSS, Baro-VNAV & RNP-RNAV.ATM – Организация воздушного движения. Doc 4444, изд. 14-е, Монреаль, ICAO, 2001.
3. **Нудельман Г.С., Оганесян А.А., Харисов В.Н.** Уязвимость систем синхронизации, основанных на использовании глобальных навигационных спутниковых систем // ОАО «ВНИИР», ОАО «ВНИИР-Прогресс», Россия, Екатеринбург, 3 – 7 июня 2013.
4. **Аль-Рубой Мудар Валхан Хамид**. Развитие глобальной навигационной спутниковой системы (GNSS). Обеспечение навигационных требований в особых условиях функционирования средств радиотехнического обеспечения полетов на примере республики Ирак. Навигация и управление воздушным движением (технические науки). Автореферат диссертации на соискание учёной степени кандидата технических наук, Санкт-Петербург – 2016.
5. Doc 9849, ICAO. Руководство по глобальной навигационной спутниковой системе (GNSS). Номер заказа: 9849 ISBN 978-92-9249-348-6 Издание второе, 2013.
6. *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, A John Volpe National Transportation System Center Final Report, August* 29, 2001.
7. Doc 9849, ICAO. Руководство по глобальной навигационной спутниковой системе (GNSS). Номер заказа: 9849 ISBN 978-92-9249-348-6 Издание второе, 2013.
8. *URL: https://docplayer.ru/63344378-Vo-vremya-operaciy-ssha-i-anglii-v-irake-a-takzhe-reshitelnoy-cifrovye-antennye-reshetki-resheniya-zadach-gps-svyaz-i-telekommunikacii.html*.
9. *URL: https://rg.ru/2016/04/23/v-iuzhnoj-koree-sozdali-navigacionnuiu-sistemu-s-pomoshchiu-sputnikov-rf.html*.
10. *Validated ICAO GNSS Standards and Recommended Practices (SARPS), November* 2000.
11. **Иванов М.П., Кашинов В.В.** Экспериментальная проверка помехозащищенности GPS // VII международная конференция «Радиолокация, навигация, связь» 24-26 апреля 2001, Воронеж, Россия.
12. *URL: https://www.vesti.ru/doc.html?id=1529388&cid=9*.
13. Информация по безопасности полётов №7, 21 ноября 2011 года // телеграмма Росавиации от 25.04.2014, №251225.
14. *URL: http://www.cnews.ru/news/top/2016-025_sboj_v_gps_dlitelnostyu_13_mikrosekund_vyzval.*
15. Радионавигационный план Российской Федерации (утверждён приказом Минпромторга России от 28 июля 2015 года №2123). Уязвимость спутниковых навигационных систем при воздействии непреднамеренных и преднамеренных помех и перспективы повышения надежности координатно-временного обеспечения.
16. *EUROCAE ED 75. Minimum Aviation System Performance Standards (MASPS) for Required Navigation Performance for RNP Area Navigation. Global positioning system. Standard Positioning Service. Performance Standard. Department of Defense USA. Washington*. DC 20301-6000, *October*. 2001.
17. ***Smith A.M., Mitchell C.N., Watson R.J., Meggs R.W., Kintner P.M., Kauristie K., Honary F.*** *Global navigation satellite system. Certification requirements for the equipment GRAS, GBAS GPS scintillation in the high Arctic associated with an auroral arc. – Space Weather*, 2008, V.6. – P.S03D01.
18. Журнал «Новости навигации», №1, 2004.
19. **Дятлов П.А., Кульбикаян Б.Х.** Радиоэлектронная борьба со спутниковыми радионавигационными системами. – Радио и связь, 2004. – 226 с. – ISBN 5-256-01750-0.
20. **Кащеев А.А., Кошелев В.И.** Оценка эффективности подавления сигналов спутниковых радионавигационных систем преднамеренными помехами // Журнал радиоэлектроники. – 2012, №7. – *URL: http://jre.cplire.ru/jre/jul12/7/text.html, 20 March, 2017. Russian*.
21. Doc 9849. Руководство по глобальной навигационной спутниковой системе (GNSS). Номер заказа: 9849 ISBN 978-92-9249-348-6.
22. ICAO AN-Conf/13-WP/15 18/05/18. Рабочий документ тринадцатой аэронавигационной конференции Монреаль. Пункт 2 повестки дня. Содействие развитию глобальной аэронавигационной системы. Комплексная стратегия в области CNS и спектра. Развитие глобальной навигационной спутниковой системы (GNSS) Канада, 9–19 октября 2018 года.
23. Понижение степени уязвимости глобальной навигационной спутниковой системы. Рабочий документ ICAO. Ассамблея — 38-я сессия. Техническая комиссия, пункт 3.5 повестки дня. Поддержка внедрения. Монреаль, 2013.
24. Журнал «Новости навигации», №1, 2004.
25. Интегрированные инерциально-спутниковые системы: сб. ст. и докл. // сост. О.А. Степанов, под общ. ред. В.Е. Пешехонова. – ГНЦ РФ ЦНИИ «Электроприбор», Санкт-Петербург, 2001.
26. Проблемы ГЛОНАСС. Технические аспекты. URL: http://rnd.cnews.ru/tech/news/top/index_science.shtml?2011/10/11/245300.
27. Шантель Дюбуа, Ограничения спутниковой навигации: проблемы GPS в Арктике. (*Chantelle Dubois. The Limits of Satellite Navigation: GPS Challenges in the Arctic*), 16 сентября 2018.

GNSS VULNERABILITY TRENDS ANALYSIS AND MAIN DIRECTIONS FOR THREAT REDUCTION

E.A. Lavrentiev, I.S. Vilegzhanin, S.U. Nesterov, D.P. Shabanov, E.N. Artemova

The article designates an important role of coordinate-time support systems (CTS) and global navigational satellite systems (GNSS) as a main component of CTS in all spheres of modern society.

At the same time, the GNSS vulnerability from unintended and intentional interference is underlined. A set of facts proving the GNSS vulnerability is performed.

The GNSS vulnerability is analyzed. An estimation to critical application of navigation-time technologies requiring protecting form interference influence (aviation, telecommunications etc.) was given. The definition to unintended and intentional interference was described. The intentional interference classification for electronic countermeasures and spoofing was represented, its brief description and proposals for GNSS vulnerability reduction from different interference types were performed.

The pulse-phase radio navigation systems (PHRNS) were considered as the most preferable ones for GNSS systems redundancy. It's noted that PHRNS are more persistent to unintended interference.

The articles concludes the effect of interference of different types on all radio navigational systems, the necessity to provide additional actions to decrease the vulnerability of navigational systems was emphasized. An advanced systems, redundant the GNSS, were underlined; an importance of introduction of jamming background control means into air traffic management system was pointed out. The significance of issues elaboration for mutual influence of radio aids and utilization of spectrum was emphasized, i.e. it's necessary to organize an integrated and system usage of all types of equipment in air traffic safety ensuring.

Поступила 1 июля 2019 года.