УДК 623.624.2

МЕТОДЫ РАДИОЭЛЕКТРОННОЙ БОРЬБЫ В ОБЛАСТИ КОСМИЧЕСКОЙ НАВИГАЦИИ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОСМИЧЕСКИХ АППАРАТОВ

Р. Б. Ковалёв

АО «Информационные спутниковые системы» им. академика М. Ф. Решетнёва», г. Железногорск, Красноярский край, Российская Федерация

Основным элементом содержания радиоэлектронной борьбы является нарушение радиообмена между радиоэлектронными средствами передачи информации путем постановки помех и фальшцелей. Вплоть до начала Второй мировой войны оно осуществлялось в отдельных средствах с помощью маскирующих помех. Для борьбы с первыми радиоэлектронными средствами извлечения информации (радиолокационными станциями) были разработаны эффективные приемы постановки пассивных помех, имитирующие реальные объекты и способствующие навязыванию противнику ложной информации. С развитием и совершенствованием средств радиоэлектронной борьбы открылись перспективы воздействия на радиоэлектронные средства дезинформирующими активными помехами, и даже если удается отфильтровать истинную информацию от ложной, наличие последней иногда значительно осложняет оценку обстановки в ходе боевых действий. Кроме того, воздействие на современную радиоэлектронную систему, имеющую в своем составе ЭВМ, может осуществляться внедрением по радиоканалу правдоподобных информационных сообщений, содержащих компьютерные вирусы, которые проникают по сети ЭВМ, вплоть до высших органов управления войсками и оружием. Наряду с этим массированное применение средств постановки помех в локальном районе приводит к изолированию таких радиоэлектронных средств от других. Наконец, современные средства радиоэлектронной борьбы, используя не только маскирующие, но и искажающие, дезинформирующие, блокирующие помехи, позволяют дезорганизовывать функционирование радиоэлектронных средств в глобальном масштабе, а реализация организационно-технических мероприятий по постановке различных помех способствует нарушению функционирования как локальных группировок радиоэлектронных средств, так и крупномасштабных радиоэлектронных систем.

Ключевые слова: помеха, приемник, орбита, защита, радионавигационный сигнал, мощность, навигационная аппаратура, радиоэлектронная борьба.

По мере все более широкого применения навигационной аппаратуры потребителей (НАП) различного назначения к ней растут требования по обеспечению высокой надежности и помехозащищенности, в том числе защиты как от мощных маскирующих помех (МП), так и от ложных имитационных помех (ИП), подобных реальным навигационным сигналам (НС).

Помехи создают на входе НАП фон, который затрудняет обнаружение радионавигационных сигналов орбитальной группировки и оценивание их параметров. Задача имитирующих помех другая – они должны заменить истинные, излученные спутником НС, ложными так, чтобы обнаружитель системы слежения и определения координат приемника не заметил подмены. Цель такой имитации – дезинформация противника относительно истинного местоположения. Простая дезинформация приводит к тому, что истинное местоположение заменяется некоторым случайным местоположением. Более амбициозная задача – управлять противником путем специального задания ему ложного маршрута [4].

Очевидны преимущества имитационных помех:

1. При воздействии ИП противник вообще не подозревает о том, что подвергся нападению, и, следовательно, не предпринимает ответных действий. В отличие от этого при выявлении МП у него есть возможность прибегнуть к целому ряду защитных действий:
   - отказаться от навигации по глобальным спутниковым навигационным системам и исполь-

DOI: 10.26732/2225-9449-2017-3-139-143

зовать автономные навигационные системы, такие как инерциальная навигационная система или магнитный компас;
- осуществлять подавление широкополосных МП с помощью адаптивной антенной решетки (ААР), узкополосных МП на основе алгоритмов спектральной режекции, импульсных МП – временной режекцией;
- принять организационные меры по физическому уничтожению источников помех.

2. Мощность принимаемой ИП принципиально должна не слишком отличаться от мощности принимаемого навигационного сигнала *S*, т.е. отношение помеха/сигнал $J/S \approx 0…20$ дБ. Для МП это отношение должно составлять $J/S \approx 50…60$ дБ, а для НАП с ААР еще больше: $J/S > 90$ дБ. Следовательно, энергетический выигрыш ИП относительно МП огромен и составляет 30…60 дБ или 70…90 дБ для НАП с ААР.
3. Основным средством защиты от помех в НАП является ААР, которая осуществляет подавление помех, мощность которых превышает уровень внутренних шумов приемника. Так как мощность ИП сопоставима с мощностью реального сигнала (уровень шумов), то ИП проходит через ААР без ослабления.

Преимущества ИП относительно МП, приведенные выше, столь значительны, что вызывают постоянный интерес к возможностям и методам создания и применения ИП. Пристальное внимание к ИП особенно обострилось в последнее время (2010–2012 годы) в связи с целой серией публикаций в отечественной и зарубежной прессе, впрямую посвященных применению ИП.

Сегодня технология спутникового координатно-временного обеспечения по средствам навигационных систем ГЛОНАСС/GPS востребована не только для объектов на поверхности Земли и в околоземном пространстве, но и для космических аппаратов, находящихся на орбитах выше, чем орбиты навигационных КА (НКА), т.е. геостационарных и высокоэллиптических (ГСО и ВЭО). Наличие соответствующих навигационных приемников на борту этих КА значительно упрощает определение их местонахождения (рис. 1) [1]. Так же как и любая другая НАП, космическая НАП может быть подвержена воздействию комплексами противоспутниковой радиоэлектронной борьбы, в том числе и ИП.

КА, находящиеся на круговых орбитах с высотами ниже 20 тыс. км (высота орбит НКА), являются более защищенными от ИП, так как их приемные антенны расположены в верхней части КА и для наведения помехи требуются другие КА, летящие над ними, что крайне сложно и дорого для реализации [5]. Приемные антенны КА, находящегося на ГСО, направлены на Землю, так как улавливают сигналы от НКА перед их заходом и выходом из-за Земли (рис. 1 [1]). Это значит, что бортовая НАП такого КА легко подвергается наведению ложного сигнала с поверхности Земли (рис. 2). В этом случае соответствующий наземный комплекс с имитационной аппаратурой постановки индивидуальной ИП для конкретного объекта с известными координатами может полностью дезориентировать КА и «увести» его из своей рабочей точки стояния с заданными координатами.

Существуют так называемые «простые» методы выявления в НАП ложных НС, которые относительно просто реализуются в современных приемниках и должны учитываться при их создании:
- слежение за абсолютной мощностью каждой несущей частоты НС;
- слежение за скоростью изменения мощности сигнала;
- слежение за относительными мощностями принимаемого сигнала;
- сравнение скоростей динамики кода и фазы;
- проверка целостности полученных данных.

Все эти методы считаются простыми в силу их давнего применения в наземной и околоземной аппаратуре потребителя НС и широкой известности. Однако необходимо учитывать существенное усложнение как самой НАП, так и их программно-математического обеспечения при использовании этих методов.

Кроме указанных способов защиты можно предложить реализуемые уже сегодня относительно более сложные способы различения сигналов НКА и ИП, использующие их пространственные отличия. Они предполагают наличие вместо одной приемной антенны нескольких разнесенных в пространстве. Разнесенные в пространстве антенны позволяют определить углы между осями объекта (условно проведенная прямая через две приемные навигационные антенны) и векторами направления сигнала за счет измерения разности фаз несущего сигнала [2, 3].

Таким образом, проанализировав полученную навигационную информацию о положении НКА (альманах) и вектор прихода сигнала, можно различить сигналы, приходящие от НКА, обусловленные различием их направлений, и от постановщика помех с равным направлением прихода всех сигналов $\varphi1^* = \varphi2^* = \varphi3^*$ (рис. 2). Единственный способ формирования пространственной радиоволны, подобной радиоволне навигационного сигнала, – это расположение постановщиков ИП на линии визирования от НАП к НКА, причем для имитируемого сигнала от одного НКА требуется свой постановщик ИП. Этот способ довольно сложен в реализации для малоподвижных наземных и околоземных по-

НКА – навигационные спутники;
КА – геостационарный спутник;
НП – навигационное поле;
R ≈ 6378 км – радиус Земли;
h ≈ 20000 км – высота орбиты НКА ГЛОНАСС/GPS;
H ≈ 40000 км – высота орбиты геостационарного спутника;
$h_н$ ≈ 5000 км – высота единого навигационного поля ГНСС

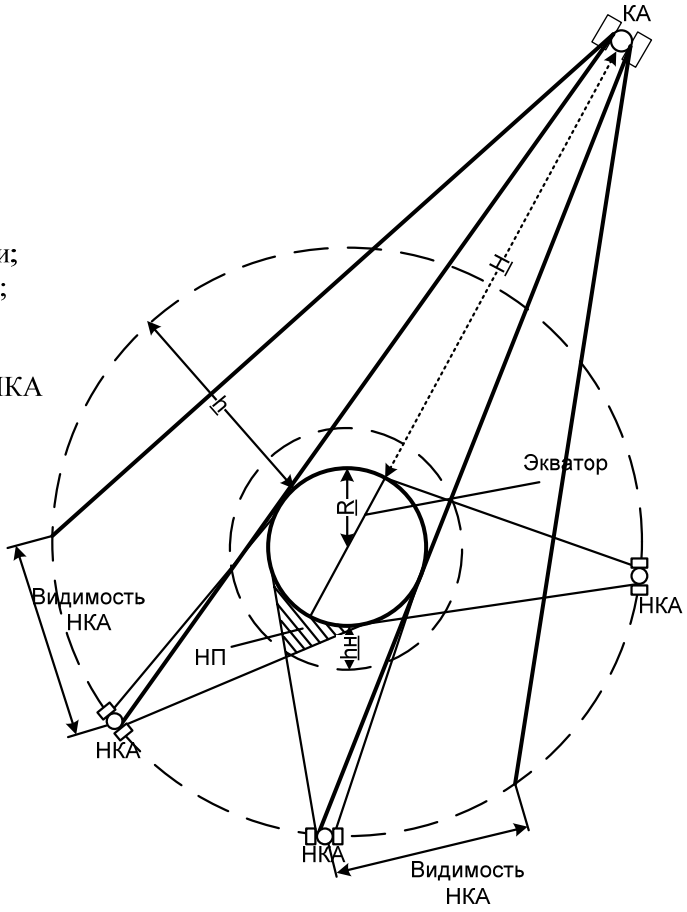

Рис. 1. Зоны видимостей местонахождения КА

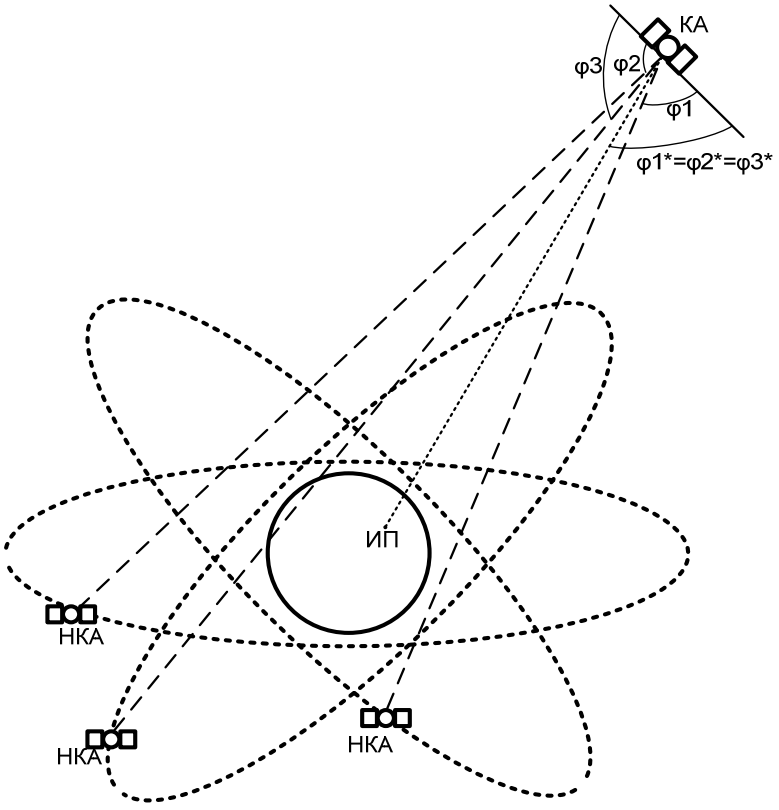

Рис. 2. Позиционирование КА

требителей НС и практически невозможен для КА на ГСО.

Наличие нескольких антенных элементов и возможность определения вектора прихода НС позволяют НАП решать не только навигационные, но и угломерные задачи. То есть становится возможным определять не только координаты, но и пространственное положение объекта относительно навигационных систем ГЛОНАСС/GPS.

Исходя из вышесказанного следует, что внедрение навигационной аппаратуры с разнесенными в пространстве антеннами на борт КА, находящегося на ГСО, позволяет без значительного удорожания и увеличения массогабаритных характеристик бортовой аппаратуры решить проблему помехозащищенности бортовой НАП за счет выявления и исключения ложных НС, а также дополнительно повысить точность пространственной ориентации КА.

Список литературы

1. Двухсистемный навигационный приемник космического аппарата. Пат. №112401 Российская Федерация / В. А. Зубавичус, А. З. Балабанов, В. А. Комаров [и др.]. № 2011121496/28, заявл. 27.05.2011 ; опубл. 10.01.2012, Бюл. №1.
2. Пичкалев А. В., Кочев Ю. В., Гребенников А. В. Радиоугломерная аппаратура для задач ориентации и стабилизации // Тезисы докладов 2-й Международной научно-технической конференции, посвященной 30-летию запуска на орбиту первого навигационного космического аппарата «Глонасс» (10–14 октября 2012 г., Железногорск) / под общ. ред. Н. А. Тестоедова ; ОАО «Информационные спутниковые системы». Сибирский государственный аэрокосмический ун-т. Красноярск, 2012. С. 142–144.
3. Харисов В. Н. ГЛОНАСС. Принципы построения и функционирования / под ред. В. Н. Харисова [и др.]. М. : Радиотехника, 2010. 800 с.
4. ГЛОНАСС и защищённость GPS [Электронный ресурс]. Режим доступа: https://dxdt.ru/2009/10/14/2721/.
5. Сетевые спутниковые радионавигационные системы / В. С. Шебшаевич, П. П. Дмитриев, Н. В. Иванцев [и др.] ; под ред. В. С. Шебшаевича. 2-е изд., перераб. и доп. М. : Радио и связь, 1993. 408 с.

История статьи
Поступила в редакцию 14 июля 2017 г.
Принята к публикации 4 сентября 2017 г.

METHODS OF ELECTRONIC WARFARE IN SPACE NAVIGATION AND PROTECTION OF SPACECRAFTS

R. B. Kovalyov
JSC Academician M. F. Reshetnev Information Satellite Systems, Zheleznogorsk, Krasnoyarsk region, Russian Federation

The main element of the electronic warfare content is the radio traffic blackout between the radioelectronic means by means of jamming countermeasures and false targets. It was carried out in separate radioelectronic means of information transmission through masking jamming up to the beginning of the Second World War. Against to the first radioelectronic means of information retrieval (by radar stations) were developed effective methods of passive jamming which simulating real objects and facilitating of false information to the opposition. With the development and improvement of electronic warfare devices were opened the prospects of impact on radioelectronic means by deception active jamming and even if it is possible to filter out true information from false information the presence of the false information sometimes significantly complicates the assessment of the situation during the military operation. In addition, the impact on the modern radioelectronic system which includes a computer can be implemented through the radio channel of plausible information messages containing computer viruses that penetrate to the computer network up to the highest army and weapon controls. Along with this the saturation of jamming countermeasures means in a local area leads to the isolation of such radioelectronic means from others. Finally, modern electronic warfare devices which using not only masking but also distorting, deception and blocking jamming they allow the disorganization of the radioelectronic means operation on a global scale, and the implementation of organizational and technical measures to establish various jamming contributes to the disruption of the functioning not only local groups radioelectronic means but also large-scale radioelectronic systems.

Keywords: jamming, receiver, orbit, protection, radio navigation signal, power, navigation equipment, electronic warfare.

References

1. Zubavichus V. A., Balabanov A. Z., Komarov V. A., Marareskul D. I., Furmanov V. V., Tsvetkova O. I., Yudin V. A., Ankudinov A. V. *Dvuhsistemnyj navigacionnyj priemnik kosmicheskogo apparata* [Two-system navigation receiver of the spacecraft]. Patent RF, no. 112401, 2012.
2. Pichkalev A. V, Kochev Yu. V., Grebennikov A. V. *Radiouglomernaya apparatura dlya zadach orientacii i stabilizacii* [Radioglobelic apparatus for orientation and stabilization problems]. *Tezisy dokladov 2-j Mezhdunarodnoj nauchno-tekhnicheskoj konferencii, posvyashchennoj 30-letiyu zapuska na orbitu pervogo navigacionnogo kosmicheskogo apparata* "*Glonass*" [Abstracts of the 2nd International Scientific and Technical Conference dedicated to the 30th anniversary of the launch of the first navigation spacecraft "Glonass"]. Siberian State Aerospace University, Krasnoyarsk, 2012, pp. 142–144.
3. Kharisov V. N., Perov A. I., Boldin V. A. *GLONASS. Printsipy postroeniya i funktsionirovaniya.* [GLONASS. Construction principles and operation]. Moscow, Radiotekhnika Publ., 2010, 800 p. (In Russian)
4. GLONASS and GPS security. Available at: https://dxdt.ru/2009/10/14/2721/ (accessed 09.07.2017).
5. Shebshaevich V. S., Dmitriev P. P., Ivantsevich N. V., Kalugin A. V., Kovalevsky E. G., Kudryavtsev I. V., Kutikov V. Yu., Molchanov Yu. B., Maksyutenko Yu. A. *Setevye sputnikovye radionavigacionnye sistemy* [Network satellite radio navigation systems]. Moscow, Radio i svyaz' Publ., 1993, 408 p. (In Russian)

Article history
Received 14 July 2017
Accepted 4 September 2017