УДК 621.391.825

Принципы создания противонавигационного поля радиопомех

Юдин В.Н.*, Камнев Е.А.**

Московский авиационный институт (национальный исследовательский университет), МАИ, Волоколамское шоссе, 4, Москва, А-80, ГСП-3, 125993, Россия

**e-mail: vn_yudin@mail.ru*

***e-mail: ekam91@yandex.ru*

Аннотация

Рассмотрены принципы создания противонавигационного поля радиопомех аппаратуре потребителей спутниковых радионавигационных систем. Выявлены возможные подходы к созданию противонавигационного поля для решения задач: противодействия опасным объектам, объектовой защиты и защиты территории. Особый интерес представляет оценка возможностей создания противонавигационного поля защиты территории. Традиционные подходы, применяемые при объектовой защите, в данном случае неприемлемы. Предложен подход, основанный на совместном использовании в составе противонавигационного поля постановщиков маскирующих (шумовых) и имитирующих радиопомех.

Ключевые слова: аппаратура потребителей, спутниковые радионавигационные системы, противонавигационное поле радиопомех.

Введение

Наблюдаемое в настоящее время и на перспективу бурное развитие спутниковых радионавигационных систем (РНС) стимулируется не только гражданскими, но и военными потребностями. В связи с этим в ситуациях конфликта возникает необходимость противодействия спутниковым РНС. Цель противодействия – затруднение успешного решения задач навигации объектами противной стороны. Противодействие аппаратуре потребителей (АП) спутниковых РНС может реализовываться в интересах решения различных задач. К таким задачам относятся следующие.

1. Противодействие опасным объектам, оснащенным АП спутниковых РНС, путем радиоэлектронного подавления (РЭП) АП. Такими объектами могут быть, например, ЛА – носители средств технической разведки, террористические и разведывательно-диверсионные группы и другие. Существенно, что при решении таких задач должна быть известна пространственная зона, в пределах которой расположены нейтрализуемые объекты.

2. Защита объектов своей стороны от оружия, наводящегося на эти объекты по информации, получаемой от АП спутниковых РНС, путем РЭП АП (объектовая защита). Защищаемыми объектами могут быть промышленные предприятия, электростанции, мосты, аэродромы и другие. Исходными данными при организации объектовой защиты обычно являются координаты защищаемых объектов, возможные типы средств поражения, а также атакоопасные направления.

3. Защита территории (региона, нескольких регионов, страны) от любых средств вооруженной борьбы, имеющих в своем составе АП спутниковых РНС, путем РЭП АП. Эта задача по своему содержанию всеобъемлющая, ее решение автоматически означает также решение частных задач 1 и 2.

Основные виды радиопомех, применяемых для создания противонавигационного поля

Возможности решения задач РЭП АП спутниковых РНС путем создания радиопомех различных видов рассмотрены в ряде работ, например, в [1, 2]. В [2] анализируются ситуации воздействия на АП активных маскирующих (шумовых) помех. Шумовые помехи (ШП) являются, как известно, универсальным средством РЭП и широко применяются на практике. Действие ШП на АП спутниковых РНС приводит к увеличению нормальных ошибок измерения псевдодальностей и, как следствие, к увеличению ошибок навигационных определений. При достаточно высокой мощности ШП реализуется предотвращение захвата навигационных сигналов (НС) спутников на слежение или срыв слежения за временной задержкой и частотой НС. В [1] рассматриваются возможности противодействия спутниковым РНС путем создания так называемых «сигналоподобных помех». Сигналоподобные помехи создаются прицельно по времени и частоте с таким расчетом, чтобы перекрыть время-частотные зоны, в которых сосредоточены пики взаимнокорреляционных функций (ВКФ) дальномерных

кодов НС спутников и соответствующих опорных кодов, формируемых в подавляемой АП. Сигналоподобные помехи обычно не обладают маскирующим действием, поскольку не создают фона. Действие таких помех может приводить к искажению ВКФ, и, как следствие, к увеличению ошибок измерения псевдодальностей. При идеальном прицеливании, когда рассогласование истинного НС и помехи не превышает долей ширины главного лепестка ВКФ, возможна реализация «увода» опорных кодов, формируемых в подавляемой АП, от истинных НС – это так называемая уводящая помеха. Действие уводящей помехи приводит к срыву слежения за задержкой НС.

В [1] отмечается, что прицеливание помех по параметрам НС сопряжено со значительными трудностями. Однако в случаях, когда подавляемая АП работает в открытом режиме, когда коды НС спутников известны, сигналоподобные помехи, как искажающие, так и уводящие, могут быть созданы с помощью специальных устройств – имитаторов [3]. Особый случай представляют сигналоподобные помехи, создаваемые с помощью ретрансляторов. В [2] отмечается, что реализация уводящей помехи на базе ретранслятора невозможна, так как в точке расположения подавляемой АП всегда имеет место неустранимое временное запаздывание ретранслируемого сигнала и соответствующего истинного НС. Попытки уменьшить эту задержку до величины, не превышающей ширины главного лепестка ВКФ, приводят к необходимости размещения в пространстве некоторого числа

ретрансляторов. Группа ретрансляторов может обеспечить перекрытие лишь относительно небольшого диапазона временных задержек, в пределы которого должна попасть задержка истинного НС. Расширение этого диапазона требует увеличения числа ретрансляторов, что может оказаться неприемлемым, по экономическим соображениям. Следует также указать на трудности обеспечения электромагнитной развязки приемных и передающих антенн ретрансляторов.

В [3, 4, 5] рассмотрены вопросы, связанные с применением против АП спутниковых РНС радиопомех имитирующего действия. Имитирующие помехи (ИмП) не создают маскирующего фона и не искажают ВКФ кодов истинных НС и опорных кодов, формируемых в АП. Имитирующие помехи создают ложные НС, идентичные по форме истинным НС, но сдвинутые относительно них по времени и по частоте. Благодаря наличию этого сдвига ИмП не могут быть средством срыва слежения за параметрами НС. Они эффективны только на этапе поиска НС и его захвата на слежение.

Если коды НС подавляемой АП известны (РНС работает в открытом режиме), то ИмП, как и рассмотренные выше помехи искажающего действия, могут быть созданы с помощью специальных имитаторов. При работе РНС в закрытом режиме реализация имитаторов невозможна. В этом случае средством создания ИмП могут быть пассивные отражатели, например, на базе уголковых конструкций, линз Люнеберга, короткозамкнутых антенн или решеток Ван-Атта [6]. Другим средством создания ИмП являются активные

ретрансляторы [7]. При создании активных ИмП неизбежно возникают трудности с обеспечением электромагнитной развязки приемных и передающих антенн ретрансляторов. Преодоление этих трудностей возможно путем пространственного разноса приемных и передающих антенн ретрансляторов.

Требования к характеристикам противонавигационного поля

Анализ содержания задач, для решения которых создается ПНП и целей создания ПНП с учетом особенностей основных видов радиопомех позволяет сформулировать основные требования к характеристикам ПНП различных видов. Рассмотрим их по отдельности.

Противонавигационное поле противодействия опасному объекту. При создании ПНП этого вида задано пространственное положение опасного объекта в виде зоны, в пределах которой он гарантированно находится. Создаваемое ПНП должно перекрывать эту зону (рисунок 1).

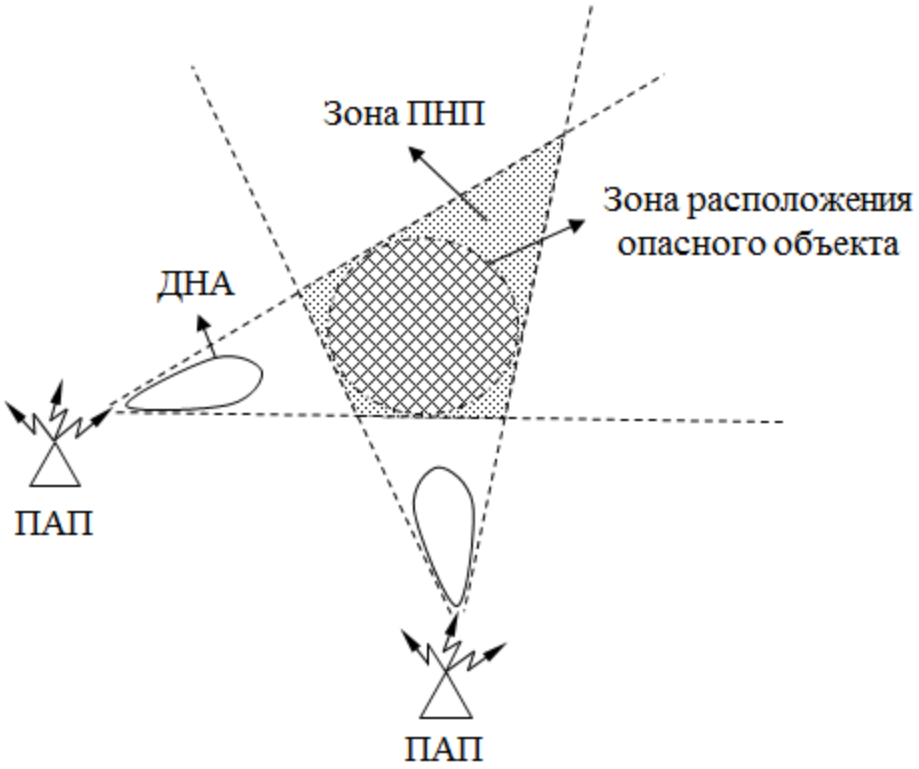

Рис.1. Противонавигационное поле противодействия опасному объекту: ПАП – постановщик активных помех; ДНА – диаграмма направленности антенны ПАП

Зона, в пределах которой создается ПНП, определяется шириной ДНА и пространственным положением ПАП. Количество ПАП, создающих ПНП в требуемой зоне, может быть различным. Основное требование к ПНП – предотвращение захвата НС спутников на слежение в пределах требуемой зоны. Средством создания ПНП могут быть постановщики ШП. Ширина спектра ШП определяется шириной спектра НС (полосой пропускания приемника АП). Требуемая мощность ШП может быть определена на основе методики, изложенной в [2].

Противонавигационное поле защиты объекта. Если направления возможных атак на защищаемый объект (ЗО) (атакоопасные сектора)

известны, то конфигурация ПНП, создаваемого для защиты ЗО, может иметь вид, представленный на рисунке 2.

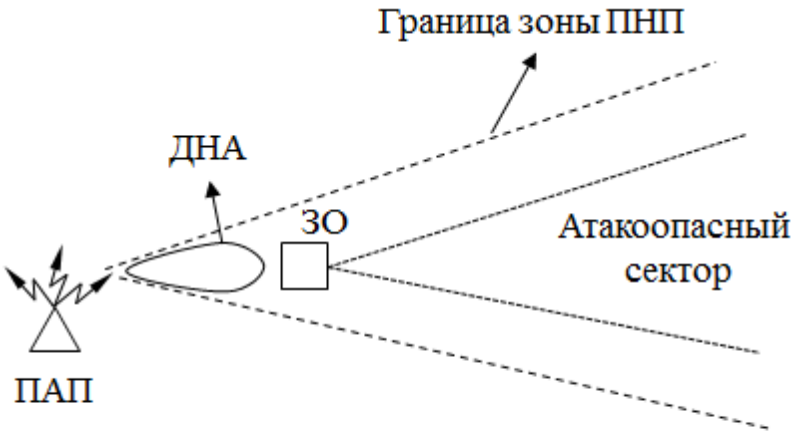

Рис.2. Конфигурация ПНП ЗО при известном атакоопасном секторе

Если атакоопасные сектора не определены, то конфигурация ПНП может иметь вид, представленный на рисунке 3.

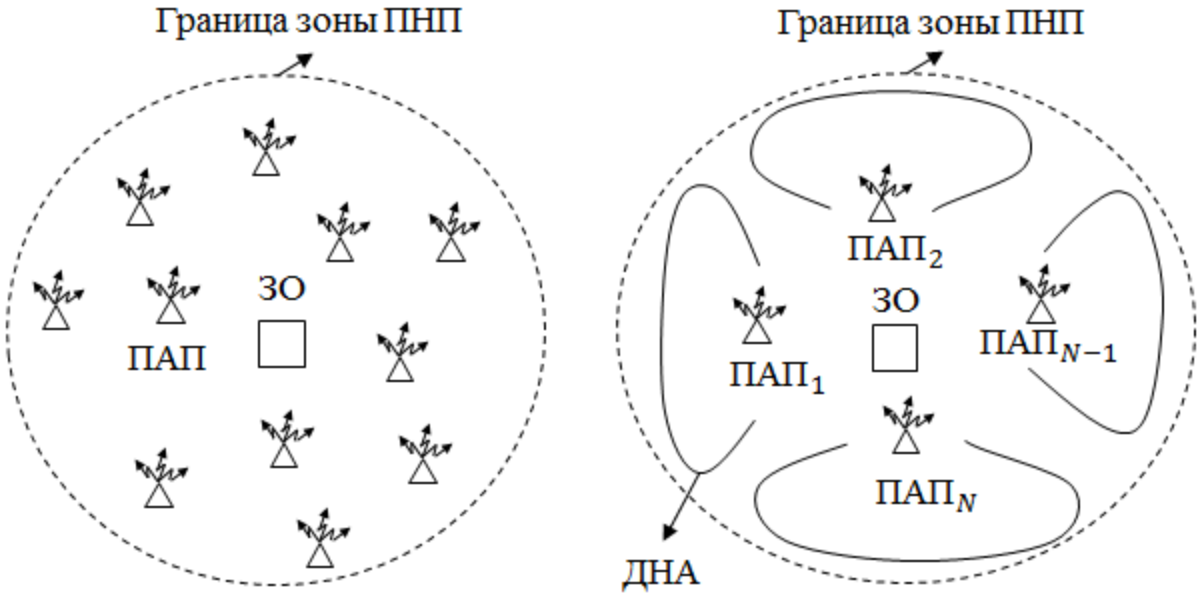

Рис.3. Конфигурация ПНП ЗО при неизвестном атакоопасном секторе:
а) применение ПАП с ненаправленной ДНА;
б) применение ПАП с направленной ДНА.

Во всех случаях основным требованием к ПНП является срыв слежения за задержкой τ и частотой f НС спутников соответствующими следящими контурами, имеющимися в составе подавляемой АП. Срыв поиска НС по τ и f при решении рассматриваемой задачи не представляет интереса. Как и при решении предыдущей задачи, средством создания ПНП могут быть постановщики ШП, прицельных по частоте НС спутников.

В случае, соответствующем рисунку 2, требуемая ширина ДНА постановщика ШП определяется шириной атакоопасного сектора. Требуемая мощность постановщика ШП зависит от положения дальней границы зоны ПНП, а также от дальности прямой видимости носителя подавляемой АП из точки расположения постановщика ШП. Методика расчетов требуемой мощности содержится в [2].

В случае, представленном на рисунке 3а, антенны всех ПАП ненаправленные в горизонтальной плоскости. Вариант конфигурации ДНА – «купол» с охватом 360° в горизонтальной и 180° (верхняя полусфера) в вертикальной плоскостях. Расстановка ПАП на местности, высота подъема ПАП над земной поверхностью, а также мощность ПАП должны обеспечивать «сплошное покрытие» требуемой зоны ПНП с учетом реального рельефа местности. Средством создания ПНП, как и в предыдущем случае, могут быть постановщики ШП. В этом случае их требуемая мощность определяется такими факторами, как наибольшее из расстояний между рассматриваемым постановщиком ШП и соседними с ним

постановщиками ШП, форма ДНА, наибольшая возможная высота полета носителей подавляемой АП, а также наличие в составе подавляемой АП средств защиты от ШП.

В случае, представленном на рисунке 3б, антенны всех ПАП направленные в горизонтальной плоскости. Каждый ПАП «обслуживает» выделенный ему угловой сектор, размер которого определяется шириной ДНА. Как и в предыдущих случаях, ПНП может быть создано с помощью постановщиков ШП. Требуемая мощность постановщиков ШП определяется по методике, изложенной в [2], с учетом расстояния от рассматриваемого постановщика ШП до границы зоны ПНП.

Противонавигационное поле защиты территории. Задачу защиты территории можно считать решенной, если обеспечивается подавление АП спутниковых РНС в любой точке защищаемой территории. Как указано выше, основным требованием к ПНП защиты территории может быть предотвращение захвата НС на слежение, и срыв слежения за параметрами НС в любой точке территории.

Реализация указанных требований возможна на базе рассмотренного выше подхода к построению ПНП объектовой защиты, иллюстрируемого рисунком 3а. При этом потребуется разместить постановщики ШП на всей защищаемой территории. Принципы расстановки постановщиков ШП на местности, требования к их мощности и форме ДНА не меняются. Однако

энергетические и аппаратурные затраты, требуемые для реализации такого подхода, могут оказаться неприемлемо большими.

Необходимость снижения затрат требует использования при создании ПНП защиты территории иных принципов и средств. В частности, перспективно использование в составе ПНП постановщиков имитирующих, искажающих и уводящих помех. Создание таких помех, как правило, не требует больших энергетических затрат. Однако, как указывалось выше, реализация помех искажающего и уводящего действия проблематична. Что касается ИмП, то они не способны реализовать требование срыва слежения за параметрами НС следящими контурами подавляемой АП.

Подход, позволяющий удовлетворить требования к ПНП защиты территории, может быть основан на совместном использовании помех маскирующего и имитирующего действия. Вариант реализации такого подхода поясняется рисунком 4.

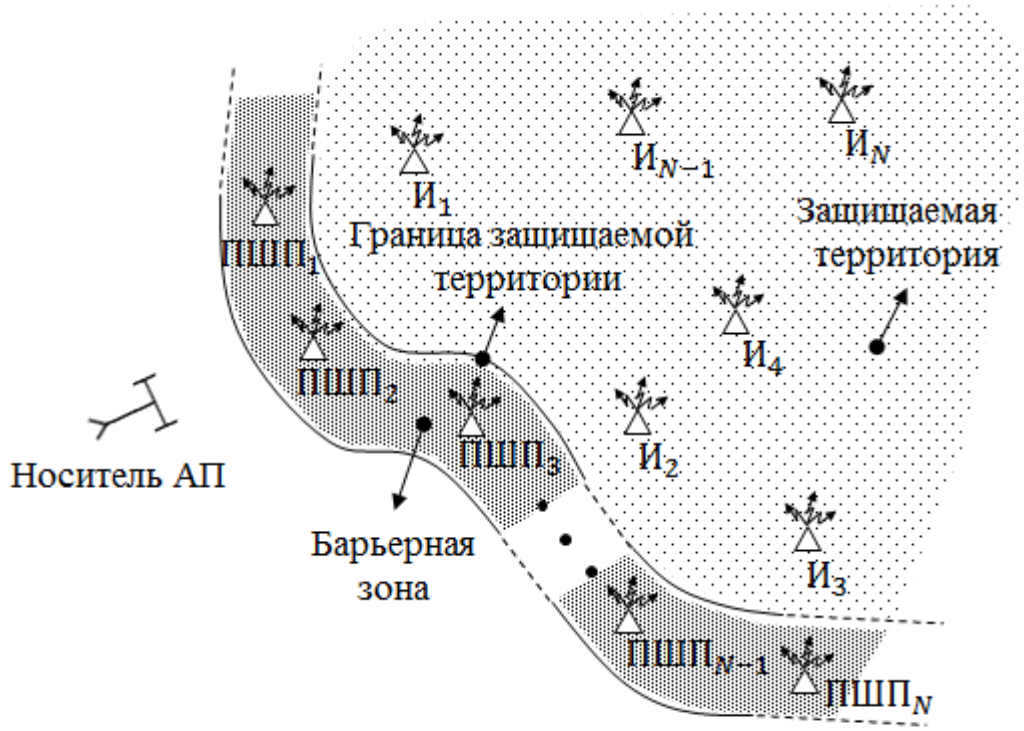

Рис.4. Конфигурация ПНП защиты территории:
а) ПШП – постановщик ШП; б) И – постановщик ИмП

Вдоль границы защищаемой территории с ее наружной стороны создается барьерная зона. В пределах барьерной зоны размещаются ПШП. На защищаемой территории размещаются постановщики ИмП. Ширина барьерной зоны и мощности ПШП выбираются таким образом, что за время, в течение которого носитель АП спутниковой РНС преодолевает барьерную зону, гарантированно реализуется срыв слежения за задержкой и частотой НС следящими контурами АП. Постановщики ИмП создают ложные НС. Расстановка постановщиков ИмП на местности и параметры излучаемых ими ложных НС выбираются таким образом, что попытки повторного захвата («перезахвата») НС после преодоления барьерной зоны гарантированно приведут к захвату на слежение ложных НС.

Разработка методики обоснования параметров постановщиков ИмП представляет самостоятельный интерес. Очевидно, при обосновании необходимо учитывать имеющиеся в составе подавляемой АП средства идентификации ложных НС. Как указано выше, вариантами постановщиков ИмП могут быть ретрансляторы и пассивные отражатели на базе уголков, линз и короткозамкнутых антенн.

Основные энергетические затраты при использовании подхода, иллюстрируемого рисунком 4, идут на создание ПНП в барьерной зоне, где размещаются постановщики ШП. Величина этих затрат зависит от протяженности границы территории (от протяженности атакоопасных участков границы). Можно, однако, утверждать, что эти затраты гораздо меньше, чем аналогичные затраты на покрытие всей территории постановщиками ШП. Что касается энергозатрат на создание ложных НС, то они, как правило, невелики и дополнительно уменьшаются при использовании в качестве постановщиков ИмП пассивных отражателей НС.

Заключение

Проведенное рассмотрение ПНП позволило выявить возможные подходы к созданию противонавигационного поля при решении различных задач. Особый интерес представляет оценка возможностей создания ПНП на защищаемой территории. Традиционные подходы, применяемые при объектовой защите, в данном случае неприемлемы. Предложен подход, основанный на совместном использовании в составе ПНП постановщиков

маскирующих (шумовых) и имитирующих радиопомех. Преимущество такого подхода заключается в том, что, благодаря покрытию основной части защищаемой территории маломощными постановщиками ИмП, он обеспечивает резкое снижение энергозатрат на создание ПНП. При обосновании характеристик ИмП необходимо учитывать имеющиеся в составе подавляемых образцов АП спутниковых РНС средства идентификации ложных НС.

Библиографический список

1. Дятлов А. П., Дятлов П. А., Кульбикаян Б. Х. Радиоэлектронная борьба со спутниковыми радионавигационными системами. - М.: Радио и связь, 2004. - 226 с.

2. Драгалин М.И. Прогнозирование критических ситуаций при функционировании аппаратуры потребителей спутниковых радионавигационных систем в условиях действия преднамеренных помех: диссертация кандидата технических наук. – М.: 05.12.14, 2003. – 191 с

3. Humphreys, T. E., B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner (2008) “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,”in Proceedings of ION GNSS 21st. International Technical Meeting of the Satellite Division, September 16-19, Savannah, GA, pp. 2314-2325.

4. Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, Todd E. Humphreys. Unmanned Aircraft Capture and Control via GPS Spoofing.

http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf [Электронный ресурс], доступ: свободный (дата обращения 11.06.2015 г.).

5. Daniel P. Shepard, Jahshan A. Bhatti, Todd E. Humphreys Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. Preprint of the 2012 ION GNSS Conference Nashville, TN, September 19–21, 2012, 15 p.

6. Куприянов А.И. Радиоэлектронная борьба. - М.: Вузовская книга, 2013. 360 с.

7. Karl-Ragmar Riemschneider, Franz Wolf, Patent US 8396432 B2, 28.05.2002.