ПРИНЦИПЫ ОБНАРУЖЕНИЯ ПРЕДНАМЕРЕННЫХ ПОМЕХ, ВОЗДЕЙСТВУЮЩИХ НА АППАРАТУРУ ПОТРЕБИТЕЛЕЙ СПУТНИКОВЫХ РАДИОНАВИГАЦИОННЫХ СИСТЕМ

Х. К Дао [1], Д. Д. Ступин [1], Р. А. Шевченко [2]

[1] Московский физико-технический институт (национальный исследовательский университет, 141701, Московская область, г. Долгопрудный, Институтский переулок, д.9
[2] АО «РТИ им. А.Л.Минца». 127083, г. Москва, ул. 8-го Марта, д. 10, стр. 1

Статья поступила в редакцию 14 мая 2019 г.

Аннотация. В статье рассмотрено влияние преднамеренных помех на работу приемников спутниковых навигационных систем летательных аппаратов (ЛА) и способы противодействия этим помехам, в том числе:

– приведена классификация преднамеренных помех, воздействующих на приемники спутниковых навигационных систем: «Энергетические» помехи (jamming) – радиопомехи, предназначенные для нарушения функционирования приемника путем подавления полезного информационного сигнала и «Имитационные» помехи («Спуфинг»-помехи (spoofing)) – радиопомехи, имитирующие сигналы навигационных спутников, в результате приема которых в приемнике решается навигационная задача с определением местоположения и параметров движения потребителя, не соответствующих действительным;

– рассмотрены существующие методы формирования «Имитационных» помех («Спуфинг»-помех (spoofing)) и алгоритмы их обнаружения и борьбы с ними;

– предложен оптимальный для решаемой задачи метод борьбы с «Имитационными» помехами – метод комплексного решения навигационной задачи с использованием данных как от спутниковых навигационных систем, так и от инерциальной навигационной системы и автономных радиотехнических систем (ДИСС, РСБН, посадочные и радионавигационные РЛС).

Ключевые слова: спутниковые радионавигационные системы (СРНС), навигационная аппаратура потребителей (НАП), спуфинг-помеха (СП).

Abstract. The article considers the impact of intentional jamming on the operation of receivers of satellite navigation systems of aircraft and methods of counteraction to jamming, including:

– the classification of intentional jamming affecting the receivers of satellite navigation systems is given: "Energy" jamming – jamming designed to disrupt the operation of the receiver by suppressing a useful information signal and "Simulation" jamming ("Spoofing"-jamming) – jamming simulating signals of navigation satellites, as a result of which the receiver solves the navigation problem with determining the location and motion parameters of the consumer not corresponding to the actual;

– the existing methods of formation of "Simulation" ("Spoofing") jamming and algorithms for their detection and neutralize are considered;

– the optimal method for solving the problem of combating "Simulation" "Simulation" ("Spoofing") jamming – a method of integrated solution of the navigation problem with its mutual solution according to both satellite navigation systems and inertial navigation system and Autonomous radio systems (DISS, VOR/DME, landing and radio navigation radar).

Key words: satellite radio navigation systems (SRNS), consumer navigation equipment, spoofing jamming.

1. Введение

В настоящее время одним из наиболее распространенных типов высокоточных систем позиционирования являются спутниковые радионавигационные системы (СРНС), которые считаются ключевым элементом навигационного обеспечения в авиации, судовождении и сухопутных перевозках.

К наиболее распространенным СРНС относятся системы ГЛОНАСС и GPS, обеспечивающие определение местоположения с точностью от единиц метров до

сантиметров (в зависимости от используемых методов и дополнительного оборудования). Важным достоинством этих систем является отсутствие ограничений на число пользователей, которым для того, чтобы пользоваться услугами СРНС, достаточно иметь навигационную аппаратуру потребителей (НАП), сопряженную с одной из названных СРНС или с обеими. Однако эти СРНС обладают одним существенным недостатком, в частности, низким уровнем помехоустойчивости, обусловленным малой мощностью принимаемых радионавигационных сигналов. Например, в системе ГЛОНАСС мощность принимаемых сигналов составляет порядка -166…-156 дБВт [2]. Влияние помех, как непреднамеренных (ионосферные, тропосферные, многолучевое распространение сигналов и. т. д), так и преднамеренных, существенно влияет на точностные характеристики навигационного обеспечения.

Выделяют два вида преднамеренных помех, которые могут воздействовать на НАП СРНС:

- «Энергетические» помехи (jamming) – радиопомехи, предназначенные для нарушения функционирования НАП СРНС путем подавления полезного информационного сигнала. К этому типу помех также следует отнести любые действия, направленные на нарушение функционирования самой СРНС, включая атаку на спутники и наземную инфраструктуру управления [1,8].
- «Имитационные» помехи («Спуфинг»-помехи (spoofing)) – радиопомехи, предназначенные для передачи на НАП СРНС ложной информации путем формирования специальными источниками сигналов, аутентичных сигналам СРНС [3].

На практике проще и надежнее реализуются энергетические помехи. Однако любое воздействие такого рода на радиоаппаратуру легко распознается и позволяет, соответственно, учитывать наличие помехового воздействия при работе аппаратуры. «Спуфинг»-помехи представляются сегодня более опасными,

так как их воздействие приводит к формированию ложной навигационной информации при отсутствии понимания о наличии помехового воздействия.

Для формирования «спуфинг»-помехи (СП) в настоящее время существуют два основных метода: «генераторный» и «ретрансляционный». Сущность этих методов, а также методы обнаружения «спуфинг»-помех рассмотрим ниже [2].

2. Методы формирования «спуфинг»-помехи

а) Генераторный метод.

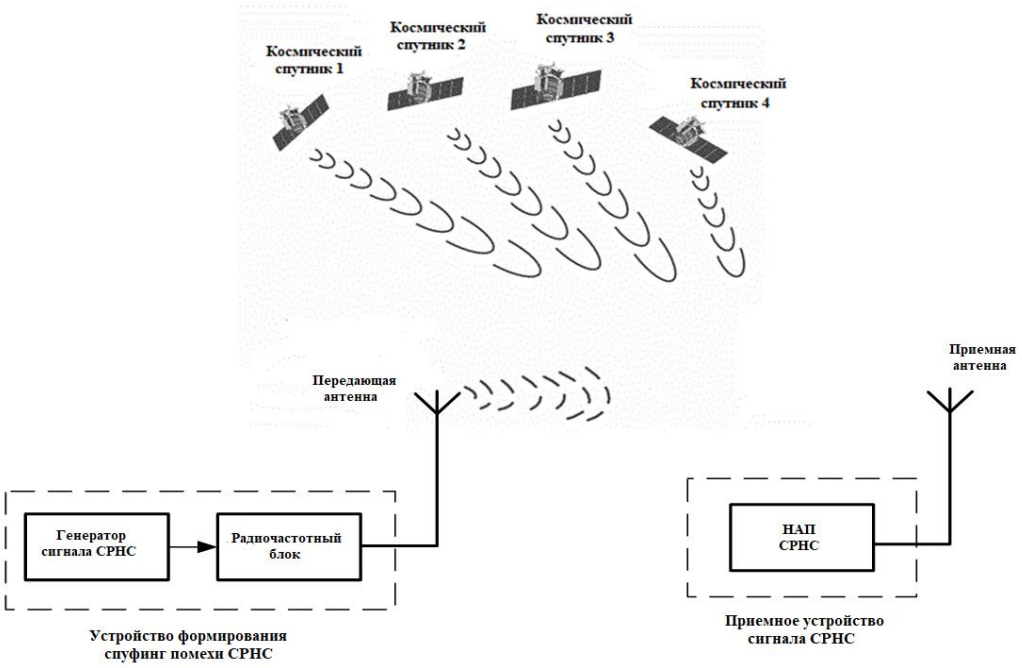

Рис 2.1. Структурная схема устройства формирования спуфинг помехи на основе генераторного метода.

На рисунке 2.1 представлена структурная схема формирования СП на основе генераторного метода. Генератор помехового сигнала формирует «спуфинг»-помеху, имеющую параметры, аналогичные параметрам сигналов СРНС, а затем использует передающую антенну для излучения помехового сигнала в направлении НАП СРНС.

В настоящее время большинство вариантов кодовых структур сигналов СРНС, используемых для гражданских применений, общеизвестны, поэтому

реализация устройства формирования СП на основе генераторного метода в большей степени применима именно в системах гражданского назначения. Сигналы же военного назначения в СРНС кодируются более длинными последовательностями; структуры этих последовательностей являются закрытыми, поэтому декодирование такого сигнала технически является сложной задачей. В связи с этим обстоятельством формирование СП для систем военного назначения генераторным методом представляется неоправданно сложным. Поэтому для создания СП системам военного назначения обычно используется ретрансляционный метод [1].

б) Ретрансляционный метод

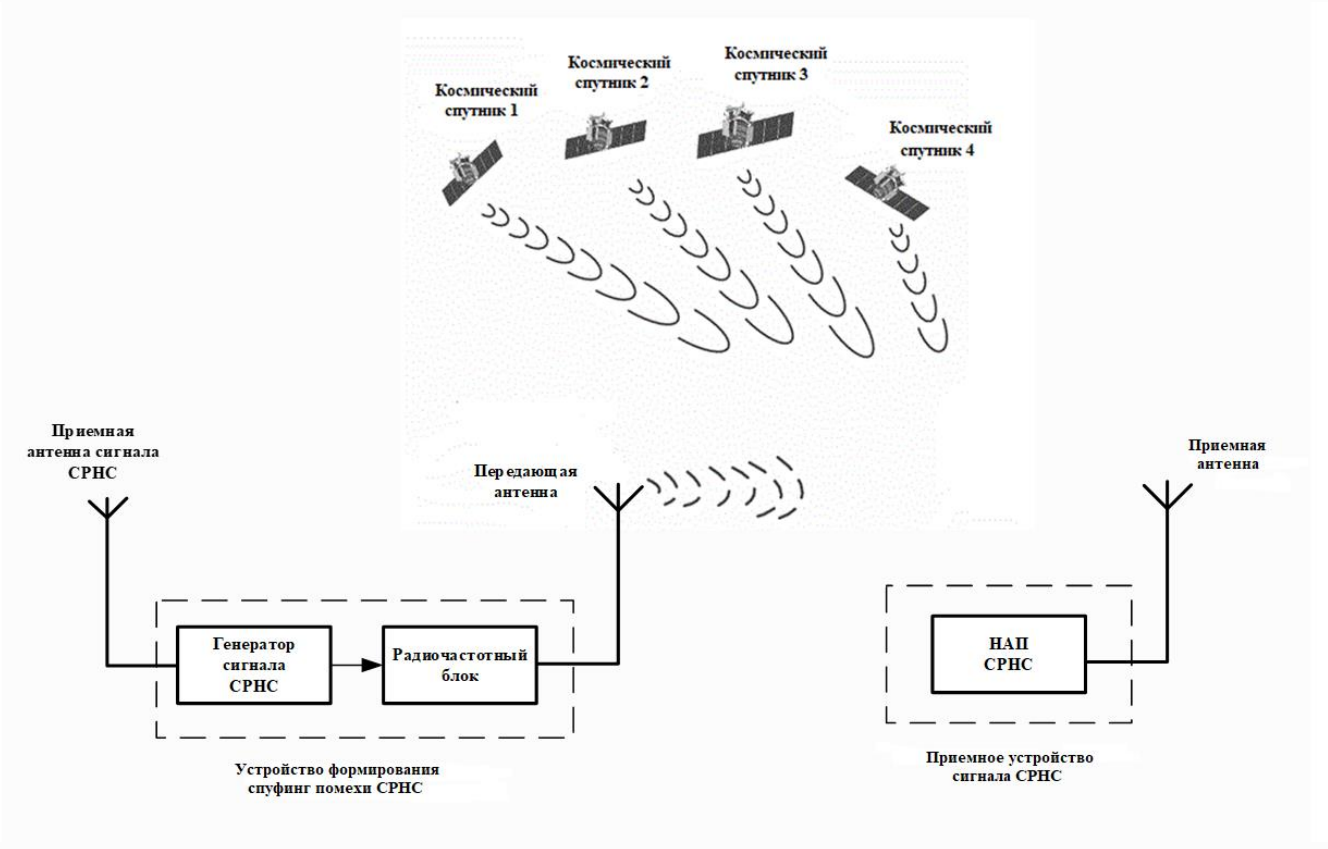

Рис 2.2. Структурная схема устройства формирования спуфинг-помехи на основе ретрансляционного метода.

При использовании ретрансляционного метода устройство формирования СП сначала получает аутентичный сигнал СРНС с помощью приемной антенны, а затем после добавления к сигналу определенной временной задержки и,

возможно, дополнительного сдвига частоты усиливает его и передает помеховый сигнал с помощью передающей антенны на НАП. НАП СРНС после получения помехового сигнала вычисляет псевдодальность до соответствующего мнимого (имитируемого) спутника, поэтому позиционирование носителя НАП СРНС производится с ошибкой. Структурная схема устройства формирования СП на основе ретрансляционного метода представлена на рис.2.2.

Оба рассмотренных метода различаются по степени сложности реализации. В первом случае используется одна приемо-передающая антенна для приема всех аутентичных спутниковых сигналов и повторной передачи искаженных сигналов [10]. В этом случае, если задержка достаточно мала, мы можем предположить, что помеха синхронизирована с информационным сигналом от спутника СРНС, который она имитирует. Этот тип «спуфинг»-помехи может быть идентифицирован НАП СРНС и, следовательно, в этом случае может быть установлен факт наличия помехи. Второй метод использует одну антенну для приема навигационных сигналов от спутников, а другую – для передачи искаженных сигналов на НАП СРНС. Если для приема сигналов используется многолучевая антенна, то оказывается возможным вносить искажения в любой из принятых со спутников сигналов. В этом случае данные позиционирования носителя могут быть существенно искажены, при этом НАП СРНС не сможет определить факт помехового воздействия [11] без использования специальных методов.

3. Модель полученного сигнала

Формирование спуфинг-помех может осуществляться как генераторным, так и ретрансляционным методами, которые представлены выше. Но использование ретрансляционного метода формирования спуфинг-помех для радиоэлектронного подавления НАП нецелесообразно [1].

Поскольку «спуфинг»-помехи предполагают формирование сигналов, которые по виду, структуре и основным параметрам аутентичны сигналам СРНС, модель такого помехового сигнала можно представить в следующем виде:

$$j^c(t) = \sum_{l=1}^{L} \sqrt{p_l^c} D_l^c(t-\tau_l^c) c_l^c(t-\tau_l^c) e^{j(\omega_l^c t + \phi_l^c)} \qquad (3.1),$$

где $D_l^c(t)$ и $c_l^c(t)$ представляют собой, соответственно, ложный псевдослучайный код навигационного сообщения *l*-ого спутника и код расширенного спектра *l*-ого спутника в устройстве формирования спуфинг-помехи ; ϕ_l^c, ω_l^c, p_l^c и τ_l^c представляют собой, соответственно, фазу, допплеровскую угловую частоту, мощность и задержку сигнала; верхний индекс *c* означает, что эти параметры относятся к «спуфинг»-помехе. Таким образом, суммарный помеховый сигнал представляет собой суперпозицию нескольких псевдослучайных «спуфинг»-сигналов, а *l* в (3.1) определяет количество этих паразитных псевдослучайных сигналов, генерируемых устройством формирования «спуфинг»-помехи [12].

Когда сигналы от $\bar{M}$ спутников и от $\bar{K}$ источников «спуфинг»-помех одновременно поступают в НАП СРНС, сигнал, поступивший в НАП СРНС может быть представлен как:

$$x(t) = \sum_{m=1}^{\bar{M}} s_m^a(t) + \sum_{k=1}^{\bar{K}} j_k^c(t) + e(t) \qquad (3.2),$$

где $s_m^a(t)$ представляет собой сигнал m-ого спутника; $j_k^c(t)$ представляет помеху, переданную k-ым устройством формирования СП; верхние индексы *a* и *c*, соответственно, означают аутентичный спутниковый сигнал и сигнал помехи; e(t) - аддитивный гауссовский белый шум.

Предполагая, что и сигнал от спутника, и множественные помехи попадают на приемную антенну НАП одновременно, используя в данной модели в качестве

примера регулярную линейную решетку (*uniform linear array*), содержащую M элементов, получим, что суммарный информационный сигнал, принятый антенной НАП СРНС, можно представить в виде [12]:

$$x(t) = \sum_{m=1}^{\bar{M}} a(\theta_m^a) s_m^a(t) + \sum_{k=1}^{\bar{K}} a(\theta_k^c)\, \mathrm{j}_k^c(t) + e(t) \qquad (3.3),$$

где $a(\theta_m^a)$ и $a(\theta_m^c)$ представляют собой весовые коэффициенты, определяющиеся направлениями приема сигналов для сигнала m-го спутника и k-го сигнала устройства формирования СП; θ_m^a и θ_m^c представляют направления, с которых приходят сигналы от спутников и от устройств формирования СП (*Direction of Arrival DOAs*) для информационного сигнала m-го спутника и k-го сигнала устройства формирования ИП; e(t) является вектором аддитивного гауссова белого шума.

Из соотношения (3.3) следует, что структура информационного сигнала и структура сигнала СП идентичны, что затрудняет решение задачи распознавания факта наличия СП и, соответственно, «борьбы» с ней.

4. Обзор возможных подходов к обнаружению «спуфинг»-помехи

Для обнаружения СП можно предложить несколько подходов. Основной задачей является определение факта наличия помехового воздействия (имитационной помехи) и обеспечение работоспособности НАП СРНС с нужным качеством при воздействии помехи.

4.1 Метод обнаружения на основе анализа мощности сигнала

Поскольку и мощность аппаратуры, размещаемой на спутнике, и дальность до спутника известны с высокой точностью, НАП СРНС, осуществляя непрерывные измерения мощности принимаемых спутниковых сигналов, может на основе обнаружения аномально мощных сигналов распознавать факт воздействия СП. Необходимым условием применимости этого метода является

наличие информации о местоположении всех навигационных спутников относительно НАП СРНС.

Контроль отношения сигнала к шуму. Отношение сигнал/шум C/N_0 является важным параметром для измерения качества сигнала СРНС. Движение спутника СРНС по орбите даже при влиянии ионосферы и, возможно, тропосферы, может приводить к плавному изменению мощности сигнала, принимаемого НАП СРНС. В момент, когда включается СП, величина C/N_0 может претерпеть резкое изменение. Поэтому НАП может обнаруживать СП при непрерывном контроле отношения C/N_0 путем обнаружения таких изменений. Кроме того, при размещении НАП СРНС на движущейся платформе за счет изменения расстояния между платформой и источником СП изменение уровня C/N_0 (даже без резких вариаций), отличающееся от прогнозируемого, может свидетельствовать о наличии СП [2].

Контроль абсолютной мощности. Мощность аутентичного сигнала СРНС, принимаемого НАП, очень низкая. Например, для сигнала GPS L1 максимальная мощность составляет приблизительно -153 дБВт [7]. Для формирования сигнала СП, имеющего «правдоподобную» мощность, необходимо знать и местоположение излучающего сигнал спутника, и местоположение НАП, и особенности среды распространения сигналов на трассе «спутник – НАП». Эта задача представляется весьма трудоемкой, поэтому вероятность добиться правдоподобного уровня мощности при формировании помехового сигнала крайне мала. Следовательно, если мощность сигнала, принимаемая НАП, значительно больше ожидаемой мощности аутентичного сигнала СРНС, это можно интерпретировать как факт воздействия СП. Метод абсолютного контроля мощности требует, чтобы НАП имела более высокую точность измерения амплитуды принимаемого сигнала, поэтому, соответственно, возрастает сложность аппаратной реализации НАП.

4.2 Методы обнаружения на основе анализа пространственных характеристик сигналов

Методы обнаружения, основанные на анализе пространственных характеристик сигналов, используют тот факт, что аппаратура формирования СП использует одну и ту же антенну для передачи нескольких помеховых сигналов, а сигналы от навигационных спутников СРНС поступают из разных направлений. В результате интерференционные сигналы пространственно коррелируют, поэтому СП можно распознать путем определения пространственной корреляции принятых сигналов с использованием технологии обработки сигналов в пространственной области.

Метод обнаружения, основанный на пространственных характеристиках, предполагает использование двух антенн [5], взаимное расположение которых фиксировано. Оценивается разность фаз сигналов, принятых этими антеннами, которая сравнивается с расчетной разностью фаз, зависящей от взаимного перемещения спутника и НАП. Сравнивая наблюдаемую разность фаз с расчетной, можно, при наличии большого рассогласования между этими значениями, предположить возможность помехового воздействия. Основной недостаток этого метода заключается в том, что для проведения наблюдений требуется довольно длительный период времени. Увеличение числа антенн повышает надежность этого метода обнаружения СП.

4.3 Методы обнаружения на основе аутентификации шифрованных сигналов

Для оборудования как гражданского, так и военного назначения обнаружение СП может быть реализовано с использованием технологии аутентификации шифрованных сигналов [5]. Однако при использовании этой технологии аппаратура обработки сигналов может вносить изменения в структуру принимаемых спутниковых сигналов, что затрудняет решение основной задачи НАП – определение местоположения носителя. Поэтому

использование такой технологии весьма проблематично, по крайней мере, в настоящее время и в ближайшем будущем.

4.4 Метод обнаружения на основе анализа структуры навигационного сообщения

Для метода обнаружения, основанных на анализе структуры самих навигационных сигналов, используются относительные временные задержки между сигналами L1 и L2 [4].

Относительная задержка между сигналами L1/L2: коды P(Y) после шифрования могут быть модулированы на полосах частот L1 и L2. Поскольку ионосфера по-разному задерживает сигналы различных частот, возникает относительная временная задержка между сигналами L1 и L2, принимаемыми НАП. Используя двухчастотную НАП и анализируя взаимную корреляцию между сигналами L1 и L2, можно видеть, что функция взаимной корреляции имеет только одно пиковое значение, а временная задержка, соответствующая этому пиковому значению, представляет собой относительную задержку по времени между сигналами на частотах L1 и L2. Сравнивая эту относительную задержку с расчетной, определяемой из информации о взаимном движении спутников и НАП, можно при наличии рассогласования между величинами задержек предполагать воздействие СП. Заметим, что эта технология распознавания может применяться только при создании спуфинг-помех с помощью специального генератора.

4.5 Метод обнаружения на основе интеграции данных от нескольких независимых навигационных систем

Интегрированная навигационная система [8] объединяет на борту носителя одну или несколько независимых систем, таких как НАП СРНС, бортовая радионавигационная система, астрономическая навигационная система и другие с инерциальной навигационной системой. Объединение данных, получаемых с помощью СРНС с данными других навигационных систем (например, с данными инерциальной навигационной системы), может помочь эффективно распознавать

факт применения СП. Сравнивая результат позиционирования, вычисленный НАП СРНС с результатами, полученными другими навигационными системами, можно, при наличии значительных рассогласований этих данных, достоверно предполагать воздействие СП на НАП СРНС. Данный метод обнаружения воздействия СП представляется в настоящее время наиболее эффективным, поскольку основывается на сравнении данных измерений, полученных от нескольких независимых источников.

5. Заключение

«Спуфинг»-помехи (имитационные помехи) в настоящее время представляют серьезную опасность для НАП СРНС, поскольку они могут не только приводить к возникновению больших ошибок при определении местоположения, но и к перехвату управления роботизированных комплексами за счет создания ложного навигационного поля. В представленной работе рассмотрено несколько подходов для решения задач обнаружения «спуфинг»-помехи (имитационной помехи), в частности, методы на основе анализа мощности сигнала, анализа пространственных характеристик, аутентификации данных и комплексного решения навигационной задачи. Анализ достоинств и недостатков рассмотренных методов показывает, что наиболее оптимальным методом борьбы является метод комплексного решения навигационной задачи с ее взаимным решением по данным как от СРНС, так и от инерциальной навигационной системы и автономных радиотехнических систем (ДИСС, РСБН, посадочные и радионавигационные РЛС) [9].

Литература

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

2. ГЛОНАСС Принципы построения и функционирования. Изд. 3-е, перераб. и доп. Под редакцией Перова Александра Ивановича и Харисова Владимира Назаровича. – М.: Радиотехника, 2005. 688 с.

3. Романов А.С., Турлыков П.Ю. Исследование влияния имитирующих помех на аппаратуру потребителей навигационной информации. Труды МАИ. Выпуск № 86, 2016 г., стр. 1-8. Режим доступа www.mai.ru/science/trudy/

4. *Орёл Д.В.* Анализ угроз функционирования аппаратуры гражданских потребителей глобальных спутниковых радионавигационных систем // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. — Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2011. — С. 44–48.

5. Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gerard Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation*, Volume 2012, Article ID 127072, 15 pages. DOI http://dx.doi.org/10.1155/2012/127072.

6. Lubbers B., Theunissen E., Oonincx *P*. Jamming and Spoofing: Effective Cyber Weapons Looking for a Defense. In: Ducheine P., Osinga F. (eds) Netherlands Annual Review of Military Studies 2017. NL ARMS (Netherlands Annual Review of Military Studies). T.M.C. Asser Press, The Hague.

7. Humphreys T.E., Ledvina B.M., Psiaki M.L., et al. Spoofing threat assessment: development of a portable GPS satellite. Q: ion GNSS Proceedings of the 21st international technical meeting of the satellite unit, September 16-19, Savannah, Georgia. 2008. p.3.2314-2325.

8. Magiera J., Katulski R. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *Journal of Applied Research and Technology*, *13*(1), 45-57. Elsevier Ltd. Retrieved April 15, 2019. Available at https://www.learntechlib.org/p/198163/.

9. Psiaki M.L., Humphreys T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270.

10. Mark L. Psiaki, Brady W. O'Hanlon. Civilian GPS Spoofing Detection Based on Dual Receiver Correlation of Military Signals. *Proceedings of ION GNSS 2011, the 24th International Technical Meeting of The Institute of Navigation*, Portland, Oregon, September 19–23, 2011, pp. 2619-2645.

11. Montgomery Yu. P., Humphreys T. E., Ledvina B. M. Autonomous receiver spoofing detection: experimental results of protecting an antenna with multiple antennas against a portable civil GPS trigger. P*roceedings of Institute of navigation national technical meeting*, 26-28 Jan, Anaheim, CA. 2009. p. 124-30.

12. Renbiao Wu, Wenyi Wang, Dan Lu, Lu Wang, Qionggiong Jia. Adaptive Interference Mitigation of GNSS. *Navigation: Science and Technology*. DOI https://doi.org/10.1007/978-981-10-5571-3.

Для цитирования:
Х. К Дао, Д. Д. Ступин, Р. А. Шевченко. Принципы обнаружения преднамеренных помех, воздействующих на аппаратуру потребителей спутниковых радионавигационных систем. Журнал радиоэлектроники [электронный журнал]. 2019. № 5. Режим доступа: http://jre.cplire.ru/jre/may19/14/text.pdf
DOI 10.30898/1684-1719.2019.5.14