

**ПРИМЕНЕНИЕ SDR-ТЕХНОЛОГИИ ДЛЯ ОЦЕНКИ
ПОМЕХОУСТОЙЧИВОСТИ НАВИГАЦИОННЫХ ПРИЕМНИКОВ**

**APPLICATION OF SDR TECHNOLOGY FOR NOISE IMMUNITY
ASSESSMENT NAVIGATION RECEIVERS**

Канд. техн. наук А.В. Фомин, канд. техн. наук С.А. Святкин, С.П. Леонтьев

Ph.D. A.V. Fomin, Ph.D. S.A. Svyatkin, S.P. Leontyev

ВКА им. А.Ф. Можайского

Важность навигационно-временного обеспечения различных потребителей в настоящее время сложно переоценить. При этом существует уязвимость навигационной аппаратуры потребителей, связанная с подменой истинных сигналов ложными, генерируемыми современными SDR-трансиверами. В статье описан макет, позволяющий формировать и излучать в эфире групповой навигационный сигнал, представлена методика формирования навигационного поля, приведены результаты исследований помехоустойчивости навигационного приемника к воздействию непреднамеренных информационно-подобных помех при различных параметрах их формирования, определены уровни устойчивого функционирования навигационной аппаратуры потребителей, сформулированы выводы об особенностях влияния рассматриваемых помех на помехоустойчивость навигационных приемников.

Ключевые слова: навигационное поле, непреднамеренная помеха, навигация, SDR-технология, программно-определяемая радиосистема.

It is difficult to overestimate the importance of navigation and time support for various consumers now. At the same time, there is a vulnerability of consumer navigation equipment associated with the substitution of true signals with false ones generated by modern SDR transceivers. The article describes a layout that allows forming and broadcasting a group navigation signal. Presents a method for forming a navigation field, presents the results of studies of the noise immunity of a navigation receiver to the effects of unintentional imitating interference with various parameters of their formation. Determines the levels of stable functioning of consumer navigation equipment, and draws conclusions about the peculiarities of the influence of the interference considered on the noise immunity of navigation receivers.

Keywords: navigation field, unintentional interference, navigation, SDR technology, software-defined radio system.

Введение

Навигационные технологии в настоящее время применяются в различных областях жизнедеятельности для определения местоположения объектов, а также временного обеспечения

различных систем. При этом открытость структуры сигналов глобальных навигационных спутниковых систем (ГНСС), а также широкая доступность современных SDR-трансиверов, способных работать на частотах навигационных систем, обуславливают потенциальную уязви-

мость навигационной аппаратуры потребителей (НАП) к воздействию непреднамеренных информационно-подобных помех. В этой связи задача оценки помехоустойчивости НАП к такого рода воздействиям является актуальной.

Принцип работы макета

Для решения поставленной задачи разработан макет (рис. 1), в основе которого лежит использование технологии SDR (Software-defined radio) — программно-определяемой радиосистемы, т.е. такой радиосистемы, в которой некоторые или все функции физического уровня (фильтрация, модуляция/демодуляция, преобразование спектра, усиление сигналов) реализуются программными средствами и могут быть программно изменены без непосредственного физического вмешательства в схему устройства.

В качестве аппаратной SDR платформы используются трансивер HackRF One, характеристики которого позволяют излучать широкополосные сигналы в диапазоне частот до 6 ГГц [12]. Исследуемый образец навигационного приемника — Garmin Nuvi 710. Навигационное поле генерируется на основе открытых сигналов ГНСС.

Принцип работы установки заключается в следующем: на ПЭВМ 1 и ПЭВМ 2 с помощью специального программного обеспечения генерируются файлы содержащие в себе отсчеты группового навигационного сигнала с «истинными» и «ложными» (имитируемыми) координатами соответственно. Первый SDR-трансивер излучает «истинный» сигнал, поступающий на вход навигационного приемника, который в свою очередь обнаруживает сигналы, следит за ними и определяет местоположение. После устойчивого приёма «истинного» сигнала включается

второй SDR-трансивер для излучения помехи («ложного» сигнала) с заданной мощностью.

Методика формирования навигационного поля

Методика формирования навигационного поля как для «истинного» сигнала, так и для «ложного» сигнала одинакова и включает в себя следующие шаги.

1. Задание координат: имитируемые координаты («истинные», «ложные») задаются в формате геодезических координат (долгота, широта).

2. Загрузка эфемеридных данных: эфемериды навигационных космических аппаратов (НКА) ГНСС распространяются различными организациями, в том числе Национальным управлением по авиации и исследованию космического пространства (NASA) [11]. Информация об эфемеридах НКА содержится в файле, имеющем стандарт RINEX [10], который представляет собой аппаратно-независимый формат обмена навигационными данными (рис. 2).

3. Определение НКА, попадающих в зону радиовидимости: радиовидимость НКА устанавливается на требуемом уровне, все НКА попадающие в зону радиовидимости (рис. 3) из имитируемой позиции («истинной», «ложной») фиксируются, остальные не учитываются.

4. Расчет задержек: при расчете задержек навигационных сигналов от НКА до имитируемой позиции используются следующим выражением:

$$\tau_i = \frac{\sqrt{(x-x_i)^2 + (y-y_i)^2 + (z-z_i)^2}}{c},$$

где x_i, y_i, z_i — координаты i -го НКА в геоцентрической фиксированной системе координат; x, y, z — координаты имитируемой позиции в ге-



Рис. 1. Структурная схема макета формирования навигационного поля

Версия файла	Тип информации	Дата записи файла	RINEX VERSION / TYPE		
2	NAVIGATION DATA	03-OCT-18 05:18	PGM / RUN BY / DATE		
Название программы	Агентство		COMMENT		
CCRINEXN V1.6.0 UX	CDDIS		IGS BROADCAST EPHEMERIS FILE		
Комментарий			Параметры ионосферной модели A0-A3		
			0.1024D-07 0.7451D-08 -0.5960D-07 -0.5960D-07		
			Параметры ионосферной модели B0-B3		
			0.8806D 0.0000D -0.1966D -0.6554D		
		Время начала отсчета	Номер недели начала отсчета		
	Коэффициенты полинома A0, A1	503808	2021 DELTA-UTC: A0, A1, T, W		
	0.000000000000D 0.266453525910D-14				
18	Сдвиг шкалы времени относительно UTC		LEAP SECONDS		
			END OF HEADER		
№КА	Эпоха	Сдвиг часов КА	Скорость ухода часов	Ускорение ухода часов	
1 18 10	3 0 0	0.0	-0.954833813012D-04	-0.477484718431D-11	0.000000000000D
	IODE	Crs	Delta n	Mo	
	0.370000000000D	0.930312500000D	0.414874424042D-08	0.108515425593D	
	Sux	e	Cus	Sqrt(A)	
	-0.490248203278D-05	0.813408102840D-02	0.800192356110D-05	0.515366898155D	
	ю	Cic	OMEGA	Cis	
	0.259200000000D	0.819563865662D-07	0.127954424727D	0.596046447754D-07	
	Toe	Cte	omega	OMEGA DOT	
	0.972459120952D	0.231750000000D	0.697617793118D	0.804854954011D-08	
	IDOT	Коды в L2	№GPS недели	Флаг данных L2P	
	-0.800033324599D-10	0.100000000000D	0.202100000000D	0.000000000000D	
	Точность положения КА	Исправность КА	TGD	IODC	
	0.200000000000D	0.000000000000D	0.558793544769D-08	0.370000000000D	
	Время передачи сообщения (секунды GPS Недели)	Интервал аппроксимации орбиты	Резерв		
	0.252018000000D	0.400000000000D	0.000000000000D	0.000000000000D	

Рис. 2. Фрагмент эфемеридных данных стандарта RINEX

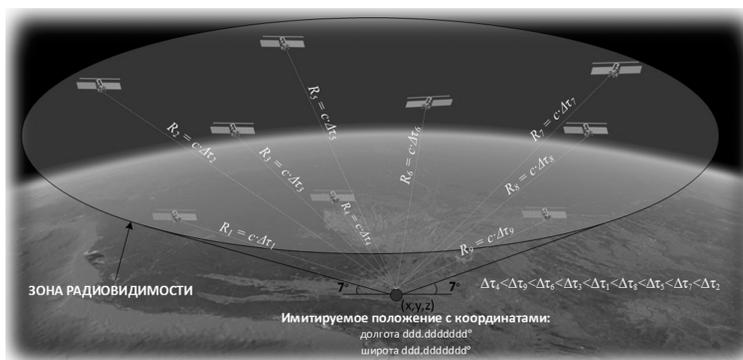


Рис. 3. Зона радиовидимости

оцентрической фиксированной системе координат; c — скорость света.

Координаты НКА (x_i, y_i, z_i) определяются путем использования эфемеридной информации на основе методики, описанной в [2].

5. Формирование навигационного сообщения для каждого имитируемого канала: структура навигационного кадра (рис. 4) содержит информацию об эфемеридах НКА, альманахе созвездия спутников, частотно-временные поправки, метки времени, параметры ионосферной мо-

дели, сведения о работоспособности бортовой аппаратуры НКА и др. [2]. При этом основная информация необходимая для решения навигационной задачи содержится в 1, 2 и 3 подкадрах навигационного сообщения. Поэтому при имитировании навигационного поля используются только эти подкадры.

6. Формирование навигационного сигнала: открытый сигнал L1C/A формируется путем модуляции несущей дальномерным кодом и информационным сообщением (рис. 5). При этом использу-

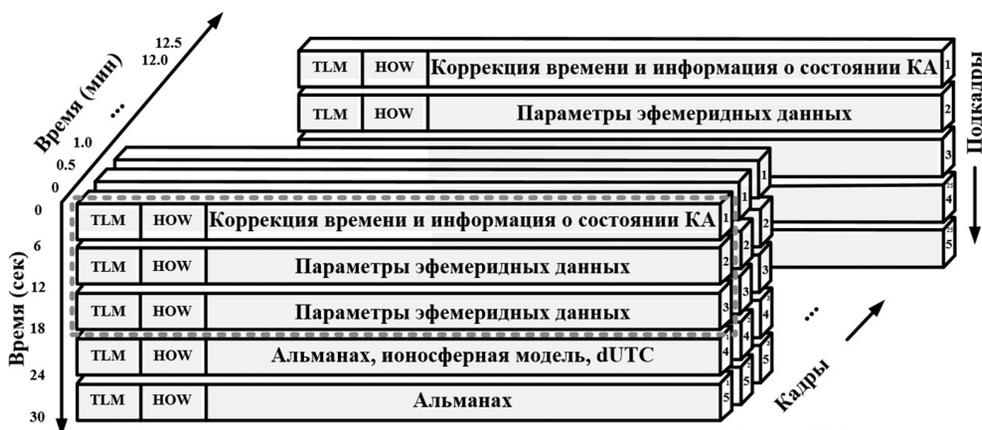


Рис. 4. Структура навигационного кадра

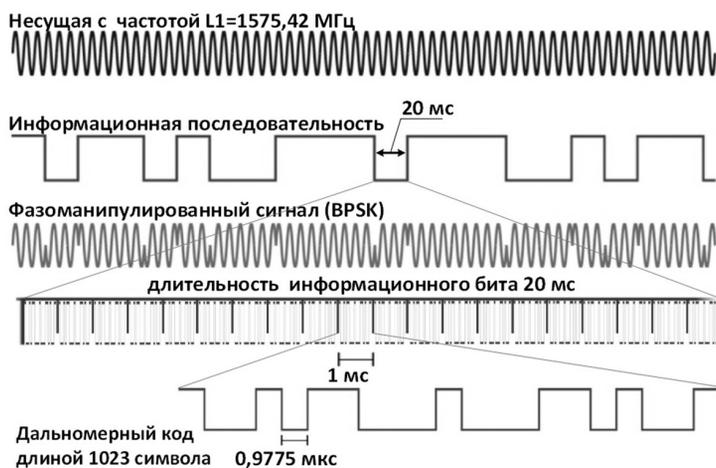


Рис. 5. Структура навигационного сигнала

ется двоичная фазовая манипуляция (BPSK). Каждый НКА излучает свой дальномерный код, т.е. реализовано кодовое разделение каналов. Исходные данные для формирования кодов приведены в [2]. На основе рассчитанных в п. 4 задержек от каждого НКА до имитируемой позиции формируются отсчеты группового навигационного сигнала с учетом частоты дискретизации SDR-трансивера HackRF One (2,6 МГц). Полученные отсчеты записываются в файл, который затем используется для формирования высокочастотного группового навигационного сигнала. При этом задержки сигналов внутри группового сигнала выстраиваются следующим образом: первым идет навигационный сигнал с наименьшей задержкой и его дальномерный код начинается с первого символа, за ним сигнал со значением задержки больше первого, но меньше остальных и его дальномерный код задерживается относительно первого на требуемую величину и т.д. (рис. 6).

На основе предложенного подхода проведена оценка помехоустойчивости НАП к воздействию непреднамеренных информационно-подобных помех. Результаты исследований приведены для статических имитируемых позиций, т.е. «истинный» сигнал и «ложный» сигнал (навязываемая помеха) имитировали неподвижного потребителя. При этом под критерием требуемого качества функционирования НАП понимается: устойчивый приём навигационного поля (НП), при обработке которого навигационный приёмник определяет истинные координаты. Изменяемыми параметрами помехи выступали:

- мощность излучения;
- удаленность имитируемого местоположения от истинного;
- смещение по передаваемому в навигационном сообщении времени между помехой и сигналом.

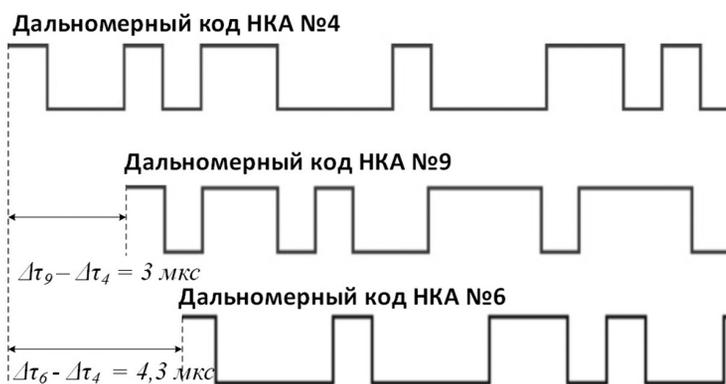


Рис. 6. Пример выстраивания задержек дальномерных кодов друг относительно друга

Результаты эксперимента

1. Определение порога устойчивого функционирования навигационного приемника.

На рис. 7 представлены: дисплей навигационного приемника Garmin Nuvi 710, на котором показаны уровни принимаемых навигационных сигналов, текущее местоположение определяемое приемником до и после воздействия помех.

На рис. 8 и 9 приведены графики зависимости вероятности и времени захвата ложного НП

(информационно-подобной помехи) от отношения P_c / P_n , отражающие результаты данного эксперимента. Оценка проводилась при следующих исходных данных: рассогласование по передаваемым координатам между истинным и имитируемым сигналами — 400 м; рассогласование по передаваемому в навигационном сообщении времени — не более 1 с.

Анализ рис. 8 и 9 показывает, что устойчивое функционирование НАП (низкая вероятность захвата ложного НП, $P_{\text{захвата}} = 0,1$ и менее) обеспечиваются при отношении $(P_c / P_n) \geq -15$ дБ.

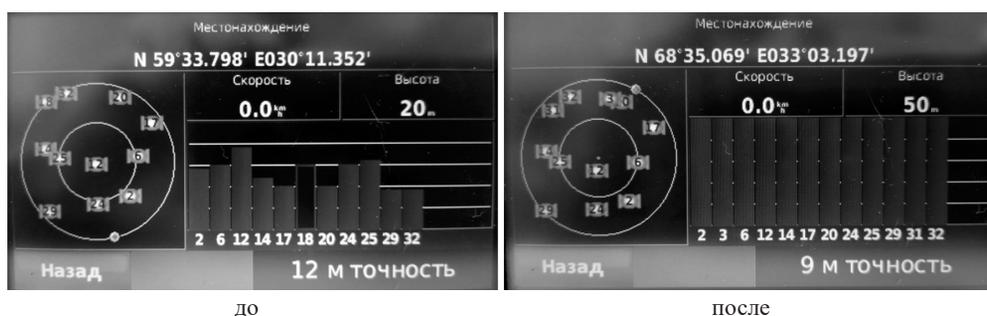


Рис. 7. Результат спуфинга НАП Garmin Nuvi 710

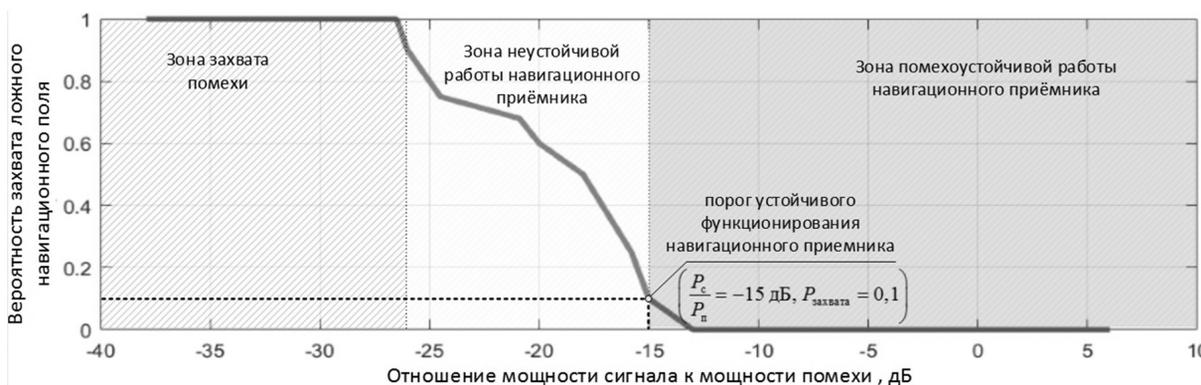


Рис. 8. График зависимости вероятности захвата ложного НП от отношения мощности сигнала к мощности помехи

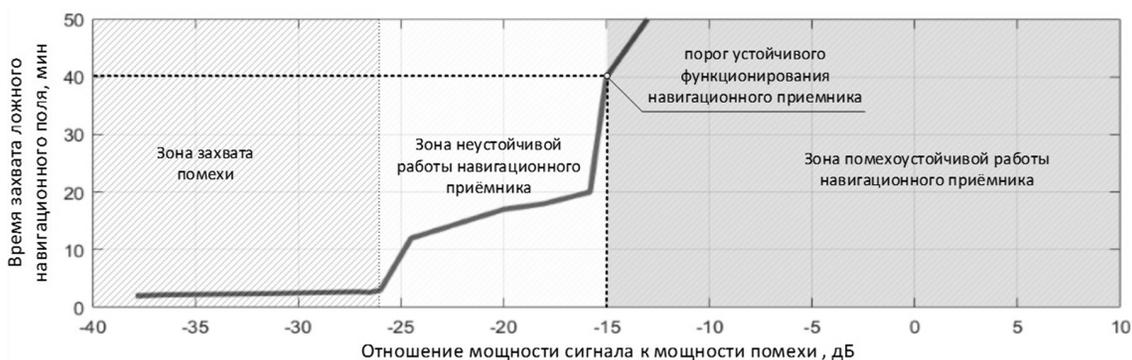


Рис. 9. График зависимости времени захвата ложного НП от отношения мощности сигнала к мощности помехи

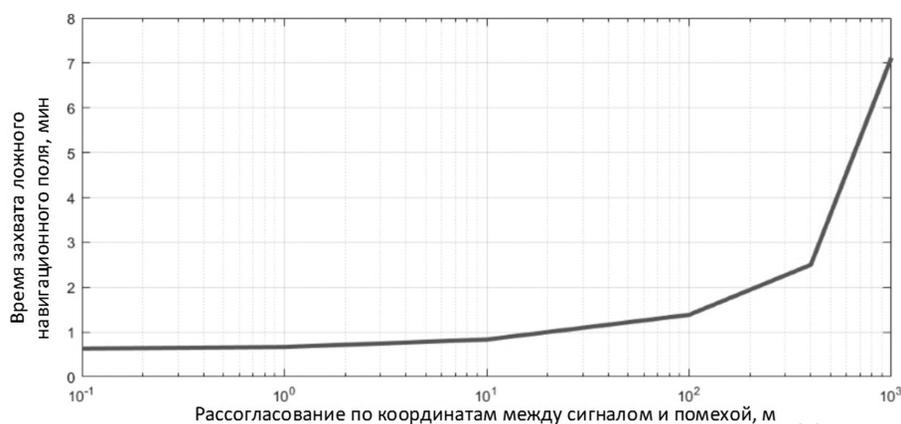


Рис. 10. График зависимости времени захвата НП от рассогласования по передаваемым координатам между истинным и имитируемым сигналами

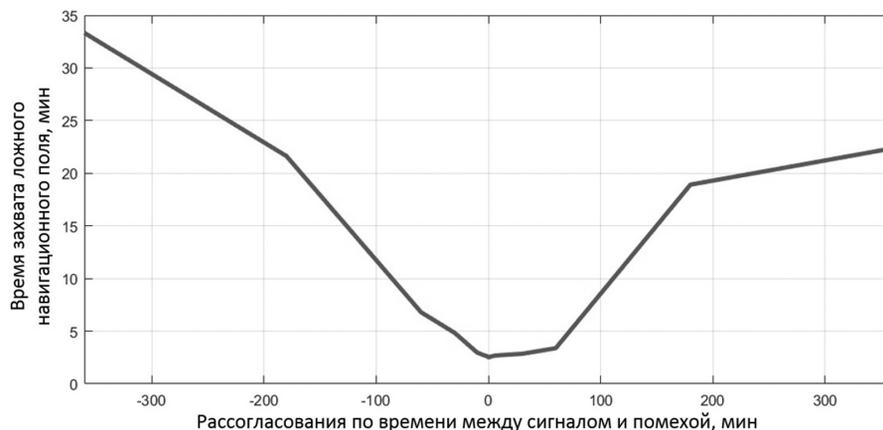


Рис. 11. Графики зависимости времени захвата ложного НП от рассогласования по времени между помехой и сигналом

2. Определение времени захвата ложного НП при различной удаленности имитируемого местоположения от истинного.

На рис. 10 приведен график зависимости времени захвата НП от удаленности имитируемого местоположения от истинного. Оценка проводилась при следующих исходных данных:

$(P_c / P_n) = -26,5$ дБ; рассогласование по передаваемому в навигационном сообщении времени между истинным сигналом и имитирующей помехой — не более 1 с.

На рис. 10 видно, что с увеличением рассогласования по координатам между сигналом и помехой, для рассматриваемого навигационно-

го приемника, возрастает время захвата ложного навигационного поля.

3. Определение времени захвата НП при различном рассогласовании по передаваемому в навигационном сообщении времени между сигналом и помехой.

На рис. 11 приведен график зависимости времени захвата НП от рассогласования по времени между истинным и имитируемым сигналами. Оценка проводилась при следующих исходных данных: $(P_c / P_n) = -26,5$ дБ; рассогласование по передаваемым координатам между истинным и имитируемым сигналами — 400 м.

Анализ рис. 11 показывает, что увеличение рассогласования по передаваемому в навигационном сообщении времени между сигналом и помехой существенно влияет на помехоустойчивость рассматриваемого навигационного приемника.

Заключение

В ходе проведенной работы разработан макет, позволяющий формировать навигационное поле с помощью трансивера, основанного на SDR-технологии. Проведена оценка особенностей воздействия непреднамеренных информационно-подобных помех на навигационный приёмник. На основе анализа полученных результатов (рис. 8, 9, 10, 11) могут быть сформулированы следующие выводы:

- на практике навигационные приемники оказываются достаточно помехоустойчивыми для непреднамеренных информационно-подобных помех низкого уровня, ввиду значительной сложности прицельного попадания параметров помехи в узкие стробы слежения за задержкой и частотой сигнала. Захват ложного навигационного поля происходит при уровнях помех, обеспечивающих предварительный срыв слежения за истинным сигналом. Устойчивое функционирование НАП (низкая вероятность захвата ложного НП, $P_{\text{захвата}} = 0,1$ и менее) обеспечиваются при отношении $(P_c / P_n) \geq -15$ дБ;

- с увеличением рассогласования по координатам между сигналом и помехой наблюдается повышение помехоустойчивости рассматриваемого навигационного приемника. Вероятнее всего, это связано с алгоритмом «допоиска» навигационного сигнала, когда после срыва слежения в каждом из каналов рассматриваемого прием-

ника поиск сигнала ведется в «районе» его потери с постепенным увеличением области поиска. Для рассматриваемого приемника наилучшая помехоустойчивость достигается при больших отклонениях по координатам между помехой и сигналом;

- при увеличении рассогласования по передаваемому в навигационном сообщении времени между сигналом и помехой наблюдается возрастание временного интервала, в течении которого происходит захват навигационного поля. Значительные (более 1 часа) скачки по времени существенно повышают помехоустойчивость рассматриваемого приемника.

Литература

1. Фомин А.В., Вознюк В.В., Маслаков П.А. Исследование помехоустойчивости аппаратуры потребителей глобальной навигационной спутниковой системы GPS на основе технологии программного приема // Труды Военно-космической академии им. А.Ф. Можайского. Вып. № 650. — СПб: ВКА им. А.Ф. Можайского. 2016. С. 33–40.
2. Interface specification. IS-GPS-200L. Navstar GPS Space Segment/Navigation User Interface / Global positioning systems directorate. Systems engineering & integration. 2020.
3. Конин В.В. Спутниковые навигационные системы. — Киев. 2008. 249 с.
4. Kai Borre. A software-defined GPS and Galileo receiver. Birkh'auser. 2007.
5. James Bao-Yen. Tsui. Fundamental of Global Positioning System Receivers: A Software Approach. Jonh Wiley and Sons, Inc. — New York. 2000.
6. Московский авиационный институт (Государственный технический университет) Каф. № 401 «Радиолокация и радионавигация» [Электронный ресурс]. Режим доступа: http://kaf401.rloc.ru/files/GPS_signals.pdf, свободный (18.08.2020).
7. Cheng X.J., Cao K.J., Xu J.N., Li B. Analysis on forgery patterns for GPS civil spoofing signals // 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09). — Seoul, Korea. November 2009. P. 353–356.
8. Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W., and Kintner P.M. Assessing the

spoofing threat: development of a portable gps civilian spoofer // 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '08) — Savannah, Ga, USA. September 2008. P. 2314–2325.

9. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки [Электронный ресурс]. Режим доступа: <https://github.com/osqzss/gps-sdr-sim>, свободный (14.08.2020).

10. Спецификация RINEX v2.11.

11. Архив космической геодезической информации Национального управления по аэронавтике и исследованию космического пространства (NASA) [Электронный ресурс]. Режим доступа: <ftp://cddis.gsfc.nasa.gov/gnss/data/daily/>, свободный (14.07.2021).

12. Официальный сайт производителя трансивера HackRF one [Электронный ресурс]. Режим доступа: <https://hackrfone.com>, свободный (14.07.2021).

References

1. Fomin A.V., Voznyuk V.V., Maslakov P.A. Investigation of noise immunity of navigation equipment of consumers of the global navigation system GPS based on the technology of software reception // Trudy Voenno-kosmicheskoy akademii imeni A.F. Mozhajskogo. Vol. № 650. — SPb: VKA. 2016. P. 33–40.

2. Interface specification. IS-GPS-200L. Navstar GPS Space Segment/Navigation User Interface / Global positioning systems directorate. Systems engineering & integration. 2020.

3. Konin V.V. Satellite navigation systems. — Kiev. 2008. 249 p.

4. Kai Borre. A software-defined GPS and Galileo receiver. Birkh'auser. 2007.

5. James Bao-Yen. Tsui. Fundamental of Global Positioning System Receivers: A Software Approach. John Wiley and Sons, Inc. — New York. 2000.

6. State Technical University department № 401 «Radar and radio navigation» [Elektronnyj resurs] Rezhim dostupa: http://kaf401.rloc.ru/files/GPS_signals.pdf, svobodnyj (18.08.2020).

7. Cheng X.J., Cao K.J., Xu J.N., Li B. Analysis on forgery patterns for GPS civil spoofing signals // 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09). — Seoul, Korea. November 2009. P. 353–356.

8. Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W., and Kintner P.M. Assessing the spoofing threat: development of a portable gps civilian spoofer // 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '08) — Savannah, Ga, USA. September 2008. P. 2314–2325.

9. The largest web service for hosting IT projects and their joint development. [Elektronnyj resurs]. Rezhim dostupa: <https://github.com/osqzss/gps-sdr-sim>, svobodnyj (14.08.2020).

10. Specification of RINEX v2.11.

11. Archive of Space Geodetic Information of the National Aeronautics and Space Administration (NASA). [Elektronnyj resurs]. Rezhim dostupa: <ftp://cddis.gsfc.nasa.gov/gnss/data/daily/>, svobodnyj (14.07.2021).

12. Official website of the manufacturer HackRF one transceivers. [Elektronnyj resurs]. Rezhim dostupa: <https://hackrfone.com>, svobodnyj (14.07.2021).