

Научная статья

УДК 621.39; 004.056

DOI:10.31854/1813-324X-2023-9-6-95-100



Характеристики уязвимости аппаратуры потребителей глобальных навигационных спутниковых систем к спуфинг-атакам

✉ Валерий Владимирович Неровный¹, valery.km@yandex.ru

✉ Павел Дмитриевич Коратаев¹, korataev2015@mail.ru

✉ Пётр Сергеевич Облов¹, oblov1997@yandex.ru

✉ Марина Юрьевна Толстых^{2,3}✉, marina_lion@mail.ru

¹Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина»,
Воронеж, 394064, Российская Федерация

²Московский государственный лингвистический университет,
Москва, 119034, Российская Федерация

³Московский университет МВД России им. В.Я. Кикотя,
Москва, 117437, Российская Федерация

Аннотация: В статье рассмотрены подходы к оценке уязвимости навигационной аппаратуры потребителей глобальных навигационных спутниковых систем (НАП ГНСС) к спуфинг-атакам, а также технологии защиты от помех и спуфинга. Предложены подходы и средства для оценки уязвимости НАП ГНСС при наличии имитирующих помех. Полученные результаты могут быть использованы разработчиками при создании НАП ГНСС нового поколения с улучшенной защитой от спуфинга.

Ключевые слова: навигационная аппаратура потребителей глобальных навигационных спутниковых систем, спуфинг, помеха, угроза, моделирование, уязвимость

Ссылка для цитирования: Неровный В.В., Коратаев П.Д., Облов П.С., Толстых М.Ю. Характеристики уязвимости аппаратуры потребителей глобальных навигационных спутниковых систем к спуфинг-атакам // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 95–100. DOI:10.31854/1813-324X-2023-9-6-95-100

Vulnerability Characteristics of Global Navigation Satellite System Consumer Equipment to Spoofing Attacks

✉ Valery Nerovny¹, valery.km@yandex.ru

✉ Pavel Korataev¹, korataev2015@mail.ru

✉ Petr Oblov¹, oblov1997@yandex.ru

✉ Marina Tolstykh^{2,3}✉, marina_lion@mail.ru

¹Military Educational and Scientific Center of the Air Force N.E. Zhukovsky and Y.A. Gagarin Air Force Academy, Voronezh, 394064, Russian Federation

²Moscow State Linguistic University,
Moscow, 119034, Russian Federation

³Kikot Moscow University of the Ministry of Internal Affairs of Russia,
Moscow, 117437, Russian Federation

Abstract: The article presents approaches to assessing the vulnerability of navigation equipment of global navigation satellite systems consumers to spoofing attacks, as well as technologies for protection against interference and spoofing. Approaches and tools are proposed for assessing the vulnerability of navigation equipment of global navigation satellite systems in the presence of simulated interference. The results obtained can be used by developers to create a new generation global navigation satellite systems with improved protection against spoofing.

Keywords: navigation equipment of consumers of global navigation satellite systems, spoofing, interference, threat, modeling, vulnerability

For citation: Nerovny V., Korataev P., Oblov P., Tolstykh M. Vulnerability Characteristics of Global Navigation Satellite System Consumer Equipment to Spoofing Attacks. *Proceedings of Telecommun. Univ.* 2023;9(6):95–100. DOI:10.31854/1813-324X-2023-9-6-95-100

Введение

Большинство современных систем перевозок и перемещений реализуются посредством поддержки глобальных навигационных спутниковых систем (ГНСС) для обеспечения точной навигации. Высокоточные приемники ГНСС на борту современных судов и транспортных средств (как в гражданской, так и военизированной областях) в большей степени заслуживают доверия. Однако ввиду динамичных в своем открытии и внедрении технологических разработок, а также вредоносной деятельности со стороны противников (злоумышленников) концепция априорного доверия к системам навигации, очевидно, становится не актуальной.

Известны множественные случаи непреднамеренной передачи ГНСС-сигналов, а также вмешательства в их прием (внутриполосные или внеполосные помехи) [1, 2]. Кроме того, набирает популярность практика обмана приемников ГНСС, сообщающих ложные данные о метаположении или времени (спуфинг, *от англ. Spoofing*). При этом демонстрировалось, что подобные деструктивные манипуляции осуществлялись с помощью относительно недорогого оборудования и с наличием небольших экспертных знаний у атакующих. Фактически структура данных, схемы модуляции и коды расширения общедоступны, в совокупности данные особенности позволяют создавать помехи и подделку.

Отмеченное подтверждает факт снижения существующих защитных барьеров для злонамеренных атак с далеко идущими последствиями. Следовательно, априорное доверие к ГНСС не релевантно, необходимы методы надежного обнаружения, оценки и борьбы с помехами и спуфингом, осуществляемых в отношении ГНСС.

К настоящему моменту в мировых масштабах однозначно не определена унифицированная практика мониторинга спуфинга навигационных сигналов, также отсутствуют юридически закрепленные критерии оценки и анализа указанных инцидентов безопасности. Вместе с тем известен ряд работ, посвященных тематике спуфинга навигационной аппаратуры потребителей ГНСС (НАП ГНСС) [1–8]. В

связи с растущей зависимостью различных отраслей промышленности от ГНСС остро стоит вопрос обработки последствия перебоев в работе ГНСС-услуг, которые могут быть критическими с точки зрения обеспечения безопасности, превенции или локализации экономического, социального или экологического ущерба.

Таким образом, востребована разработка подходов к способам и средствам снижения уязвимости ГНСС к спуфинг-атакам, включая резервное копирование метаданных о навигации, позиционирования, времени, полное использование текущих программ модернизации ГНСС, мониторинг и расширение целостности систем, а также технологии защиты от помех и противодействия спуфингу.

Подходы к оценке уязвимости навигационной аппаратуры потребителей глобальных навигационных спутниковых систем к спуфинг-атакам

В зарубежной технической литературе термин Spoofing используется для обозначения имитирующих помех. Работы, посвященные его анализу и изучению в отношении НАП ГНСС, ведутся, в основном, по двум направлениям:

- формирование алгоритмов и технологий создания имитирующих помех НАП ГНСС [1, 2];
- разработка способов и мер защиты от имитирующих помех [5–7].

Однако остается открытым вопрос оценки уязвимости НАП ГНСС к спуфинг-атакам. Цель данной работы – определение характеристик уязвимости НАП ГНСС к спуфинг-атакам, которые смогут впоследствии дополнить и сформировать унифицированный методологический аппарат к обеспечению безопасности ГНСС, например, в системе менеджмента (управления) уязвимостями.

В современной НАП ГНСС оценка параметров навигационных сигналов в каналах обработки осуществляется в несколько стадий. На стартовой итерации происходит предварительная (грубая) оценка параметров навигационных сигналов, на втором этапе формируются точные текущие оценки параметров (задержки и доплеровского смещения частоты, ДСЧ) навигационных сигналов [3, 4]. Первый

этап реализован поиском навигационных сигналов по соответствующим параметрам, второй – использованием следящих систем за фазой, частотой и задержкой навигационных сигналов.

Необходимо отметить, что поиск навигационных сигналов определяется как задача оценки его задержки и ДСЧ, которые принимаются постоянными на интервале наблюдения. При поиске осуществляется перебор с заданным шагом всего диапазона значений задержки и ДСЧ. Для каждого значения задержки и ДСЧ в каналах обработки вычисляется огибающая, которая сравнивается с порогом и принимается решение о наличии сигнала. За оценку значений параметров принимаются значения задержки и ДСЧ, при которых произошло превышение порога. При отсутствии сигнала анализируются следующие значения параметров, а при его наличии происходит переключение канала обработки в режим слежения за задержкой и ДСЧ.

Аппаратная реализация поиска сигналов в аппаратуре потребителей глобальных навигационных спутниковых систем

При аппаратной реализации алгоритмов поиска сигналов в НАП ГНСС используются режимы «полного поиска» и «допоиска», что обусловлено количеством априорной информации о значениях задержки и ДСЧ принимаемого сигнала. Режим «полного поиска» применяется для случая, когда исходная информация о задержке и ДСЧ-сигнала представлена в недостаточном объеме, отсутствует или является достаточно грубой. Данная ситуация характерна для начального включения НАП ГНСС, когда не имеется никаких сведений о текущих эфемеридах и текущем времени в приемнике. Позиция «допоиска» действована для случая, когда имеется достаточно априорных сведений о характеристиках задержки и ДСЧ с некоторой точностью, что возможно для следующих событий:

- при включении НАП ГНСС присутствуют исходные данные о показателях задержки и ДСЧ либо от внешних источников, либо информация генерируется из данных сохраненного с прошлого сеанса альманаха системы;
- после срыва слежения за сигналом с целью перезахвата сигнала и повторного вхождения в режим слежения;
- при приеме сигнала навигационного спутника из состава орбитальной группировки, появившегося из-за линии радиогоризонта в зоне видимости НАП ГНСС.

Для оценки уязвимости к спуфинг-атакам НАП ГНСС можно представить в виде обобщенной схемы (рисунок 1).

В работе [5] была проведена экспериментальная оценка качества функционирования НАП ГНСС в

условиях спуфинг-атаки при слежении за параметрами навигационных сигналов, а публикация [6] посвящена теоретической оценке качества функционирования НАП ГНСС в условиях спуфинг-атаки при поиске навигационных сигналов.

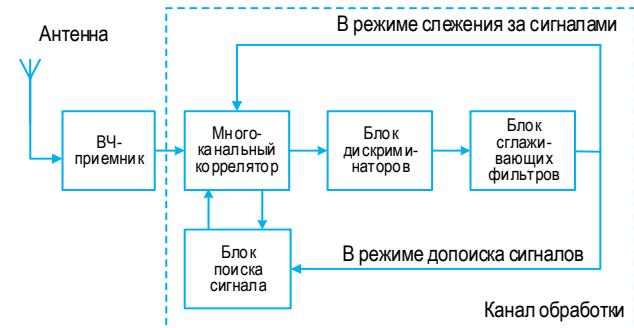


Рис. 1. Обобщенная схема НАП ГНСС для оценки уязвимости к спуфинг-атакам

Fig. 1. Generalized Diagram of Navigation Consumers Equipment of Global Navigation Satellite System (GNSS) for Assessing Vulnerability to Spoofing Attacks

Анализ, приведенных в работах [5, 6] результатов показывает, что захват следящими системами имитирующей помехи происходит при превышении помехи над сигналом не менее 20 дБ, а захват при поиске навигационных сигналов происходит при превышении помехи над сигналом не менее 2–4 дБ. Таким образом, можно сделать вывод о том, что наибольшая уязвимость НАП ГНСС к спуфинг-атаке будет при поиске навигационных сигналов. При этом одинаковой уязвимостью к спуфинг-атаке в НАП ГНСС будут обладать режимы «полного поиска» и «допоиска».

Ограничение задачи исследования и эксперимента

При выборе показателя уязвимости к спуфинг-атаке НАП ГНСС необходимо учитывать следующие ограничения и допущения:

- НАП ГНСС находится в зоне действия источника ложных навигационных сигналов;
- уровень имитирующих помех превышает уровень навигационных сигналов на 2–4 дБ;
- для успешного проведения спуфинг-атаки достаточно приема и обработки хотя бы одной помехи, имитирующей навигационные сигналы;
- в начальный при воздействии спуфинг-атаки момент НАП ГНСС осуществляет слежение за параметрами навигационных сигналов, а переключение в режим «допоиска» происходит при приеме сигнала одного или нескольких навигационных спутников из состава орбитальной группировки, появившегося из-за линии радиогоризонта в зоне видимости.

С учетом ограничений и допущений в качестве показателя целесообразно выбрать:

– время появления T_{nc} одного или нескольких навигационных спутников из состава орбитальной группировки из-за линии радиогоризонта в зоне видимости НАП ГНСС;

– вероятность уязвимости к спуфинг-атаке P_{ca} , которая определяется как вероятность появления за заданное время в зоне видимости НАП ГНСС одного или нескольких навигационных спутников.

Для наблюдателя, находящегося в области пространства, где размещена НАП ГНСС, время T_{nc} будет случайной величиной. Ради количественной оценки статистических характеристик величины T_{nc} (математического ожидания, дисперсии и функции распределения) была разработана программа для ЭВМ, в которой моделируется динамика изменения пространственной конфигурации созвездий различных ГНСС.

Работа программы моделирования изменений пространственной конфигурации созвездий ГНСС

Основу программы составляет модель невозмущенного движения спутников, которая задается математическими соотношениями [7]:

$$X = (R_3 + H_{nc}) \times \\ \times (\cos \omega_n \cdot \cos \lambda - \sin \omega_n \cdot \sin \lambda \cdot \cos i), \quad (1)$$

$$Y = (R_3 + H_{nc}) \cdot \\ \times (\cos \omega_n \cdot \cos \lambda + \sin \omega_n \cdot \sin \lambda \cdot \cos i), \quad (2)$$

$$Z = (R_3 + H_{nc}) \cdot \sin \omega_n \cdot \sin i, \quad (3)$$

$$\omega_n = \omega_0 + t_{\text{тек}} \cdot \frac{2\pi}{T_{cp}} \quad (4)$$

$$\lambda = \lambda_0 + t_{\text{тек}} \cdot \frac{2\pi}{T_{cp}}, \quad (5)$$

где X, Y, Z – геоцентрические координаты навигационного спутника; H_{nc} – высота орбиты навигационного спутника; ω_0 – начальное значение Аргумента перигея; λ_0 – начальное значение долготы восходящего узла; R_3 – радиус Земли; i – текущее значение наклонения орбиты навигационного спутника; T_{cp} – среднее значение драконического периода обращения навигационного спутника; ω_n – Аргумент перигея (рад); $t_{\text{тек}}$ – текущее время, на которое рассчитываются параметры движения спутника (сек.).

Исходными данными для программы являются геодезические координаты НАП ГНСС и вектора начальных геоцентрических координат навигационного спутника. В каждый момент времени в программе рассчитывается количество видимых спутников и время появления нового спутника в зоне видимости НАП ГНСС.

Для вновь появившегося i -го спутника определяется значение времени T_{nci} . После завершения работы программы формируется выборка значений времени T_{nc} объемом N для каждой ГНСС. После

ранжирования для каждой выборки определяются: выборочные средние, выборочные значения среднеквадратического отклонения и эмпирические функции распределения [8]:

$$\bar{T}_{nc} = \frac{1}{N} \sum_{i=1}^N T_{nci}, \quad (6)$$

$$\sigma_{T_{nc}} = \sqrt{\frac{1}{N} \sum_{i=1}^N (T_{nci} - \bar{T}_{nc})^2}, \quad (7)$$

$$F_n(T_{nc}) = \frac{n_{T_{nc}}}{N}, \quad (8)$$

где \bar{T}_{nc} – выборочное среднее; $\sigma_{T_{nc}}$ – выборочное значение среднеквадратического отклонения; $F_n(T_{nc})$ – эмпирическая функция распределения; $n_{T_{nc}}$ – количество значений меньше T_{nc} .

Результаты моделирования

С использованием разработанной программы в среде MatLab/Simulink получены статистические характеристики случайной величины T_{nc} для ГНСС ГЛОНАСС, GPS, ГАЛИЛЕО и КОМПАСС, которые приведены в таблице 1, где N – объем выборки.

ТАБЛИЦА 1. Статистические характеристики T_{nc} для ГНСС ГЛОНАСС, GPS, ГАЛИЛЕО и КОМПАСС

TABLE 1. Statistical Characteristics of T_{nc} for GNSS GLONASS, GPS, GALILEO and KOMPASS

Тип ГНСС	N	\bar{T}_{nc} , сек	$\sigma_{T_{nc}}$, сек
ГЛОНАСС	3408	2534	1497
GPS	4883	2065	1217
ГАЛИЛЕО	4251	2030	1447
КОМПАСС	4505	1916	1487

Эмпирические функции распределения случайной величины T_{nc} для ГНСС ГЛОНАСС, GPS, ГАЛИЛЕО и КОМПАСС приведены на рисунке 2.

Полученные эмпирические функции распределения позволяют определить вероятность уязвимости к спуфинг-атаке за заданное время как:

$$P_{ca}(T_{nc3} < T_{nc}) = F(T_{nc3}). \quad (9)$$

Для времени $T_{nc3} = 600$ сек вероятность уязвимости к спуфинг-атаке составила для НАП ГНСС: ГЛОНАСС – 0.075, GPS – 0.25, ГАЛИЛЕО – 0.18, КОМПАСС – 0.2.

Разброс значений вероятности уязвимости к спуфинг-атаке P_{ca} для НАП, осуществляющим функционирования по сигналам разных ГНСС, можно объяснить различным количеством навигационных спутников, а также пространственными конфигурациями орбитальных группировок.

Заключение

Сигналы ГНСС уязвимы к помехам, которые блокируют прием навигационных сообщений прием-

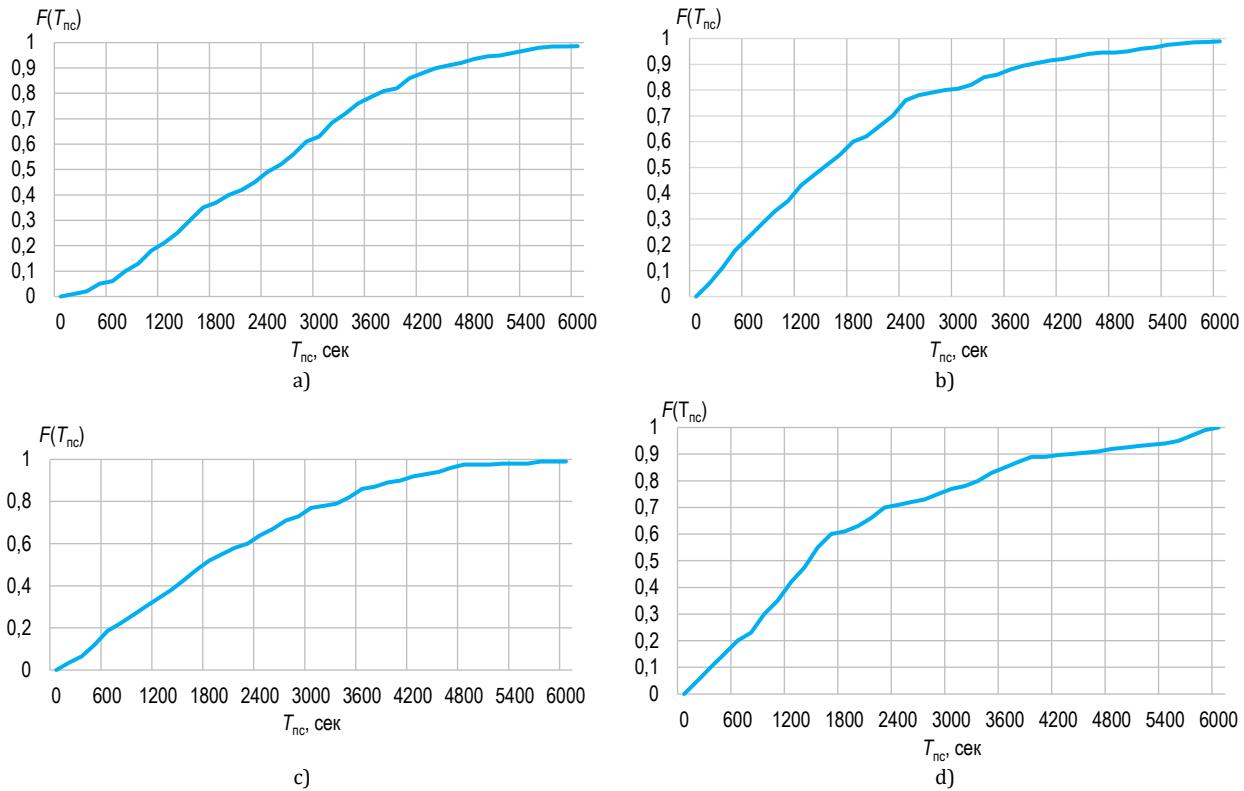


Рис. 2. Эмпирическая функция распределения случайной величины T_{nc} для ГНСС ГЛОНАСС (а), GPS (б), ГАЛИЛЕО (с) и КОМПАСС (д)

Fig. 2. Empirical Distribution Function of random Variable T_{nc} for GNSS GLONASS (a), GPS (b), GALILEO (c) and KOMPASS (d)

никами, а также к спуфингу, который манипулирует местоположением и временем, вычисляемых приемниками. В условиях растущей зависимости от ГНСС для определения местоположения, навигации и синхронизации времени, чтобы избежать возможных последствий преднамеренных и не-преднамеренных атак на сигналы, следует уделять особое внимание шагам по оценке и снижению уязвимости НАП ГНСС, а также технологиям защиты от помех и противодействия спуфингу.

Отмеченные виды представляют собой тип радиопомех ГНСС, которые возникают, когда слабые сигналы спутниковой системы подавляются более сильными радиосигналами на той же частоте, при этом спуфинг можно отождествлять как интеллектуальную форму вмешательства, во время работы которой расположенный поблизости радиопередатчик посылает ложные сигналы в целевой приемник.

В данной работе были проанализированы процессы поиска навигационных сигналов, которые определяются как задача оценки его задержки и ДСЧ, которые принимаются постоянными на интервале наблюдения, с целью определения характеристик уязвимости НАП ГНСС к спуфинг-атакам. С учетом ограничений и допущений в качестве показателя были выбраны время появления T_{nc} одного или нескольких навигационных спутников из состава орбитальной группировки из-за линии ра-

диогоризонта в зоне видимости НАП ГНСС и вероятность уязвимости к спуфинг-атаке P_{ca} .

Полученные путем моделирования эмпирические функции распределения позволили определить вероятность уязвимости к спуфинг-атаке навигационных приемников, работающих с сигналами различных ГНСС. Из результатов можно сделать вывод: воздействие спуфинг-атак снижает эффективность функционирования аппаратуры потребителя, не зависимо от типа спутниковой навигационной системы, с которой она сопряжена. Однако наилучшую устойчивость к спуфинг-атакам демонстрирует аппаратура, функционирующая по сигналам отечественной системы ГНСС ГЛОНАСС.

Полученные в данном эксперименте результаты могут быть использованы отечественными организациями-разработчиками при создании НАП ГНСС нового поколения с улучшенной защитой от спуфинга, а также в качестве дополнения к процессам управления уязвимостями НАП ГНСС на всем жизненном цикле системы менеджмента безопасности, включая этапы мониторинга и оценки их применимости, определения уровня критичности применительно к НАП ГНСС, определения методов и приоритетов устранения и принятия мер, направленных на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

Список источников

1. Лемешко Н., Патшин А. Оценка качества функционирования спутниковых навигаторов при наличии помех с использованием векторных генераторов R&S SMW200A и R&S SMBV100B // Электроника: наука, технология, бизнес. 2020. № 3. С. 122–125. DOI:10.22184/1992-4178.2020.194.3.122.125
2. Рубцов Н.С. Алгоритм защиты от спуффинга аппаратуры потребителей спутниковых навигационных систем // Известия Тульского государственного университета. Технические науки. 2018. № 4. С. 92–101.
3. Перова А. И., Харисова В.Н. ГЛОНАСС. Принципы построения и функционирования. М.: Радиотехника, 2010. 800 с.
4. Яценков В.С. Основы спутниковой навигации. Системы GPSNAVSTAR и ГЛОНАСС. М.: Горячая линия – Телеком, 2005. 272 с.
5. Лемешко Н., Патшин А. Оценка качества функционирования спутниковых навигаторов при наличии помех с использованием векторных генераторов R&S SMW200A и R&S SMBV100B Часть 2 // Электроника: наука, технология, бизнес. 2020. № 4. С. 78–84. DOI:10.22184/1992-4178.2020.195.4.78.84
6. Неровный В.В., Кирюшкин В.В., Бабусенко С.И., Коратаев П.Д., Облов П.С. Вероятностные характеристики системы поиска и обнаружения навигационных сигналов в условиях имитирующих помех // Радиотехника. 2023. Т. 87. № 7. С. 60–66. DOI:10.18127/j00338486-202307-07
7. Grewal M.S., Weill L.R., Andrews A.P. Global Positioning Systems, Inertial Navigation, and Integration. John Wiley & Sons, Inc., 2001. DOI:10.1002/0471200719
8. Советов Б.Я., Яковлев С.А. Моделирование систем: учеб. для вузов. М.: Высшая школа, 2001. 343 с.

References

1. Lemeshko N., Patshin A. Evaluation of Satellite Navigators Performance Under Interference Using R&S sMW200A and R&S sMBV100B Vector Generators. *Electronics: Science, Technology, Business*. 2020;3:122–125. DOI:10.22184/1992-4178.2020.194.3.122.125
2. Rubtsov N.S. Algorithm for protection of GNSS Recievers from Spoofing. *Izvestia Tula State University*. 2018;4:92–101.
3. Perova A.I., Kharisova V.N. *GLONASS. Principles of Construction and Functioning*. Moscow: Radiotekhnika Publ.; 2010. 800 p.
4. Yatsenkov V.S. *Basics of Satellite Navigation. GPSNAVSTAR and GLONASS Systems*. Moscow: Goryachaya liniya – Telekom Publ.; 2005. 272 p.
5. Lemeshko N., Patshin A. Evaluation of Satellite Navigators Performance Under Interference Using R&S SMW200A and R&S SMBV100B Vector Generators Part 2. *Electronics: Science, Technology, Business*. 2020;4:78–84. DOI:10.22184/1992-4178.2020.195.4.78.84
6. Nerovny V.V., Kiryushkin V.V., Babusenko S.I., Korataev P.D., Oblov P.S. Probabilistic Characteristics of the Navigation Signal Search and Detection System Under Conditions of Simulated Interference. *Radioengineering*. 2023;87(7):60–66. DOI:10.18127/j00338486-202307-07
7. Grewal M.S., Weill L.R., Andrews A.P. *Global Positioning Systems, Inertial Navigation, and Integration*. John Wiley & Sons, Inc.; 2001. DOI:10.1002/0471200719
8. Sovietov B.Ya., Yakovlev S.A. *Modeling of systems*. Moscow: Vysshaya shkola Publ.; 2001. 343 p.

Статья поступила в редакцию 05.11.2023; одобрена после рецензирования 20.11.2023; принята к публикации 04.12.2023.

The article was submitted 05.11.2023; approved after reviewing 20.11.2023; accepted for publication 04.12.2023.

Информация об авторе:

НЕРОВНЫЙ Валерий Владимирович	доктор технических наук, доцент, профессор кафедры приемных и передающих радиоустройств (средств и связи РТО) Военно-воздушной академии им. проф. Н.Е. Жуковского и Ю.А. Гагарина  https://orcid.org/0009-0006-2385-2718
КОРАТАЕВ Павел Дмитриевич	кандидат технических наук, старший преподаватель кафедры авиационных систем и комплексов радионавигации и радиосвязи Военно-воздушной академии им. проф. Н.Е. Жуковского и Ю.А. Гагарина  https://orcid.org/0009-0000-3634-2772
ОБЛОВ Пётр Сергеевич	адъюнкт кафедры приемных и передающих радиоустройств (средств и связи РТО) Военно-воздушной академии им. проф. Н.Е. Жуковского и Ю.А. Гагарина»  https://orcid.org/0009-0005-5885-6463
ТОЛСТЫХ Марина Юрьевна	кандидат технических наук, доцент кафедры международной информационной безопасности института информационных наук Московского государственного лингвистического университета, доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя  https://orcid.org/0009-0001-2223-7709