***ТРАНСПОРТНЫЕ СИСТЕМЫ***
***2.9.1 – Транспортные и транспортно-технологические системы страны, ее регионов и городов, организация производства на транспорте;***
***2.9.4. – Управление процессами перевозок;***
***2.9.6 – Аэронавигация и эксплуатация авиационной техники;***
***2.9.8 – Интеллектуальные транспортные системы***

УДК 621.396.96:621.396
DOI: 10.26467/2079-0619-2025-28-6-8-24

# Technique for improving the immunity of a satellite navigation receiver to intended jamming

**R.O. Arefyev**[1], **N.G. Arefyeva**[1], **O.N. Skrypnik**[2]
[1]*Irkutsk branch of the Moscow State Technical University of Civil Aviation, Irkutsk, Russia*
[2]*Belarusian State Aviation Academy, Minsk, Republic of Belarus*

**Abstract:** Modern unmanned air vehicles (UAV) are equipped with satellite navigation receivers to provide stability in space and maintain the desired track. The satellite navigation receivers feature low noise immunity that can result in loss of satellite signals and, hence, in deviation from the desired track or control loss. The paper presents a technique for improving the immunity of a satellite navigation receiver under wide- and narrow-band interference as well as deceptive interference. The technique was implemented through the analysis of NMEA output data of a satellite navigation receiver. The main advantage of the proposed technique is the use of relatively small computational power of the onboard computer. The proposed technique is based on the analysis of the signal/noise ratio, the number of navigation satellites used as well as the integrity of the output coordinates of an UAV receiver. The proposed technique allowed developing an algorithm for detecting the interference which consists of two stages. At the first stage, presence of interference is identified, the second stage implies the comparison of the output coordinates of the receiver with the desired ones making it possible to assess the effects of deceptive interference. The algorithm is implemented in the G programming language in the LabVIEW environment. The technique and the algorithm for identifying the interference were tested by conducting a series of semi-natural experiments with the CH-3803M signal simulator which allowed estimating the threshold values of signal levels from navigation satellites in the presence of interference. As a test sample the ATGM336H multisystem satellite navigation receiver was used that provides a possibility to select a satellite navigation system (GLONASS, GPS or BeiDou) or to use their combination for solving an UAV navigation problem. The authors conducted a series of experiments for assessing the effects of different interference on the performance of the ATGM336H satellite navigation receiver.

**Key words:** UAV, spoofing, GNSS, signal/noise ratio, NMEA, noise immunity.

**For citation:** Arefyev, R.O., Arefyeva, N.G., Skrypnik, O.N. (2025). Technique for improving the immunity of a satellite navigation receiver to intended jamming. Civil Aviation High Technologies, vol. 28, no. 6, pp. 8–24. DOI: 10.26467/2079-0619-2025-28-6-8-24

# Методика повышения помехоустойчивости приемника спутниковой навигации к воздействию преднамеренных помех

**Р.О. Арефьев**[1], **Н.Г. Арефьева**[1], **О.Н. Скрыпник**[2]
[1]*Иркутский филиал Московского государственного технического университета гражданской авиации, г. Иркутск, Россия*
[2]*Белорусская государственная академия авиации, г. Минск, Республика Беларусь*

**Аннотация:** Современные беспилотные воздушные суда (БВС) оснащены приемниками спутниковой навигации для решения задач стабилизации в пространстве и выдерживания заданной траектории полета. При этом приемники спутниковой навигации отличаются низкой помехоустойчивостью, что может привести к потере сигналов от спутников и, как следствие, к отклонению БВС от заданного маршрута либо к потере управляемости. В данной работе представлена методика повышения помехоустойчивости приемника спутниковой навигации при воздействии широкополосной и узкополосной помех, а также уводящей помехи. Методика реализована на основе анализа выходных данных с приемника спутниковой навигации, формируемых в формате NMEA. Основным достоинством предлагаемого подхода является использование относительно небольших вычислительных ресурсов бортового вычислителя. Предлагаемая методика основана на анализе соотношения сигнал/шум, количества навигационных спутников, используемых в решении навигационной задачи, а также на целостности выходных координат приемника БВС. На основе предложенной методики разработан алгоритм обнаружения воздействия помех, который состоит из двух этапов. На первом этапе определяется наличие помех, второй этап предполагает анализ выходных координат приемника по отношению к планируемым, что позволяет определить воздействия уводящей помехи. Алгоритм реализован на языке программирования G в программной среде LabVIEW. Методика и алгоритм обнаружения помех протестированы путем проведения ряда полунатурных экспериментов с помощью имитатора сигналов СН-3803М, что позволило оценить пороговые значения уровней сигналов от навигационных спутников при наличии помех. В качестве тестируемого образца использовался мультисистемный приемник спутниковой навигации ATGM336H, который обладает возможностью выбора спутниковой навигационной системы (ГЛОНАСС, GPS или BeiDou) или их комбинации для решения задачи навигации БВС. Проведена серия экспериментов по оценке влияния помех различных видов на характеристики приемника спутниковой навигации ATGM336H.

**Ключевые слова:** БВС, спуфинг, GNSS, соотношение сигнал/шум, NMEA, помехоустойчивость.

**Для цитирования:** Арефьев Р.О., Арефьева Н.Г., Скрыпник О.Н. Методика повышения помехоустойчивости приемника спутниковой навигации к воздействию преднамеренных помех // Научный вестник МГТУ ГА. 2025. Т. 28, № 6. С. 8–24. DOI: 10.26467/2079-0619-2025-28-6-8-24

## Introduction

Unmanned Aircraft Systems (UAS) represent a dynamically developing cluster within the aviation industry. The fields of application for UAS are extensive, and new areas for their use are constantly emerging. Furthermore, the prospect involves an increasingly widespread use of UAS performing autonomous flights.

The feasibility and efficiency of autonomous UAS flights depend on the quality and reliability of aeronautical provision. The primary means for performing autonomous flight are satellite navigation systems (GNSS), which offer a global coverage area, high accuracy, and unlimited throughput capacity. However, there are also a number of problems [1–9] that affect the efficiency of satellite navigation use, the most significant of which is the low interference immunity of GNSS receivers. This is because the signals from navigation satellites (NS) at the input of the receiving antenna have a very low level, and even a low-level external interference is sufficient to suppress the weak signals from the NS. Moreover, there are intentional interference signals that imitate the structure of the NS signals, which can cause the receiver to determine false coordinates and generate false flight trajectories for the UAS, making the use of airspace unsafe for other users. Such interference is called meaconing, and the substitution of GNSS signals is known as spoofing (meaning – to substitute, deceive, falsify) [10–13]. The study [14] provides an analysis of statistical data for 2024, showing an increase in spoofing incidents during regular flights of manned aviation. Therefore, an urgent scientific task arises to determine the presence of spoofing and to counteract it, which will enhance flight safety and the efficiency of aeronautical provision for both manned and unmanned aviation.

The main spoofing scenarios are as follows:

using a jammer to force the GNSS receiver from tracking mode into signal search and acquisition mode, and after resetting the correlator, to feed a false satellite signal to the receiver input to form a false trajectory. This scenario is considered a crude type of spoofing;

using a GNSS receiver on the jammer to obtain identical signal delays and Doppler frequency shift values necessary for generating synchronous spoofing with a higher signal level compared to the levels of signals from the NS, which will allow substitution with a false signal. This type of spoofing is more complex and harder to detect.

According to [15, 16], the following methods for spoofing detection exist:

- determining the signal amplitude;
- determining the signal direction of arrival;
- determining the signal arrival time;
- correlating GNSS receiver data with data from other onboard navigation systems;
- authentication using signal encryption;
- determining the signal polarization type;
- detecting vector tracking loops.

To use any of these methods, it is necessary to know the structure of specific GNSS receivers and the algorithms they implement for searching, detecting NS signals, and tracking their delay and frequency. In practice, most GNSS receivers installed on UAS are separate modules with a closed structure, which limits the use of most of the mentioned spoofing detection methods.

Study [2] assessed the interference immunity of a multi-system GNSS receiver module like the ATGM336H under the influence of narrowband interference. The structure of this receiver module allows for separate processing of signals from each system. It was experimentally established that when interference is present at the GPS frequency, the module's performance for the GLONASS system also degrades due to the specifics of intermediate frequency selection in the receiver path.

The GNSS module, connected to the UAS onboard controller, outputs a data packet with coordinates for stabilizing the UAS in space and executing the assigned flight. However, if false GNSS signals are received, the UAS will perform a flight not according to the assigned route, which may be detected by the operator (external pilot) with a significant delay. Therefore, it is necessary to determine the moment when spoofing begins and affects the GNSS receiver in order to promptly notify the operator for making decisions regarding further flight control and excluding information from the satellite receiver from the control loop. For this purpose, a modification in the UAS architecture is proposed, based on the analysis of output data from the satellite receiver. This task can be performed by the flight controller if it has sufficient computational performance, or an additional microcontroller may be required.

This paper presents a methodology for detecting spoofing generated according to the two scenarios considered above, based on the analysis of output data from the ATGM336H receiver module.

## Output Data of the ATGM336H Receiver Module

The ATGM336H is a compact satellite receiver designed to determine user coordinates, speed, and precise UTC time when operating with signals from GPS, GLONASS, and BeiDou systems. Key features of the receiver module:

1. Support for UART interface for data exchange and configuration.
2. Support for high data transfer rates (up to 115200 baud).
3. Low power consumption.
4. Compact size, ensuring easy integration into various devices.
5. Built-in active antenna.
6. High-precision positioning (up to centimeter level) using additional technologies.

The ATGM336H receiver module has a number of characteristics that make it applicable and effective in various fields, including UAS navigation.

The output data from the receiver is a data packet in NMEA0183 format.

"NMEA is a common standard for representing navigation data in text format (ASCII). This protocol is used to transmit GNSS data from the receiver to external devices that are unable to decode the specific manufacturer's receiver navigation message."[1]

The NMEA protocol defines a standard data format that includes information about geographic position, speed, time, course, and other flight parameters. These data are transmitted as text messages containing special codes and fields to identify the type of information.

For developing an algorithm to detect and counter a spoofing attack, it is proposed to analyze data on the parameters of signals received

[1] NMEA-0183 Navigation Data Representation Standard. (2024). OrientSystems. Available at: https://orsyst.ru/blog/nmea (accessed: 23.02.2025).

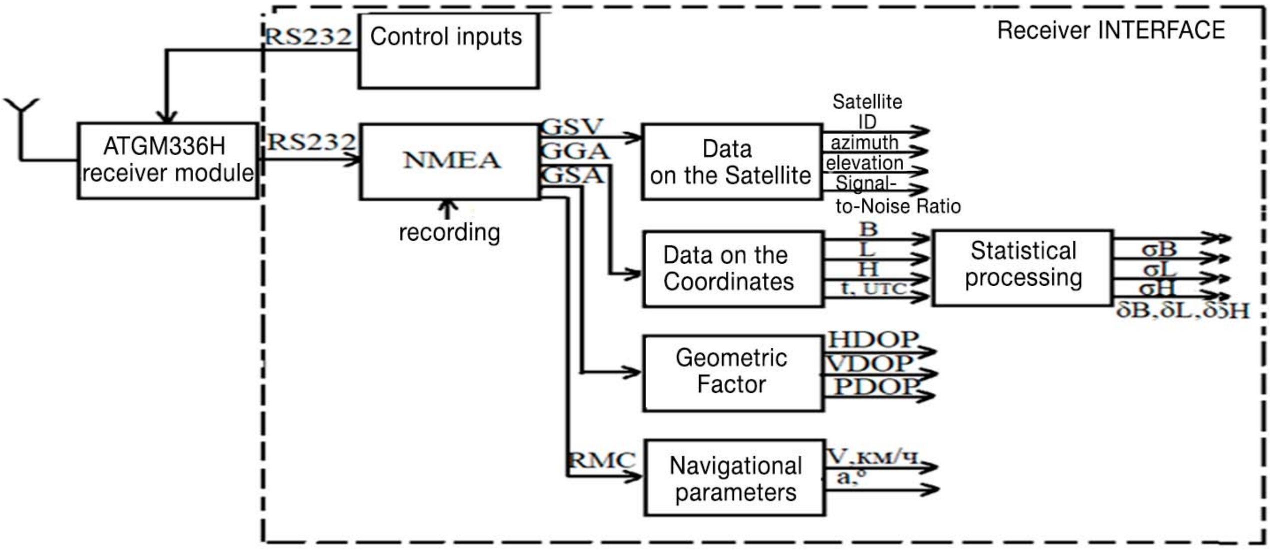


**Fig. 1.** The interface of the ATGM336H receiving module

from the NS, such as the signal-to-noise ratio, satellite azimuth and elevation angle, as well as information about the UAS location and flight parameters. This information can be obtained from the NMEA protocol (from GGA, GSV, and RMC messages). The selection of these messages provides a complete set of receiver data and gives a full picture of the navigation conditions.

An analysis of publications by other authors on the use of NMEA protocol data for spoofing detection has been conducted. For instance, study [13] reviews existing methods for determining spoofing, indicating the possibility of analyzing NMEA protocol data. Work [17] presents the main NMEA protocol messages that can be used for spoofing detection and provides results of testing different types of receivers in the presence of spoofing. In [18], a software platform for comprehensive analysis of NMEA messages from two simultaneously operating receivers located at a fixed distance is presented. The authors describe the main methods: checking navigation parameters (speed and altitude); estimating pairwise distances between receivers; checking ephemeris; monitoring time scale offset; monitoring the signal-to-noise ratio (determining the maximum signal level). The work shows that for maritime transport, the most effective method for determining spoofing is the method of estimating pairwise distances between receivers. The method of monitoring the signal-to-noise ratio was not used in this work.

## Structural Diagram of the Interface for the Satellite Navigation Receiver

A software interface for the ATGM336H receiver module has been developed to study interference immunity, assess accuracy characteristics, and for a number of other tasks. The interface, whose structural diagram is shown in Figure 1, was developed in the LabVIEW graphical programming environment.

The ATGM336H receiver module is connected to a PC via an RS232 serial port and transmits data to the interface at a specified baud rate for further processing. Relevant information is extracted from the GSV, GGA, GSA, and RMC messages. Specifically: data about satellites in view (satellite ID, azimuth, elevation, and Signal-to-Noise Ratio (SNR), measured in dB-Hz) are extracted from the GSV messages. The coordinates determined by the receiver module and the time are extracted from the GGA messages. These coordinates then undergo statistical processing to obtain the Root Mean Square Error (RMSE) and plots of coordinate measurement errors. Information about the UAS's speed and course of movement is extracted from the RMC messages. The developed interface also allows for the processing of GSA messages to extract the GNSS Geometric Dilution of Precision (GDOP) values, which can be used to assess the influence of the geometry of the current satellite constellation on the accuracy of coordinate measurements.

The developed interface also allows for generating commands in the form of PCAS messages to modify the settings of the receiver module. For example, using the appropriate command, one can select the satellite system(s) for the receiver module to operate with, change the output data rate, and more.

The obtained and processed data are subsequently analyzed. Based on this analysis, the receiver module configuration can be adjusted using the generated commands, which can improve its performance in the presence of interference.

## Spoofing countermeasure methodology

The analysis of existing methods for generating false signals indicates that the most straightforward way to perform spoofing currently is by using HackRF One equipment (a software-controlled platform) and an external radio signal amplifier. Consequently, the methodology for detecting meaconing interference must be generalized and include several key criteria for spoofing detection.

As noted earlier, the primary indicator for detecting spoofing onboard a UAS will be the assessment of Signal-to-Noise Ratio (SNR) levels, which allows for the detection of interference that precedes the spoofing signal. Therefore, another indicator for detecting a spoofing signal will be the comparison of the onboard flight plan with the data received from the GNSS receiver. Based on this, the methodology for identifying a spoofing attack consists of two stages:

1. Analysis of the Signal-to-Noise Ratio at the receiver input to identify specific signal levels that may indicate the presence of interference.

2. Comparison of additional information, such as the flight plan (coordinates, course, speed), with data received from the GNSS receiver, which allows for the detection of discrepancies and serves as a basis for reacting to spoofing.

## Determining threshold Signal-to-Noise Ratio levels

The determination of threshold Signal-to-Noise Ratio levels for spoofing detection was performed using a CN-3803M satellite signal simulator. One of the advantages of this simulator is its ability to vary the output signal power in the range from −150 dBm to −100 dBm. Under real-world operating conditions, the typical signal level for a receiver is approximately −120 dBm [2, 19].

Signals from GLONASS and GPS navigation satellites were simulated. The receiver's antenna was placed next to the simulator's antenna.

A series of experiments was conducted with different output signal levels from the simulator, which is equivalent to changing the SNR in the presence of fixed-level interference. The experiments aimed to determine the maximum and minimum signal levels at the receiver input that lead to extreme SNR values. The minimum SNR level is the threshold value at which the navigation solution is computed with very coarse accuracy.

Under normal receiver operating conditions, a decrease in SNR to the minimum threshold value is unlikely. Firstly, during UAS flight at altitude, the receiver is not subject to multipath effects, signal shadowing, and other degrading factors, so the SNR remains relatively stable. Secondly, in the case of wideband or narrowband interference, a decrease in SNR levels is observed for all satellites (depending on the satellite receiver's structure) used in the navigation solution. Therefore, it is necessary to evaluate the average SNR value across signals from all navigation satellites included in the solution.

As an example, Figure 2 shows a graph of the relationship between SNR and the input signal level for GPS navigation satellite No. 3. It follows from Figure 2 that a decrease in the input signal level leads to a decrease in SNR.

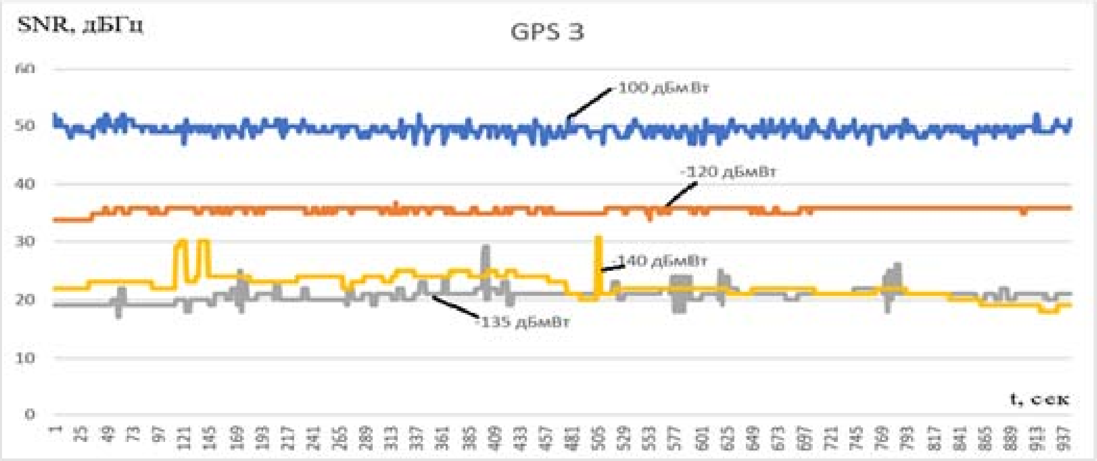


**Fig. 2.** SNR of GPS satellite No. 3 at different input levels

**Table 1**

Average SNR values for different input signal levels

| Input signal level dBm | −100 | −120 | −135 | −140 |
|---|---|---|---|---|
| Average SNR GPS, dB-Hz | 50.6 | 38.8 | 26.4 | 24.2 |
| Average SNR GLONASS, dB-Hz | 52 | 39.6 | 28.6 | 23.3 |

Table 1 presents the average SNR values for the visible GLONASS and GPS constellations separately, calculated using formula (1):

$$M_{GPS,ГЛОНАСС} = \frac{1}{N_{GPS,ГЛОНАСС}} \sum_{i=1}^{N_{GPS,ГЛОНАСС}} SNR_i\ , \qquad (1)$$

where $N$ is the number of visible satellites of the observed system; $i$ is the serial number of a visible satellite of a specific system.

The table shows that decreasing the input signal level below −135 dBm does not lead to a significant degradation of the SNR. At the maximum signal level of −100 dBm, the SNR is approximately 50 dB-Hz for the GPS system and 52 dB-Hz for the GLONASS system, which is not observed under real-world operating conditions. Therefore, an average SNR value for the entire visible constellation of 50 dB-Hz can be used as an upper threshold indicating the presence of meaconing interference.

When receiving signals at critical levels of −135 dBm and −140 dBm, the receiver cannot maintain stable tracking of navigation satellites. This leads to satellites being intermittently included in and excluded from the navigation solution (fig. 3, curve 1 – number of satellites at an input signal level of −135 dBm, curve 2 – at −140 dBm). This primarily affects satellites with the longest ranges (typically those near the horizon).

The Root Mean Square Errors (RMSE) of the receiver's coordinate determination, evaluated over a 950-second time interval, were as follows:

for an input signal level of −135 dBm: latitude σB = 46.8 m, longitude σL = 204.7 m, altitude σH = 3.8 m;

for an input signal level of −140 dBm: latitude σB = 60.7 m, longitude σL = 92.6 m, altitude σH = 6.3 m;

for an input signal level of −120 dBm (the level under real-world operating conditions of the receiver): latitude σB = 2.2 m, longitude σL = 3.8 m, altitude σH = 0.07 m.

Figure 4 shows the plots of coordinate determination errors (latitude error δB – curve 1, longitude error δL – curve 2, altitude error δH – curve 3) for an input signal level of −135 dBm

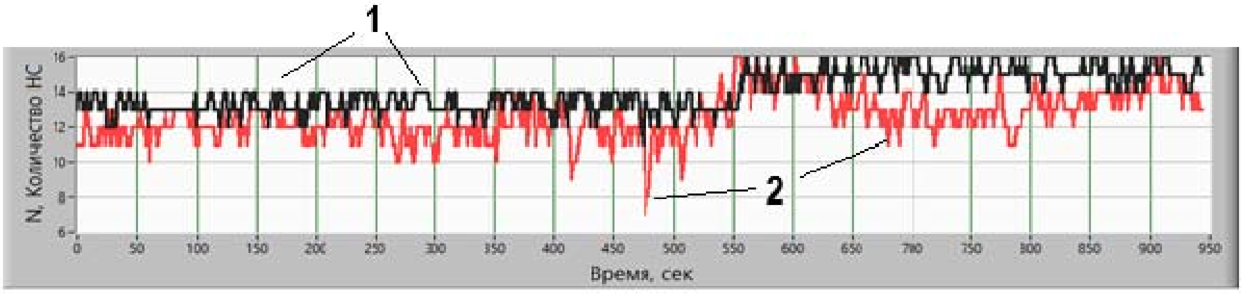
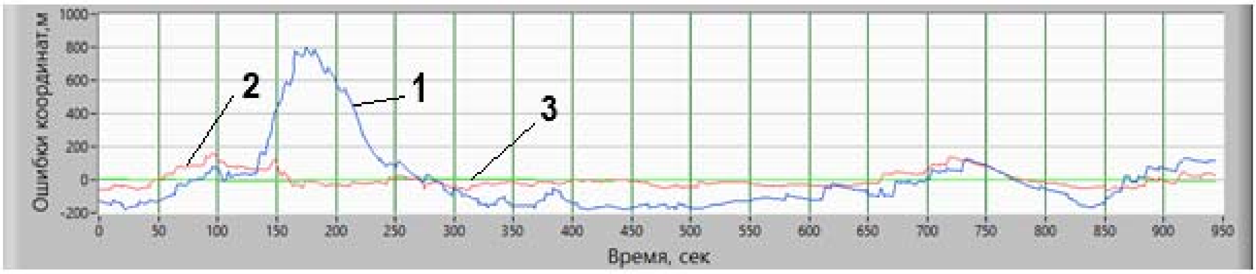
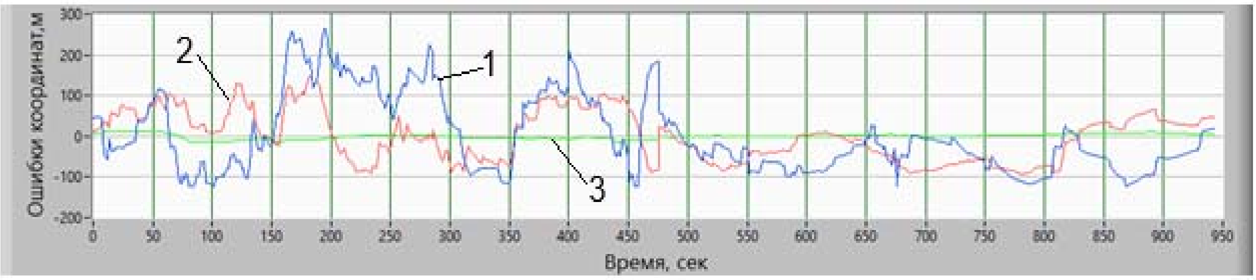


**Fig. 3.** Number (N) of satellites used in solution



a



b

**Fig. 4.** Positioning errors in solving a navigation problem with GLONASS/GPS constellation at the input level of −140 dBmW

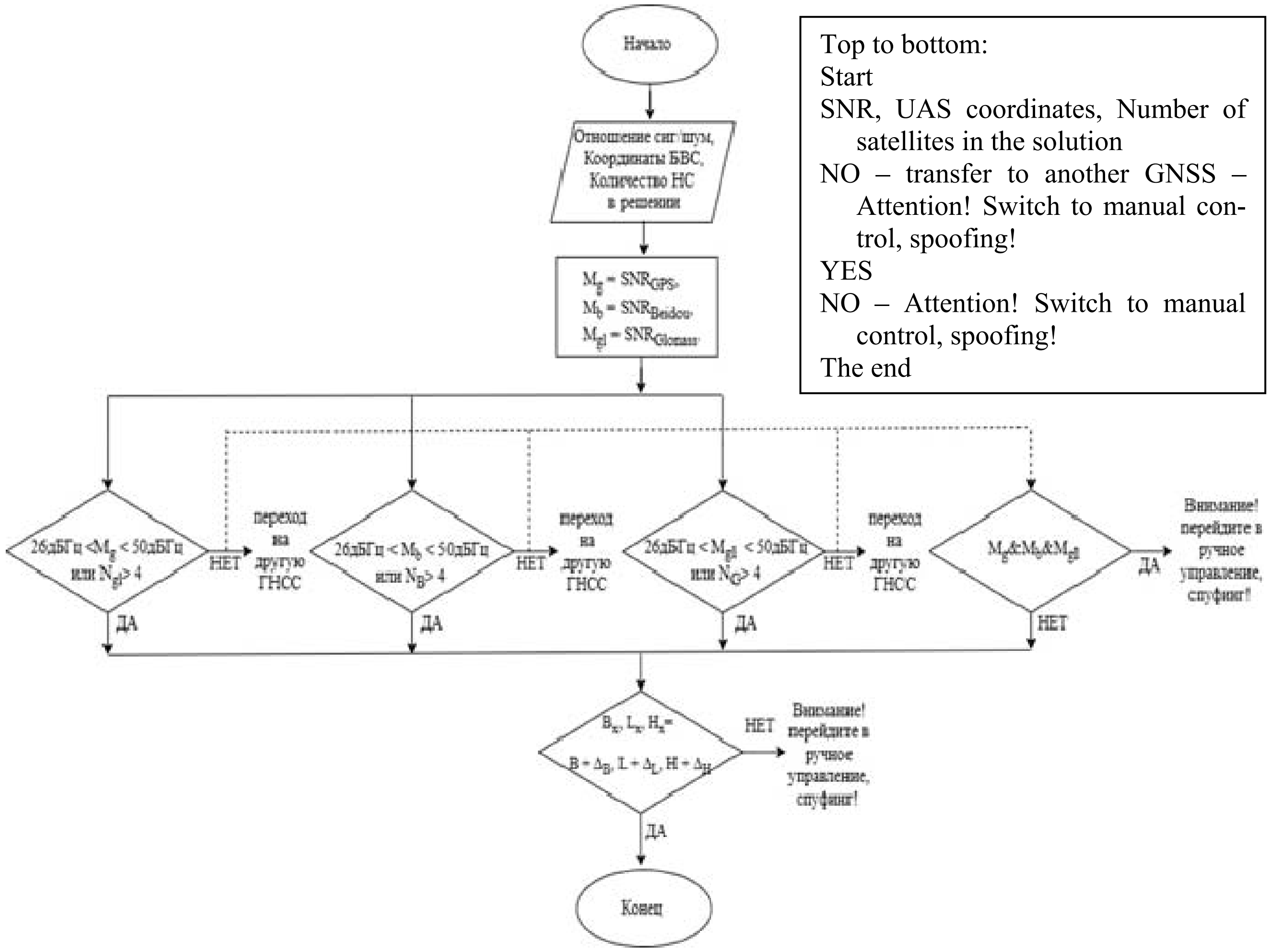
(fig. 4, *a*) and −140 dBm (fig. 4, *b*). Figure 4b shows that due to the instability of horizon satellites, the horizontal coordinate measurement errors vary significantly.

Based on the obtained results, a threshold of 26 dB-Hz should be selected for the minimum signal level. This level is unacceptable under the real-world operating conditions of a GNSS receiver, allowing for the detection of interference.

Thus, to determine the presence of interference that disrupts the satellite navigation receiver's correlator, a lower threshold of 26 dB-Hz will be used. In the case of meaconing interference (spoofing), an upper threshold of 50 dB-Hz will be used. Therefore, the following inequality is used as the criterion for detecting interference:

$$26\ dB\text{-}Hz \le M_{GPS,ГЛОНАСС,Beidou} \le 50\ dB\text{-}Hz.$$

To exclude from the proposed criterion the influence of SNR level reductions from satellites that are entering or leaving the receiver tracking zone, a second criterion must be added. This criterion will be the comparison of the number of satellites used in the GNSS receiver navigation solution against a specified value. The specified value for the number of satellites for each navigation system is chosen as 4, since this is the minimum number required to solve the naviga-


Начало
Отношение сиг/шум,
Координаты БВС,
Количество НС
в решении
$M_g$ = $SNR_{GPS}$,
$M_b$ = $SNR_{Beidou}$,
$M_{gl}$ = $SNR_{Glonass}$
26дБГц <$M_g$ < 50дБГц или $N_{gl}$> 4
НЕТ
переход на другую ГНСС
ДА
26дБГц < $M_b$ < 50дБГц или $N_B$> 4
НЕТ
переход на другую ГНСС
ДА
26дБГц < $M_{gl}$ < 50дБГц или $N_G$> 4
НЕТ
переход на другую ГНСС
ДА
$M_g$&$M_b$&$M_{gl}$
ДА
Внимание! перейдите в ручное управление, спуфинг!
НЕТ
$B_x$, $L_x$, $H_x$= $B + Δ_B$, $L + Δ_L$, $H + Δ_H$
НЕТ
Внимание! перейдите в ручное управление, спуфинг!
ДА
Конец

Top to bottom:
Start
SNR, UAS coordinates, Number of satellites in the solution
NO – transfer to another GNSS – Attention! Switch to manual control, spoofing!
YES
NO – Attention! Switch to manual control, spoofing!
The end

**Fig. 5.** The algorithm for detecting the interference

tion task and is sufficient when using satellites from other systems when the GNSS receiver operates in a multi-system mode. Therefore, the general criterion for detecting interference impact is as follows:

$$4 \le N \vee 26\ dB\text{-}Hz \le M_{GPS,ГЛОНАСС,Beidou} \le 50\ dB\text{-}Hz. \quad (2)$$

## Algorithm for Interference Detection

The algorithm for detecting interference in navigation receivers is presented in Figure 5.

In the first step of the algorithm, the input data from the receiver is set. This includes SNR values for the three systems ($SNR_{GPS}$, $SNR_{GLONASS}$, $SNR_{Beidou}$), the number of satellites used in the navigation solution ($N_{GPS}$, $N_{GLONASS}$, $N_{Beidou}$), the current UAS coordinates ($B_x$, $L_x$, $H_x$), and the UAS flight plan coordinates (B, L, H), which are defined during the pre-flight preparation stage.

In the second step, the average SNR value for the visible constellation is calculated separately for each system ($SNR_{GPS}$, $SNR_{GLONASS}$, $SNR_{Beidou}$) according to expression (1).

In the third step, the calculated average SNR values for each system are compared with condition (2). If the condition is not met for one of the systems, it is assumed that narrowband interference is present at the input of the receiver on the frequency of that specific navigation system. Consequently, a command is automatically generated for the GNSS receiver to exclude this satellite system from the navigation solution. This will lead to improved coordinate determination accuracy and more stable receiver operation.

If the condition is not met for all systems simultaneously, a decision is made that wideband interference is present at the receiver input. In this case, an informational message is generated for the UAS operator about the inability to further use the GNSS receiver, and a recommendation is provided to take manual control of the UAS flight. This allows for avoiding the first stage of spoofing impact.

If the condition is met for at least one of the systems, the algorithm proceeds to the next verification stage.

During the fourth step, the output UAS coordinates are compared with the flight plan coordinates. This stage allows for the detection of meaconing interference, particularly in cases where malicious actors did not generate interference to reset the GNSS receiver's correlator or where the satellite signal substitution occurred before the GNSS receiver was powered on.

If this condition is met, no spoofing is detected, and the algorithm repeats from the beginning with updated data from the receiver.

If the condition is not met, an automatic message is generated for the UAS pilot, instructing a transition to manual control of the UAS. Simultaneously, the GNSS receiver is disconnected from the onboard controller to prevent further diversion of the UAS along a false trajectory.

To prevent false triggers of this condition due to positioning errors, a certain tolerance ($\Delta_B$, $\Delta_L$, and $\Delta_H$) is added to each calculated coordinate value from the flight plan. In this work, $\Delta_B$ and $\Delta_L$ were set to 10 meters (converted to degrees of latitude and longitude), and $\Delta_H$ was set to 5 meters, which helps avoid abrupt altitude changes. The UAS flight altitude is determined using the GNSS receiver at altitudes above 60 meters; at altitudes below 60 meters, a barometric altimeter with optical stabilization systems is used for altitude determination.

Thus, the developed algorithm ensures that the GNSS receiver onboard the UAS can continue solving the navigation task under the influence of narrowband interference at an acceptable level on one system's frequency. It also provides a warning to the operator if wideband interference is present at the GNSS receiver input, or in the case of satellite signal spoofing that has caused the receiver's output coordinates to deviate from the assigned flight route coordinates

## Test Results of the Algorithm Using Hardware-in-the-Loop Simulation

Figure 6 shows the test bench used for testing the interference detection algorithm. The bench includes:

- a CN-3803M signal simulator, which generates navigation satellite signals for the GPS and GLONASS systems according to a predefined scenario where a stationary object is located at a point with zero coordinates;
- a HackRF One module, used as a source of narrowband interference with a signal level of 15 dBm;
- a dual-band wideband interference transmitter with a power of 1 Watt;
- the GNSS receiver module under test, an ATGM336H.

Testing of the developed algorithm was conducted in four stages:

1. Generating narrowband interference on the GPS frequency and on the frequency of the first GLONASS frequency channel.
2. Generating a signal with the simulator above the threshold level, corresponding to the GNSS signal being suppressed by a spoofing signal of higher power.
3. Generating wideband interference.
4. Spoofing the satellite signals, leading the UAS to follow a false trajectory.

## Results of the Study on the Impact of Narrowband Interference on the GPS Frequency and the First GLONASS Frequency Channel

Using the HackRF One module, interference was applied at the GPS L1 frequency of 1575.42 MHz with a power of 30 mW. The interference source antenna was placed next to the antennas of the simulator and the receiver.

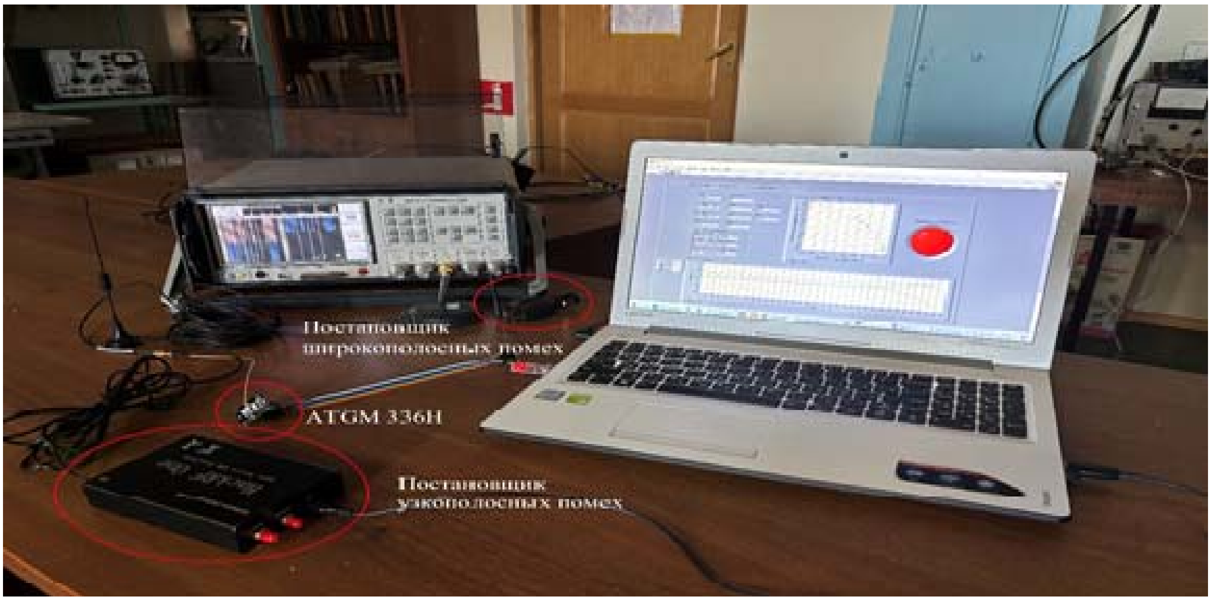
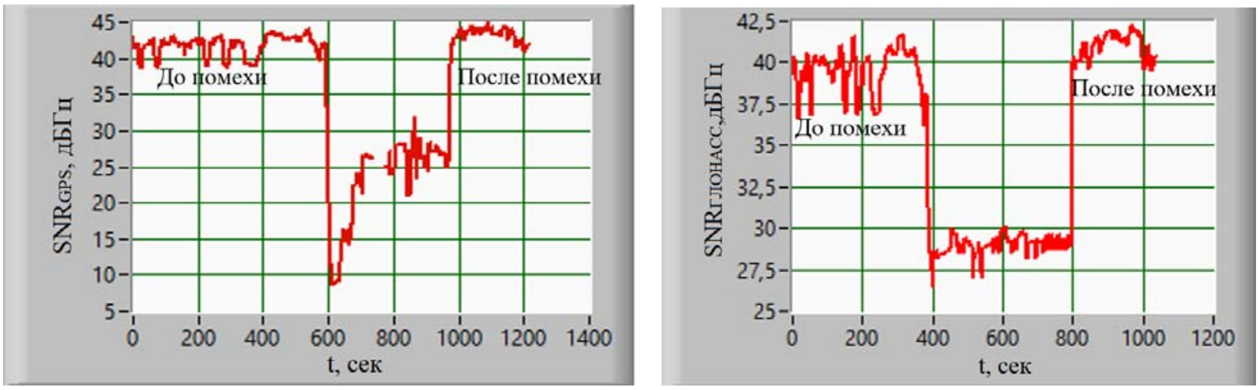

Постановщик широкополосных помех
ATGM 336H
Постановщик узкополосных помех

**Fig. 6.** The test bench for testing the algorithm for detecting the interference



a b

**Fig. 7.** SNR levels: *a* – SNR$_{\text{GPS}}$, *b* – SNR$_{\text{GLONASS}}$
Left to right – before interference – after interference

Figure 7 shows the graphs of the changes in the average SNR$_{\text{GPS}}$ and SNR$_{\text{GLONASS}}$. The results show that the time samples do not coincide, which is associated with the different signal search and acquisition times for the GPS and GLONASS systems.

The sharp drop in SNR$_{\text{GPS}}$ to approximately 8 dB-Hz (fig. 7, *a*) is related to the moment the narrowband interference was generated. During the entire period of interference, unstable tracking of the signals from GPS satellites is observed.

The sharp drop in SNR$_{\text{GLONASS}}$ (fig. 7, *b*) is related to the structure of the ATGM336H module, specifically the passage of one of the harmonics during frequency conversion in the GLONASS channel. However, the SNR$_{\text{GLONASS}}$ level remains above the set lower threshold of 26 dB-Hz. Therefore, solving the navigation task using the GLONASS system is possible, and the algorithm generates a command to disable the GPS system signals.

Figure 8 shows the coordinate measurement errors of the ATGM336H module (latitude error δB – curve 1, longitude error δL – curve 2, alti-

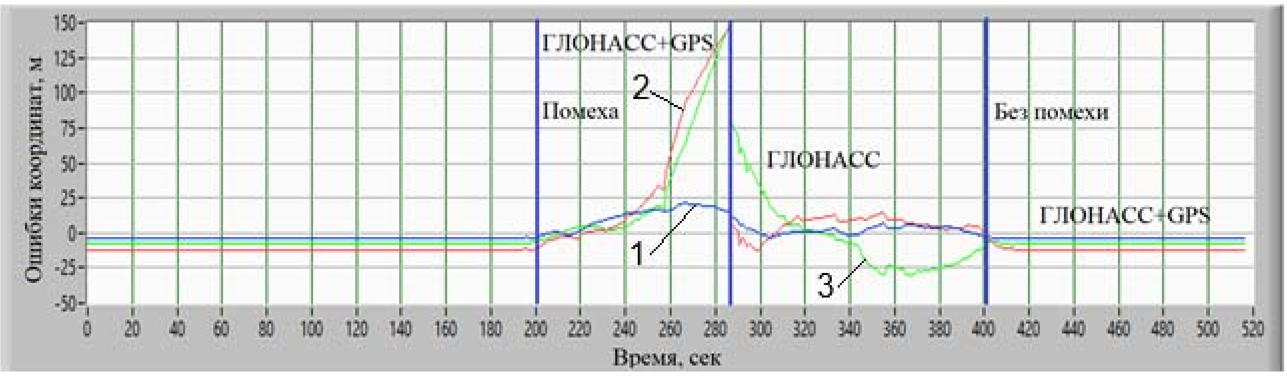


**Fig. 8.** Positioning errors with interference at the GPS frequency
Left to right – Glonass – interference – without interference

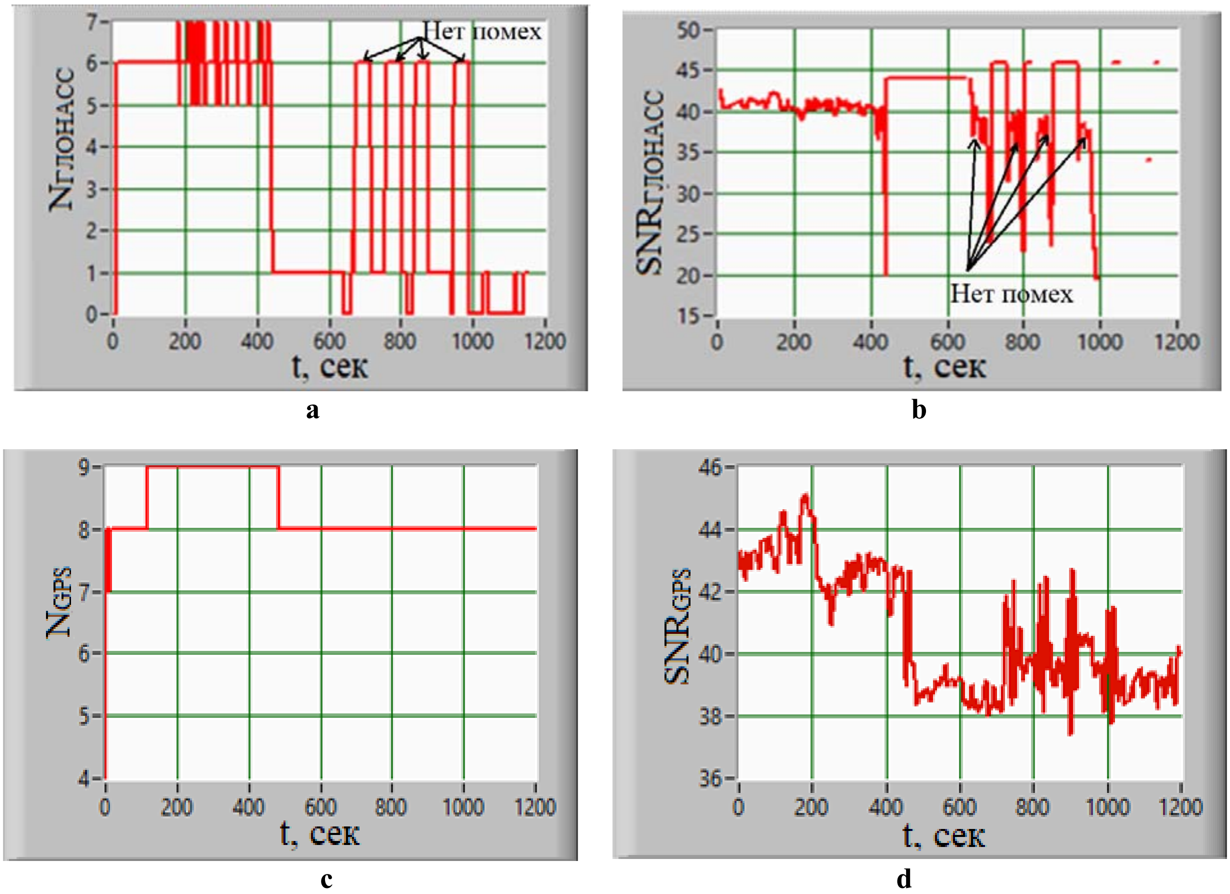


**Fig. 9.** The results of the experiment: *a* – number of GLONASS satellites ised in solution;
*b* – $\mathrm{SNR}_{\mathrm{GLONASSC}}$; *c* – number of GPS satellites ised in solution; *d* – $\mathrm{SNR}_{\mathrm{GPS}}$

tude error δH – curve 3). The figure highlights the moment when the interference was applied, which led to an increase in coordinate determination errors.

After the algorithm generated the command to disable GPS signal reception, a decrease in coordinate measurement errors is observed. This indicates that the GNSS receiver can still be used, albeit with a greater error compared to its accuracy before the interference began.

When narrowband interference is applied at a frequency of 1602 MHz, corresponding to one of the GLONASS frequency channels, a loss of

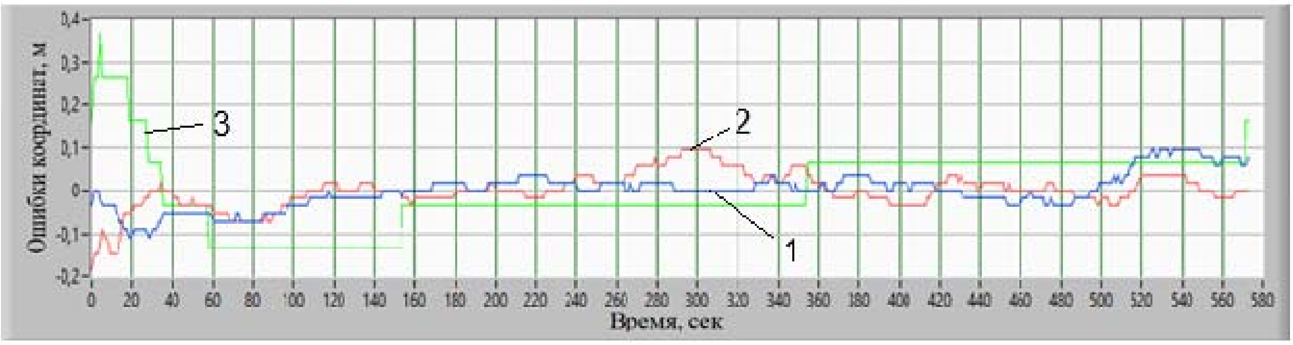
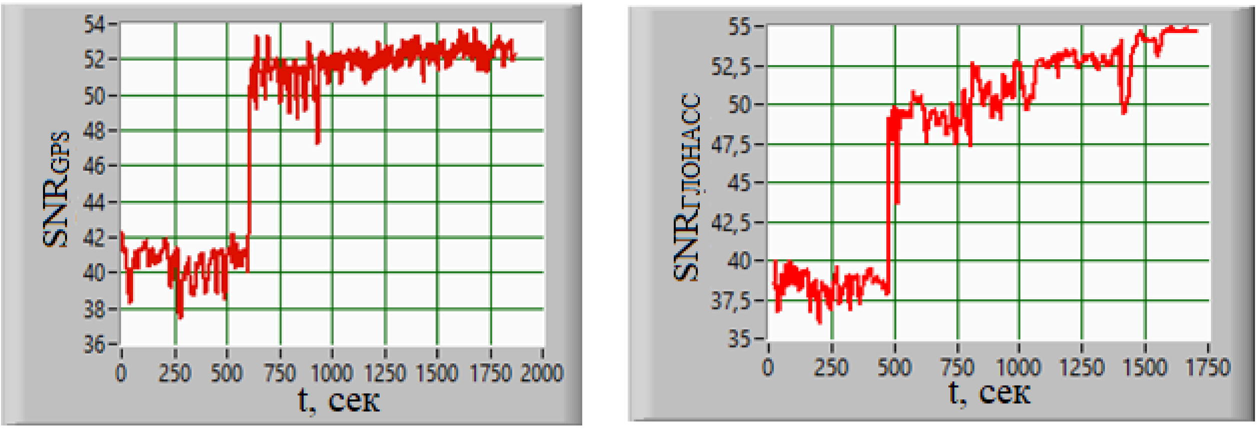


**Fig. 10.** Positioning errors with interference at the GLONASS frequency



a b

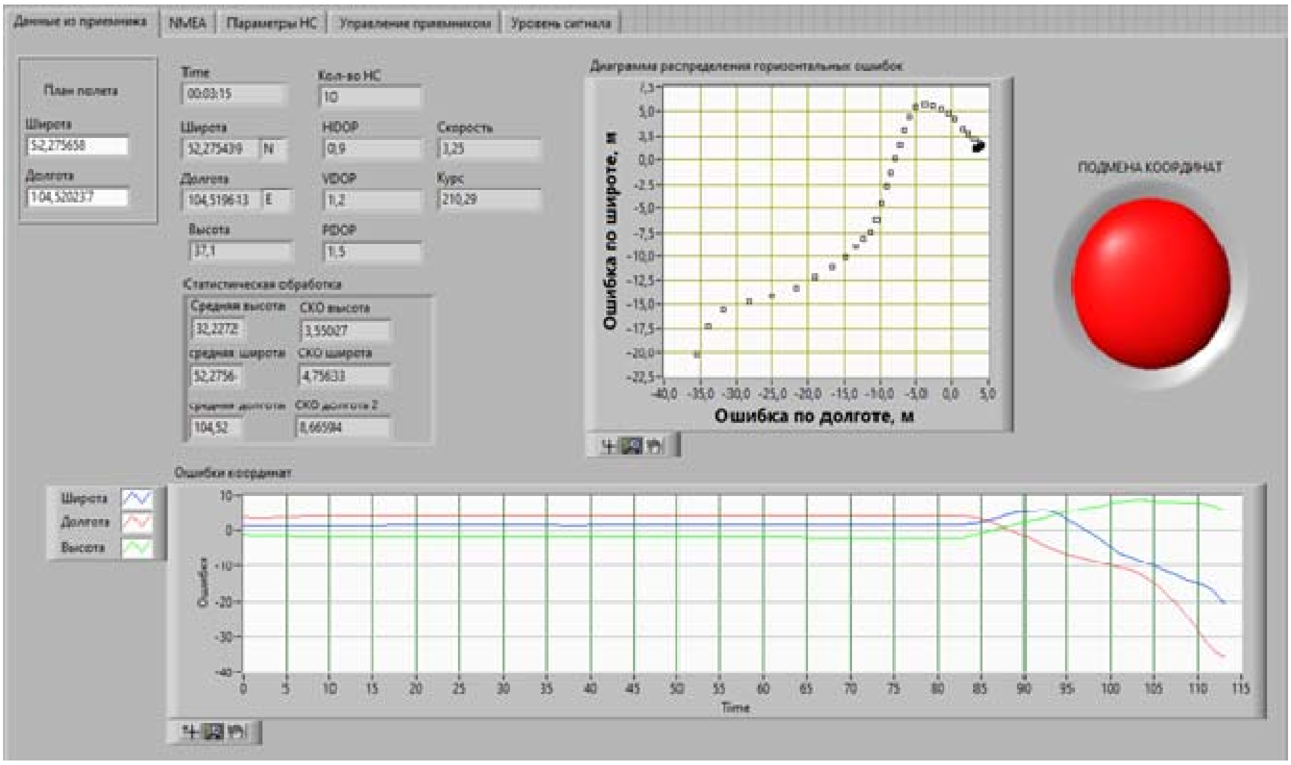
**Fig. 11.** The results of the experiment: *a* – $\mathrm{SNR}_{\mathrm{GPS}}$; *b* – $\mathrm{SNR}_{\mathrm{GLONASS}}$

tracking for almost all signals from GLONASS satellites is observed.

Figure 9 shows graphs of the number of satellites N (fig. 9, *a*, *c*) used in the solution for each system and the average SNR values (fig. 9, *b*, *d*). The marked moments on the graphs for the number of satellites in the solution and for $\mathrm{SNR}_{\mathrm{GLONASS}}$ (fig. 9, *a*, *b*) are associated with a short-term cessation of the interference, which did not significantly affect the overall coordinate measurement accuracy. A significant degradation of $\mathrm{SNR}_{\mathrm{GPS}}$ is not observed; therefore, the receiver operates with good coordinate determination accuracy (fig. 10, where curve 1 is error δB, curve 2 is error δL, and curve 3 is error δH).

## Results of the study on the influence of a high-level spoofing signal

Setting the simulator to a high output signal level (exceeding the level of the real GNSS signal) caused an increase in $\mathrm{SNR}_{\mathrm{GPS}}$ and $\mathrm{SNR}_{\mathrm{GLONASS}}$, exceeding the established threshold of 50 dB-Hz (fig. 11, *a*, *b*). Consequently, the algorithm generated the appropriate alert message. This event is displayed on the interface of the software module developed in the LabVIEW environment (fig. 12). In a practical implementation, this message should be sent to the UAS flight controller and then via the C2 (Command and Control) link to the UAS operator's console.



План полета

Широта: 52,275658

Долгота: 104,520237

Time: 00:03:15

Кол-во НС: 10

Широта: 52,275439 N

HDOP: 0,9

Скорость: 3,25

Долгота: 104,519613 E

VDOP: 1,2

Курс: 210,29

Высота: 37,1

PDOP: 1,5

Статистическая обработка

Средняя высота: 32,2272

СКО высота: 3,55027

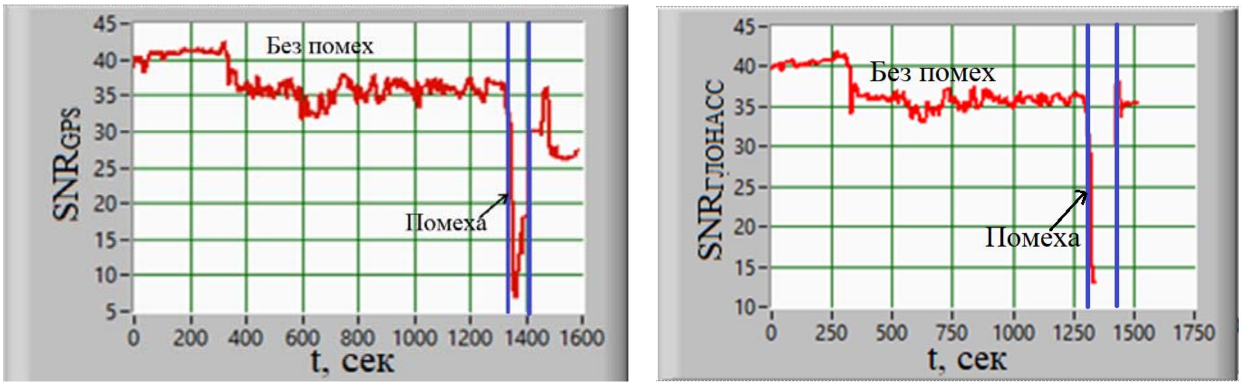
средняя широта: 52,2756

СКО широта: 4,75633

средняя долгота: 104,52

СКО долгота 2: 8,66594

**Fig. 12.** The interface of the programming module



a b

**Fig. 13.** The results of the experiment: *a* – SNR$_{\text{GPS}}$; *b* – SNR$_{\text{GLONASS}}$

## Results of the Study on the Impact of Wideband Interference

Even a brief activation of powerful wideband interference leads to the complete suppression of both GPS and GLONASS satellite signals. Figure 13 shows the moment the interference signal was activated and the subsequent drop in SNR$_{\text{GPS}}$ and SNR$_{\text{GLONASS}}$ below the threshold value. In this case, coordinates from the GNSS receiver become unavailable, resulting in a loss of navigation and stabilization for the UAS. Consequently, the algorithm generates a message for the UAS operator, instructing them to switch to manual control of the UAS.

## Results of the Study on Meaconing Interference Leading to UAS Trajectory Deviation

At this stage, external jammers were not used. It is assumed that false GNSS signals are being fed to the receiver input, which will cause the UAS to deviate from its assigned flight route.

To test the developed algorithm, a scenario was written for the CN-3803M simulator. In this scenario, for the first two minutes, the UAS is at coordinates B = 52.2756°, L = 104.520237°, H = = 30 m, which match the flight plan. Subsequently, the simulator generates signals imitating UAS movement at a constant speed and a course of 0° (spoofing signals), corresponding to movement along a false trajectory.

When spoofing is present, the current UAS coordinates do not match the flight plan coordinates, and the coordinate spoofing indicator is activated (fig. 12).

Under real-world conditions, if this condition is met, a message will be generated for the pilot to take manual control, and data from the GNSS receiver will not be used by the UAS navigation controller. This prevents the UAS from being led astray along a false trajectory.

## Conclusion

This work presents a methodology for detecting the impact of narrowband interference, wideband interference, and spoofing signals on a GNSS receiver. An interface for a data processing program was developed for the actual ATGM336H receiver module, enabling subsequent analysis to identify the type of interference. The program interface, based on the developed algorithm, allows for generating alerts to the UAS pilot when the satellite receiver cannot be used, and for selecting a satellite system depending on the frequency of the narrowband jamming. Thus, the interference immunity of the GNSS receiver is enhanced, and the situational awareness of the UAS operator in complex jamming environments is improved.

## References

1. **Tolstikov, A.S, Ushakov, A.E.** (2018). Countering spoofing and improving the noise immunity of coordinate-time definitions of GNSS technologies. *Interekspo Geo-Sibir*, no. 9, pp. 319–327. (in Russian)

2. **Arefyev, R.O., Skrypnik, O.N., Mezhetov, M.A.** (2023). The research of the immunity of the multisystem GNSS receiver. *Crede Experto: transport, society, education, language*, no. 2, pp. 28–43. DOI: 10.51955/2312-1327_2023_2_28 (in Russian)

3. **Grant, A., Williams, P., Ward, N., Baske, S.** (2009). GPS jamming and the impact on maritime navigation. *The Journal of Navigation*, vol. 62, no. 2, pp. 173–187. DOI: 10.1017/S0373463308005213

4. **Hofmann-Wellenhof, B., Lichtenegger, H., Wasle, E.** (2008). GNSS-global navigation satellite systems: GPS, GLONASS, Galileo, and more. Springer Wien New York, 547 p.

5. **Kaplan, E., Hegarty, C.** (2005). Understanding GPS: principles and applications. 2nd ed. Artech house on Demand, 726 p.

6. **Soloviev, Yu.A.** (2000). Satellite navigation systems. Moscow: Eko-Trendz, 270 p. (in Russian)

7. **Voznuk, V.V., Maslakov, P.A., Fomin, A.V.** (2016). The research of the interference immunity of users' GPS equipment based on the SDR technology. *Trudy Voenno-kosmicheskoy akademii imeni A.F. Mozhayskogo*, no. 650, pp. 33–40. (in Russian)

8. **Glomsvoll, O., Bonenberg, L.K.** (2017). GNSS jamming resilience for close to shore navigation in the Northern Sea. *The Journal of Navigation*, vol. 70, no. 1, pp. 33–48. DOI: 10.1017/S0373463316000473

9. **Glomsvoll, O.** (2014). Jamming of GPS & GLONASS signals. Department of Civil Engineering, Nottingham Geospatial Institute, 80 p.

10. **Meng, L., Yang, L., Yang, W., Zhang, L.** (2022). A survey of GNSS spoofing and anti-spoofing technology. *Remote sensing*, vol. 14, issue 19, ID: 4826. DOI: 10.3390/rs14194826 (accessed: 23.02.2025).

11. **Psiaki, M.L., Humphreys, T.E.** (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270. DOI: 10.1109/JPROC.2016.2526658

12. **Junzhi, L., Wanqing, L., Qixiang, F., Beidian, L.** (2019). Research progress of GNSS spoofing and spoofing detection technology. *In: 2019 IEEE 19th international conference on communication technology (ICCT)*. Xi'an, China, pp. 1360–1369. DOI: 10.1109/ICCT46805.2019.8947107

13. **Radoš, K., Brkić, M., Begušić, D.** (2024). Recent advances on jamming and spoofing detection in GNSS. *Sensors*, vol. 24, issue 13, ID: 4210. DOI: 10.3390/s24134210 (accessed: 23.02.2025).

14. **Melnichenko, S.** (2024). Spoofing – New Heights. *AviaSafety.ru*. 2024. Available at: https://aviasafety.ru/47840/ (accessed: 23.02.2025). (in Russian)

15. **Broumandan, A., Siddakatte, R., Lachapelle, G.** (2017). An approach to detect GNSS spoofing. *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 8, pp. 64–75. DOI: 10.1109/MAES.2017.160190

16. **Liu, Y., Li, S., Fu, Q., Liu, Z.** (2018). Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system. *Sensors*, vol. 18, issue 5, ID: 1433. DOI: 10.3390/s18051433 (accessed: 23.02.2025).

17. **Lee, D.K., Miralles, D., Akos, D. et al.** (2020). Detection of GNSS spoofing using NMEA messages. *In: 2020 European Navigation Conference (ENC)*, IEEE, Germany, Dresden, pp. 1–10. DOI: 10.23919/ENC48637.2020.9317470

18. **Spravil, J., Hemminghaus, C., von Rechenberg, M., Padilla, E., Bauer, J.** (2023). Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. *Journal of Marine Science and Engineering*, vol. 11, issue 5. ID: 928. DOI: 10.3390/jmse11050928 (accessed: 23.02.2025).

19. **Perov, A.I., Kharisov, V.N.** (2010). GLONASS. Principles of construction and operation. 4th ed., revised and enlarged. Moscow: Radiotekhnika, 801 p. (in Russian)

## Список литературы

1. **Толстиков А.С., Ушаков А.Е.** Противодействие спуфингу и повышение помехоустойчивости аппаратуры потребителя глобальных навигационных спутниковых систем // Интерэкспо Гео-Сибирь. 2018. № 9. С. 319–327.

2. **Арефьев Р.О., Скрыпник О.Н., Межетов М.А.** Исследование помехоустойчивости мультисистемного GNSS приемника // Crede Experto: транспорт, общество, образование, язык. 2023. № 2. С. 28–43. DOI: 10.51955/2312-1327_2023_2_28

3. **Grant A.** GPS jamming and the impact on maritime navigation / A. Grant, P. Williams, N. Ward, S. Baske // The Journal of Navigation. 2009. Vol. 62, no. 2. Pp. 173–187. DOI: 10.1017/S0373463308005213

4. **Hofmann-Wellenhof B., Lichtenegger H., Wasle E.** GNSS-global navigation satellite systems: GPS, GLONASS, Galileo, and more. New York: Springer Wien, 2008. 547 p.

5. **Kaplan E., Hegarty C.** Understanding GPS: principles and applications. 2nd ed. Artech house on Demand, 2005. 726 p.

6. **Соловьев Ю.А.** Системы спутниковой навигации. М.: Эко-Трендз, 2000. 270 с.

7. **Вознюк В.В., Маслаков П.А., Фомин А.В.** Исследование помехоустойчивости аппаратуры потребителей глобальной навигационной спутниковой системы GPS на основе технологии программного приема // Труды Военно-космической академии имени А.Ф. Можайского. 2016. № 650. С. 33–40.

8. **Glomsvoll O., Bonenberg L.K.** GNSS jamming resilience for close to shore navigation in the Northern Sea // The Journal of Navigation. 2017. Vol. 70, no. 1. Pp. 33–48. DOI: 10.1017/S0373463316000473

9. **Glomsvoll O.** Jamming of GPS & GLONASS signals. Department of Civil Engineering, Nottingham Geospatial Institute, 2014. 80 p.

10. **Meng L.** A survey of GNSS spoofing and anti-spoofing technology / L. Meng, L. Yang, W. Yang, L. Zhang [Электронный ресурс] // Remote sensing. 2022. Vol. 14, iss. 19. ID: 4826.

DOI: 10.3390/rs14194826 (дата обращения: 23.02.2025).

**11. Psiaki M.L., Humphreys T.E.** GNSS spoofing and detection // Proceedings of the IEEE. 2016. Vol. 104, no. 6. Pp. 1258–1270. DOI: 10.1109/JPROC.2016.2526658

**12. Junzhi L.** Research progress of GNSS spoofing and spoofing detection technology / L. Junzhi, L. Wanqing, F. Qixiang, L. Beidian // 2019 IEEE 19th International Conference on Communication Technology (ICCT). China, Xi'an, 2019. Pp. 1360–1369. DOI: 10.1109/ICCT46805.2019.8947107

**13. Radoš K., Brkić M., Begušić D.** Recent advances on jamming and spoofing detection in GNSS [Электронный ресурс] // Sensors. 2024. Vol. 24, iss. 13. ID: 4210. DOI: 10.3390/s24134210 (дата обращения: 23.02.2025).

**14. Мельниченко С.** Спуфинг – новые высоты [Электронный ресурс] // AviaSafety.ru 2024. URL: https://aviasafety.ru/47840/ (дата обращения: 23.02.2025).

**15. Broumandan A., Siddakatte R., Lachapelle G.** An approach to detect GNSS spoofing // IEEE Aerospace and Electronic Systems Magazine. 2017. Vol. 32, no. 8. Pp. 64–75. DOI: 10.1109/MAES.2017.160190

**16. Liu Y.** Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system / Y. Liu, S. Li, Q. Fu, Z. Liu [Электронный ресурс] // Sensors. 2018. Vol. 18, iss. 5. ID: 1433. DOI: 10.3390/s18051433 (дата обращения: 23.02.2025).

**17. Lee D.K., Miralles D., Akos D. et al.** Detection of GNSS spoofing using NMEA messages // 2020 European Navigation Conference (ENC). IEEE, Germany, Dresden, 2020. Pp. 1–10. DOI: 10.23919/ENC48637.2020.9317470

**18. Spravil J.** Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring / J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, J. Bauer [Электронный ресурс] // Journal of Marine Science and Engineering. 2023. Vol. 11, iss. 5. ID: 928. DOI: 10.3390/jmse11050928 (дата обращения: 23.02.2025).

**19. Перов А.И., Харисов В.Н.** ГЛОНАСС. Принципы построения и функционирования. 4-е изд., перераб. и доп. М.: Радиотехника, 2010. 801 с.

## Information about the authors

**Roman O. Arefyev,** Candidate of Technical Sciences, Associate Professor, Associate Professor of the Aviation Radioelectronic Equipment Chair, Irkutsk Branch of the Moscow State Technical University of Civil Aviation, aqua160905@mail.ru.

**Natalya G. Arefyeva,** Candidate of Technical Sciences, Associate Professor, Associate Professor of the Aviation Radioelectronic Equipment Chair, Irkutsk Branch of the Moscow State Technical University of Civil Aviation, n_astrahanceva_awesome@mail.ru.

**Oleg N. Skrypnik,** Doctor of Technical Sciences, Professor, Professor of the Organization of Traffic and Ensuring Safety in Air Transport, Belarusian State Aviation Academy, skripnikon@yandex.ru.

## Сведения об авторах

**Арефьев Роман Олегович,** кандидат технических наук, доцент, доцент кафедры авиационного радиоэлектронного оборудования Иркутского филиала МГТУ ГА, aqua160905@mail.ru.

**Арефьева Наталья Геннадьевна,** кандидат технических наук, доцент, доцент кафедры авиационного радиоэлектронного оборудования Иркутского филиала МГТУ ГА, n_astrahanceva_awesome@mail.ru.

**Скрыпник Олег Николаевич,** доктор технических наук, профессор, профессор кафедры организации движения и обеспечения безопасности на воздушном транспорте Белорусской государственной академии авиации, skripnikon@yandex.ru.

| | | | |
|---|---|---|---|
| Поступила в редакцию | 27.06.2025 | Received | 27.06.2025 |
| Одобрена после рецензирования | 01.08.2025 | Approved after reviewing | 01.08.2025 |
| Принята в печать | 20.11.2025 | Accepted for publication | 20.11.2025 |