Influence of Protective Signals on Dangerous Signals of High-Frequency Imposition

Larysa Kriuchkova[1], Ivan Tsmokanych[2], Maksym Vovk[3], Nataliia Mazur[1], and Oleksandr Bohdanov[1]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[2] *State Research Institute of Cyber Security and Information Protection, 6 block 3 building Maksyma Zaliznyaka str., Kyiv, 03142, Ukraine*
[3] *State University of Telecommunications, 7 Solomyanska str., Kyiv, 03110, Ukraine*

Abstract

The method of active protection of information from interception by methods of high-frequency imposition is considered, in which targeted jamming protective signals are introduced into the environment used for the delivery of probing oscillations both at the fundamental frequency and at the combinatorial harmonics of the probing signal, which by destroying the informative parameters of dangerous signals render them unfit for their intended use, and issues related to the evaluation of the effectiveness of protective signals on dangerous high-frequency interference signals. The results of an experimental evaluation of the effectiveness of the influence of interfering protective signals on dangerous signals of high-frequency imposition and the value of the protection coefficients at fixed frequencies for various protection conditions are presented.

Keywords

Interception of information, high-frequency imposition, dangerous signal, interfering protective signal, parameters of protective signals, evaluation of efficiency.

1. Introduction

In the general problem of ensuring information security, the issue of protecting confidential information is one of the most important. Effective methods of interception of confidential information on objects of information activity are methods of high-frequency imposition [1–2]. Channels of information leakage are formed due to acoustic-electric transformations, which are formed during the simultaneous impact on the elements of technical means of confidential speech signals and probing high-frequency signals if radical measures were not taken to prevent the penetration of high-frequency currents inside the technical means [3–5].

Currently, two methods of intercepting information through high-frequency imposition channels are used:

- Using contact or inductive introduction of a high-frequency signal into electrical circuits that have functional or parasitic connections with the main technical means.
- By irradiating the source of information with a high-frequency electromagnetic signal and receiving the reflected modulated signal.

In the paper [6], the authors proposed a method of active protection of information from interception by high-frequency imposition methods, in which targeted jamming protective signals are introduced into the medium used for the delivery of probing oscillations both at the fundamental frequency and at the combinational harmonics of the probing signal, which by destroying the informative parameters of dangerous signals, they make them unsuitable for their intended use:

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: l.kriuchkova@kubg.edu.ua (L. Kriuchkova); ivakobor@ukr.net (I. Tsmokanych); leny_mowe@ukr.net (M. Vovk); n.mazur@kubg.edu.ua (N. Mazur); o.bohdanov (O. Bohdanov)
ORCID: 0000-0002-8509-6659 (L. Kriuchkova); 0000-0002-5085-8457 (I. Tsmokanych); 0000-0003-1781-6762 (M. Vovk); 000-0001-7671-8287 (N. Mazur); 0009-0005-2605-6189 (O. Bohdanov)

- The first protective signal is a harmonic signal to create the effect of “beating” with a dangerous signal of high-frequency imposition.
- The second protective signal is an oscillatory frequency signal.

Based on the results of the simulation [7] and experimental studies [8, 9] performed in the LabVIEW environment version 20.0.1, we determined the parameters of the interfering protective signals aimed at destroying dangerous signals of high-frequency imposition with various types of carrier frequency modulation. The purpose of the research was to find the parameters of protective signals capable of ensuring the maximum possible destruction of the informative parameters of a dangerous signal, and, as a result, creating countermeasures against the interception of confidential information by interested parties.

A fragment of the signal simulation results is shown in Fig. 1.

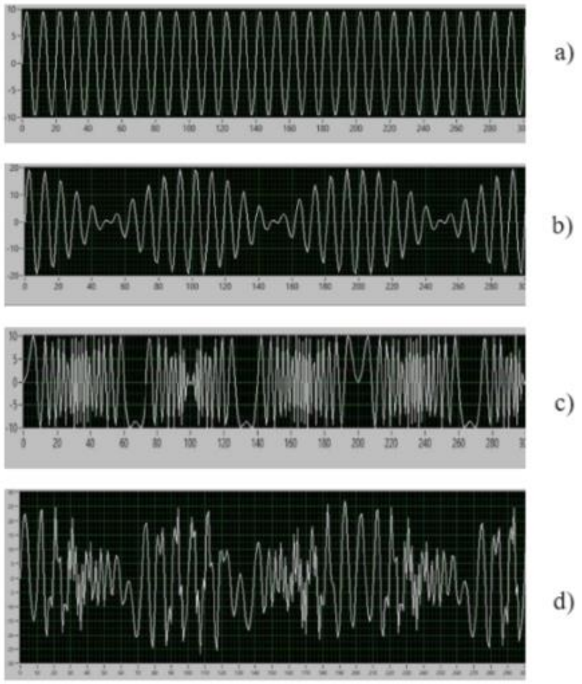

Figure 1: Image of signals (a) dangerous signal, (b) resulting beating signal, (c) protective signal of oscillating frequency, (d) resulting dangerous signal

The purpose of our research was to experimentally evaluate the ability of protective jamming signals to ensure the destruction of informative parameters of dangerous signals of high-frequency imposition.

2. Experimental Evaluation of the Effectiveness of Interference Protective Signals

The assessment of the level of protection of information against leakage through high-frequency imposition channels is carried out by international and national standards, as well as by regulatory documents [10–12]. In many countries, regulatory documents provide for the use of ratios SNR (Signal-to-noise ratio, S/N)—measures used in science and engineering to determine how strongly the signal is distorted by noise. It is defined as the ratio of the useful signal power to the noise power [13, 14].

The selection of efficiency criteria is of primary importance for evaluating the effectiveness of the impact of protective signals on dangerous high-frequency imposition signals. The practice has established [15–17] that as a criterion for the effectiveness of radio communication means, such an indicator should be chosen that satisfies the following basic requirements: the indicator must meet the purpose of the research and reflect the main purpose of the radio communication means; the indicator must be related to the characteristics (parameters) of the radio communication device and be sensitive to changes in these characteristics; the indicator should be as simple as possible [18, 19].

Experimental studies were carried out to confirm theoretical information and carry out a general assessment of the effectiveness of the proposed method in compliance with the relevant requirements for reliability.

The scheme of construction of the experiment depends on the chosen criterion of the degree of effectiveness of the proposed method. At the same time, the criterion must meet the requirements of the simplicity of experimenting using standardized radio measuring devices and the unequivocalness of the results obtained.

Experimental studies were carried out according to the established Methodology for evaluating the effectiveness of protective signals on dangerous high-frequency signals [20]. The list of equipment for conducting experimental research is presented in Fig. 2.

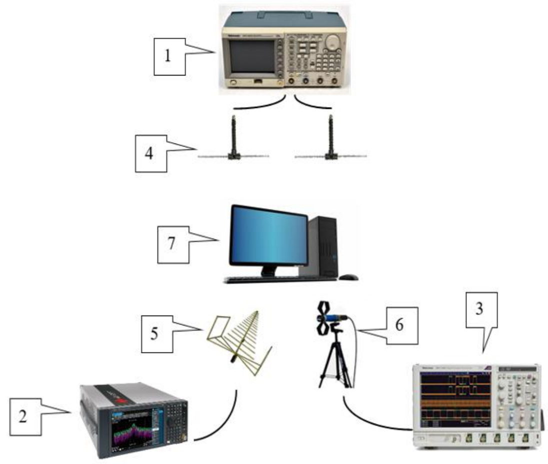

Figure 2: List of equipment for conducting experimental research (1) Tektronix AFG 3252 Arbitrary Signal Generator, (2) Keysight PXA Signal Analyzer N9030B spectrum and signal analyzer, (3) Tektronix DPO 7254 oscilloscope, (4) Complex of dipole antennas Tuned Dipole Antenna FCC, (5) White periodic antenna SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25–7000 MHz, (6) Antenna electric EMA-2000, (7) Stationary personal computer (PC)

The methodology includes the following actions:

1. Prepare control and measuring devices for work according to their operating instructions.
2. Connect and turn on the measuring equipment according to the operating instructions. Ensure reliable grounding.
3. After 15–30 minutes after switching on, check the functioning of the equipment according to the list presented in Fig. 2.
4. Place the measuring antennas at a distance of 1 m from the PC. The antennas must be in a parallel plane to the front part of the PC. At the same time, it is necessary to ensure that the geometric centers of the frame antenna and PC are on the same axis.
5. On the PC run a test program that simulates the maximum workload on the selected interface.
6. In the range of 0–2 GHz, fix the frequencies according to the clock with the maximum signal level, then choose the one that has the best quality/level ratio, and at this same frequency, turn on the first channel of the generator, which amplifies the protective probing signal, setting the signal level 30 dBμV.
7. Turn on the second channel of the generator, setting the signal level to 30 dBμV.
8. Add to the signal from channel 2 of the generator the effect of "rocking" the frequency, alternately adding and subtracting 400 kHz (approximately the average value is selected from the optimal range of the difference in frequencies of protective and dangerous signals, which provides the effect of "beating" frequencies—Fig. 1b).

According to the created Methodology, a test program that simulates the maximum workload on a given interface is launched on a PC for an experimental study of the effectiveness of interfering protective signals. A monitor interface (with VGA (DE-15) connector) is selected, as the monitor may display restricted information that may be intercepted.

Ideal conditions are simulated when the attacker can intercept information by the high-frequency imposition method, namely: he knows the location of the PC on which restricted information is processed, and he has the technical means that allow interception.

The clock frequency of the monitor/monitor interface is determined experimentally.

1. In the range of 0–2 GHz, frequencies are determined according to the clock with the maximum signal level, after which the one (1812.5255 MHz) that has the best quality/level ratio is selected, and at this same frequency, the first channel of the generator with a signal level of 30 dBμV is switched on, which amplifies the useful signal.

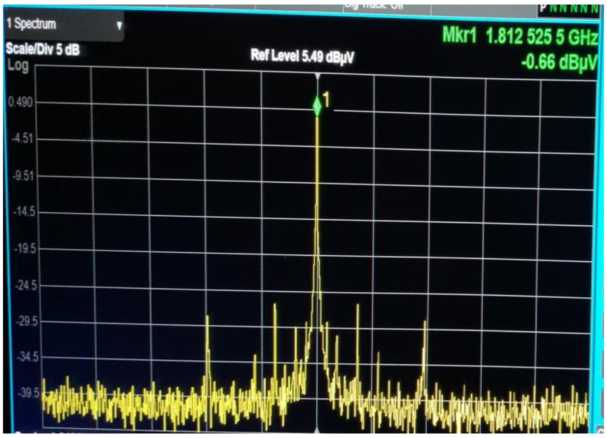

Figure 3: Photographic image of the signal on the analyzer screen

Result: a dangerous signal with a level of minus 0.66 dBμV was determined.

2. The second channel of the generator with the signal level is turned on 30 dBμV and a frequency of 1812.4255 MHz.

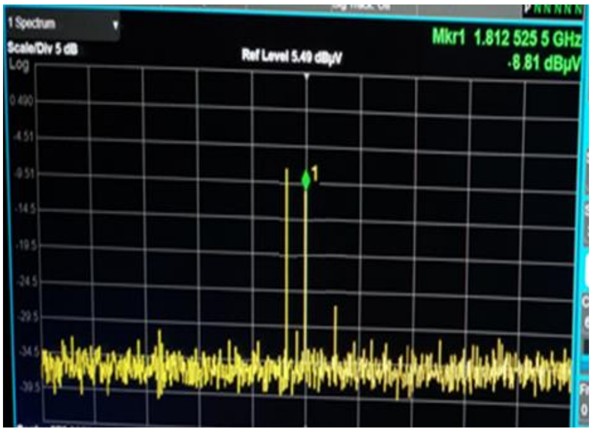

Figure 4: Photographic image of the signal on the analyzer screen

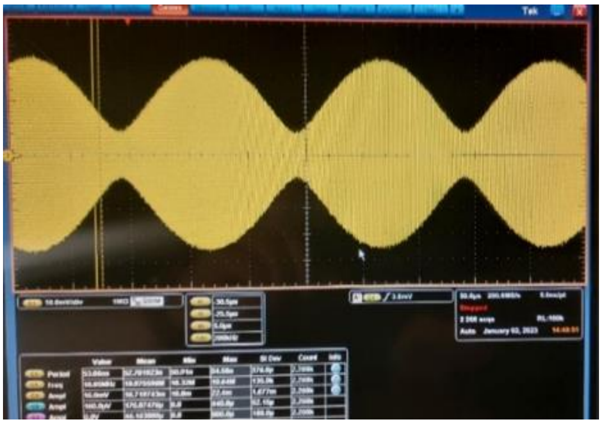

Figure 5: Photographic image of the signal on the analyzer screen

Result: a significant decrease in the level of the useful signal to minus 8.81 dBμV (Fig. 4) was recorded due to the "beating" effect (Fig. 5), which occurs with the participation of the useful signal (which is amplified by the signal from the generator channel 1) and the signal from the generator channel 2. The probability of interception of information decreases already after carrying out such a procedure because the lower level of the useful signal reduces the probability that the attacker will be able to intercept the information qualitatively and without distortion.

3. A frequency "swing" effect ±400 kHz is added to the signal from the 2nd channel of the generator (frequency range from 1812.0255 to 1812.8255 MHz).

Result: formation of band noise and distortion of a dangerous signal along with a decrease in the overall level of all signals (the maximum signal level in the middle is minus 15.92 dBμV) (Fig. 6).

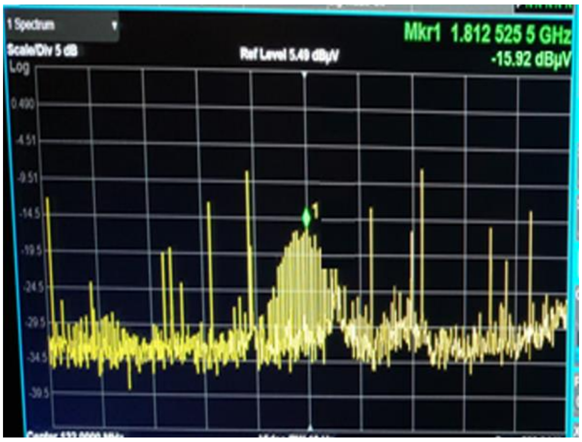

Figure 6: Photographic image of the signal on the analyzer screen

In this way, the probability of an attacker intercepting information decreases again. With the help of "swinging," the informative parameters of a dangerous signal are partially destroyed (reduction of the signal level, signal distortion, noise of the range within the scope of "swinging" frequencies).

3. Determination of the Coefficient of Protection of Information Against Leakage and the Possibility of Reproduction

To evaluate the effectiveness of interference protection signals, the concept of protection factor is used, which is understood as the minimum necessary ratio of the interference power to the signal power at the input of the receiver within the bandwidth of its linear part, which ensures a given loss of information.

The value of the protection factor of the radio communication line is determined by the type of interference and its spectral characteristics, the disorder of the interference relative to the resonant frequency of the interfering receiving device, and the type of modulation used in the radio line.

The condition for determining the protection factor based on the minimum necessary ratio of the interference power to the signal power is related to the fact that the protection factor must be the threshold value of this ratio so that it can be used to determine the boundary of the protection zone.

The protection factor is calculated according to the formula:

$$K_3 = \frac{U_г}{U_c}, \qquad (1)$$

where K_3 is a protection factor, $U_г$ is the energy component of the signal, measured in the band, which is necessary to intercept the signal, when the generator is turned on with the effect of “beating” and “swinging” the frequency, taking into account the coefficient of correction of the antenna (data from the calibration/verification certificate or factory documentation), U_c is the energy component of the dangerous signal, measured in the band, which is necessary to intercept the signal, with the influence of the enemy’s generator on it/or the clean signal, taking into account the antenna correction factor (data from the calibration/verification certificate or factory documentation).

According to the conducted experiments, the protection coefficients for the following cases were calculated:

1. Under the condition that the equipment is turned on, a test program is launched that simulates the maximum workload on the specified interface without the operation of protective equipment. Accordingly, the attacker has the opportunity to unhindered intercept a signal that contains information with limited access, using high-frequency imposition

$$K_{31} = \frac{10^{\frac{-3}{20}}}{10^{\frac{-7}{20}}} = 0.6 \qquad (2)$$

2. If the equipment is turned on, a test program is launched that simulates the maximum workload on the specified interface and with the operation of protective equipment

$$K_{32} = \frac{10^{\frac{3}{20}}}{10^{\frac{-7}{20}}} = 4.42 \qquad (3)$$

Fig. 7 shows the comparative characteristics of energy component signals in the range of 0-2 GHz in three cases:

1. Signal to noise level, without included equipment on which information with limited access is processed.
2. A useful signal influenced by an enemy generator/or a pure signal.
3. Signal when the generator is turned on with the effect of “beating” and “oscillating” the frequency.

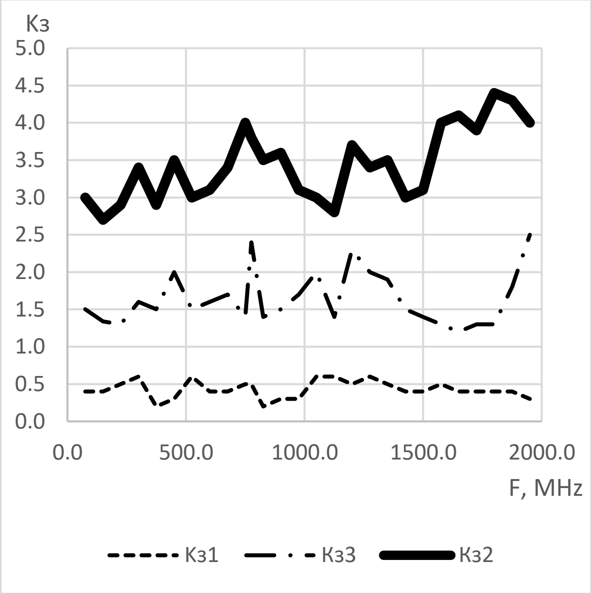

Figure 7: Comparative characteristics of the energy components of the signal for different protection conditions in the range of 0–2 GHz

Fig. 8 shows the values of the protection coefficients at fixed frequencies in the range of 0–2 GHz for various protection conditions:

1. If there is no protection of information against leakage and the actions of an intruder regarding its interception.
2. Under the condition of using the high-frequency imposition method to protect information from leakage and the actions of an intruder about its interception.

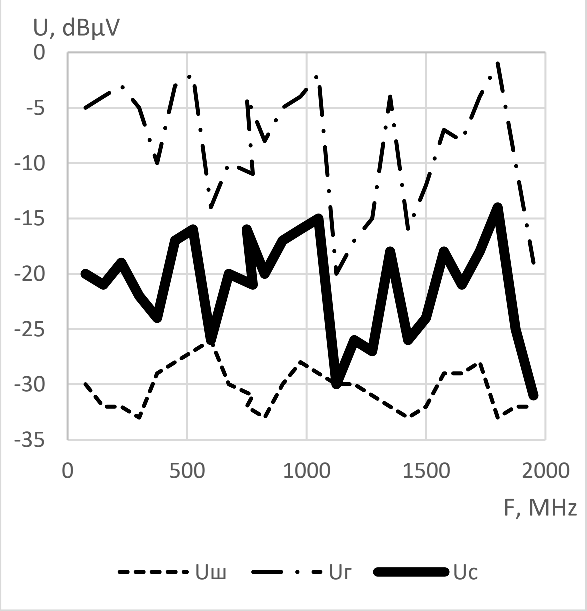

Figure 8: The value of the protection coefficients at fixed frequencies for various protection conditions in the range of 0–2 GHz

3. Under the condition of using the proposed high-frequency imposition method (with the use of “beating” and “rocking” effects) to protect information from leakage and the attacker's work to intercept it.

The analysis of the energy components of the signal (Fig. 7) and the values of the security coefficients (Fig. 8) allows us to state that the use of the proposed active method using the effect of “beating” and “oscillating” frequencies reduces the probability of interception of information and its reproduction by 1.5–3 times compared to using the usual active method.

4. Conclusions

1. The value of the protection factor as a measure of the effectiveness of interference protective signals is determined by the type of interference and its spectral characteristics, the disorder of the interference relative to the resonance frequency of the probing signal, and the type of modulation used in the radio line. The most important issue in determining the protection factor is the concept of information loss.

2. An improved model for calculating the coefficient of information security assessment, which, unlike the existing ones, is built based on a comparison of energy components measured in bands sufficient for interception of dangerous and protective signals, provides a quantitative assessment of security based on the established value of the coefficient, taking into account the parameters and values of the dangerous signal.

3. It was established that the values of the protection factor $K_3 \geq 2$. The effectiveness of information protection increases by 1.5–3 times depending on the frequency range.

4. The proposed method of experimental assessment of the ability of protective signals to ensure the destruction of informative parameters of dangerous signals of high-frequency imposition allows for a qualitative investigation of the effectiveness of the proposed method of protection.

5. The obtained distortions of the dangerous signal make it impossible to reproduce the intercepted information according to the specified values of the protection factor, which ensures the protection of information against leakage by high-frequency imposition channels.

6. Scientific results can be used by research and development organizations and state structures in the development and improvement of information security assessment methods during the instrumental control of various objects of information activity of critical infrastructure and solving complex problems regarding information protection at objects of information activity of critical infrastructure.

7. The use of active information protection methods does not exclude the need for passive protection (shielding, filtering, etc.).

8. Directions for further research can be:
   - Improvement of the criteria for assessing information security of various objects of information activity of critical infrastructure.
   - Development of recommendations for improving the existing methods of special studies to assess the security of information against leakage through channels of high-frequency imposition.

A study of approaches regarding the technical implementation of the proposed method of information protection against leakage through high-frequency imposition channels.

References

[1] S. Ivanchenko, et al., Technical Channels of Information Leakage. The Order of Creation of Complexes of Technical Protection of Information: the Textbook of NTUU “KPI” (2016).

[2] L. Kriuchkova, I. Tsmokanych. Overview of Methods of Protection of Acoustic Information Against Leaks by Channels Formed by High-Frequency Impositions, Int. J. Innov. Technol. Social Sci. 3(31) (2021). doi: 10.31435/rsglobal_ijitss/30092021/7685.

[3] V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information

Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.

[4] V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.

[5] V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.

[6] L. Kriuchkova, I. Tsmokanych, M. Vovk, Advanced Method of Protection of Confidential Information from Interception by High-Frequency Imposition Methods, Comput. Syst. Inf. Technol. 3 (2022) 14–20.

[7] L. Kriuchkova, et al., Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition, Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3188 (2021) 265–272.

[8] L. Kriuchkova, I. Tsmokanych, Aspects of Determining the Parameters of Protective Effects on Probing Signals of High-Frequency Imposition, Cybersecur. Educ. Sci. Tech. 2(18) (2022) 197–204.

[9] L. Kriuchkova, I. Tsmokanych, Improvement of Protective Effects on Dangerous High-Frequency Impression Signals, Cybersecur. Educ. Sci. Tech. 3(19) (2023) 243–253.

[10] Regulation on technical protection of information in Ukraine, approved by the Decree of the President of Ukraine dated (1999). URL: https://zakon.rada.gov.ua /laws/show/1229/99#Text

[11] Law of Ukraine "On Information Protection in Information and Telecommunication Systems". URL: https://zakon.rada.gov.ua/laws/show/ 80/94-%D0%B2%D1%80#Text

[12] DSTU EN ISO/IEC 15408-1:2022 Information Technology. Protection Methods. Evaluation Criteria. Part 1. Introduction and General Model, EN ISO/IEC 15408-1:2020, IDT; ISO/IEC 15408-1:2009, IDT.

[13] I. Bogachuk, V. Sokolov, V. Buriachok, Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers, in: 5th International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (2018) 581–585. doi: 10.1109/INFOCOMMST.2018.8632151.

[14] Z. Hu, et al., Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range, Data-Centric Business and Applications 48 (2020) 675–709. doi: 10.1007/978-3-030-43070-2_29.

[15] I. Chesanovskyi, A. Ivanov, I. Gurman, Increasing the Immunity of Signal Processing in Incoherent Radar Systems, Bulletin of the National Technical University of Ukraine Kyiv Polytechnic Institute, Series: Radio equipment, Radio Equipment Construction (2013).

[16] V. Tsyporenko, Analysis of the Spectrum Width of a Radio Signal with an Unknown Phase Spectrum, Bulletin of ZHTU, Series: Technical Sciences (1(48)) (2009) 127–130.

[17] V. Kononov, Types and Methods of Evaluation of Measurement Results by Means of Measuring Equipment, Inf. Proces. Syst. (5) (2011) 45–49.

[18] V. Astapenya, et al., Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems, in: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/picst54195.2021.9772161.

[19] V. Astapenya, et al., Last Mile Technique for Wireless Delivery System using an Accelerating Lens, in: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (2020). doi: 10.1109/picst51311.2020.9467886.

[20] L. Kriuchkova, et al., Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 261-268.