Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition

Larysa Kriuchkova[1], Ivan Tsmokanych[2], Svitlana Shevchenko[1], Oleksandr Bohdanov[1], and Nataliia Mazur[1]

[1] Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine
[2] State University of Telecommunications, 7 Solomenskaya str., Kyiv, 03110, Ukraine

Abstract

A method of protection against the interception of confidential information 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 provides more effective protection of information from interception, is considered. The results of experimental studies aimed at determining the parameters of effective interfering protective signals capable of destroying the informative parameters of dangerous signals generated by high-frequency imposition methods are presented.

Keywords

Interception of information, high-frequency imposition, probing signal, dangerous signal, obstruction protective signal.

1. Introduction

Information that has a certain seal of secrecy and may contain data that in a certain way may affect the security of the state and its citizens circulates on the objects of information activity. Such information may be susceptible to interception attempts. As a result of the action of many factors, technical channels for the leakage of confidential information may be formed spontaneously or intentionally. Taking into account the importance of information, measures and means aimed at ensuring the protection of acoustic information and information processed in information systems are applied [1–4].

Effective methods of interception of confidential information on objects of information activity are methods of high-frequency imposition (then—HF-imposition, HFI) [5–9]. High-frequency intrusion means a method of unauthorized obtaining of information, in which radio signal probing of the premises or its conductive communications takes place, in which the negotiations are taking place. As a result of interaction with technical means or specially implemented devices, sounding signals are modulated by speech. If in the specified circles there are elements whose parameters (inductance, capacity, or resistance) change under the influence of low-frequency signals, then a secondary field of high-frequency radiation modulated by a low-frequency signal will be created in the surrounding space [10].

Currently, two methods of HFI intercepting information through 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.

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: l.kriuchkova@kubg.edu.ua (L. Kriuchkova); ivakobor@ukr.net (I. Tsmokanych); s.shevchenko@kubg.edu.ua (S. Shevchenko); o.bohdanov@kubg.edu.ua (O. Bohdanov); n.mazur@kubg.edu.ua (N. Mazur)
ORCID: 0000-0002-8509-6659 (L. Kriuchkova); 0000-0002-5085-8457 (I. Tsmokanych); 0000-0002-9736-8623 (S. Shevchenko); 0009-0005-2605-6189 (O. Bohdanov); 0000-0001-7671-8287 (N. Mazur)

The block diagram of the channel of high-frequency imposition is presented in Fig. 1, where G is the generator, R is the receiver, CL is the communication line, CS is the communication system, WP is ways of penetration, BTMS is the basic technical means and systems, ATMS is auxiliary technical means and systems, ME is the modulating element.

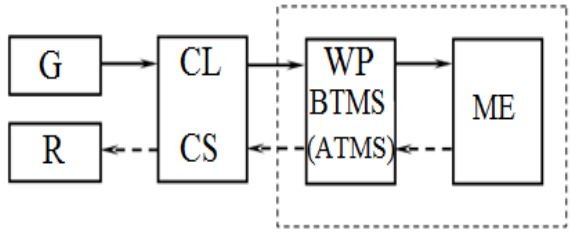

Figure 1: Block diagram of the channel of high-frequency imposition

In work [11], the authors proposed a new method of technical protection of information from interception by HFI methods, the essence of which is the application of combined active interference, which changes the properties of the sounding high-frequency signal. The basis of the method is the well-known physical fact of "beating" between oscillations of close frequencies.

Since when intercepting information by HFI methods, amplitude, frequency, and phase modulation of the transmitted signal can occur, it is necessary to take measures to block the possibility of receiving information when using any of these modulations.

As stated in [12], the method of blocking information interception channels using high-frequency imposition methods was taken as the basis for improvement, in which targeted active jamming protective signals aimed at destroying informative parameters are introduced into the environment used for the delivery of probing oscillations dangerous signal with different types of carrier frequency modulation:

- 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.

Taking into account that the interception of information can be carried out both on the main frequency and on the harmonics of a dangerous signal, it is proposed to create protective signals not only concerning the main frequency but also relative to the harmonics of the dangerous signal [13]. Thus, the effects of "beating" and "rocking" of dangerous signals will be followed both on the fundamental frequency and on the combinational harmonics of the probing signal, which will provide more effective protection of confidential information from interception.

The essence of the improved method is to implement the protection system as follows:

1. Using the method of radio monitoring [14], the frequency of the probing signal of high-frequency imposition is detected at the object of information activity.
2. In the case of detection of a probing signal by the above-mentioned method, a set of protective signals is formed, aimed at destroying the informative parameters of dangerous signals of high-frequency imposition, not only at the fundamental frequency but also at the combinational harmonics of the probing signal.

2. Tasks of Experimental Research

Experimental studies were conducted to achieve the following results:

- Determination of parameters of interfering protective signals capable of destroying informative parameters of dangerous signals.
- Determination of the range of effectiveness of protective signals.
- Confirmation or refutation of the effectiveness, sufficiency, and reliability of protective signals to ensure the protection of information from leakage.

The task of experimental research is an objective assessment of the ability of a protective signal to ensure the destruction of informative parameters of dangerous signals:

- Ensuring the protection of information from leakage by blocking interception channels by the method of high-frequency imposition.
- The effectiveness of destroying an informative signal due to the formation

of a “beating” effect with a dangerous high-frequency imposition signal.

- Finding the parameters of protective signals capable of ensuring the maximum possible destruction of informative parameters of dangerous signals at the fundamental frequency and the combinational harmonics of the probing signal, and, as a result, creating countermeasures against the interception of confidential information by interested parties.

A generalized scheme for conducting experimental research is presented in Fig. 2.

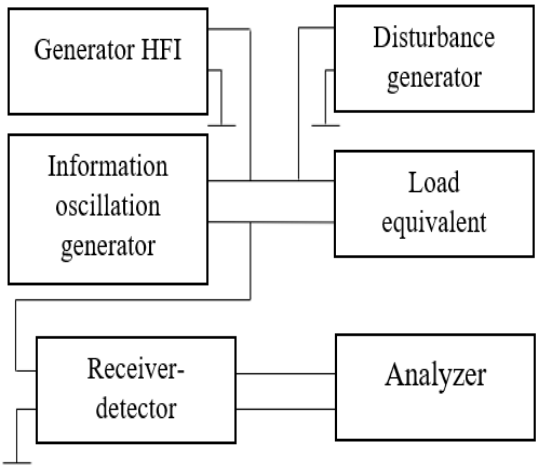

Figure 2: Generalized scheme of conducting experimental research [15]

Disturbance generator functions:

1. Form and change the frequency of the main oscillation of the influence on the signal HFI.
2. Change the control range of the oscillation frequency and the level of the main frequency.
3. Change the swing speed range of the fundamental frequency.
4. Form and change parameters of noise signals.
5. Change the general level of the interference signal.
6. Make these changes independently of each other.
7. Use each of the types of interference signal changes while disabling the rest of the influencing factors.

A standard oscilloscope, frequency meter, and voltmeter can be used to measure the parameters of the probing signal and interference signal (these devices are not shown in the scheme).

3. Determination of the Parameters of Interfering Protective Signals Capable of Destroying the Informative Parameters of Dangerous Signals

We have already determined the parameters of effective interfering protective signals aimed at destroying the informative parameters of dangerous signals formed by the methods of high-frequency imposition using simulation modeling in the LabVIEW environment [13, 16].

Experimental studies were carried out in a shielded room of the II class using a complex of instruments and devices (Fig. 3) (then—Complex), which includes:

1. Arbitrary signal generator Tektronix AFG 3252.
2. Spectrum and signal analyzer ROHDE&SCHWARZ FSW 13 (Signal&Spectrum Analyser, 2 Hz – 13.6 GHz).
3. Oscillograph Tektronix DPO 7254 (Digital Phosphor Oscilloscope).
4. A complex of dipole antennas Tuned Dipole Antenna FCC.
5. Folding bilogical antenna SAS-521F-7 25–7000 MHz.
6. Electric antenna EMA-2000 0.009–2000 MHz.
7. Stationary personal computer (monitor, mouse, keyboard, system unit) (then—PC).

Let’s note that this Complex is assembled from existing devices and devices, the composition and number of equipment may change depending on the circumstances.

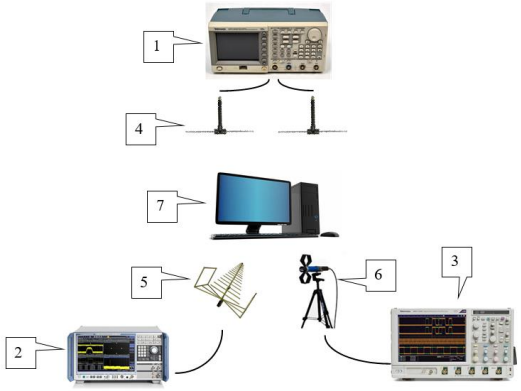

Figure 3: List of equipment for conducting experimental research consisting of (1) arbitrary signal generator Tektronix AFG 3252; (2) spectrum and signal analyzer ROHDE&SCHWARZ FSW 13; (3) oscillograph Tektronix DPO 7254; (4) a complex of dipole antennas Tuned Dipole Antenna FCC; (5) folding bilogical antenna SAS-521F-7; (6) electric antenna EMA-2000; (7) stationary personal computer

According to GOCT 30373-95 "Electromagnetic compatibility of technical means. Test equipment. Shielded chambers. Classes, basic parameters, technical requirements, and test methods" [17] the shielding efficiency of the II class shielded room is 30-80 dB depending on the range. Constructive execution is indecipherable.

A PC is considered as a technical means by which confidential information is processed, and on the elements of which probing signals of high-frequency imposition can be directed.

With the help of a signal generator, a dangerous high-frequency signal and a targeted active jamming protective signal aimed at destroying the informative parameters of a dangerous signal with various types of carrier frequency modulation are set. With the help of a spectrum analyzer, the presence of dangerous and protective signals in the amplitude-frequency spectrum is recorded. The presence of dangerous and protective signals in the amplitude-time spectrum is recorded by an oscillograph.

According to the operating instructions, the control and measuring devices were prepared for work. The measuring antennas were located at a distance of 1 m from the PC and were in a parallel plane to the front part of the PC. At the same time, the geometric centers of the frame antenna and the imaginary geometric center of the PC were on the same axis.

3.1. Determination of the Effective for Destruction of the Frequency Difference Between the Protective and Dangerous Signal

A signal generator was used to create a protective signal and a dangerous signal by choosing arbitrary starting frequencies for both signals.

With the set bandwidth (RBW) of the measuring equipment of 30 Hz and the frequency span (Frequency span) of 500 kHz, a detector of peak values (PK, PEAK) was installed on the spectrum analyzer.

Figure 4: Photographic representation of signals on the screen of the analyzer

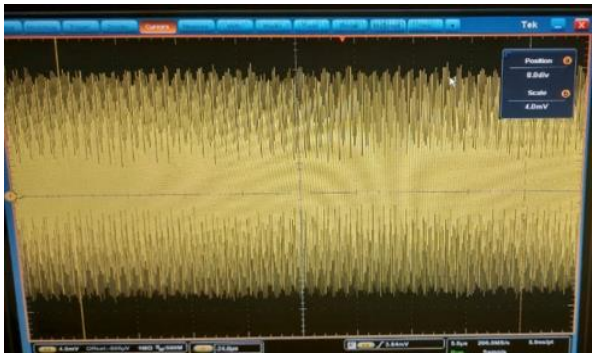

Figure 5: Photographic representation of signals on the oscillograph screen

When setting the value of the frequency difference to 44 MHz (Fig. 4), the effect of frequency "beating" is not observed (Fig. 5).

When the frequency difference between the dangerous and protective signal was gradually reduced and its value was set to 1 MHz (Fig. 6), signs of the "beating" effect were detected

(Fig. 7). Accordingly, this is the extreme value of the frequency at which the effect required for protection is provided.

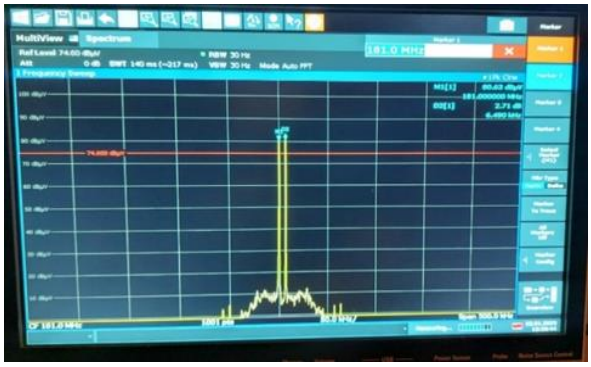

Figure 6: Photographic representation of signals on the screen of the analyzer

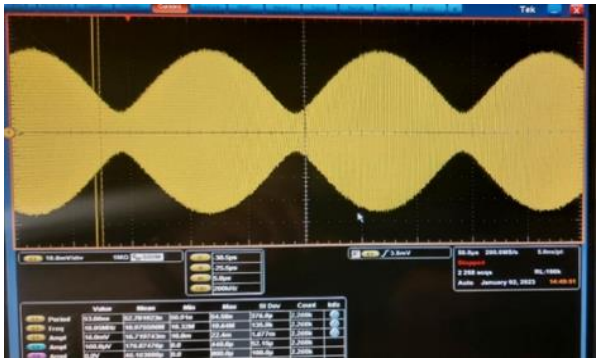

Figure 7: Photographic representation of signals on the oscillograph screen

When the frequency difference between the dangerous and protective signal is further reduced and its value is set to 6 kHz (Fig. 8), a steady phenomenon of "beating" is recorded (Fig. 9).

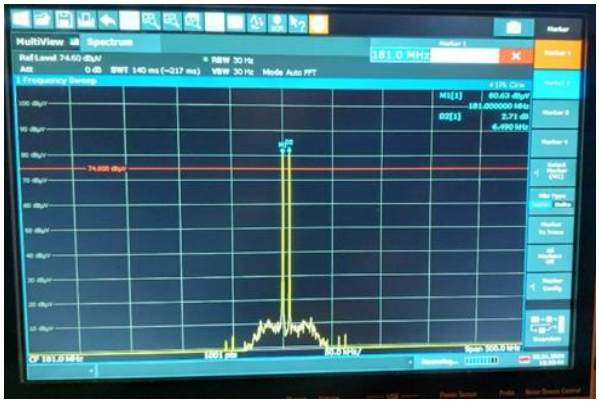

Figure 8: Photographic representation of signals on the screen of the analyzer

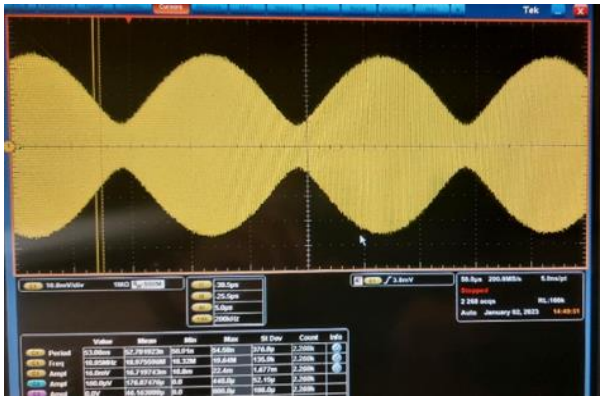

Figure 9: Photographic representation of signals on the oscillograph screen

3.2. Research of the Effect of the Phase Difference Between the Protective and Dangerous Signal on Ensuring the "Beating" Effect

With the help of a signal generator, a protective signal and a dangerous signal were created, choosing the initial frequencies for both signals that provide the effect of "beating" frequencies. Changes in the phase of the dangerous signal were applied, namely a shift of 10°.

With the set bandwidth (RBW) of the measuring equipment of 30 Hz and the frequency span (Frequency span) of 500 kHz, a detector of peak values (PK, PEAK) was installed on the spectrum analyzer.

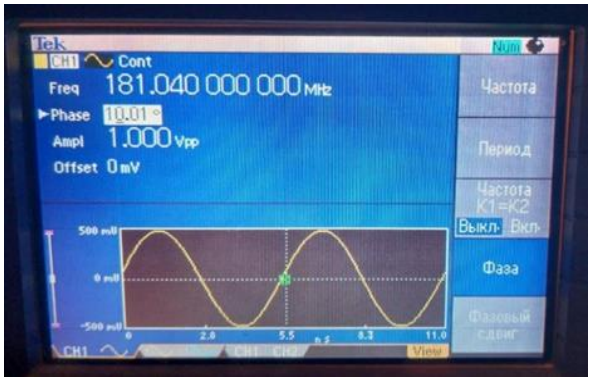

Figure 10: Photographic representation of the phase shift of one of the signals on the generator screen

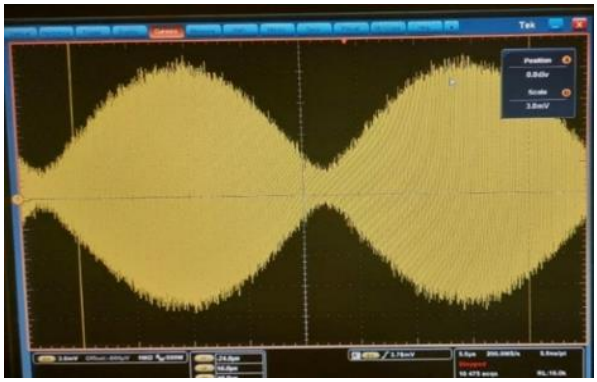

Figure 11: Photographic representation of signals on the oscillograph screen

3.3. Research of the Formation of the Effect of "Beating" Frequencies When Using Two Signal Generators with Different Characteristics Instead of One Two-Channel Generator

This experimental research was conducted to investigate the dependence of the formation of the "beating" frequency effect on the signal generators themselves. An auxiliary generator was used for the experiment ROHDE&SCHWARZ SMA100B Signal Generator 8 kHz – 3 GHz. Having determined the signal frequency and the frequency difference, the corresponding levels were set on the two signal generators. Under the same conditions, with the use of a two-channel generator, the effect of "beating" frequencies is observed (Fig. 8). According to the results of using two different generators (Fig. 12), such an effect is not observed (Fig. 13).

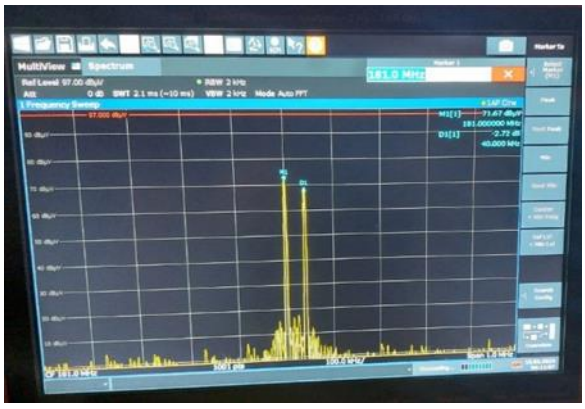

Figure 12: Photographic representation of signals on the screen of the analyzer

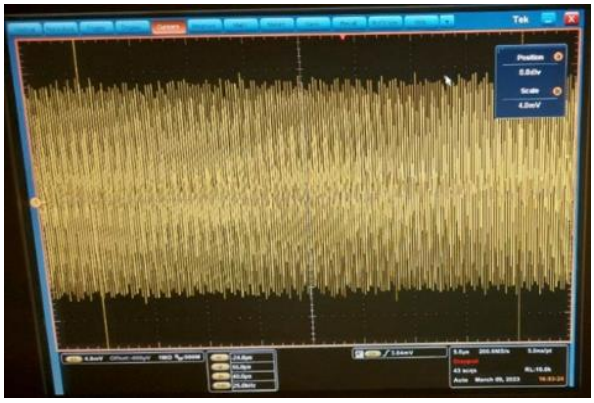

Figure 13: Photographic representation of signals on the oscillograph screen

In the future, it is planned to carry out research according to the generalized scheme (Fig. 2) using the load equivalent.

4. Conclusions

1. High-frequency imposition (probing) is a very effective way of intercepting information circulating in technical means that directly process confidential information if the latter did not include radical measures during its development to prevent the penetration of high-frequency currents inside this equipment.
2. The high-frequency imposition method is based on the use of the physical phenomenon of reflection of high-frequency energy supplied from a special generator from an unmatched load representing the total resistance of any nonlinear or parametric circuit of technical means, the value of which changes under the influence of a dangerous signal according to the law inherent in this signal.
3. The effectiveness of the high-frequency imposition method is generally defined as the result of the interaction of the following technical systems:
   - Information interception systems.
   - Information transmission, processing, and storage systems.
   - Communication systems.

   A priori results of the interaction of these systems can be assessed by conducting a system analysis of the

functioning of a complex technical system consisting of the three indicated components.

4. The use of active protection methods—so-called information destruction systems—can only be recommended in conjunction with well-executed passive protection, shielding, filtering, and decoupling, to further increase the degree of protection efficiency.
5. As a measure of quantitative assessment of the degree of information security in technical processes that directly process confidential information, the permissible probability of information leakage can be taken.
6. During experimental investigations, it was established:
   - to achieve the "beating" effect of frequencies, it is necessary to select signal generators that are as similar to the output characteristics as possible.
   - when the frequency difference is greater, less than 1 MHz between the vulnerable signal and the probe signal, the effect of "beating" frequencies is not avoided.
   - changing the phase of one of the signals does not in any way contribute to the effect of "beating" frequencies.

References

[1] 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.

[2] Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecom-munications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922.

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

[4] V. Astapenya, V. Sokolov, D. Ageyev, Experimental Evaluation of an Accelerating Lens on Spatial Field Structure and Frequency Spectrum, in: IEEE Ukrainian Microwave Week (2020) 203–206. doi: 10.1109/ukrmw49653.2020.9252755.

[5] U. Katoryn, et al., Large Encyclopedia of Industrial Espionage, Poligon (2000).

[6] S. Lenkov, D. Peregudov, V. Khoroshko, Methods and Means of Information Security, vol. 1, Unauthorized Receipt of Information, Aryi (2008).

[7] S. Lenkov, D. Peregudov, V. Khoroshko Methods and Means of Information Security, vol. 2, Information Security, Aryi (2008).

[8] V. Kondratyonok, O. Churco, A. Bakurenko, The Using of High Frequency Domination MethoD for Organization of Information Intelligence Technical Channels for Data Processing Systems, BSUIR reports, Military Academy of the Republic of Belarus (2008) 12–16.

[9] O. Provozyn, V. Geleznyak, V. Khoroshko, Features of the Protection of Information in the Flow Through the Channel Created Using the High-Frequency "Imposition" Method, Modern Inf. Telecommun. Technol. Materials Int. Sci. Technical Conf. 4 (2015) 28–30.

[10] H. Hulak, et al. Formation of requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021, vol. 2923 (2021) 137–142.

[11] S. Lenkov, et al., (2009), Principles of Blocking Information Retrieval by HF-Imposition Methods, Bulletin of Taras Shevchenko National University of Kyiv, Mil. Spec. Sci. 22 (2009) 36-39.

[12] O. Rybaljsjkyj, Method of Information Protection, National Academy of Internal Affairs (2011).

[13] 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 (2021) 14–20. doi: 10.31891/CSIT-2021-5-2.
[14] A. Rembovsky, et al., Radio Monitoring: Problems, Methods, and Equipment, Springer (2009).
[15] O. Rybaljsjkyj, V. Khoroshko, L. Krjuchkova, Experimental Studies of a New Method of Protection Against RF Imposition, Bulletin of Volodymyr Dahl East Ukrainian National University 6(136) 1 (2009) 94–96.
[16] L. Kriuchkova, et al (2022) Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition, in: Cybersecurity Providing in Information and Telecommunication Systems II (2021) 265–272.
[17] Electromagnetic Compatibility of Technical Means. Test Equirment. Shielded chambers. Classes, Basic Parameters, Technical Requirements and Test Methods (2001).