Experimental determination of protective signal parameters for effective "swinging" of the carrier frequency of high-frequency imposition

Larysa Kriuchkova[1,†], Ivan Tsmokanych[2,†], Nataliia Mazur[1,*,†], Denys Tarasenko[3,†] and Viktoriia Osadcha[4,5,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*
[2] *State Research Institute of Cyber Security and Information Protection, 6-3 Maksyma Zaliznyaka str., 03142 Kyiv, Ukraine*
[3] *Security Service of Ukraine, 33 Volodymyrska str., 01001 Kyiv, Ukraine*
[4] *Kielce University of Technology, 17B Al. Tysiąclecia Państwa Polskiego, 25-314 Kielce, Poland*
[5] *Bogdan Khmelnitsky Melitopol state Pedagogical University, 59 Naukove Mistechko str., Zaporizhzhia 69000, Ukraine*

Abstract

The publication is devoted to the improvement of protective effects on dangerous signals formed by high-frequency imposition to ensure the maximum possible destruction of their informative parameters and, as a result, reliable blocking of information leakage channels. The results of experiments are presented, the purpose of which was to determine the parameters of a protective signal aimed at ensuring the effect of "swinging" the carrier frequency of dangerous high-frequency interference signals.

Keywords

interception of information, method of high-frequency imposition, probing signal, dangerous signal, interfering protective signal, parameters of protective signals

1. Introduction

Since the distant 1860s, when James Clerk Maxwell mathematically predicted the existence of electromagnetic waves capable of transmitting energy in space, engineers and scientists are constantly looking for new ways to apply radio frequency technologies, in particular, in the objects of information activities, where the interception of confidential data is a critical problem. High-frequency (HF) "imposition" is a fairly effective way of intercepting information that circulates in technical means of receiving, processing, storing, and transmitting information or is provided in auxiliary technical means and systems, if radical measures were not laid down in the latter during their development, that prevent the penetration of high-frequency currents into this equipment.

The frequency of the high-frequency signal depends both on the parameters of the matching elements of the communication line (for example, the parameters of the matching transformers) and on the characteristics of the nonlinear elements, on which the probing signal can be modulated by informative low-frequency signals arising, for example, due to the microphone effect or in the presence side electromagnetic radiation. The resulting signal is intercepted by the leak channel organizer. The impact of extraneous high-frequency oscillations applied to nonlinear elements by power supply circuits or through the surrounding space leads to the appearance of combination frequencies that are difficult to predict in advance and are emitted into the surrounding space. Therefore, to protect information from leakage due to HF imposition, as a rule, a passive method of protection is used, which consists of shielding the computer or placing it in a shielded cabinet or room, as well as in the installation of broadband filters in the power supply circuits, which makes it possible to increase the security of computers the computer from the influence of HF signals.

Active network equipment can also be a source of electromagnetic oscillations. These oscillations along the wires of the cable system of the data transmission network penetrate the computer and can cause additional informative radiation at combination frequencies. In this regard, the radiation spectrum of the same computer when operating autonomously and when working in a network can be significantly different, and cable systems of data transmission networks, especially made of unshielded copper wires or unshielded twisted pair, can be an additional antenna for all side electromagnetic radiation of the computer, including those arising during the Soft TEMPEST attack [1]. The use of shielded wires or shielded

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

alara54@ukr.net (L. Kriuchkova);
ivakobor@ukr.net (I. Tsmokanych);
n.mazur@kubg.edu.ua (N. Mazur);
box@ukr.net (D. Tarasenko);
vikosa2007@gmail.com (V. Osadcha)

0000-0002-8509-6659 (L. Kriuchkova);
0000-0002-5085-8457 (I. Tsmokanych);
0000-0001-7671-8287 (N. Mazur);
0000-0001-5730-7917 (D. Tarasenko);
0009-0001-6180-8172 (V. Osadcha)

twisted pairs significantly improves the situation but does not guarantee the suppression of in-phase inductions.
It is impossible to design and install a filter in the cable system of the data transmission network that suppresses side emissions and external high-frequency interference signals, similar to the filters installed in power supply circuits. After all, the side emissions of the computer are concentrated in the same frequency range as the spectrum of pulses transmitted by the cable system in the process of network exchange.

The above allows us to conclude that even in the presence of shielding of the processing device and the cable system, the task of protecting information from leakage due to HF imposition is reduced to combating dangerous signals generated by high-frequency imposition.

According to our proposed method of protecting information against leakage through HF channels [2], first, in the presence of a probing signal, its frequency is determined, after which interfering protective signals are formed, aimed at destroying the informative parameters of dangerous HF signals by providing the effects of "beating" and "swinging" of the carrier frequency of dangerous signals of high-frequency imposition.

The parameters of the protective signal, aimed at ensuring the beating effect, are explained in [3] and determined experimentally in [4].

The purpose of this publication is to determine the parameters of a protective signal aimed at ensuring the effect of "swinging" the carrier frequency of dangerous high-frequency interference signals.

2. Search for carrier frequencies of HF signals

The main difficulty in finding and analyzing the leakage channel is to determine the potential frequencies and amplitudes of HF signals. In this regard, it is necessary to conduct preliminary practical research of active network equipment with further development of methods and technical means of protection against leakage of information in electrical channels of digital data transmission at the expense of HF imposition. At the same time, it can already be safely assumed that the protection of data transmission networks with a bandwidth of 100 Mbit/s and above from HF signals will require the development of fundamentally new approaches based on frequency search algorithms for the organization of leakage channels, as well as active monitoring of networks for the presence of "suspicious" harmonics in their spectra.

To determine the carrier frequencies of dangerous signals, the receiver must receive signals in the entire expected range of HF frequencies. Therefore, one of the main characteristics of the search receiver is the frequency range.

Viewing the studied range can be carried out both sequentially in time (search method) and simultaneously over the entire range (non-search method).

Sequential search is organized by sequential frequency tuning of a single-channel receiver, which is called panoramic. Single-channel construction significantly reduces the volume of equipment compared to multi-channel, however, with sequential search, the search time increases.

The frequency-parallel sound of signals is produced using a multi-channel receiver. In this new range of sound frequencies Δf_p is divided by a filter system into several sub-ranges. The filter throughput levels are greater than one-to-one. The filter bandwidth ΔF_{Φ} is inversely proportional to the number of channels n, and if the channels are identical $\Delta F_{\Phi} = \Delta f_p / n$.

The frequency of the received signal is determined by the channel number at the output of which the response was received. In this case, the accuracy of frequency determination is equal to half of the bandwidth $\delta f = \Delta F_{\Phi}/2$, and the resolution (the minimum frequency difference of two signals at which they are perceived separately) is determined by the frequency shift of adjacent channels $\Delta f = \Delta F_{\Phi}$.

Non-search methods of frequency determination include a variety of multi-channel reception, which is called matrix reception. Radio monitoring is carried out by a matrix of receiving elements, the steps of which ensure consistent frequency refinement.

At the first stage, n_i receiving elements are tuned to frequencies $f_{\mathrm{i}} + i\Delta F_i (i = 0, \pm 1, \pm 2, \dots)$ and cover the entire reconnaissance range of frequencies $\Delta f_p = n_i \Delta F_i$. They make it possible to estimate the frequency of received oscillations with an accuracy of ΔF_i and transfer these oscillations for further refinement to the next intermediate frequency f_2.

In the second stage, n_2 receiving elements are tuned to frequencies $f_2 + i\Delta F_2 (i = 0, \pm 1, \pm 2, \dots)$ and overlap the frequency range $\Delta F_1 = n_2 \Delta F_2$. They allow specifying the oscillation frequency with an accuracy of $\Delta F_2 > \Delta F_1$ and transfer the accepted oscillations to the next intermediate frequency f_3, etc.

The resolution of the matrix receiver is determined by the bandwidth of the filters of the last stage $\Delta F_m = \Delta f_p / (n_1 n_2 n_3 \dots n_m)$. With the total number of receiving elements $n = n_1 + n_2 + n_3 + \cdots + n_m$ the resolution of the matrix receiver is significantly higher than that of a multi-channel receiver with the same number of channels.

In essence, a multichannel filter system performs a direct Fourier transform at discrete frequencies. Therefore, parallel search can be implemented based on known methods of spectral analysis using optical or digital signal processing. Digital methods of frequency determination provide high accuracy and are well-matched with computing devices for subsequent signal processing.

To measure frequency, circuits are used that implement modifications of two basic methods: a digital frequency meter and a digital period meter [5]. Therefore, the signal processing structure can be represented both in the time and frequency domain. In this case, secondary identification features selected in one of the channels can be used as primary features in another processing channel. For the frequency domain, the main tool for solving this problem is the discrete Fourier transform (DFT) or fast Fourier transform (FFT).

The probability P_p can serve as a general characteristic of the success of radio monitoring. Radio monitoring will be successful if, firstly, in the search process, a dangerous signal enters the bandwidth of the receiver and, secondly, the energy of the signal turns out to be sufficient for its detection against the noise background. Therefore,

$$P_p = P_n D, \quad (1)$$

where D is the probability of correct detection.

It is known from the theory of signal detection that the probability of correctly detecting a signal with random amplitude and phase (which is precisely what a dangerous signal is) is determined by the expression

$$D = F^{\frac{1}{1+\rho}}, \quad (2)$$

where F is given probability of a false alarm, ρ is the signal-to-noise ratio at the output of a band-pass or matched filter:

$$\rho = \frac{P_c \tau_{\text{cp}}}{N_0}, \quad (3)$$

where P_c is the power of the received signal, τ_{cp} is the average duration of the signal, N_0—noise spectral density.

3. Description of the protective signal

A protective signal is used to ensure the effect of "swinging" the carrier frequency of the dangerous signal (Fig. 1), the frequency of which varies according to a linear law:

$$\omega(t) = \omega_0 + \alpha t \quad (4)$$

where $\alpha = 2\Delta\omega/\tau$, $\Delta\omega = 2\pi\Delta f$ is frequency deviation, τ is pulse duration. The frequency varies from $\omega_{min} = \omega_0 - \Delta\omega$ to $\omega_{max} = \omega_0 + \Delta\omega$.

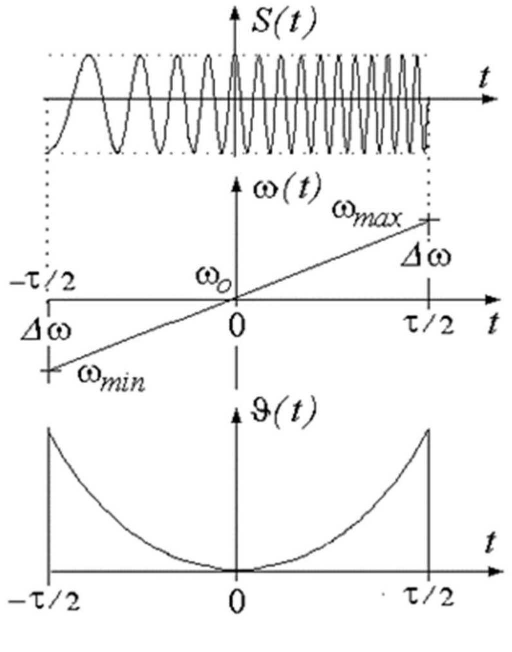


Figure 1: Protective signal

Modulation signal phase:

$$\vartheta(t) = \int \alpha t dt = \frac{1}{2}\alpha t^2, |t| \le \frac{\tau}{2} \quad (5)$$

Period of oscillation of the average frequency $T_0 = \frac{2\pi}{\omega_0} = 1/f_0$. Number of periods T_0 on the length τ is equal to $N_0 = \tau/T_0$. Frequency modulation depth $m = \frac{\Delta\omega}{\omega_0} = \Delta f/f_0$.

The main parameter of the protective signal is its base B, equal to the product of duration τ by deviation Δf:

$$B = \Delta f \tau = N_0 m \quad (6)$$

The oscillation spectrum (Fig. 2) is quite complex. It is expressed through special functions—Fresnel integrals. Because according to (5) the phase *ϑ(t)* here is an even function, all components of the spectrum have an even distribution relative to the frequency ω₀.

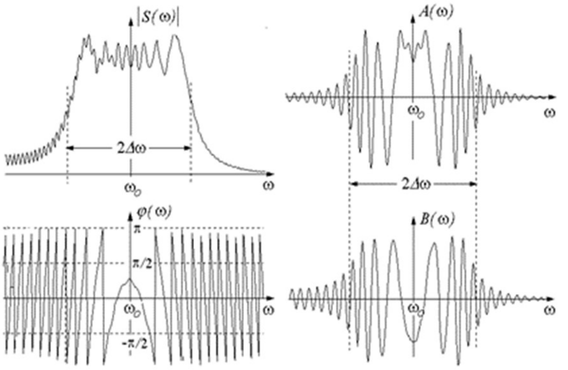


Figure 2: The spectrum of the protective signal with the base B=15 and $\varphi_0 = 0$

The module $|S(\omega)|$ is similar in shape to a trapezoid, the width of which at half the height is equal to $2\Delta\omega$, and the slopes are steeper, the larger the base *B*. The phase spectrum is described by the formula

$$\varphi(\omega) \approx \frac{\pi}{4} - \frac{B}{2}(\frac{\omega - \omega_0}{\Delta\omega})^2 \quad (7)$$

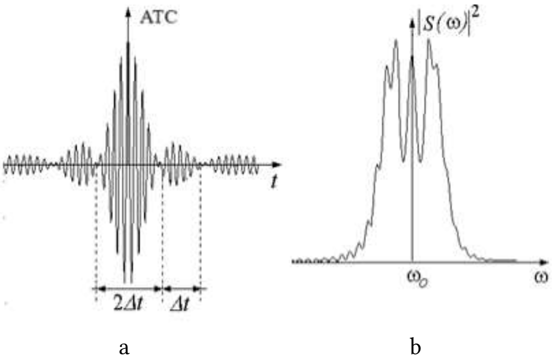
The autocorrelation function, the envelope of which is close in shape to the function $sin\Delta\omega t/\Delta\omega t$ (Fig. 3), with a petal width of

$$\Delta t \approx \frac{1}{2\Delta f} = \frac{\tau}{2B}. \quad (8)$$

Within the central lobe of width $2\Delta t$ *N* periods *T₀* of carrier frequency oscillations are placed:

$$N = \frac{2\Delta t}{T_0} \approx \frac{\frac{\tau}{T_0}}{B} = \frac{N_0}{B} = \frac{1}{m} \quad (9)$$

At *B*>>1 the central lobe has the form of a narrow correlation peak. The ratio $\frac{\tau}{2\Delta T} = B$ is called the compression coefficient.



a b

Figure 3: Autocorrelation function of the signal-deficient (a) and its spectrum (b) for N0=40, B=5, and m=1/8

4. Results of experimental research

Experimental research was directly aimed at achieving such results:

- Changes in the parameters of factory-safe signals can ensure the restoration of informative parameters of unsafe signals by avoiding the effects of “beating” and “swinging” of frequency.
- Limited to the range of effective dry signals when the frequency swing effect is stagnant.
- Confirmation or determination of the effectiveness, sufficiency, and reliability of chemical signals for the protection of information in the flow.

The main purpose of the experimental research was to objectively assess the effectiveness of a safe signal and destroy the informative parameters of unsafe signals:

- Ensuring the protection of information in the current flow by blocking interdiction channels using the high-frequency communication method.
- Checking the effectiveness of the destruction of the informative signal for the additional creation of the effect of “swinging” the frequency when interacting with an unsafe high-frequency interference signal.
- Search for parameters of weak signals, which can maximally change the informative parameters of weak signals, both at the main frequency and at the combination harmonics of the probe signal, thereby preventing the overload of confidential information.

The established experimental research scheme is shown in Fig. 4.

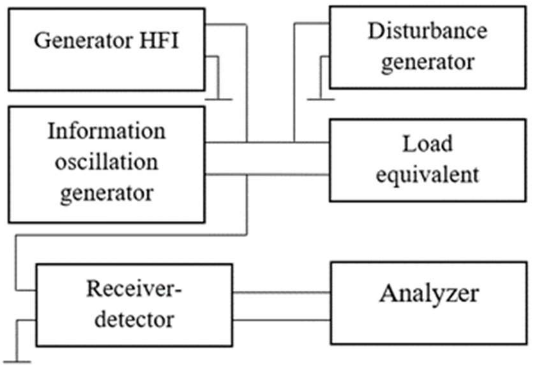


Figure 4: The experimental research scheme has been formalized [6]

The parameters of effective industrial dry signals, direct to the transformation of informative parameters of unsafe signals, generated by high-frequency forcing methods, have already been determined by us through the process of simulation modeling in the LabVIEW core [7, 8] and experimental research [2].

Experimental researches, similar to those before [2], were carried out in a shielded, class II-class with a different complex of accessories and devices (Fig. 3) (hereinafter referred to as the Complex), which includes:

- Signal generator Tektronix AFG 3252.
- Signal spectrum analyzer ROHDE&SCHWARZ FSW 13 (Signal&Spectrum Analyzer, 2 Hz – 13.6 GHz).
- Tektronix DPO 7254 oscilloscope (Digital Phosphor Oscilloscope).
- The complex of dipole antennas Tuned Dipole Antenna FCC.
- White-periodic antenna SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25 MHz–7000 MHz.
- Electrical antenna EMA-2000 0.009–2000 MHz.
- Personal computer of a stationary type (monitor, “Mouse” type manipulator, keyboard, system unit) (hereinafter—PC).

Note that this complex is assembled from existing devices and equipment, the composition and quantity of equipment may change depending on the circumstances.

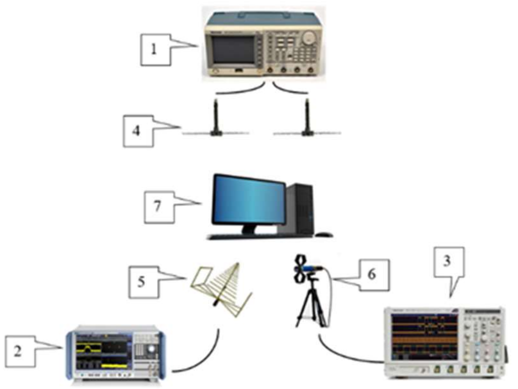


Figure 5: List of equipment for conducting experimental research in the composition: 1—Tektronix AFG 3252 free-form signal generator; 2—Spectrum and signal analyzer ROHDE&SCHWARZ FSW 13; 3—Tektronix DPO 7254 oscilloscope; 4—Complex of dipole antennas Tuned Dipole Antenna FCC; 5—White periodic antenna SAS-521F-7; 6—Antenna electric EMA-2000; 7—Stationary personal computer

According to GOST 30373-95 “Electromagnetic compatibility of technical means. Test equipment. Shielded chambers. Classes, basic parameters, technical requirements, and test methods” [9] the shielding efficiency of the II class shielded room is 30–80 dB depending on the range. Constructive performance is indecipherable.

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

The signal generator creates a protective and dangerous signal by choosing arbitrary starting frequencies for both signals.

When the transmission band (RBW) of the measuring equipment is set to 30 Hz and the frequency span (Frequency span) is 500 kHz, a detector of peak values (PK, PEAK) is installed on the spectrum analyzer.

A personal computer of a stationary type is used as a technical means by which confidential information is processed and which can be exposed to probing signals of high-frequency imposition. With the help of a signal generator, a dangerous HF signal, and a targeted active jamming signal are created, which are aimed at destroying the informative parameters of the dangerous signal using various types of carrier frequency modulation [10–14]. The spectrum analyzer records the presence of both dangerous and protective signals in the amplitude-frequency spectrum, and the oscilloscope displays them in the time domaini.

According to the instructions, the control and measuring equipment is properly prepared for operation. The measuring antennas were located at a distance of 1 m from the PC, while they were in a parallel plane to the front of the PC, and their geometric centers were aligned along one axis.

For the spectrum analyzer, the bandwidth (RBW) was set to 30 Hz and the frequency span (Frequency span) to 500 kHz, and the detector of peak values (PK, PEAK) was selected. Images on the oscilloscope screen demonstrate how changing the parameters of the protective signal affects the distortion of the information parameters of the dangerous signal.

The following figures show step-by-step photographic images of the oscilloscope screen and visually show the dependence of the quality of the distortion of the information parameters of the dangerous signal by the protective signal when the parameters of the protective signal are changed:

1. This image shows the maximum distortion of the information parameters of a dangerous signal under the influence of a protective signal using the method of “swinging” the frequency. The distortion effect is observed at a frequency gap within Δω=±400 kHz, which indicates the optimal parameters for the protective signal. This confirms the signal's ability to effectively destroy information in a dangerous channel.

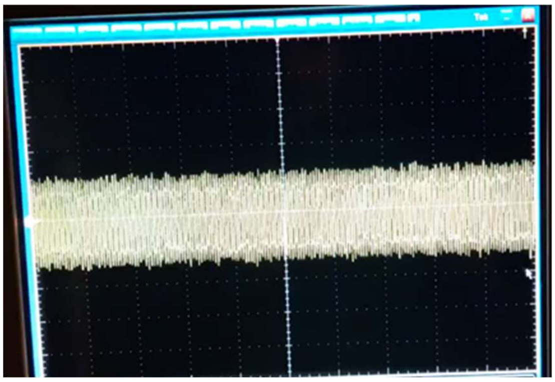


Figure 6: Photographic image of an oscilloscope sweep

2. There is a partial distortion of the information parameters of the dangerous signal. However, due to the significant difference in frequencies between the dangerous and protective signals (Δω≫400 kHz), the method of “swinging” the frequency turned out to be insufficiently effective. This result demonstrates that too large a frequency difference allows you to separate the signals and avoid maximum destruction.

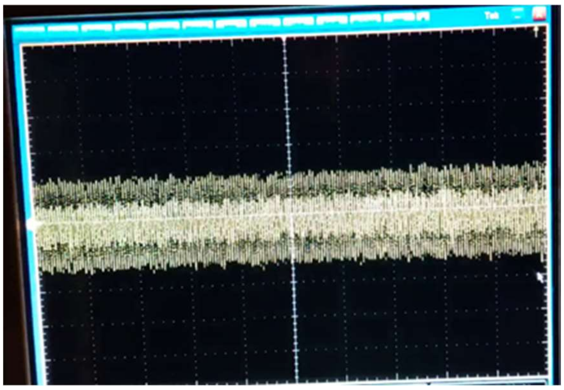


Figure 7: Photographic image of an oscilloscope sweep

3. After the return of the frequency gap to the permissible limits (Δω=±400 kHz), the recovery of the effective destruction of the information parameters of the dangerous signal is observed. This step demonstrates the importance of fine-tuning the frequencies to achieve the maximum efficiency of the “swing” method.

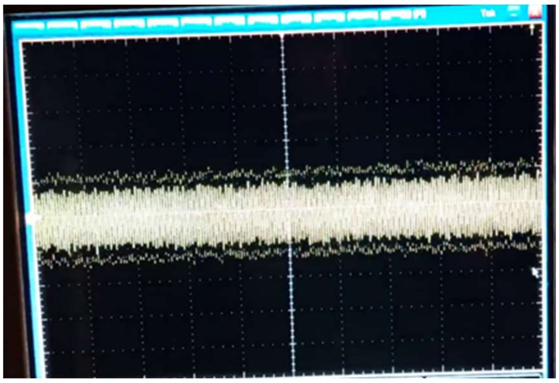


Figure 8: Photographic image of an oscilloscope sweep

4. Similarly to the previous figure, the maximum distortion of the dangerous signal at the optimal frequency difference is shown. This image confirms that within Δω=±400 kHz, the protective signal can destroy the information component of the dangerous signal.

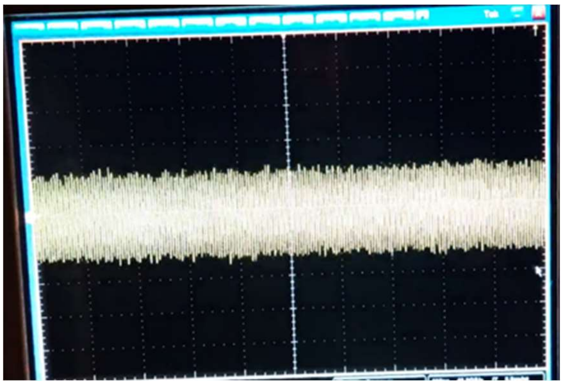


Figure 9: Photographic image of an oscilloscope sweep

5. As in Fig. 7, a partial distortion of the dangerous signal is observed, but the efficiency of the frequency "swinging" method drops again due to too large a frequency difference (Δω≫400 kHz). This confirms that with significant frequency gaps, protective and dangerous signals can be separated.

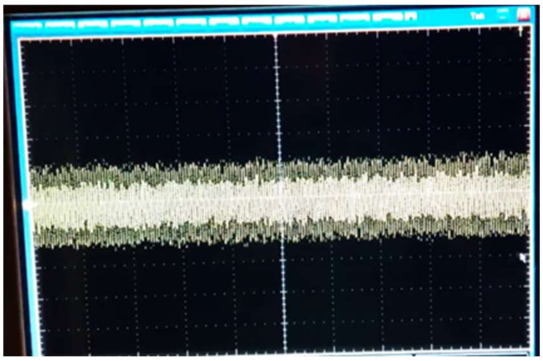


Figure 10: Photographic image of an oscilloscope sweep

6. Displays the maximum distortion of information parameters at a frequency gap of Δω=±400 kHz. This once again confirms that it is important to keep this parameter within the specified limits for the effective operation of the frequency "pumping" method.

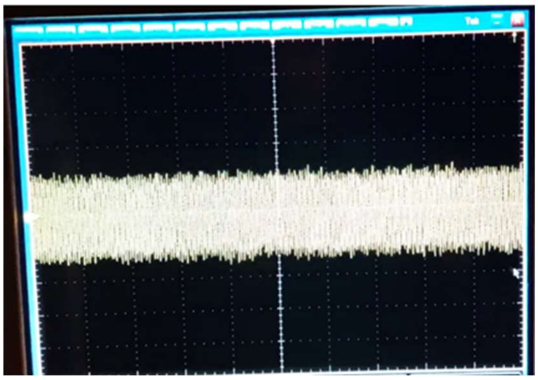


Figure 11: Photographic image of an oscilloscope sweep

7. Distortion of the information parameters of the dangerous signal is observed, but the method of "swinging" the frequency is not effective enough due to the large frequency difference Δω≫400kHz between the dangerous and protective signal (it is possible to separate the dangerous and protective signal), similarly to item 2.

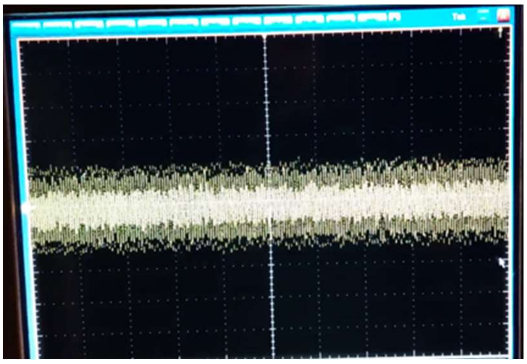


Figure 12: Photographic image of an oscilloscope sweep

8. When the frequency difference between the dangerous and protective signals is increased significantly more than the effective range (Δω≫400kHz), there is no destruction of the informational parameters of the dangerous signal.

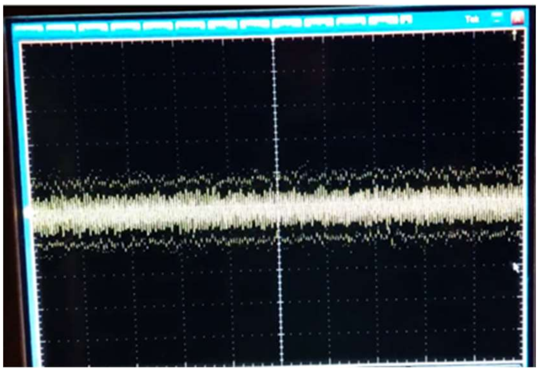


Figure 13: Photographic image of an oscilloscope sweep

9. A renewal of the destruction of the information parameters of the dangerous signal is observed when the frequency difference is set to the extreme permissible limit (Δω=400kHz).

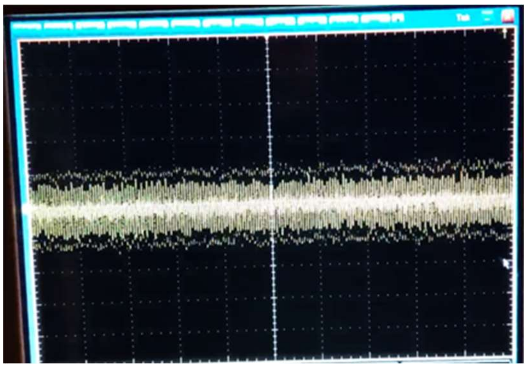


Figure 14: Photographic image of an oscilloscope sweep

10. Similarly to point 1, distortion of the information parameters of the dangerous signal is observed.

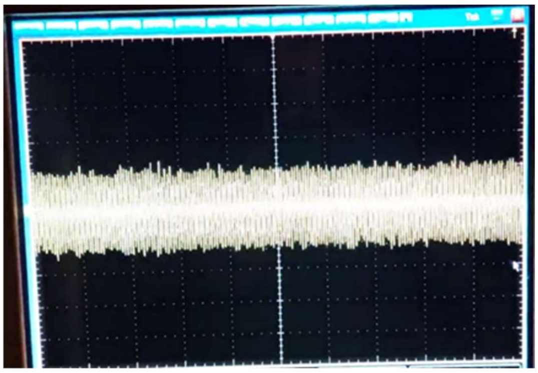


Figure 15: Photographic image of an oscilloscope sweep

11. Distortion of the information parameters of the dangerous signal is observed, but the method of “pumping” the frequency is not effective enough due to the large frequency difference Δω≫400kHz between the dangerous and protective signal (it is possible to separate the dangerous and protective signal), similarly to point 2.

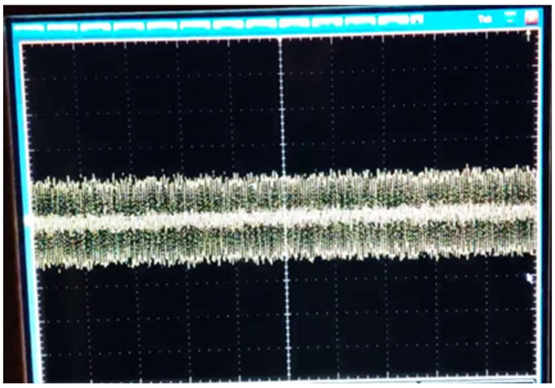


Figure 16: Photographic image of an oscilloscope sweep

12. Analogously to point 2, when the difference in frequencies of dangerous and protective signals increases, the information parameters of the dangerous signal are distorted, but the method of “swinging” the frequency is not effective enough due to the large frequency difference Δω≫400kHz between the dangerous and protective signals (it is possible to separate the dangerous and protective signals.

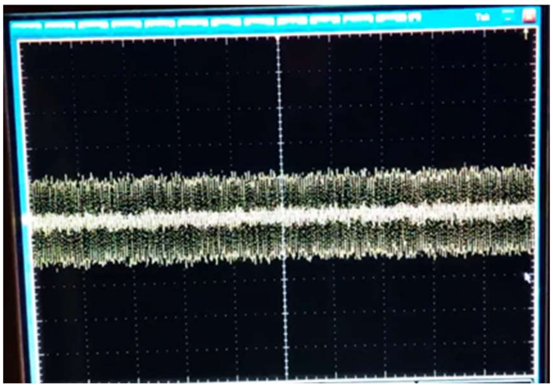


Figure 17: Photographic image of an oscilloscope sweep

In addition to the frequency deviation between the dangerous and protective signals, the effectiveness of the frequency “swinging” method can be significantly reduced in several other conditions:

1. The type of modulation of the dangerous signal

Different types of modulation may respond differently to the “frequency swing” method. For example, amplitude-modulated (AM) signals can be more sensitive to such interference, while frequency modulation (FM) can partially compensate for the influence of the interfering signal. This can lead to the fact that the information parameters of the dangerous signal will undergo less destruction, which reduces the effectiveness of the protection.

2. Noise and other external disturbances.

The presence of additional noise sources or extraneous interference in the frequency range can affect the accuracy of the experimental results. If extraneous signals have close frequency characteristics to the protective signal or dangerous signal, this can complicate the analysis process and affect the ability of the protective signal to destroy informative parameters.

3. Bandwidth of measuring equipment.

The accuracy of the measurements depends on the bandwidth (RBW) settings of the spectrum analyzer and the oscilloscope. If the bandwidth is too wide, fine details of the signal may be lost or unwanted frequencies may be superimposed. A bandwidth that is too narrow can miss important frequencies, affecting the accuracy of measurements and the effectiveness of “frequency swinging”.

4. Duration of exposure of the protective signal.

Another important factor is the duration of the protective signal. If the protective signal is not active long enough or at certain time intervals, it may not reach the required level of destruction of the dangerous signal. In this case, the “frequency swing” method may be less effective, since the dangerous signal may recover after the end of the protective signal.

5. Interaction of signal harmonics.

During the experiment, it was established that, in addition to the fundamental frequency, informative parameters can be hidden in the harmonics of the signal. If the frequency harmonics of the dangerous signal do not fall within the range of the protection signal, this can reduce the effectiveness of the distortion of the dangerous signal. The “frequency swing” method may be less effective in the case of signals with very strong harmonics that are outside the protection signal range.

6. Screened room.

The effectiveness of the frequency swing method also depends on the quality of the shielding of the room where the experiments are conducted. Although the Class II shielded room used provides a fairly high degree of protection (30–80 dB), there may still be signal leaks that affect the results. In real conditions, without this level of shielding, the results may be slightly different.

Thus, in addition to the frequency deviation between the dangerous and protective signals, it is important to consider other factors that can reduce the effectiveness of the "frequency swing" method. This will make it possible to more accurately assess the real capabilities and limitations of protective signals when applied in practice.

The selection of efficiency criteria is of primary importance for evaluating the effectiveness of the impact of protective signals on dangerous HF signals.

One of the important criteria for evaluating the effectiveness of a protective signal is the signal-to-noise ratio reduction indicator (SNR Reduction) [15]. This indicator allows you to determine how intensively the protective signal affects the dangerous signal, destroying its informative parameters.

The reduction in SNR is a direct indicator of how well the protective signal reduces the informativeness of the dangerous signal. As the SNR decreases, the receiver receives a more distorted signal, making it difficult to decode or correctly perceive the original information. For example, in digital systems, a decrease in SNR can lead to an increase in the number of errors when decoding a signal (an increase in the Bit Error Rate, BER).

The effectiveness of destroying the informative parameters of a dangerous signal by reducing the SNR is especially important in conditions where the dangerous signal is transmitted through unstable communication channels. In such cases, even a slight decrease in SNR can significantly affect the quality of the information stream, making interception or analysis of the signal almost impossible.

To reduce the SNR as effectively as possible, it is important to properly adjust the protection signal parameters such as amplitude, frequency, and waveform. The use of broadband or pulse jammers can be particularly effective, as such signals are capable of creating significant interference over a wide frequency spectrum. In addition, the "frequency swing" method used in the protective signal contributes to the dynamic change of the interference parameters, which makes them less predictable and more effective in destroying the dangerous signal.

In general, SNR reduction is one of the key criteria for evaluating the effectiveness of protective signals, as it directly affects the ability of the transmitted signal to retain its informativeness. With the correct setting of the parameters of the protective signal, a significant reduction in SNR can be achieved, which guarantees a high level of protection against the interception of information.

In this study, the SNR Reduction criterion is used to evaluate the effectiveness of the protection signal generated by the frequency swing method. SNR serves as a quantitative indicator that allows you to assess how strongly the protective signal destroys the informative parameters of the dangerous signal.

First, the comparison of SNR values before and after exposure to the protective signal confirms its ability to distort informative components. A significant decrease in SNR indicates that a dangerous signal becomes less suitable for decoding and analysis, thereby increasing the level of protection of confidential information.

Secondly, SNR Reduction helps to determine the "frequency swing" parameters, namely the limits of $\Delta\omega=\pm400$ kHz, at which the largest reduction in SNR is achieved, indicating effective blocking of the informative signal in this particular range. This information is important for optimizing the parameters of protective signals in future studies.

5. Conclusions

As a result of the experimental research, it was established that the effectiveness of destroying the informative parameters of dangerous signals with the help of interfering protective signals significantly depends on the choice of the frequency range of the "swing" frequency. The range where the frequency difference between dangerous and protective signals does not exceed ±400 kHz turned out to be the most effective.

It has been confirmed that the method of "swinging" the frequency is an effective means of protecting information from interception since a dangerous signal undergoes significant distortions when interacting with a protective signal. However, with a significant deviation in the frequencies of the dangerous and protective signals, a decrease in the effectiveness of the protective signal is observed, which indicates the need for accurate equipment adjustment to achieve the maximum protective effect.

The practical significance of the obtained results lies in the possibility of their application in various fields, in particular in information security systems, where the interception of confidential data is a critical problem. The method can be effectively implemented to protect data in corporate networks, government institutions, and critical infrastructure facilities.

Further research can be focused on the development of a methodology for evaluating the effectiveness of protective signals on dangerous HF signals.

References

[1] M. G. Kuhn, Soft Tempest: Hidden Data Transmission using Electromagnetic Emanations (1998).

[2] L. Kriuchkova, et al., Influence of Protective Signals on Dangerous Signals of High-Frequency Imposition, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 419–425.

[3] 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, vol. 3550 (2023) 261–268.

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

[5] X. C. Qin, Z. F. Pan, J. Q. Zhang, A Digital Implementation of Delay Relevant Frequency

Measurement Technology Based on CORDIC Algorithm, International Conference on Education, Management and Medicine (2015) 1087–1091. doi: 10.2991/emim-15.2015.207.

[6] O. V. Rybaljsjkyj, V. A. Khoroshko, L. P. Krjuchkova, Experimental Studies of a new Method of Protection against RF Imposition, Bulletin of Volodymyr Dahl East Ukrainian National University, 6(136) (2009) 94–96.

[7] 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.

[8] 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, vol. 3188 (2021) 265–272.

[9] GOST 30373-95 “Electromagnetic Compatibility of Technical Means. Test Equipment. Shielded Chambers. Classes, Basic Parameters, Technical Requirements and Test Methods”.

[10] V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi: 10.1109/AICT61584.2023.10452421.

[11] V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4. doi: 10.1109/AICT61584.2023.10452687.

[12] 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.

[13] 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.

[14] 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.

[15] Y. Zhang, et al., Optimization Model of Signal-to-Noise Ratio for a Typical Polarization Multispectral Imaging Remote Sensor, Sensors, 22(17) (2022). doi: 10.3390/s22176624.