Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition

Larysa Kriuchkova[1], Maksym Vovk[1], Ivan Tsmokanych[1], and Denys Tarasenko[1]

[1] *State University of Telecommunications, 7 Solomyanska str., Kyiv, 03110, Ukraine*

Abstract

A method of blocking information interception channels by high-frequency "imposition" methods is considered, in which targeted active noise protection signals are introduced into the medium used to supply probe oscillations, aimed at destroying the informative parameters of dangerous signals, which prevents interception of speech information. The LabVIEW simulation determines the parameters of the effective noise protection signals for the destruction of the informative parameters of the dangerous signals generated by the high-frequency "imposition" signals.

Keywords

Information protection, information interception, high-frequency imposition method, probing signal, dangerous signal, interference protection signal, simulation modeling, LabVIEW.

1. Introduction

In the context of global informatization of society, the real security of the state largely depends on the security of its information resources and technologies. In the general problem of information security, the issue of protection of confidential information is one of the most important. This is due, in particular, to the fact that the share of confidential information in the overall information flow is a significant part [1].

Protection of national confidential information has become one of the main priorities of state policy, including in our country. Assignment of information to the category of restricted access and its classification is an important component of the theory and practice of information security. An important task at the objects of information activities is to prevent the interception of confidential information, which is provided by blocking the technical channels of information leakage [2].

One of the effective methods of interception of confidential information at the objects of information activity is the methods of high-frequency "imposition" [3]. High-frequency "imposition" means a method of unauthorized receipt of information, in which probing occurs the radio signal of the room or its conductive communications, in which negotiations are taking place. Because of interaction with technical means or specially implemented devices, there is modulation of probing signals by speech signals. If these circuits have elements whose parameters (inductance, capacitance or resistance) change under the action of low-frequency signals, then in the surrounding space will create a secondary field of high-frequency radiation, modulated by a low-frequency signal.

Currently, two methods are used to intercept information through high-frequency "imposition" channels:

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

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine

EMAIL: alara54@ukr.net (L. Kriuchkova); leny_mowe@ukr.net (M. Vovk); ivakobor@ukr.net (I. Tsmokanych); box@ukr.net (D. Tarasenko)
ORCID: 0000-0002-8509-6659 (L. Kriuchkova); 0000-0003-1781-6762 (M. Vovk); 0000-0002-5085-8457 (I. Tsmokanych); 0000-0001-5730-7917 (D. Tarasenko)

Given the importance of information, measures and tools are applied to ensure the protection of acoustic information and information processed in information systems. There is a method of blocking the signal of interception of information by the method of high-frequency “imposition,” the essence of which is to use a combined active interference (protective signal) aimed at destroying the informative parameters of the dangerous signal [4–6].

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

1. The method of radio monitoring at the object of information activity detects the frequency of the dangerous signal.

2. In case of detection of a dangerous signal by the above-mentioned method, the high-frequency generator generates protective signals aimed at destroying the informative parameters of the dangerous signal, which makes it impossible to intercept information.

The purpose of our research was to find the parameters of security signals that can ensure the maximum possible destruction of the informative parameters of the dangerous signal, and, as a result, to counteract the interception of confidential information by stakeholders.

2. Determination of Parameters of Effective Protection Signals

In radio engineering has long been known the phenomenon of the occurrence of beats between two harmonic oscillations close in frequency, described by the well-known formula:

$$s_\Sigma(t) = s_1(t) + s_2(t) = A_{m1}\sin\omega_1 t + A_{m2}\sin\omega_2 t = 2A_{m1}A_{m2}\cos\frac{\omega_1 - \omega_2}{2}t \cdot \sin\frac{\omega_1 + \omega_2}{2}t\,. \quad (1)$$

As a result of the interaction of two such vibrations, new vibrations arise with a frequency

$$\omega = \frac{\omega_1 + \omega_2}{2} \quad (2)$$

and variable amplitude, the maximum values of which are repeated with a frequency.

$$\Omega = \omega_1 - \omega_2 \quad (3)$$

This phenomenon can be used to protect against high frequency intrusion. Indeed, if the frequency of the probing signal is measured, then it is always possible to radiate into the surrounding space (or direct into a conductive medium) a signal with a frequency close to the frequency of the probing signal of high-frequency intrusion. As a result of their interaction, beats are formed, one of the properties of which is a change in the phase of the resulting vibration when the envelope passes through zero.

Since, when reading information in this way, both amplitude, frequency and phase modulation of the re-emitted signal can occur, it is necessary to take measures to block the possibility of obtaining information when using any of these modulations. Interference for signals with phase modulation will be the change in the phase of the resulting oscillation at the moment of its amplitude crossing through zero. But if such moments are kept constant (i.e. choose a constant frequency of the input oscillation), then the information retrieval system can be easily adapted to such interference. Therefore, it makes sense to make the frequency of the introduced oscillation oscillate within some small limits, ensuring the occurrence of the beat phenomenon. To do this, you can swing the frequency to the left and right of the average value, for example, according to a linear law. And to introduce chaos in the frequency tuning process, the main (master) linear control signal can be added with a random low-frequency signal, which will provide protection from frequency and amplitude-modulated information retrieval.

For the final noise of the acquired acoustic information, the emitted input signal can be added with another random low-level signal (in order to preserve the fundamental frequency of the input harmonic signal), overlapping the audio frequency range.

On the basis of the results of the displayed signals, the values of the parameters of the recorded signals [7], for active countering the transfer of information by the methods of high-frequency navalization, the formulation of the recorded signals with the advanced parameters:

- The first signal is a harmonic carrier signal, with a frequency removed by 10% from the frequency of the dangerous signal. The effect of the first protection signal on the dangerous signal has a beating effect.

- The second signal is an oscillation frequency signal in the range from 5% to 20% of the frequency of the dangerous signal.

Such a combined effect on the dangerous signal leads to the effective destruction of the information contained in the dangerous signal, and prevents the interception of information.

3. Research

To achieve this goal, simulations were conducted using the package LabVIEW ver. 20.0.1.

The research was carried out according to the working block diagrams, which consist of three main parts:

- A group of generators that generate a dangerous signal in the sum of signals (indicated by a red square).
- A group of generators that generate a protection signal in the sum of the signals (indicated by a green square).
- A group of control devices for signal monitoring (indicated by a blue square).

3.1. Research of the Influence of Protective Signals on the Amplitude-Modulated Dangerous Signal

The purpose of the first research was to test the effectiveness of the protection signals on the dangerous signal with amplitude modulation (Fig. 2a). The studies were performed according to the block diagram shown on Fig. 1.

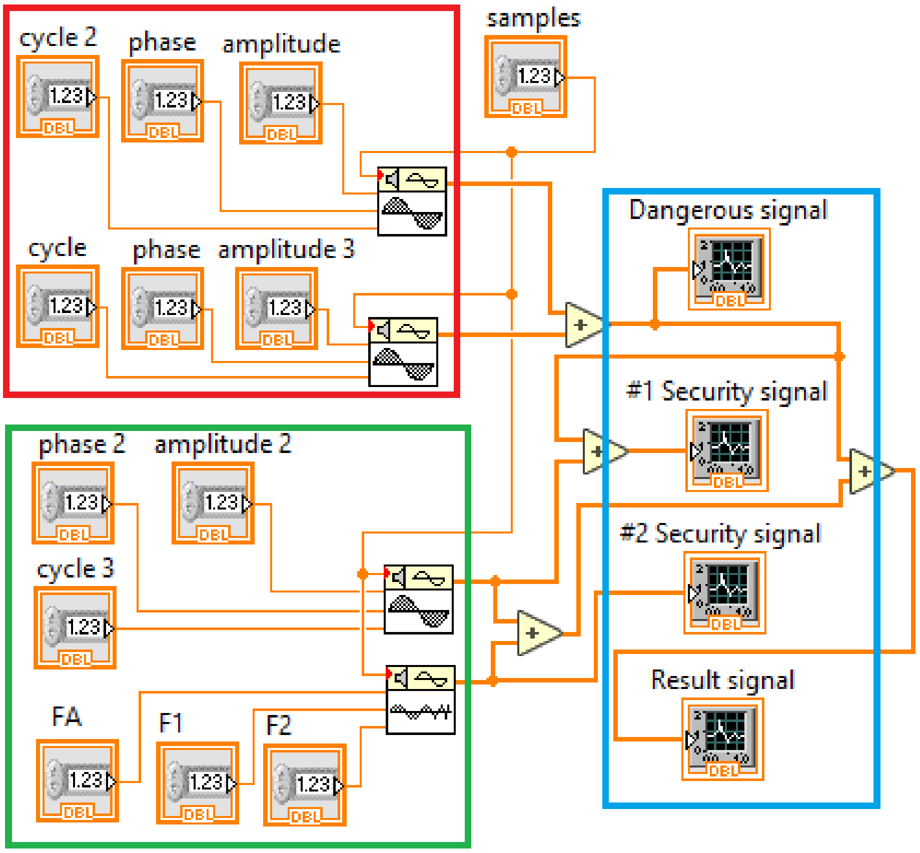

Figure 1: Block diagram by the study of the influence of protective signals on the amplitude-modulated dangerous signal

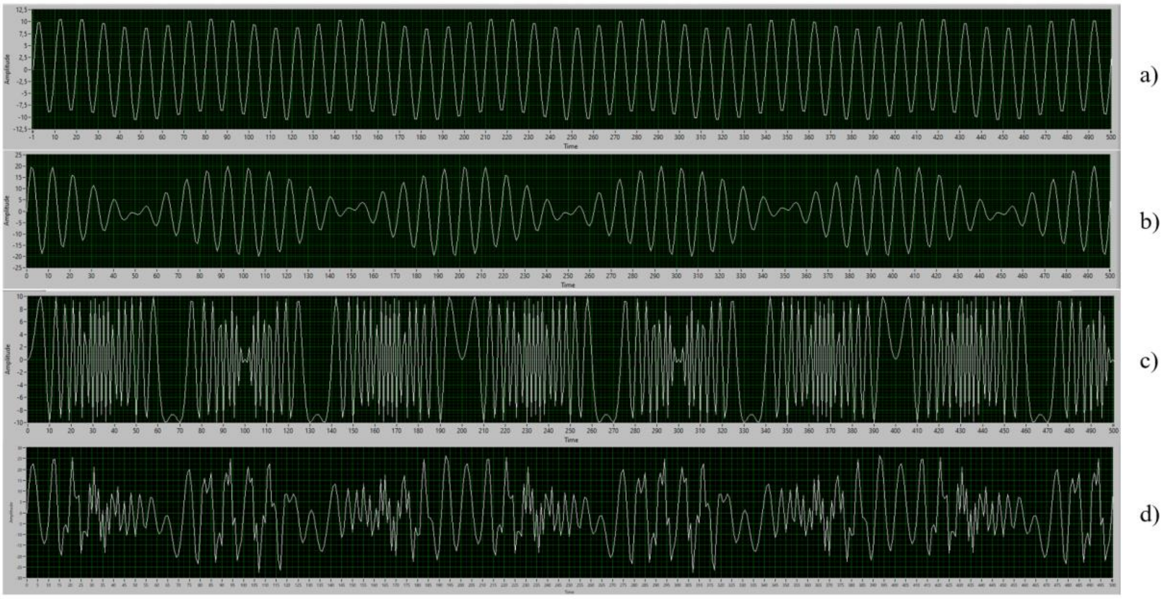

Figure 2: Image of signals of research of influence of protective signals on amplitude-modulated dangerous signal. (a) image of the dangerous signal with amplitude modulation, (b) image of the resulting dangerous signal under the influence of the first protective signal, (c) image of the second protective signal, (d) image of the resulting dangerous signal)

Taking into account the data obtained as a result of the study, namely—the image of the resulting signal (Fig. 2d), we can conclude that the effective destruction of the information component of the dangerous signal with amplitude modulation.

3.2. Research of the Influence of Protective Signals on the Phase-Modulated Dangerous Signal

The purpose of the second research was to test the effectiveness of the protective signals on the dangerous signal with phase modulation (Fig. 4a). The studies were performed according to the block diagram presented in Fig. 3.

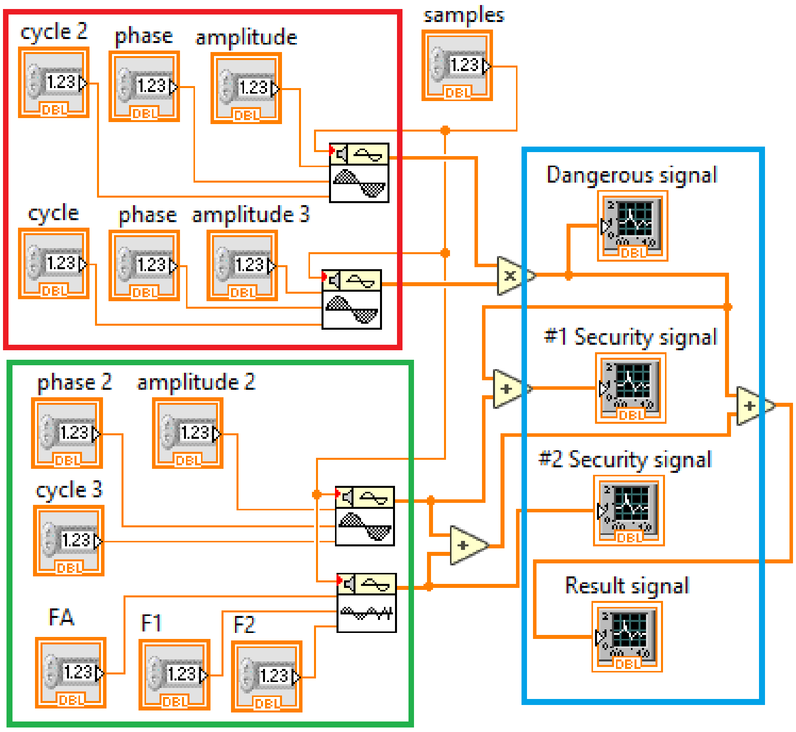

Figure 3: Block diagram of the study of the influence of protective signals on the phase-modulated dangerous signal

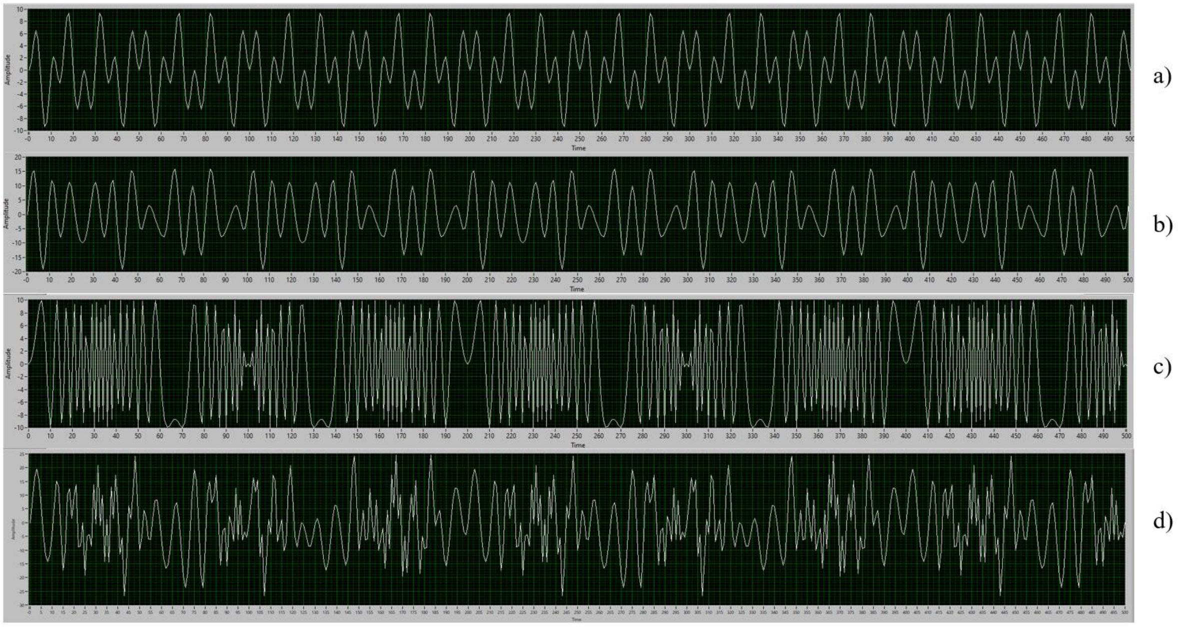

Figure 4: Image of signals of research of influence of protective signals on a phase-modulated dangerous signal: (a) image of the dangerous signal with phase modulation, (b) image of the resulting dangerous signal and the first protection signal, (c) image of the second protection signal, (d) image of the resulting signal

Taking into account the data obtained as a result of the research, namely—the image of the resulting signal (Fig. 4d), we can conclude that the effective destruction of the information component of the dangerous signal with phase modulation.

3.3. Research of the Influence of Protective Signals on a Frequency-Modulated Dangerous Signal

The purpose of the third research was to test the effectiveness of the protective signal on the frequency-modulated dangerous signal (Fig. 6a). The studies were performed according to the block diagram presented in Fig. 5.

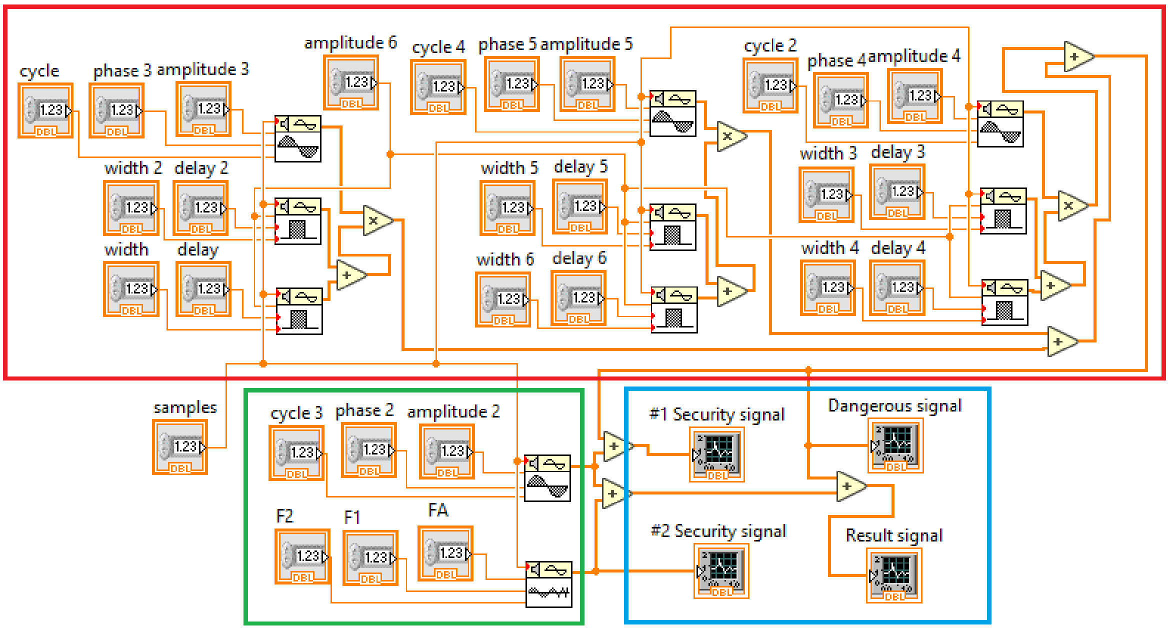

Figure 5: Block diagram of the research of the influence of protective signals on the frequency-modulated dangerous signal

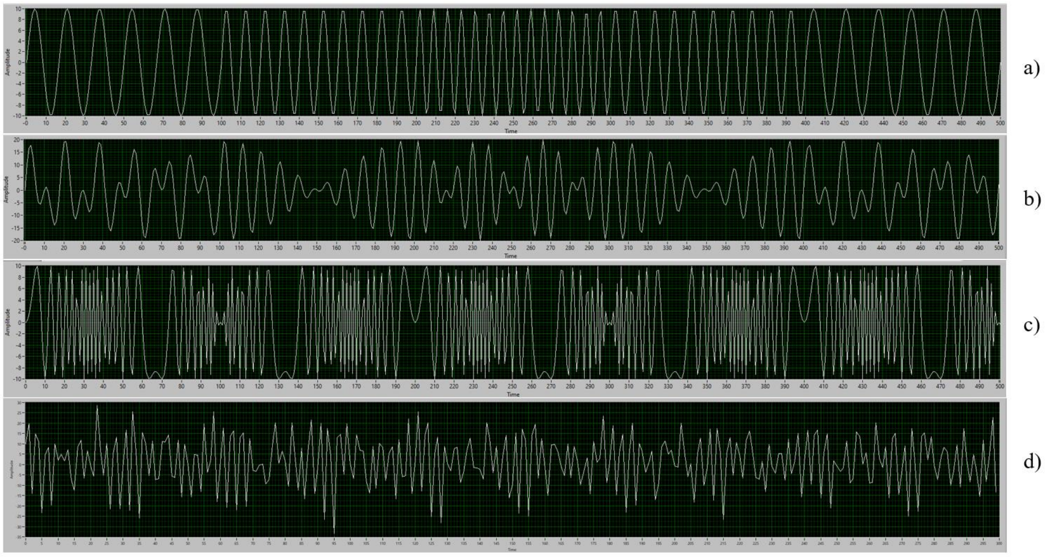

Figure 6: Image of signals of research of influence of protective signals on the frequency-modulated dangerous signal: (a) image of the dangerous signal with frequency modulation, (b) image of the resulting dangerous signal and the first protection signal, (c) image of the second protection signal, (d) image of the resulting signal

Taking into account the data obtained as a result of the research, namely the image of the resulting signal (Fig. 6d), we can conclude that the effective destruction of the information component of the dangerous signal with frequency modulation.

3.4. Research of the Influence of Protective Signals on Dangerous Signals with Amplitude and Angular Modulations

The purpose of the fourth research was to test the effectiveness of the protective signal on the dangerous signal with amplitude and angular modulations (Fig. 8a).

The researches were performed according to the block diagram presented in Fig. 7.

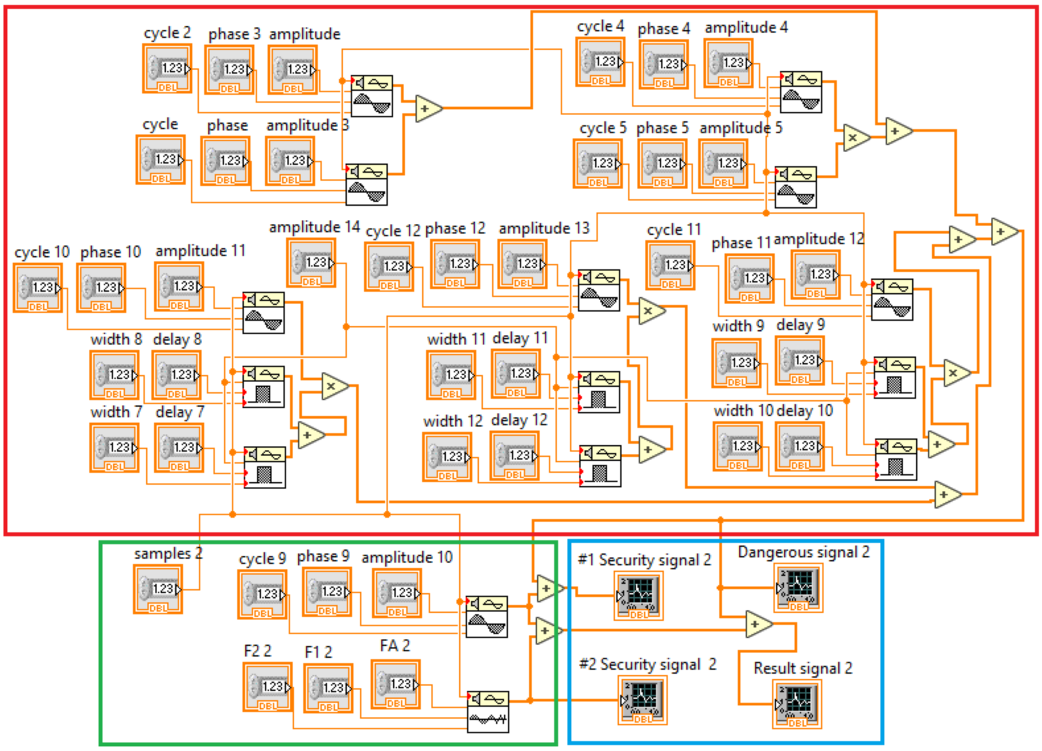

Figure 7: Block diagram of the research of the influence of protective signals on dangerous signals with amplitude and angular modulations

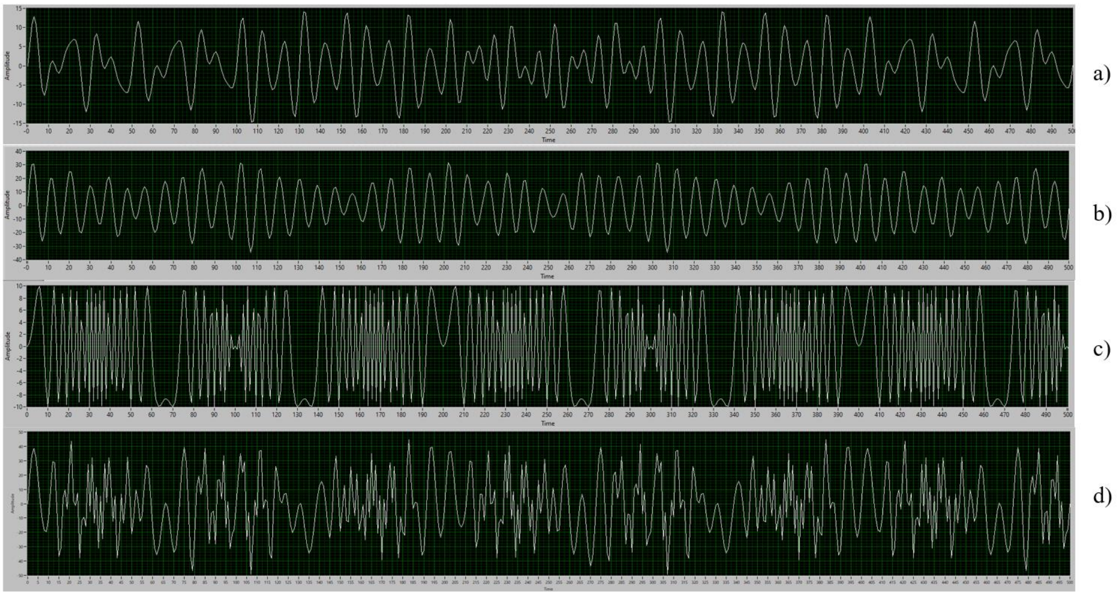

Figure 8: Image of signals of research of influence of protective signals on dangerous signals with amplitude and angular modulations: (a) image of the dangerous signal with frequency modulation, (b) image of the resulting dangerous signal and the first protection signal, (c) image of the second protection signal, (d) image of the resulting signal)

Taking into account the data obtained as a result of the research, namely the image of the resulting signal (Fig. 8d), we can conclude that the effective destruction of the information component of the dangerous signal with amplitude-angular modulation.

Given that the interception of information can be carried out both on the fundamental frequency and on the harmonics of the dangerous signal, the formation of protective signals should be carried out not only relative to the fundamental frequency, but also relative to the harmonics of the dangerous signal [8]. Thus, the phenomena of “beating” and “swinging” of dangerous signals will be traced both on the fundamental frequency and on the harmonics, which will make it impossible to intercept information.

4. Conclusion

Based on the results of research, we have determined the parameters of security signals aimed at blocking dangerous signals of high-frequency “imposition” with different types of carrier frequency modulation.

The proposed method of protection of acoustic information from interception using high-frequency “imposition” changes the properties of dangerous signals and makes them unusable for their intended purpose.

The received distortions of a dangerous signal prevent reproduction of the intercepted information that allows to provide protection of the information against a leak by channels of high-frequency imposing.

5. References

[1] V. Astapenya, V. Sokolov, D. Ageyev, Experimental Evaluation of an Accelerating Lens on Spatial Field Structure and Frequency Spectrum, in: 2020 IEEE Ukrainian Microwave Week, 2020. https://doi.org/10.1109/ukrmw49653.2020.9252755

[2] 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. IEEE. https://doi.org/10.1109/picst54195.2021.9772161

[3] L. Kriuchkova, O. Provozin, Interception of speech information by methods of high-frequency “imposition,” Modern protection of information, 3 (31), 74–80, 2017.

[4] S. Lenkov, et al., Principles of blocking information retrieval by means of HF-imposition, Bulletin of the Taras Shevchenko National University of Kyiv. Military Special Sciences., iss. 22, 36–39, 2009.

[5] O. Ribalskiy, V. Khoroshko, L. Kriuchkova, Experimental studies of a new method of protection against RF intrusion, Bulletin Volodymyr dahl East ukrainian national university 6(136), part 1, 94–96, 2009.

[6] O. Rybalsky, et al., Patent 95365 Ukraine, MPK (2011.01) H04K 3/00. The method of information protection, applicant and patent owner National Academy of Internal Affairs. a200913327, bull. 14, 2011.

[7] L. Kriuchkova, M. Vovk, The method of blocking the channels of active radio devices, Problems of cybersecurity of information and telecommunication systems: Collection of materials of reports and abstracts IV International scientific-practical conference (PCSITS), The Taras Shevchenko National University of Kyiv, 48–49, 2021.

[8] L. Kriuchkova, I. Tsmokanych, An advanced method of protecting information from leakage through high-frequency intrusion channels, in: Collection of abstracts XIII International scientific-practical conference “Computer systems and network technologies” (CSNT), National Aviation University, 62–63, 2021.