UDC 621.3
DOI: 10.31891/CSIT-2021-5-2

LARYSA KRIUCHKOVA, IVAN TSMOKANYCH, MAKSYM VOVK
State University of Telecommunications, Kyiv, Ukraine

ADVANCED METHOD OF PROTECTION OF CONFIDENTIAL INFORMATION FROM INTERCEPTION BY HIGH-FREQUENCY IMPOSITION METHODS

The processes of formation of technical channels of leakage of confidential information on objects of information activity by methods of high-frequency imposition, physical essence of process of formation of dangerous signals by modulation of probing high-frequency signal by acoustic signals, conditions of formation of basic and auxiliary technical means and systems of dangerous signals are considered. As a basis for improvement, a method of blocking information interception channels by high-frequency imposition is used, in which target active noise protection signals are introduced into the medium used to supply probing oscillations, aimed at destroying informative parameters of dangerous signal with different types of carrier modulation. It is proposed to form a set of protective signals for the destruction of informative parameters of dangerous signals both on the fundamental frequency and on the combinational harmonics of the probing signal, which provides more effective protection of confidential information from interception. The parameters of effective noise protection signals, capable of destroying the informative parameters of dangerous signals of high-frequency imposition on the fundamental frequency and combinational harmonics of the probing signal, have been determined by mathematical and simulation modeling. Basic recommendations for the formation of protective signals are formulated.

Keywords: Information protection, information interception, high-frequency imposition method, probing signal, dangerous signal, interference protection signal, parameters of protection signals, modeling.

ЛАРИСА КРЮЧКОВА, ІВАН ЦМОКАНИЧ, МАКСИМ ВОВК
Державний університет телекомунікацій

УДОСКОНАЛЕНИЙ МЕТОД ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ВІД ПЕРЕХОПЛЕННЯ МЕТОДАМИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

Розглянуто процеси формування технічних каналів витоку конфіденційної інформації на об'єктах інформаційної діяльності методами високочастотного нав'язування, фізичну сутність процесу утворення небезпечних сигналів шляхом модуляції зондуючого високочастотного сигналу акустичними сигналами, умови формування в колах основних та допоміжних технічних засобів і систем небезпечних сигналів. В якості базового для вдосконалення взято спосіб блокування каналів перехоплення інформації методами високочастотного нав'язування, при якому в середовище, використовуване для подачі зондуючого коливання, вводяться прицільні активні завадові захисні сигнали, спрямовані на руйнування інформативних параметрів небезпечного сигналу з різними видами модуляції несійної частоти. Запропоновано для захисту конфіденційної інформації на об'єктах інформаційної діяльності формувати сукупність захисних сигналів для руйнування інформативних параметрів небезпечних сигналів як на основній частоті, так і на комбінаційних гармоніках зондуючого сигналу, що забезпечує більш ефективний захист конфіденційної інформації від перехоплення. Шляхом математичного та імітаційного моделювання визначено параметри ефективних завадових захисних сигналів, здатних забезпечити руйнування інформативних параметрів небезпечних сигналів високочастотного нав'язування на основній частоті та комбінаційних гармоніках зондуючого сигналу. Сформульовано базові рекомендації щодо формування захисних сигналів.

Ключові слова: Захист інформації, перехоплення інформації, метод високочастотного нав'язування, зондуючий сигнал, небезпечний сигнал, захисний сигнал, параметри захисних сигналів, моделювання.

Introduction

On the objects of information activity circulate information that has a certain classification or may contain data that may in some way affect the security of the state and its citizens. Because of this, this information may be subject to interception attempts. As a result of the action of many factors, technical channels of leakage of confidential information may be formed spontaneously or intentionally. Given the importance of information, measures and tools are applied to ensure the protection of acoustic information and information processed in information systems.

An effective method of intercepting confidential information in the objects of information activities is the method of high-frequency imposition. The method of high-frequency imposition is based on the use of the physical phenomenon of reflection of high-frequency energy from uncoordinated load [1]. The formation of the technical channel of information leakage is carried out by probing the radio signal of the room in which the negotiations take place, or its conductive communications. As a result of interaction with technical means or specially implemented devices, the probing signals are modulated by speech. 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.

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

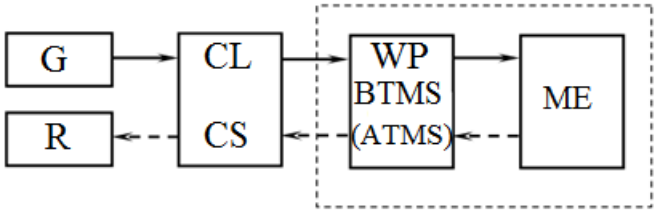

Fig. 1. Block diagram of the channel of high-frequency imposition

Currently, two methods are used to intercept information by the method of high-frequency imposition:

- 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.

The task is to create an effective method of protecting confidential information from leakage through high-frequency imposition channels.

Related Works

Today, passive, active and combined methods of protecting information from interception are used. There is also a division into organizational and technical methods of information protection.

Information protection from high-frequency intrusion in wire channels is carried out using both organizational and technical measures.

Organizational measures include [2]:

• use of telephones made in a protected form;

• physical control of telephone lines for the presence of connections (at distances up to 100 m from the device, which corresponds to the maximum range of this type of information interception systems);

• disconnecting telephones from the network during negotiations.

It should be noted that it is quite problematic to organize constant control of telephone lines in real urban conditions. This can only be done if the organization is located in a separate building or if you have your own automatic telephone exchange. Disconnecting devices from the line during negotiations also cannot be attributed to reliable measures: experience shows that this is often forgotten. Therefore, there can be no reliable protection without the use of technical means.

Technical measures are carried out in the following areas [2]:

• instrumental control of radiation for the detection of probing high-frequency signals in communication lines;

• installation of passive protection schemes.

The disadvantage of the considered protection method is the ability to turn off the equipment for intercepting information during the check, therefore, episodic control is not entirely reliable.

A guaranteed countermeasure is to bypass the line or microphone of the handset with a capacitor with a capacity of about 10 nF [3]. The sounding signal, according to the laws of physics, “follows the path of least resistance”, and the capacitor for high frequency has a relatively low resistance compared to the microphone.

To detect the fact of exposure, it is necessary to carry out either constant radio monitoring, or to provoke the opposing side to use reconnaissance means at a certain time. The panoramic radio receiver or spectrum analyzer is switched to the maximum view mode with the minimum sensitivity, and the study of the electronic situation in the area of the object is carried out (all powerful radiations are identified). The antennas are turned towards the possible location of the transmitters. After that, it is enough to fix the appearance of the probing signals. The main difficulty is periodic false alarms: radio telephones in adjacent premises, radio beacons for various purposes, powerful radio stations of the army and special services that do not work constantly.

Another method of protection is room shielding. The method is effective, the only problem is that it is very expensive and drastically reduces the ergonomic characteristics of the room. Protecting windows and doors is particularly challenging. Another direction is the placement of premises allocated for holding confidential events in buried reinforced concrete basements.

The purpose of passive and active methods of protection is to reduce the signal-to-noise ratio at the boundary of the controlled area to values that ensure the impossibility of isolating a dangerous information signal by an intelligence agent. In passive methods of protection, the reduction of the signal-to-noise ratio is achieved by reducing the level of the dangerous signal, in active methods - by increasing the noise level [4].

Authors V.A. Vorona and V.O. Kostenko note [4] that the method of interception of information by high-frequency imposition is difficult to detect because it has a wide range for the selection of operating frequencies, while devices whose work is aimed at detecting high-frequency imposition signals are often able to perform in a narrow frequency range.

In [4] offers an option to protect information from interception by organizing the noise of the channel in a certain frequency band. In this case, the data transmission will be carried out with certain distortions. Accordingly, the attacker will need to periodically repeat the parameters of his dangerous signal, which in practice is very difficult to implement. However, even in this case, the attacker has the opportunity to analyze the entire spectrum formed by high-frequency imposition, to accumulate variations in signals and to identify important parts [5]. Therefore, this method also does not guarantee full protection of information.

Among the known methods of protection of acoustic information is one [6], which is based on radiation into the surrounding space of a broadband noise (barrier) or noise-like interference. This method allows to protect acoustic information, but when using high-frequency imposition, it is ineffective, because to form a leakage channel uses a powerful harmonic external imposition signal (sounding signal) of stable frequency, which allows you to select a sounding signal and receive a signal re-radiant. A significant disadvantage of the use of broadband blocking interference is the possible disruption of their own communication channels under the conditions of interference and reducing the range of protection of objects due to inefficient costs of the interference resource.

Aiming noise has a significant energy gain compared to the barrier, but its implementation requires information about the values of the frequencies of the probing signals of imposition. Obtaining such information is time consuming, which in the ephemerality of the conflicting interaction of dangerous and protective signals requires special solutions.

Authors Lizunov S.I. and Razumovsky K.I. note the following disadvantages of active means of protection [7]:

- Prolonged stay of staff in a room with noise generators can adversely affect their health.
- When changing the location of the information signal sources, the overall signal level in the room may change in such a way that the signals can be detected outside the room, despite the noise.
- It is necessary to make noise in a wide range of frequencies. The limits of this range cannot always be clearly defined due to the beating of several signals, as well as the possible external high-frequency influence.
- The presence of suppressive radiation unmasks the object and may interfere with the operation of other foreign devices outside the controlled area.
- The use of active means involves constant additional actions (for example, preparation of the complex for work, inclusion, exclusion, prevention, constant checking of its efficiency, etc.).
- Additional power supplies required.

The authors believe that a more promising area is the development of passive methods of information protection, including shielding, but among the disadvantages are high cost, rather complex installation and, if metal screens are used, large dimensions.

N. Smailov and A. Baturgaliyev suggest [8] to use active means of information protection, in particular noise generators, but note that due to high-frequency imposition there is a possibility of interception of information through the signals of these generators.

The authors of [9] consider it necessary to consider the method of interception of information by high-frequency intrusion through network cables and adapters. It is noted that the element through which the high-frequency imposition interacts with the low-frequency signals may be an element of the network adapter or modem. For example, it can be any nonlinear element, and the role of the modulator can be performed by a video card. Under such conditions, the interception of information becomes possible. Accordingly, measures should be taken to ensure the security of information.

In [10] the leakage of speech information through alarm loops is considered and the use of passive filters in the system of information protection against leakage is proposed. Describes a method that allows to attenuate informational electrical signals in the connecting lines of assistive devices and systems that have arisen as a result of acousto-electrical transformations of speech information.

It has been noted that with high-frequency imposition, information leakage channels can be formed both in the power supply and grounding circuits and in the environment [5]. This adds variability to the attacker and increases the chances of intercepting information.

Unfortunately, we cannot include materials for official use in the analysis, but even recent publications suggest that the task of creating an effective method of protecting confidential information from interception by high-frequency intrusions remains relevant.

Purpose

As a basis for improvement, we took a method of blocking information interception channels by high-frequency imposition, in which the medium used to supply the probing oscillations, are introduced sighting active noise protection signals aimed at destroying the informative parameters of the dangerous signal with different types of carrier frequency [11–13]:

- first protection signal - harmonic signal to create a "beating" effect with a dangerous signal of high-frequency imposition;
- the second protection signal is the oscillation frequency signal.

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 is proposed not only in relation to the fundamental frequency, but also in relation to the harmonics of the dangerous signal [14]. Thus, the effects of "beating" and "swinging" of dangerous signals will be traced 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 a protection system as follows:

1. The method of radio monitoring at the object of information activity reveals the frequency of the probing signal of high-frequency imposition.

2. In case of detection of the above-mentioned method of a probing signal, the set of the protective signals directed on destruction of informative parameters of dangerous signals of high-frequency imposing not only on the basic frequency, but also on combinational harmonics of a probing signal is formed.

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 dangerous signals at the fundamental frequency and the combinational harmonics of the probing signal, and, as a result, to counteract the interception of confidential information by stakeholders.

Proposed technique

As basic recommendations for the formation of protection signals, a method of generating radio signals with angular modulation simultaneously on several harmonics of the oscillation of the carrier frequency is proposed [15].

There are a number of implementations of angular modulation:

1. The principle of distribution of the frequency spectrum into a certain number of bands and their subsequent transfer within the carrier oscillation.

2. The principle of multiplication of the original, rather low carrier frequency, followed by multiplication of the modulation index, after which the frequency conversion is used, as a result of which the frequency deviation and, accordingly, the modulation index remain unchanged, but the carrier frequency decreases a certain number of times.

3. Quadrature method.

The first two methods have some disadvantages, including the complexity of implementation, a significant parasitic change in frequency due to possible instability of the generator, etc.

Therefore, a quadrature method of increasing the angular modulation index is more reliable and perfect [15]. It allows to compensate amplitude-phase distortions of phase-modulated signals at arbitrarily set modulation index.

The quadrature method includes:

forming with a high-frequency generator and phase shifter on π/2 quadrature components, which are described by the following laws:

$$u_1 = U_1 cos\omega t \quad (8)$$

$$u_2 = U_1 sin\omega t \quad (9)$$

forming by means of cosine and sinusoidal converters of modulating voltage, respectively, control signals:

$$e_k = E_y \cos\left[m_\varphi sin\Omega t\right] \quad (10)$$

$$e_c = E_y \sin\left[m_\varphi sin\Omega t\right] \quad (11)$$

quadrature multiplication of high-frequency and low-frequency components (8) from (10) and (9) from (11) in balance modulators with coefficient $k_{\text{БМ}} = 1$;

assembly of high-frequency quadrature components in a linear adder, resulting in the formation of the output phase-modulated signal:

$$u_c = U_1 E_y\left[cos\omega t cos\left(m_\varphi sin\Omega t\right) - sin\omega t sin\left(m_\varphi sin\Omega t\right)\right] = U_{c1}\cos\left(\omega t + m_\varphi sin\Omega t\right) \quad (12)$$

where $U_{c1} = U_1 E_y$ – constant amplitude.

From formulas (1) - (5) it follows that it is possible to obtain a phase-modulated signal with any arbitrarily given modulation indices m_φ. The implementation of the quadratic method does not reduce the resulting stability of the transmitter frequency and there is no fundamental limit associated with the choice of carrier frequency, and does not require complex matching of high-frequency and low-frequency modulator paths due to lack of control reactive elements. The above factors allow the use of a quadrature method to implement angular modulation in the generator, which is used to protect information from leakage through the high-frequency imposition channel.

Results

The harmonic hazard signal is described by the following equation:

$$x_1 = A\cos\omega_1 t \quad (12)$$

Accordingly, the security signal has the form:

$$x_2 = A\cos\omega_2 t \quad (13)$$

To study the effect of "beating" we use the equation of the resulting signal, which has the following form:

$$x(t) = 2A\cos\Delta\omega t\cos\omega t \quad (14),$$

where $\Delta\omega = \frac{\omega_1-\omega_2}{2}$, $\omega = \frac{\omega_1+\omega_2}{2}$.

Effective "beating" of signals is observed only at a certain difference of frequencies of dangerous and protective signals, providing distortion of parameters of dangerous signal.

Figure 2 shows the image of the "beating" effect of harmonic oscillations with close frequencies (harmonic oscillations with a constant frequency Ω, the amplitude of which slowly changes from $|A_1 - A_2|$ to $A_1 + A_2$).

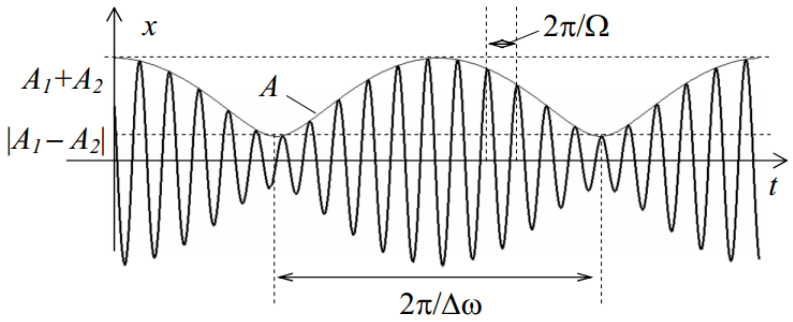

Fig. 2. Image of the effect of "beating" of harmonic oscillations with close frequencies

Using mathematical modeling in the environment MathCad 13 [14] determined the optimal range of values of security signals to ensure the phenomenon of "beating": 0,005≤Δω≤0,3, where Δω – the difference between the frequencies of dangerous and protective signals. Figures 3 and 4 shows the options for the interaction of dangerous and protective signals:

As can be seen from Fig. 3, at $|\omega_1 - \omega_2|$=1 MHz, where ω_1 = 800 MHz – dangerous signal frequency, a ω_2 – protection signal frequency, "beating" of signals is practically absent and destruction of informative parameters of a dangerous signal is not provided.

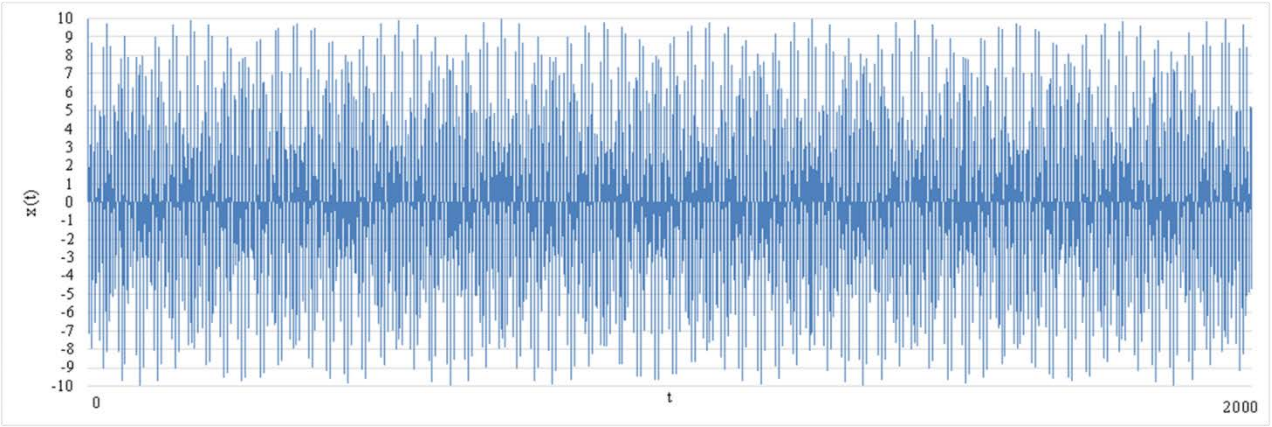

Fig. 3. Image of the resulting dangerous signal provided Δω=1 MHz

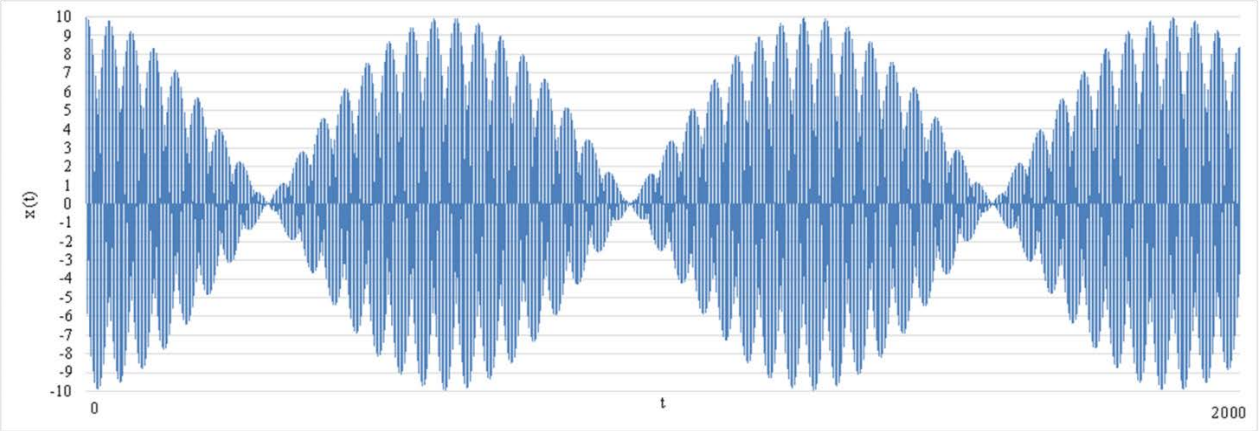

Fig. 4. Image of the resulting dangerous signal provided Δω=0,01 MHz

Instead, when $|\omega_1 - \omega_2|$=0,01 MHz there is a clear effect of "beating", which indicates the destruction of the informative parameters of dangerous signals (Fig. 4).

The range of the oscillating frequency protection signal was determined by simulation studies using a packet

LabVIEW version 20.0.1 [16].

Based on the results of research on determining the parameters of security signals, to actively counteract the interception of information by high-frequency imposition methods, it is proposed to form security signals with the following parameters:

- the first protection signal is a harmonic carrier frequency, with a frequency 10% distant from the frequency of the dangerous signal. The effect of the first protection signal on the dangerous signal has a "beating" effect;
- the second protection signal is an oscillation frequency signal in the range from 5% to 20% of the dangerous signal frequency.

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 (Fig. 5, d).

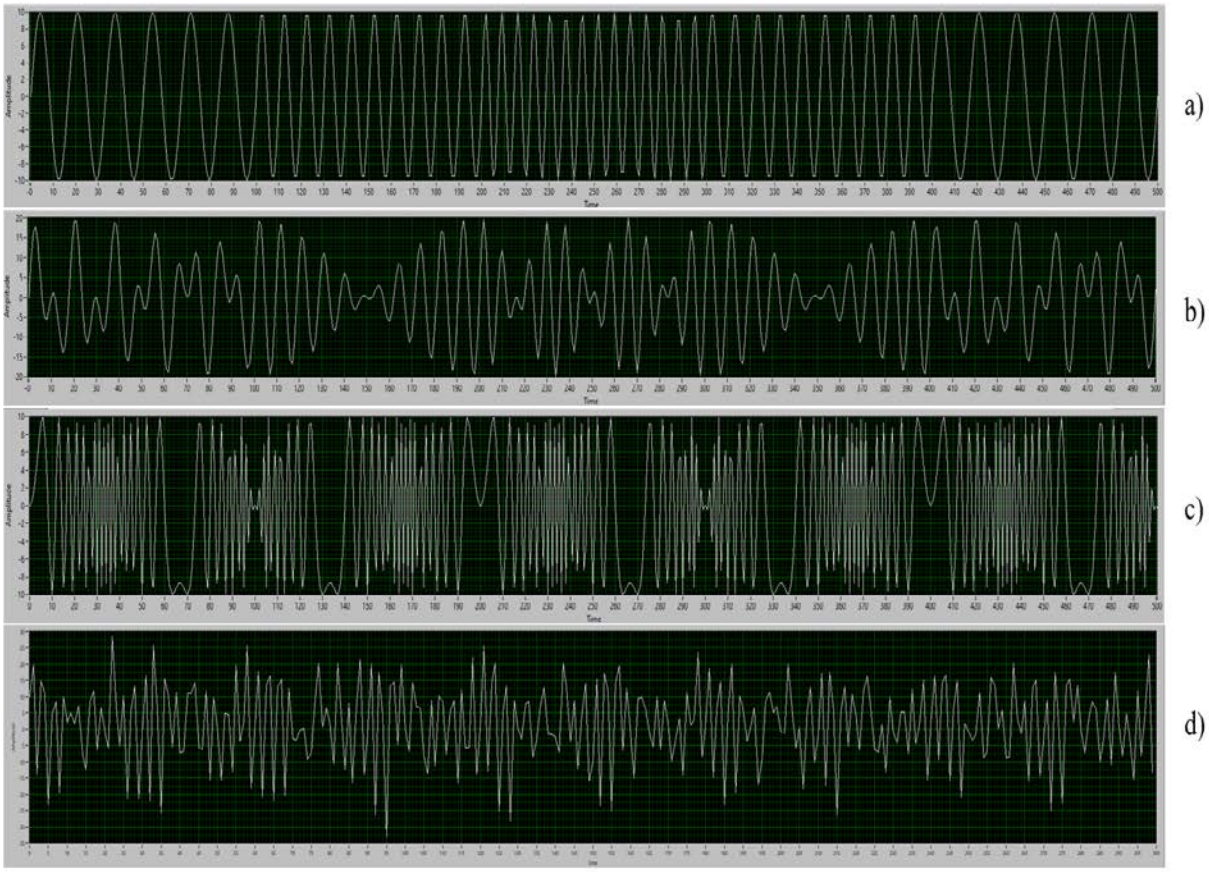

Fig. 5 Image of signals of research of influence of protective signals on the frequency-modulated dangerous signal (a - image of the dangerous signal with frequency modulation, b - image of the resulting dangerous signal and the first protection signal, c - image of the second protection signal, d - image of the resulting signal)

Conclusions

Through mathematical modeling in the MathCad environment and simulation studies using the LabVIEW package, it was found that a harmonic protection signal with a frequency removed by 10% from the frequency of the dangerous signal provides a stable "beating" effect, thereby destroying the informative parameters of the dangerous signal. The use of an oscillating frequency protection signal in the range from 5% to 20% of the dangerous signal frequency increases the efficiency of destruction of the information contained in the dangerous signal.

The formation of a set of security signals on the objects of information activities, aimed at destroying the informative parameters of dangerous signals of high-frequency imposition, not only on the fundamental frequency, but also on the combinational harmonics of the probing signal, provides effective protection of confidential information from interception.

References

1. Kriuchkova L.P., Provozin O.P. Interception of speech information by methods of high-frequency "imposition". Modern information protection. 2017. №3(31). P. 74–80.

2. Katorin, Y. F., Razumovsky, A. V., Spivak, A. I. (2012). Zashchita informatsii tehnicheskimi sredstvami. Spb: NIU ITMO, 416.

3. U.V. Lykov, A.D. Morozova, V.D. Kukush, A.S. Parfenov. RESEARCH OF THE HF-IMPOSITIONS METHOD FOR UNAUTHORIZED REMOVAL OF INFORMATION FROM TELEPHONE LINES. Scientific Journal «ScienceRise» №7/2(12)2015. P. 51-57.

4. Vorona V.A., Kostenko V.O. Methods and means of information protection against leakage through technical channels. Computational nanotechnology. 2016. № 3. P. 208–223.

5.Ustroistva, realizuiushchie metody vysokochastotnogo naviazyvaniia. Available at: http://allrefs.net/c9/3gg62/p5/?full.

6. Kriuchkova L.P., Tsmokanych I.V. (2021) Overview of Methods of Protection of Acoustic Information Against Leaks by Channels Formed by High-Frequency Impositions. International Journal of Innovative Technologies in Social Science. 3(31). doi: 10.31435/rsglobal_ijitss/30092021/7685.

7. S.I. Lyzunov, K.I. Rozumovskyi. APPLICATION OF SCREEN STRUCTURES TO PROTECT INFORMATION // Collection of abstracts of the annual scientific-practical conference among students, teachers, scientists, young scientists and graduate students "Science Week - 2019. Faculty of Radio Electronics and Telecommunications", Zaporizhzhia, 15-19 April 2019, Zaporizhia National Technical University. – Z.: ZNTU, 2019. P. 112-115.

8. Nurzhigit Smailov, Askhat Batyrgaliyev. Assessment of exposure to high-frequency imposition noise generators // The 17th INTERNATIONAL SCIENTIFIC CONFERENCE INFORMATION TECHNOLOGIES AND MANAGEMENT 2019, April 25-26, 2019, ISMA, Riga, Latvia. P. 58-59.

9. V.A. Kondratyonok, O.V. Churco, A.M. 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. P. 12-16.

10. V.A. Rokshyn, G.G. Vardazaryan, I.V. Kalyberda. DEVELOPMENT OF A METHOD FOR PROTECTING VOICE INFORMATION AGAINST LEAKAGE THROUGH AN ACOUSTOELECTRIC CHANNEL THROUGH TWO-WIRE SIGNALING LOOPS. Collection of scientific papers of the VII annual scientific-practical conference of teachers, students and young scientists "YOUNG SCIENCE - 2019", Pyatigorsk, 2019. P. 197-200.

11. Patent 95365 Ukraine, IPC (2011.01) H04K 3/00. Method of information protection / Rybaljsjkyj O.V., Khoroshko V.O., Krjuchkova L.P., Dzhuzha O.M., Orlov Ju.Ju.; applicant and patent owner National Academy of Internal Affairs. - № a200913327; declared 22.12.2009; 55 publ. 25.07.2011, Bull. № 14.

12. Lenkov S.V., Rybaljsjkyj O.V., Khoroshko V.A., Krjuchkova L.P. (2009), «Principles of blocking information retrieval by HF-imposition methods». Bulletin of Taras Shevchenko National University of Kyiv. Military special sciences, 22. P. 36-39.

13. Rybaljsjkyj O.V., Khoroshko V.A., Krjuchkova L.P. Experimental studies of a new method of protection against RF imposition // Bulletin of Volodymyr dahl east ukrainian national university №6 (136). Part 1, 2009. P. 94–96.

14. Kriuchkova L.P., Tsmokanych I.V. An improved method of protecting information from leakage through high-frequency imposition channels // Collection of abstracts XIII International scientific-practical conference "Computer systems and network technologies" (CSNT-2021), Kyiv, 15–17 April 2021 p., National Aviation University. – K.: NAU, 2021. P. 62–63.

15. Sherstyukov S.A. The method of forming radio signals with angular modulation simultaneously on several harmonics of the carrier frequency oscillation. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2012. №2. P. 35–46.

16. Kriuchkova L.P., Vovk M.O. 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); Kyiv, 15-16 April 2021 року; Taras Shevchenko National University of Kyiv. – K.: PPC " Kyiv University" 2021. P. 48–49.

Larysa Kriuchkova **Лариса Крючкова**	D. Sc. (Engineering), Associate Professor, Professor of the Department of Information and Cyber Security Systems, State University of Telecommunications (7, Solomenskaya Str., Kyiv, 03110, Ukraine). E-mail: alara54@ukr.net http://orcid.org/0000-0002-8509-6659	доктор технічних наук, доцент, професор кафедри систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій, м. Київ, Україна
Ivan Tsmokanych **Іван Цмоканич**	Master's of Cybersecurity, PhD student of the Department of Information and Cyber Security Systems, State University of Telecommunications (7, Solomenskaya Str., Kyiv, 03110, Ukraine). E-mail: ivakobor@ukr.net https://orcid.org/0000-0002-5085-8457	аспірант кафедри систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій, м. Київ, Україна
Maksym Vovk **Максим Вовк**	Master's of Cybersecurity, PhD student of the Department of Information and Cyber Security Systems, State University of Telecommunications (7, Solomyanska Str., Kyiv, 03110, Ukraine). E-mail: leny_mowe@ukr.net. https://orcid.org/0000-0003-1781-6762	аспірант кафедри систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій, м. Київ, Україна