UDC 355.404.7
DOI: 10.15587/2706-5448.2023.286193

Yevhen Pavlenko

DETERMINATION OF SIGNAL LEVEL FOR PROTECTION OF INFORMATION IN CASE OF ITS INTERCEPTION BY TECHNICAL MEANS OF INTELLIGENCE

The object of the current paper is the protection of information in the conditions of its interception by technical means of intelligence. According to this goal, considered the existing mathematical model of signal interception using radio-technical intelligence. In course of investigation, for getting final results based existing mathematical model analyzed the optimal scheme of signal detection with the help of intelligence receiver. As a result of this activity occurs four potential cases of signal detection which compared with established threshold H and accompanied by one of two error types: incorrect decision about the signal absence or incorrect indication of its presence. On the basis of the given cases suggested one of the possible variant for protecting of signal that goes beyond the controlled zone.

Using such dependencies as: an expression of the power flux density of radio electronic device antenna on its distance to the receiver in the direction of maximum radiation, the formula of signal power at the input of the receiving antenna, the ratio of the antennas coefficient of amplification and its effective scattering area was obtained: the dependence for calculating the power of output signal sufficient for reception within the controlled zone, but insufficient for its interception by technical means beyond its borders. Also, obtained graphical dependencies of minimal coefficient of amplification of transmitter antenna from maximal coefficient of amplification of transmitter antenna, from wavelength of radiation and from distance between transmitter and receiver.

Based on research results formed the conclusion regarding proposed method of information protection based on the mathematical model of the information leakage channel applying for radio intelligence.

Keywords: *telecommunication, radio engineering, technical protection of information, signal reduction, signal interception, radio intelligence.*

Received date: 01.07.2023
Accepted date: 21.08.2023
Published date: 24.08.2023

How to cite
Pavlenko, Y. (2023). Determination of signal level for protection of information in case of its interception by technical means of intelligence. Technology Audit and Production Reserves, 4 (1 (72)), 25–28. doi: https://doi.org/10.15587/2706-5448.2023.286193

1. Introduction

One of the most important stages of building technical protection of the informational system is detection possible channels of leakage of confidential information. Modulation such technical channels allow to identify and regulate possible risks and issues, as well as to propose ways of preventing and counteracting such dangers. The reasonable necessity of this research lies in expansion and improvement of existing ways and methods of protection the information in tasks of countering means of technical intelligence.

In the context of current topic considered modern methods of protecting the information from leaks via technical channels, as well as methods of reducing the probability of its interception by technical means. Thus, in paper [1] proposed wire-tap channel concept information protection which is transmitted using radio phone against eavesdropping outside of controlled zones. Use of this approach reduces significantly the sizes of the territory to be secure against possible eavesdropping. In this case the users of indoor radio telephones do not need in encryption/decryption of messages, in article [2] on bases of eavesdropping when some applications call the mobile phone's microphone module and gather the user's voice and transmit information illegally proposed scheme, using the access authority of mobile phone's microphone, network access, user trust and etc. Current scheme compared with some of the existing protection software, when the invisible eavesdropping happened. In work [3] the noise in anti-eavesdropping system based on acoustic masking is analyzed and the loudness and sharpness which affect the subjective hearing comfort are quantitatively calculated. Experiments show that the proposed method and system can effectively mitigate the redundancy and annoying noise in the speech-protected area. It can significantly reduce the loudness and sharpness of the noise in the protected area and improve the auditory comfort of the talk participant. In paper [4] two digital receivers for detection and modulation classification of non-stationary signals, including signals with low probability of interception are analyzed. They can be used to identify and monitor signals for both civilian and military applications. Work [5] considered new basis for representation a low probability of interception (LPI) signal under digital electronic supported measures (ESM) of their detection, established analog-to-

ISSN 2664-9969

digital conversation (ADC) noise model and adaptation of ADC and Fourier processors and its criteria, presented way of detection of the LPI signal with unknown parameters presented, discussed comparative analysis of obtained graphic probability of detection vs signal-to-noise ratio at different fault probabilities families for optimal and presented methods. Paper [6] combined Strong Signal Masking (anti-interception technology) with Orthogonal Frequency Division Multiplexing (method of data transmission) and anti-intercepting transmission scheme in physical layer is taken as the research direction. In article [7] proposes lawful interception scheme for secure VoIP (Voice over IP) communications using TTP (Trusted Third Party). This scheme enables to do lawful interception and restrict the ability of law enforcement agency because the session key only validates during one session. Aim of work [8] is to ensure high reliability, noise immunity and the degree of information protection against interception in IIoT (Industrial Internet of Things) critical in speed, reliability and safety under the influence of natural and deliberate electromagnetic interference.

Thus, *the aim of this research* is to provide the protection of information in conditions of its interception using technical means by determination level of output signal.

2. Materials and Methods

The mathematical model used in study [9, 10] includes three main blocks:

1) block for calculating signal/noise ratio at the input of intercept receiver during intelligence of radio-electronic device under specified conditions;

2) block of describing the process of conversion of received input signal by elements of radio receiver;

3) block for calculating of information indicator that characterizes the effectiveness of radio receiver in the process of intelligence.

Let's briefly illustrate the main content of used model.

Presented optimal scheme of detecting deterministic signal and unknown parameter λ can take only one of two values λ=1 (in received oscillation signal is present); λ=0 (in received oscillation signal is absent).

Let the accepted fluctuation $\xi(t)$ represent the sum:

$$\xi(t)=\lambda s(t)+n(t),\ 0\le t\le T,$$

where $n(t)$ – white noise; $s(t)$ – useful signal of known shape (deterministic signal), which is completely located in the observation interval.

As for the a priori information of the parameter λ, let's assume that the a priori probabilities of the presence and absence of the signal $W_{pr}(1)$, $W_{pr}(0)$ are known.

With continuous processing of the accepted implementation, the posterior probability of presence of deterministic signal (λ=1) determined by formula:

$$W_{ps}(1)=kW_{pr}(1)\exp\left\{-\frac{1}{N_0}\int_0^T\left[\xi(t)-s(t)\right]^2dt\right\}.$$

The posterior probability of no signal (λ=0), obviously equal to:

$$W_{ps}(0)=kW_{pr}(0)\exp\left\{-\frac{1}{N_0}\int_0^T\xi^2(t)dt\right\},$$

moreover:

$$W_{pr}(0)+W_{pr}(1)=1.$$

Also, below presented four implementations of random oscillation: first two represent the noise at the output of the matched filter q_n, and other two represent the sum of signal and noise $q=q(1)$. Let's set some threshold H. For the specific implementations shown in Fig. 1 it can be observed that the noise in first implementation does not exceed the threshold. In second implementation, there is no signal, but noise value exceeds the threshold. In the third implementation, the sum of the signal and noise exceeds the threshold, and in fourth implementation despite the signal presence threshold is not reached.

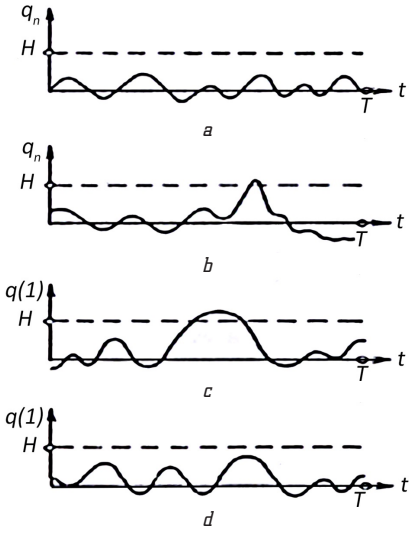

Fig. 1. Four possible cases when signal is detected against background noise [9]: *a, c* – correct decision; *b, d* – wrong decision

From the considered four cases, in two of them (Fig. 1, *a, c*) made correct decision, in other two (Fig. 1, *b, d*) – the wrong one. If to take another threshold H, described situation may change.

Thus, it can be concluded that the signal presence or absence accompanied by errors of two types:

1) despite the signal absence, noise exceeds the threshold as a result making wrong decision about the signal presence (first type error);

2) although the signal is present, but the limit level is not exceeded, so that making an erroneous decision about signal absence (second type error).

Fig. 2 demonstrates the optimal scheme of detecting deterministic signal against a background noise.

If threshold level exceeded, making decision about the signal presence. If threshold is not exceeded, established the signal absence.

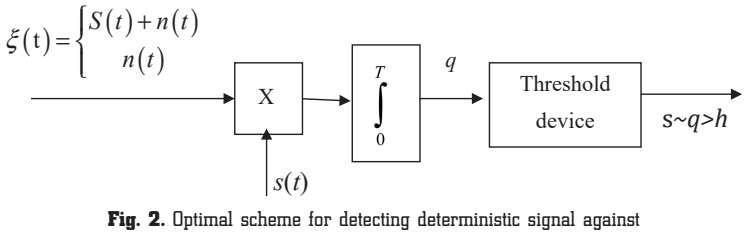

Fig. 2. Optimal scheme for detecting deterministic signal against background noise

3. Results and Discussions

Let's consider one of the possible ways to protect the output signal. With known distance from transmitter to receiver and maximal coefficient of amplification of receiver antenna, it is possible to calculate the magnitude of the signal which is sufficient for reception within the controlled zone, but insufficient for its interception by means of technical intelligence outside the controlled zone.

Suppose the source of radiation is an antenna of radio electronic device, which characterized by coefficient of amplification G_t, then the power flux density on distance D in the direction of maximum radiation calculated by expression:

$$PFD = \frac{P_\Sigma G_t}{4\pi D^2}, \quad (1)$$

where PFD – power flux density at the receiving antenna, W/m^2; P_Σ – power of radiation source, W; G_t – coefficient of directional action of antenna of radio-electronic device; $4\pi D^2$ – area of a sphere of radius D, approximating the front of an electromagnetic wave; D – distance from radio electronic device to the receiver, m. With known effective area of the receiving antenna S, the power of signal at the input of the receiving antenna is equal to:

$$P_{sr} = S \cdot PFD. \quad (2)$$

The coefficient of amplification of antenna G_r and its effective scattering area S connected by ratio:

$$S = \frac{\lambda^2 G_r}{4\pi}, \quad (3)$$

where λ – wavelength of radiation, meters.

Taking into account formulas (1), (2) can be written as:

$$P_{sr} = \frac{P_\Sigma \lambda^2 G_r G_t}{16\pi^2 D^2 K_s}, \quad (4)$$

where K_s – antenna sidelobe ratio.

Therefore, with known values of D (distance from receiver to transmitter) and $G_{r\,max}$ (maximal coefficient of amplification of receiver antenna), it is possible to calculate the minimum value of transmitted signal by regulating corresponding coefficient $G_{t\,min}$:

$$G_{t\,\min} = \frac{P_{sr} 16\pi^2 D^2 K_s}{G_{r\,\max} P_\Sigma \lambda^2}. \quad (5)$$

This dependence can be described in Fig. 3–5.

Thus, if means of technical intelligence located outside the controlled zone, then the value of the transmitter signal will not reach the threshold level H of technical intelligence means (Fig. 1, *d*), which provides the protection of current output signal.

The obtained results can be applied as a one of the possible ways of protection the output signal which spreads beyond the control area in cases of its interception by means of technical intelligence.

The limitation of using such method is a constant consideration and calculation of the distance between receiver and transmitter of the output signal and corresponding maximal coefficient of amplification of receiver antenna.

The conditions of martial law in Ukraine affected timelines of the research and increased the terms of its conduction.

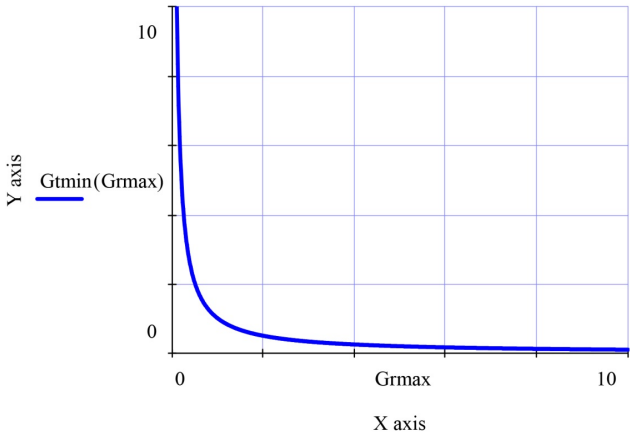

Fig. 3. Dependence of minimum coefficient of amplification of transmitter antenna from $G_{r\,\max}$

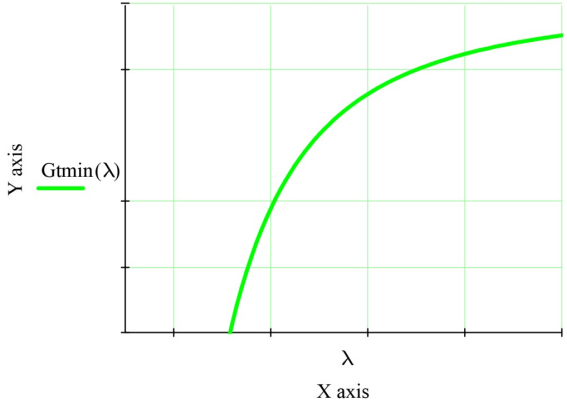

Fig. 4. Dependence of minimum coefficient of amplification of transmitter antenna from λ

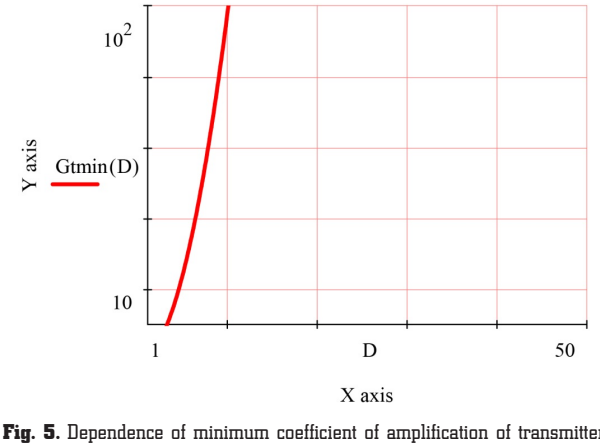

Fig. 5. Dependence of minimum coefficient of amplification of transmitter antenna from D

Further research should be directed to investigation the possible ways of automatic determination desired level of signal in cases of its protection against interception by technical means of intelligence.

4. Conclusions

In course of current investigation, the existing mathematical model of the information leakage channel in the

ISSN 2664-9969

conditions of radio intelligence is analyzed. The optimal scheme of deterministic signal detection is considered (Fig. 2) and four possible scenarios of signal detection against background noise (Fig. 1). Based on last one (Fig. 1, *d*) presented potential variant of protecting the output signal. According to which, when with known distance from transmitter to receiver and maximal coefficient of amplification of the receiver antenna presented dependence for calculating the value of signal which is sufficient for reception within the controlled zone, but insufficient for its interception by technical means outside the controlled zone. Thus, if the means of technical intelligence will be outside the controlled zone, then the value of the transmitter signal will not reach the threshold level *H* of technical intelligence means, which will provide the protection of the output signal.

Conflict of interest

The author declares that he has no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The research was performed without financial support.

Data availability

The manuscript has no associated data.

References

1. Korjik, V., Yakovlev, V., Babkov, I. (1997). The wire-tap channel concept against eavesdropping of indoor radio telephone. *Proceedings of 8th International Symposium on Personal, Indoor and Mobile Radio Communications – PIMRC'97*. Helsinki, 2, 477–479. doi: https://doi.org/10.1109/pimrc.1997.631047
2. Zhao, J., Han, Z., Zhang, H., Liu, R. (2014). The design and implementation of invisible eavesdropping protection application. *2014 12th International Conference on Signal Processing (ICSP)*. Hangzhou, 2394–2397. doi: https://doi.org/10.1109/icosp.2014.7015423
3. Jiang, J., Li, Y., Ma, X., Zhang, P., Fan, Y., Hao, Q. (2017). Research on noise quality in anti-eavesdropping system based on acoustic masking. *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. Chennai, 823–827. doi: https://doi.org/10.1109/wispnet.2017.8299876
4. Lopez-Risueno, G., Grajal, J., Yeste-Jeda, O. A., Sanz-Osorio, A., Moreno, J. A. (2003). Two digital receivers based on time-frequency analysis for signal interception. *2003 Proceedings of the International Conference on Radar (IEEE Cat. No.03EX695)*. Adelaide, 394–399. doi: https://doi.org/10.1109/radar.2003.1278774
5. Yavorskyy, B. (2004). Detection of low probability of interception signals in bases of almost periodical functions. *Proceedings of the International Conference Modern Problems of Radio Engineering, Telecommunications and Computer Science*. Lviv-Slavsko, 487–490.
6. Xu, X., Jing, T. (2019). Design of Strong Signal Masking Covert Communication Transmission Scheme Based on OFDM System. *2019 IEEE 19th International Conference on Communication Technology (ICCT)*. Xi'an, 169–173. doi: https://doi.org/10.1109/icct46805.2019.8947096
7. Yoon, S., Jeong, J., Jeong, H., Won, Y. (2008). Lawful Interception Scheme for Secure VoIP Communications Using TTP. *International Symposium on Computer Science and its Applications*. Hobart: TAS, 149–152. doi: https://doi.org/10.1109/CSA.2008.31
8. Serkov, A., Tkachenko, V., Kharchenko, V., Pevnev, V., Trubchaninova, K. (2020). A Method to Enhance the Bandwidth and Noise Immunity of IIoT When Exposed to Natural and Intentional Electromagnetic Interference. *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkiv, 527–532. doi: https://doi.org/10.1109/picst51311.2020.9467929
9. Siahaeva, O. O. (2012). *Doslidzhennia ta rozrobka matematychnoi modeli dzherela nebezpechnoho syhnalu vtraty informatsii v bankivskykh systemakh*. Kharkiv, 24.
10. Stepanov, M., Boiko, J., Pavlenko, Y. (2023). Determining the required signal level and masking noise to protect information in the conditions of its interception by technical means. *Measuring and computing devices in technological processes, 2*, 21–27. doi: https://doi.org/10.31891/2219-9365-2023-74-3

Yevhen Pavlenko, *Postgraduate Student, Department of Applied Radioelectronics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-0451-3861, e-mail: sl1mvsshady@gmail.com*