Method of Detecting Dangerous Signals of a Given Frequency Range*

Oleksandr Laptiev [1,†], Yuriy Shcheblanin[1,†], Tetiana Laptieva[2,*,†] , Ivan Parkhomenko [1,†]

Sergey Laptiev[1†]

[1] *Taras Shevchenko National University of Kyiv, Volodymyrska Str., 60, Kyiv, 01033, Ukraine*

[2] *State University of Trade and Economics / Kyiv National University of Trade and Economics, Kyoto Str., 19, Kyiv, 02156, Ukraine*

Abstract

The article presents a novel method for detecting dangerous radio signals within a specified frequency range, leveraging Bayesian hypothesis testing. With the increasing sophistication of covert technical means, such as radio beacons and hidden transmitters, traditional detection techniques based on spectral analysis or power measurement are often insufficient. These modern devices employ low-power transmission, frequency agility, and signal masking to avoid detection. To address this challenge, the authors propose a statistically robust approach rooted in Bayesian inference, which allows for the integration of prior knowledge about signal characteristics and noise behavior. The methodology formalizes the detection task as a binary hypothesis test: the presence (H_1) or absence (H_0) of a dangerous signal in the observed data. By applying Bayes' theorem, the model updates prior probabilities with empirical observations, enabling more accurate and adaptive decision-making under uncertainty. The study derives key performance metrics, including false alarm probability, signal detection probability, and overall error probability, demonstrating how these indicators improve with the incorporation of additional signal features. Simulation results show that increasing the number of detection parameters from four to seven raises the success rate of identifying dangerous transmissions from 80% to 95%, confirming the effectiveness of the proposed method. This Bayesian framework enhances the reliability and precision of radio monitoring systems, particularly in complex electromagnetic environments where classical methods fail. The research contributes to the field of information security by offering a principled and flexible solution for countering technical espionage and preventing unauthorized data leakage via radio channels. The proposed method can be implemented in practical operations of technical protection services, significantly improving the efficiency of signal detection and strengthening the overall security posture of critical information infrastructure.

Keywords

Wireless networks, information protection, radio channel, information flow, radio bookmarks, random radio signals, cyberspace.

1. Introduction

Information has become one of the most valuable economic assets that influence the competitiveness of enterprises, government institutions, and other entities in modern society. The acquisition of confidential information without direct physical access has evolved into a new form of technological activity known as "technical espionage." Among the most common methods for acquiring sensitive data is the use of specialized technical means designed to covertly obtain and transmit data via radio channels. These devices are often referred to as radio beacons, radio bugs, or covert listening devices.

Radio beacons can vary significantly in their design: from simple analog transmitters to complex digital systems equipped with data storage modules, remote control capabilities, encryption, and environmental adaptability. The primary goal of such devices is to ensure maximum concealment of

Proceedings of the Workshop on Scientific and Practical Issues of Cybersecurity and Information Technology at the V international scientific and practical conference Information security and information technology (ISecIT 2025), June 09–11, 2025, Lutsk, Ukraine

* Corresponding author. Oleksandr Laptiev

† These authors contributed equally.

olaptev@knu.ua (O. Laptiev); yurii.shcheblanin@knu.ua (Y. Shcheblanin); tetiana1986@ukr.net (T. Laptieva); ivan.parkhomenko@knu.ua(I. Parkhomenko); salaptiev@gmail.com (S. Laptiev)

0000-0002-4194-402X (O. Laptiev); 0000-0002-3231-6750 (Y. Shcheblanin); 0000-0002-5223-9078 (T. Laptieva); 0000-0001-6889-9284 (I. Parkhomenko)); 0000-0002-7291-1829 (S. Laptiev)

their operation. This is achieved through the use of low-power transmitters, careful selection of operating frequencies, limited transmission duration (activation only when necessary), and the application of signal masking techniques.

As a result, the challenge of detecting such devices becomes increasingly relevant, especially at facilities where critical or classified information is stored or processed. Traditional detection methods based on spectral analysis, power measurement, or visual inspection have limited effectiveness when modern concealment technologies are employed. Therefore, researchers are increasingly turning to statistical approaches—particularly hypothesis testing—as a foundation for building automated radio monitoring analysis systems.

Hypothesis testing is one of the fundamental statistical tools used to verify assumptions about the parameters of random processes. In general, it involves comparing two mutually exclusive hypotheses: the null hypothesis (H_0) and the alternative hypothesis (H_1). The null hypothesis assumes no significant changes or relationships in the process under study, while the alternative suggests their presence. Based on collected data, a statistical analysis is performed to determine whether the null hypothesis should be accepted or rejected.

In the context of radio monitoring, this method can be applied to detect anomalies in the spectrum that may indicate the presence of illegal transmissions. For instance, if the background noise level in a certain frequency band significantly exceeds the expected level, it may suggest the presence of a hidden transmitter. Thus, hypothesis testing becomes an important tool for automating the analysis of radio environment conditions.

According to [1], the formalization of the hypothesis testing problem involves determining the probability of Type I error (rejecting a true H_0) and Type II error (accepting a false H_0). To ensure optimal decision-making, various criteria are used, such as the Neyman-Pearson criterion, the maximum likelihood criterion, or the Bayesian criterion. The latter becomes particularly relevant when prior knowledge about the signal's occurrence probability is available.

Works [2] and [3] examine the classification of hypothesis testing into single-sample and two-sample procedures. Single-sample methods are used to test hypotheses about a single distribution, whereas two-sample methods are used to compare two independent datasets. However, in most cases, these methods are discussed within the general framework of mathematical statistics, without specific adaptation to physical processes such as radio signals.

Studies [4] and [5] demonstrate the advantages of the Bayesian approach to hypothesis testing compared to classical methods. Classical algorithms, including the maximum likelihood method, do not account for prior information, which can lead to increased error rates in uncertain situations. In contrast, the Bayesian approach allows for the integration of knowledge about the signal model, its probability of occurrence, and the statistical characteristics of noise.

A key distinction of the Bayesian approach is that model parameters are treated as random variables with known or estimated prior distributions. This enables real-time adaptation of the model, which is critically important in tasks involving the detection of weak, short-term, or chaotic signals.

In works [6] and [7], two main strategies for implementing Bayesian learning from data are described. The first, known as the Search and Score method, involves searching for the optimal model structure by maximizing a quality criterion, such as the Akaike Information Criterion (AIC) or the Bayesian Information Criterion (BIC). The second strategy employs constraint-based algorithms, which infer conditional independence between variables based on statistical tests.

Although machine learning offers opportunities for data analysis automation, expert assessments and analytical models often remain more reliable under high uncertainty. This is especially true for specialized tasks such as detecting radio signals in complex electromagnetic environments.

Considering the current state of research, the limitations of existing detection methods, and the need to improve the efficiency of radio monitoring, it is scientifically justified to develop a Bayesian approach to hypothesis testing for identifying dangerous signals within a specified frequency range at information-sensitive sites.

Therefore, it is relevant to develop a Bayesian hypothesis testing method for detecting dangerous signals of a given frequency range at objects of information activity. This will enhance the effectiveness of radio monitoring systems, ensure reliable protection of information resources, and prevent the loss of confidential data..

Based on the above, the development of a method of Bayesian hypothesis testing for detecting dangerous signals of a given frequency range at the objects of information activity is relevant.

2. Main part

In various information systems, it is often necessary to solve problems related to distinguishing certain random processes. This primarily refers to the task of radio monitoring of a given frequency range, digital measurement systems and calculation of parameters of dangerous noise-like signals in technical channels of information leakage [10-13] .

The tasks of random signal recognition are related to the problems of statistics, and its solution is based on the application of the theory of statistical hypothesis testing using appropriate measures (dimensions).

To consider this issue, we will present the basic information that allows us to solve the problem of observing random signals in discrete time.

Let the result of radio monitoring (observation) receive a vector x, which is the value of a vector random variable X, which takes values from the radio monitoring frequency range (observation space) Ωx.

We take into account that random signals of the radio monitoring range can be an additive mixture, a multiplicative mixture or a combined mixture.

That is, one of a given set of fully known signals, which are given by the expression

$$S_i = [S_i, S2i, \dots S_{ni}]^T, i \in [0, m-1], \quad (1)$$

and noise (interference) with a given probability distribution density.

Then the task of detecting a dangerous signal is a special case of recognition when m = 2 and one of the signals is identically zero: S0 = 0.

For example, when recognizing two signals S0 and S1 against the background of combined additive V and multiplicative U noise on observation x, hypothesis testing should be carried out

$$H_0 : X = U_S^0 + V, H_1 : X = U_S^1 + V, \quad (2)$$

where is $U = diag[U_1, U_2, \ldots, U_n]$ a random matrix of divisions of multiplicative noises;

$V = [V_1, V_2, \ldots, V_n]^T$ is a random vector of additive noise divisions.

The task of testing the hypotheses described by expression (1) can be presented in a parametric form.

Let the random variable ϑ take values from the set

Ωϑ = {0;1}. An available implementation would be a random variable described by the expression

$$\begin{aligned} X &= (1-\vartheta)(U_{S0}+V) + \vartheta(U_{S1}+V) = \\ &= (1-\vartheta)U_{S0} + \vartheta U_{S1} + V \end{aligned} \tag{3}$$

It is necessary to test the hypotheses

$$H_0 : \vartheta = 0,\ \vartheta = 1. \tag{4}$$

The given example shows that, given the task of detecting (recognizing) the probable value (dangerous signal) X depends on some random value (depends on the state of nature), the value of which ϑ must be determined in a specific experience.

Note that with this formulation, the tasks of detection and estimation of signal parameters do not fundamentally differ and are solved in the same way.

We will assume that the conditional distribution function $F_{X|\vartheta}(x \mid \theta) = P\{X < x \mid \vartheta = \theta\}$ (conditional density of the probability distribution) $W_{xv}(x \mid \theta)$ and the density of the probability distribution $W_v(\theta)$ are known at the beginning of the study.

For the given example, the action space A consists of two elements: a0 and a1, which respectively mean the acceptance of the hypothesis $H_0(\hat{\theta} = 0)\ i\ H_1(\hat{\theta} = 1)$.

The solution space D consists of all mappings d: Ωx ⟶ A of the vector of observations into available actions. Thus, the frequency space of radio monitoring is divided into two areas: $\Omega_x = \{x \mid d(x) = a_0\}$ acceptance of hypothesis H0 (commitment of action a0 and the area $\Omega_x = \{x \mid d(x) = a_1\}$ } acceptance of hypothesis H1 (commitment of action a1). The task of optimal signal detection synthesis is to perform this breakdown. Note that the regions and may be disjoint.

With this formulation of the task, each action is assigned a mutually unambiguous assessment of the state (parameter) of nature, therefore the space A and Ωθ can be equated: A = Ωθ. Each action (decision about the value of the random parameter Ωθ in a specific experience) is accompanied by losses, which are described by the loss function $L : \Omega_\theta \times A \to R^+$ R — a set of real positive numbers. The loss function maps the estimate of this parameter to each true value of the state (parameter) of nature Ωθ. Since the decision $\hat{\theta} = \hat{\Omega}$ can be accompanied by errors, in the event of an error, the person making the decision suffers losses, which are described by the loss function. It is clear that the loss function is an integral function. At the same time, the losses in the case of a correct decision should be greater than the losses in the case of a wrong decision

$$L = (\theta, \hat{\theta}) > L = (\theta, \theta) \quad \theta \neq \hat{\theta},$$
$$A = \Omega_\theta, \; d(x) = \hat{\theta} \quad . \tag{4}$$

We assign a risk to each solution d = d(x) and the state of nature

$$R(\theta, d) = \int_{\Omega x} L(\theta, d(x) W_{X|\theta}(X \mid \theta) dx =$$
$$= E\{L(\theta, d(X \mid \theta) = 0\} \quad . \tag{5}$$

To detect dangerous signals, namely to test the hypotheses of the presence of dangerous signals, we will apply the Bayes estimation method.

Bayesian hypothesis testing represents a robust statistical framework that enables researchers to assess the relative plausibility of competing hypotheses in light of observed data. Unlike classical frequentist methods, which primarily rely on p-values to reject a null hypothesis without directly quantifying the evidence in favor of alternative explanations, Bayesian hypothesis testing provides a more comprehensive and interpretable approach. It allows for the incorporation of prior knowledge or expert beliefs about the hypotheses before observing the data, making it especially valuable in domains where such information is available or critical for decision-making.

In this framework, each hypothesis is assigned a prior probability distribution that reflects existing knowledge or assumptions regarding its likelihood. Once empirical data are collected, Bayes' theorem is applied to update these prior probabilities, yielding posterior probabilities that quantify the degree of belief in each hypothesis after considering the observed data. This process not only supports hypothesis evaluation but also facilitates model comparison and uncertainty quantification in a probabilistically coherent manner.

A key feature of Bayesian hypothesis testing is its ability to compute the Bayes factor — a quantitative measure of the strength of evidence favoring one hypothesis over another. The Bayes factor is defined as the ratio of the marginal likelihoods of the data under two competing hypotheses, weighted by their respective prior probabilities. When the Bayes factor exceeds 1, it indicates that the data provide more support for the first hypothesis compared to the second; conversely, values below 1 suggest stronger support for the alternative hypothesis [14,15].

This methodological advantage makes Bayesian hypothesis testing particularly suitable for applications in fields such as signal processing, cybersecurity, and information protection, where decisions must often be made under uncertainty and with limited data. For instance, in the detection of covert radio signals or anomalies in electromagnetic environments, Bayesian techniques can improve classification accuracy by integrating prior knowledge about signal characteristics and noise behavior [16–19]. As a result, the Bayesian approach offers a flexible, principled, and highly informative alternative to traditional hypothesis testing methodologies.The Bayesian decision rule $d^* = d^*(x) \in A$ is chosen from the condition of minimum average risk

$$r(d^*) = \min_{d \in D} \int_{\Omega\theta} R(\theta, d(x) W_\theta(\theta) d(\theta) \quad . \tag{6}$$

It is possible to determine that the Bayesian decision function can be found from the condition of minimum posterior risk.

Characteristics of the detector. Under the condition A = Ωɵ = {0;1}), the main characteristics of the detector are:

a) the probability of a false alarm ɑ = P {d(X) = 1 | ɵ = 0}, which is equal to the probability of accepting the hypothesis H1 about the presence of a useful signal while there is no useful signal;

b) the possibility of passing a signal β = P{d(X) = 0 | ɵ = 1}, which is equal to the probability of accepting the hypothesis H0 about the absence of a useful signal while a useful signal is present;

c) probability of correct detection Qd = P {d(X) = 1 | ɵ = 1} = 1-β, is equal to the probability of accepting the hypothesis H1 about the presence of a useful signal while the useful signal is actually present;

d) the probability of a complete error Qd = ɑP { ɵ = 0} + βP { ɵ = 1}.

The quantity ɑ is called the level of significance of the criterion d(x), and the quantity Qd is called the power of the criterion.

Bayesian hypothesis testing, adapted for the detection of whistleblowing signals, is a powerful and flexible statistical method for detecting dangerous signals of a given frequency range, which can help information security professionals make more informed decisions and draw more accurate conclusions. In general, this method can take into account complex models with many parameters and hypotheses that may be difficult to analyze using classical methods.

3. Overview of results and sources

The basis of the decision-making method in probabilistic-statistical research is a mathematical model of the investigated process, which is characterized by its structure. A correct assessment of the structure makes it possible to make a correct decision based on such a model.

The concept of the structure of a mathematical model includes the following elements [1, 2, 20-23]:

1. dimensionality of the model (the number of equations forming the model);

2. order of the model (maximum order of the difference or differential equation included in the model);

3. nonlinearity and its type (nonlinearity with respect to variables or non-linearity with respect to parameters);

4. the time (or lag) of delay (at the entrance) and its assessment;

5. disturbance and its type (deterministic or random, type of distribution, probability distribution parameters);

6. restrictions on model variables and parameters.

Let’s consider a practical application. Conducted radio monitoring and detected, for example, 52 unknown random signals. We denote by A the event which means that a signal exceeding the amplitude threshold was detected from these signals, and by B – the event which means that a signal of unknown frequency modulation was detected. Obviously, these events are dependently related, since their intersection means that we have detected an unknown signal, i.e. A ∩ B={unknown signal}.

Thus, the probability that we detect an unknown signal of unknown frequency modulation is

$$p(A \cup B) = p(A) + p(B) - p(A \cap B) =$$
$$= \frac{13}{50} + \frac{4}{50} - \frac{1}{50} = \frac{16}{50} = 0,8$$

Thus, the probability of detecting an unknown signal from an unknown frequency-pulse modulation will be 80%.

How can we take not four signs of detection of dangerous signals, signals which may be signals of means of secretly obtaining information, but more, for example, five, then six and seven signs. That should significantly increase the probability of detecting random signals. This hypothesis was verified by simulation. We leave other conditions for the analysis unchanged. Then we get for five

$$p(A \cup B) = p(A) + p(B) - p(A \cap B) =$$
$$= \frac{13}{50} + \frac{5}{50} - \frac{1}{50} = \frac{17}{50} = 0,85$$

That is, the probability became 85%, which corresponds to theoretical statements.

If we use not five, but six signs of detection when detecting the signals of radio jamming devices, with unchanged initial conditions, we will get

$$p(A \cup B) = p(A) + p(B) - p(A \cap B) =$$
$$= \frac{13}{50} + \frac{6}{50} - \frac{1}{50} = \frac{18}{50} = 0,9$$

That is, the probability became 90%, which also corresponds to theoretical statements.

If we use not six, but seven signs of detection when detecting the signals of radio jamming devices, with unchanged initial conditions, we will get

$$p(A \cup B) = p(A) + p(B) - p(A \cap B) =$$
$$= \frac{13}{50} + \frac{7}{50} - \frac{1}{50} = \frac{19}{50} = 0,95$$

That is, the probability became 95%, which also corresponds to theoretical statements.

It should be borne in mind that there are many parameters for detecting radio signals. Therefore, probabilities must be carefully applied in mathematical calculations.

For a visual proof of the proposed method, we present a graphic representation. A graphic presentation of the results of the methodology is presented in Fig. 1.

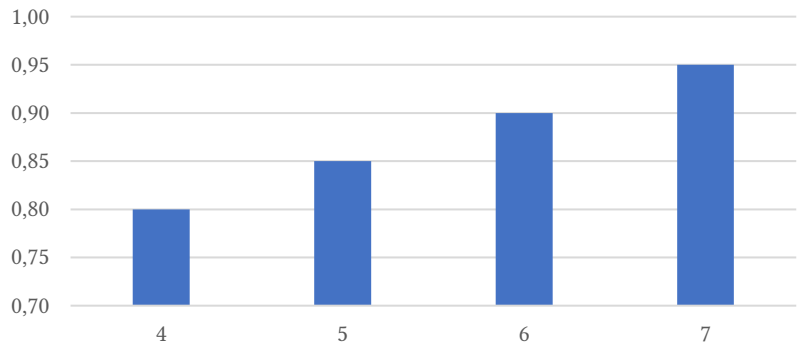

Figure 1: Graphical results of practical use of the method

Fig. 1 presents a graphical representation of the practical application of the proposed Bayesian hypothesis testing method for the detection of dangerous radio signals within a specified frequency range. The graph illustrates the relationship between the number of signal detection features (parameters) used in the analysis and the corresponding probability of successfully identifying potentially hazardous transmissions, such as those emitted by covert information-gathering devices operating on radio channels.

On the x-axis, the number of detection parameters increases incrementally from four to seven. These parameters may include characteristics such as amplitude threshold exceedance, frequency modulation type, signal duration, spectral density distribution, and temporal correlation with known interference patterns. The y-axis represents the probability of signal detection expressed as a percentage.

As shown in the figure, when only four detection features are applied, the probability of identifying a dangerous signal reaches approximately 80% . With the inclusion of a fifth feature, this probability rises to 85% , indicating improved accuracy due to additional contextual information. Further enhancement is observed when six features are utilized, resulting in a detection probability of 90% . Finally, with the integration of a seventh detection parameter, the success rate reaches 95% , demonstrating that each added characteristic significantly contributes to the overall effectiveness of the detection process.

This trend confirms the theoretical assumption that increasing the number of relevant signal features enhances the reliability and precision of the decision-making mechanism based on Bayesian hypothesis testing. It also supports the practical applicability of the method in real-world scenarios where early and accurate detection of unauthorized transmissions is critical for information security.

4. Conclusion

Based on the conducted research of hypothesis testing methods with the aim of their application for detecting dangerous signals within a specified frequency range, it has been proven that the adapted Bayesian hypothesis testing method offers significant advantages over traditional classical approaches. This method provides higher accuracy in detecting dangerous radio signals, especially under conditions of uncertainty and in the presence of complex-structured noise.

The Bayesian approach enables specialists in information security not only to formalize the decision-making process but also to consistently update their prior beliefs based on new empirical data. This results in more substantiated, reliable, and flexible conclusions, which are critically important in tasks related to the detection of covert information-gathering devices. Unlike classical methods, which rely on p-value analysis and often fail to provide a quantitative measure of the strength of evidence, Bayesian methodology allows for a quantitative assessment of hypothesis probabilities, offering richer informational support for decision-making.

Simulation results have shown that the use of additional signal parameters — increasing from four to seven — during hypothesis testing increases the probability of detecting dangerous signals from 80% to 95%. This demonstrates the effectiveness of the proposed method. Such an improvement of 15% is significant and confirms the theoretical assumptions regarding the advantages of the Bayesian approach under real-world radio monitoring conditions.

Thus, the advantages of the adapted Bayesian hypothesis testing method for detecting dangerous signals within a given frequency range unquestionably confirm the feasibility of its implementation in the practical operations of technical information protection services. The proposed approach can be successfully applied to enhance the efficiency of radio monitoring systems, ensure the integrity and confidentiality of information, and counteract technical channels of data leakage.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] O.Laptiev, V.Savchenko, A. Kotenko, V.Akhramovych, V.Samosyuk, G.Shuklin, A.Biehun. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21. https://www.ijcnis.org/index.php/ijcnis/article/view/4882

[2] Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54. https://www.ijcnis.org/index.php/ijcnis/article/view/4902

[3] Oleksandr Laptiev, Volodymyr Tkachev, Oleksii Maystrov, Oleksandr Krasikov, Pavlo Open'ko, Volodimir Khoroshko, Lubomir Parkhuts. The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS). Vol 13, No 2, August 2021 pp.271-277. ISSN: 2073-607X (Online). DOI : https://doi.org/10.54039/ijcnis.v13i2.5008

[4] Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, P. 67–70.

[5] Khudov, H., Berezhnyi, A., Yarosh, S., Oleksenko, O., Khomik, M., Yuzova, I., Zvonko, A., Yarovyi, S., Glukhov, S., & Sobora, A. (2023). Improving a method for detecting and measuring coordinates of a stealth aerial vehicle by a network of two small-sized radars. Eastern-European Journal of Enterprise Technologies, 6(9 (126), 6–13.

[6] Oleksandr Laptiev, Nataliia Lukova-Chuiko, Serhii Laptiev, Tetiana Laptieva, Vitaliy Savchenko, Serhii Yevseiev. Development of a Method for Detecting Deviations in the Nature of Traffic from the Elements of the Communication Network. International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv – Odesa, Ukraine. P.1-9 ISBN 978-966-676-818-9.

[7] Mashkov O.A., Sobchuk V.V., Barabash O.V., Dakhno N.B., Shevchenko H.V., Maisak T.V. Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. // Mathematical Modeling and Computing, 2019, Vol. 6, No 2, pp. 344 – 357. https://doi.org/10.23939/mmc2019.02.344

[8] Sobchuk, V. V., & Zelenska, I. O. (2023). Construction of asymptotics of the solution for a system of singularly perturbed equations by the method of essentially singular functions. Bulletin of Taras Shevchenko National University of Kyiv. Physics and Mathematics, (2), 184–192. https://doi.org/10.17721/1812-5409.2023/2.34

[9] Kapustian, O.A.; Kapustyan, O.V.; Ryzhov, A.; Sobchuk, V. Approximate Optimal Control for a Parabolic System with Perturbations in the Coefficients on the Half-Axis. Axioms 2022, 11, 175. https://doi.org/10.3390/ axioms11040175

[10] Sobchuk, V.; Barabash, O.; Musienko, A.; Tsyganivska, I.; Kurylko, O. Mathematical Model of Cyber Risks Management Based on the Expansion of Piecewise Continuous Analytical Approximation Functions of Cyber Attacks in the Fourier Series. Axioms 2023, (12), 924. https://doi.org/10.3390/axioms12100924

[11] Sobchuk, V., Olimpiyeva, Y., Musienko, A., Sobchuk, A. Ensuring the properties of functional stability of manufacturing processes based on the application of neural networks CEUR Workshop Proceedings, 2021, 2845, pp. 106–116. ISSN 16130073

[12] Valentyn Sobchuk, Oleg Barabash, Andriy Musienko and Olha Svynchuk (2021) Adaptive accumulation and diagnostic information systems of enterprises in energy and industry sectors. E3S Web of Conferences: 1st Conference on Traditional and Renewable Energy Sources: Perspectives and Paradigms for the 21st Century (TRESP 2021). January 22-23, 2021. Volume 250 (2021) Prague, Czech Republic. pp. 82 – 87. https://doi.org/10.1051/e3sconf/202125008002

[13] V. Savchenko, V. Zaika, M. Trembovetskyi, G. Shuklin, L. Berkman, K. Storchak, I. Rolin, "Composite Radioisotope Coating Parameters and Reflecting Characteristics Calculation Selection Method," in International Journal of Advanced Trends in Computer Science and Engineering, Vol. 8, No. 5, pp. 2246-2251, 2019. doi: 10.30534/ijatcse/2019/60852019

[14] V. Savchenko, V. Tolubko, L. Berkman, et al. "Model of an alternative navigation system for high-precision weapons," in The Journal of Defense Modeling and Simulation, 19(3), 255-262, 2022. doi: 10.1177/1548512920921955

[15] Dakhno, N., Leshchenko, O., Kravchenko, Y., Dudnik, A., Trush, O., Khankishiev, V. "Dynamic model of the spread of viruses in a computer network using differential equations". IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT` 2021 - Proceedings, 2021, pp. 111–115.

[16] Khudov H., Tahyan K., Lishchenko V., Misiuk H., Bashynskyi V., Fakadii O., Maslenko O., Herda M., Lavrut T., Nedilskyi V. (2023), The Creation of a Hidden Radar Field for the Detection of Small Aerial Objects due to the Use of Signals from Telecommunication Systems, International Journal of Applied Engineering and Technology 5(3), pp. 9-17.

[17] Bondarenko V., Kravchenko Y., Salkutsan S., Tyshchenko M. “Synthesis of the Structure of Multilevel Hierarchical Systems of Increased Survivability Based on a Subjective Probability Model”, IEEE 2nd International Conference on Advanced Trends in Information Theory, ATIT`2020 - Proceedings, pp. 138–142.

[18] Riabtsev V., Kravchenko Y., Salkutsan S., Tyshchenko M., Sharadkin D., Bondarenko V. “Information model of decision support in the design of information and communication systems based on the customer's profile”, IEEE 2nd International Conference on Advanced Trends in Information Theory, ATIT`2020 - Proceedings, pp. 234–237.

[19] Dudnik, A., Kravchenko, Y., Trush, O., Leshchenko, O., Dakhno, N., Rakytskyi, V. Study of the features of ensuring quality indicators in multiservice networks of the Wi-Fi standard. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, pp. 93–98.

[20] Kravchenko, Y., Leshchenko, O., Dakhno, N., Radko, M. Comparative evaluation of a universities websites quality. CEUR Workshop Proceedingsthis link is disabled, 2022, 3132, pp. 166–175.

[21] Yudin, O.,Mashkov, O., Kravchenko, Y., Cherniak, A., Salkutsan, S., Tyshchenko, M. “Reconfiguration of computations in multiprocessor computing system”. IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT` 2021 - Proceedings, 2021, pp. 169–173.

[22] Dakhno, N., Leshchenko, O., Kravchenko, Y., Dudnik, A., Trush, O., Khankishiev, V. “Dynamic model of the spread of viruses in a computer network using differential equations”. IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT` 2021 - Proceedings, 2021, pp. 111–115.

[23] S. Lienkov, O. Sieliukov, E. Lienkov, I. Tolok, V. Loza. Evolution of Radars Resolution Capability Using Simulation Mathematical Model. Proceedings 5th International Conference “Methods and Systems of Navigation and Motion Control”. ISBN: 978-153865870-3 – Kyiv, 2018. – P. 195 – 197.