I.J. Wireless and Microwave Technologies, **2026, 2, 1-15**
Published Online on April 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.02.01

Methodological Foundations of Calculating Cybersecurity from Specialized Determinants of Communication Networks

Volodymyr Akhramovych
Department of Cybersecurity of the State University "Kyiv Aviation Institute", Kyiv, Ukraine**.**
E-mail: 12z@ukr.net
ORCID ID https://orcid.org/0000-0002-0086-9131

Vadym Akhramovych
Computing Center of the National Academy of Statistics, Accounting and Auditing, Kyiv, Ukraine
E-mail: 12zstzi@gmail.com
ORCID ID: https://orcid.org/0009-0003-2787-8745

Alla Kobozieva
Department of Technical Cybernetics and Information Technology n.a. Prof. R.V. Merkt, Odesa National Maritime University, Odesa, Ukraine
E-mail: alla_kobozeva@ukr.net
ORCID ID: https://orcid.org/0000-0001-7888-0499

Oleksandr Laptiev *
Department of Cyber Security and Information Protection
Faculty of Information Technology, Taras Shevchenko National University of Kyiv
E-mail: olaptiev@knu.ua
ORCID ID https://orcid.org/0000-0002-4194-402X
*Corresponding Author

Received: 06 March, 2025; Revised: 31 October, 2025; Accepted: 20 January, 2026; Published: 08 April, 2026

Abstract: The article proposes a conceptually new approach to assessing cybersecurity in modern communication networks, which is based on taking into account specialized determinants — sociotechnical parameters that reflect the structural and functional complexity of network interactions. Such determinants include the centrality of nodes, the level of mutual support, the intensity of information exchange, the degree of community connectivity, user popularity, and other non-trivial characteristics that traditional protection mechanisms based on static models ignore. The central idea of the study is to formalize the dynamic stability of the cybersecurity system by building a nonlinear mathematical model that takes into account the nonlinear relationships between these determinants and the general state of network security. Methodologically, the problem is reduced to the formulation of a system of ordinary differential equations that describes the evolution of the system state under the influence of external and internal disturbances, in particular, cyberattacks. For the analytical study of stability, the method of exceptions and solution of the corresponding homogeneous characteristic equation was used, which allows for to identification the conditions of asymptotic stability. Numerical modeling was performed in the MATLAB/Multisim environment, where phase portraits were synthesized, which clearly demonstrate the stable behavior of the system even in the maximum load mode and in the presence of large-scale attacks. The obtained quantitative results confirm that the proposed model adequately reproduces the dynamics of cyber defense and provides the ability to predict the state of the system under conditions of variable network parameters. The key scientific contribution is the development of methodological principles that combine the theory of nonlinear dynamical systems, graph theory, and sociotechnical analysis to form an adaptive, predictive architecture of cyber defense, focused on complex, evolutionary communication networks.

Index Terms: Communication networks, cybersecurity, parameters, system, modeling, mathematical equations with derivatives, specialized determinants, oscillatory processes, nonlinearity, stability.

This work is open access and licensed under the Creative Commons CC BY License.

1. Introduction

Today, cybersecurity in communication networks is provided by “standard approaches”, such as the use of routers, firewalls, antivirus software, protection subnets, access methods, etc. However, these approaches do not take into account the influence of specialized determinants of communication networks, such as mutual support, user popularity, interconnectedness, mutual dependence, common beliefs, close and distant ties, node centrality, information dissemination rate, expansion of network boundaries, number of communities, etc. In addition, the assessment of stability and transformation processes is often carried out empirically or based on commonly used methods of detecting attacks and cybersecurity, which have a descriptive style and are considered separately from various mathematical and technical aspects.

Improved conceptual foundations for supporting cybersecurity in communication networks demonstrate advantages due to the modernization of the protection method, which takes into account the influence of specialized determinants of the communication network and their overall effect, as well as nonlinear relationships between them. The formulation of specialized determinants of networks and external influences eliminates the shortcomings of "standard approaches".

Thus, the developed method of cybersecurity in communication networks, in comparison with the existing ones, along with numerical indicators, takes into account the complex values of specialized determinants of the network and their effects. This contributes to the simultaneous allocation of indicators of network cyber protection, phase diagrams, dynamic processes, and their visualization through graphs, diagrams, tables, etc.

The method of assessing the impact of harmful factors on the characteristics of cybersecurity in communication networks, which has the features of using a system of mathematical equations with derivatives, taking into account the complex characteristics of the attack, is a gain of the created methodological foundations of providing cybersecurity. Determining the impact of specialized determinants of the communication network on cyber protection and the complex action of all parameters makes it possible to predict and calculate these characteristics, which is significant for the formation of new communication networks and the improvement of existing ones.

2. Literature Survey and Problem Statement

In the article [1], a linear mathematical model was developed, and a study of the model of personal data protection from a complex of specific network parameters and data transmission intensity in communication networks (CNS) was conducted. The dependences of: the volume of information flow in CNS on the components of information protection, personal data, and data flow speed; system security on the size of the system (and on the volume of personal data); threats to information security from a complex of social determinants (SD) were considered.

A system of linear equations was obtained, which consists of the equation: the rate of change of information flow from the security of CNS and coefficients reflecting the impact of security measures, the volume of personal data, the leakage rate, the change in the information protection indicator from the complex of specific network parameters, its size, and the security of personal data.

Mathematical and graphical dependencies of the frequency of natural oscillations of the system, the oscillation period and the damping coefficient are presented. However, nonlinear interactions between socio-technical determinants and the dynamics of their impact on the stability of the system were not taken into account.

Simulation modeling is carried out for values with a deviation from the stationary position of the system. As a result of simulation modeling, it is proven that the social network protection system is nonlinear.

In the article [2], statistical mechanics of topology and network dynamics are considered. After reviewing empirical evidence, the authors discuss the main models and analytical tools covering random graphs, small-world networks, and scale-free networks, the theory of evolving networks, and the interaction between topology and network resilience to failures and attacks. In [3,4,7], the conceptualization, measurement, and interpretation of centrality in affiliated networks are discussed. It is noted that at a more substantive level, centrality measures summarize a node’s participation in a network or its contribution to network cohesion. In [6], equations for various generalizations of the clustering coefficient and local efficiency for weighted undirected graphs are given. In [8,9], models of information diffusion in a social network are considered. It is noted that an individual’s opinion is largely determined by his influential neighbors. Such opinions propagate through social networks. In [10,11], models of trust and reputation of users are investigated, and these models are reviewed. Models of information influence, control and confrontation are considered. In article [12], a model of information interaction in a social network is studied. In article [13], it is noted that a graph is formed by pairwise equiprobability connections of half-edges with each other to form edges. Such models are used to adequately describe various communication networks and the Internet. The limiting distributions of the maximum degree of a vertex and the number n are obtained. In article [14], configuration graphs with randomly equally distributed degrees of vertices are considered. The degree of each vertex is equal to the number of noticeable half-edges emanating from it. The graph is constructed by pairwise equiprobability connections of half-edges with each other to form edges. Such a graph allows loops and multiple edges. Configuration graphs are widely used to model complex communication networks, including the Internet, social, transport, and telephone networks. The distribution of

degrees of vertices may be unknown. It is only assumed that it has a finite mathematical expectation and the variance is also finite, or that some rather weak restrictions on the asymptotic behavior of the distribution are satisfied. In [15], a new model of social network growth is proposed, which involves the random addition of new vertices, the preferential selection of vertices to establish connections with existing ones, and the restriction of the second end of these connections to neighbors of neighbors. This model generates a graph whose vertices are distributed by the number of connections in an exponential manner with a distribution index that varies in a wide range of values. In [16,17], an overview of the main modern directions in the theory of random graphs is given. An overview of the main modern directions in the theory of random graphs is given. The connection of random graph models with transport problems is emphasized. In studies [2–17] (including the analysis of random graphs, node centrality, information diffusion models, trust, reputation, etc.), the focus is mainly on topological or static properties of networks, without integrating these characteristics into a single nonlinear dynamic model of cybersecurity.

None of the publications has proposed a mathematical apparatus based on differential equations that describes the influence of specialized determinants (e.g., node interdependence, information propagation speed, number of communities, etc.) on the temporal evolution and stability of the cybersecurity system.

Thus, existing studies leave unresolved a key scientific problem - the lack of methodological foundations for quantitative, dynamic, and nonlinear modeling of cybersecurity, taking into account socio-technical determinants of communication networks. This is the basis of the scientific novelty of this article.

3. The Purpose and Problems of the Research

It is necessary to assess the dynamic properties of the cybersecurity system (SC) in the communication network (MC) from (SC) networks.

To simulate a nonlinear SC taking into account the influence of SC in the MC. To investigate the stability of cybersecurity in the MC.

The purpose of the study is to develop a methodology for cybersecurity data taking into account (SC) in the MC.

The closest in content is the work [1] – where the focus is on the parameters of the SC complex, and their effects on the cybersecurity of the MC. It is confirmed that the model is nonlinear. The disadvantage is that the nonlinear model of cybersecurity data in the MC has not been studied. This article is devoted to finding a solution to this situation.

The analysis will take into account the correlation between the parameters of the SC in the MC when studying and optimizing SC data.

The main objectives of the study:

- assessment of the quantitative relationship between the parameters of cybersecurity of the MS and the impact of the SD complex based on the phase portraits of the cybersecurity system.

In the following equations, elements from Table 1 will be used

Table 1. Elements used

Елемент	Element description
R	reputation of the MS participant
r	the number of MS participants with whom the MS participant can exchange data
t	the MS participant located at a certain vertex
n	the number of vertices in the MS
$\sum_{v \in V} C_{v1}$	об’єм з’єднань в МС
$C_D{}'(i)$	the central role of the node in the MS
P	the favorable influence between MS participants
N	the unfavorable influence between MS participants
V_i	a parameter indicating the impact of data security threats from the interaction between MS participants on the cybersecurity of the information system
α	parameter - indicates the tendency of the MS participant to ensure interaction
β	parameter - describes the demand for the participant
θ	the level of connectivity of the graph (score - the number of connections L)
ρ	a sign of the model's orientation to dyad symmetry
x_i	the degree of connectivity of the MS vertex at time t
Z_p	a parameter indicating the effect of measures regarding the cybersecurity of the SM
Cv	a parameter indicating the effect of measures regarding the action of the data leakage rate
C_k	a parameter indicating the effect of measures on the effect of the amount of data on its loss

Елемент	Element description
D_i	a parameter indicating the effect of measures on the effect of mutual support between MS participants on the cybersecurity of the system
C_{d2}	a parameter indicating the effect of measures on the effect of the size of the system on cyber protection
C_{d1}	a parameter indicating the effect of measures on the effect of cybersecurity on data leakage
Q	the amount of information in the MS
Z	an indicator of MS cyber protection
DR	a parameter indicating the effect of measures on the effect of cybersecurity threats caused by reputational losses in the interaction of participants on the security of the MS
$(t(r+1)\,\hat{}\,(-f))$	a parameter indicating the effect of measures on the effect of cyber threats from the spread of information between participants on the security of the MS;
$(\frac{\sum_{v\in V} C_{v1}}{n^2})$	a parameter indicating the effect of measures on the effect of the impact of cybersecurity threats, an indicator of the cluster structure of the MS on the integrity
$(P-N)(P+N)$	a parameter indicating the effect of measures on the effect of cyber threats from the mutual influence of participants on the integrity of the MS
$(\alpha+\beta+\theta+\rho)V$	parameter indicating the effect of measures regarding the action of cyber threats to data from the interaction of participants on the integrity of the MS
$(\frac{1}{n_i} + \frac{x_1}{\sum_{i=1} x_i})$	parameter indicating the effect of measures regarding cyber threats to data from the growth of the MS on integrity
$\ln(n) / ln\ln(n)$	parameter indicating the effect of measures regarding cyber threats to data from the number of transitions between users on the integrity of the MS

All elements are presented in the table in relative units.

3. Methodology

The study focuses on the dynamic nonlinear cybersecurity system in the MS, taking into account the specifics of key determinants. The main result of this manuscript is the creation of a mathematical model that includes two stages and a number of measures. According to the provisions of cybersecurity, two stages are distinguished: calculation and forecasting the impact of key determinants on the quantitative indicators of the SC in the MS, as well as determining the stability of the protection system. The main task of the first stage is to establish the impact of key determinants on the functioning of the SC in the MS. The second stage focuses on the construction and analysis of phase portraits of the cybersecurity system. The first stage involves the use of methods for establishing the impact of key determinants on the cybersecurity system in the MS, including: creation of a nonlinear system of mathematical equations with derivatives; iterative procedures1; elimination methods2; determination of a joint solution of a homogeneous equation3. method of variation of constants for finding a general solution of a non-homogeneous equation 4. In the second stage, phase portraits are determined by solving a nonlinear equation of the second degree, which is implemented by creating a module for data processing in MatLab. The description of the model includes a clear sequence of steps for its implementation and achieving practical results. Thanks to the implementation of the first stage and its components, it will be possible to determine quantitative indicators of the impact of key determinants in the MS on the cybersecurity system. Thus, it will be possible to predict these indicators and determine them in real time. Thanks to the second stage with the corresponding steps, it will be possible to obtain different types of phases of the indicator Z=f(t) associated with the impact of threats, including under conditions of their maximum values.

4. Proposed Methodology

The study of the graphical relationships of the linear system [1] indicates the nonlinear properties of the system. Therefore, we add nonlinear components (2) to the system of equations (1)

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)Q \\ \dfrac{dZ}{dt} = \dfrac{\sum\limits_{i=1}^{n} (C_D{}'(i) - C_D(i))}{(n-1)(n-2)} + D + DR + (t*(r+1)\wedge(-f)) - (\dfrac{\sum\limits_{v\in V} C_{v1}}{n^2}) + (P-N)*(P+N) + \\ ((\alpha+\beta+\theta+\rho)V) + (\dfrac{1}{n\,i} + \dfrac{x_1}{\sum\limits_{i=1}^{n} x_i}) + (\ln(n) / ln\ln(n)) - Q(C_{d2} + C_{d1}) \end{cases} \quad (1)$$

Let us establish the following notation

$$Y13 = \frac{\sum\limits_{i=1}^{n} (C_D{}'(i) - C_D(i))}{(n-1)(n-2)} + D + DR + (t*(r+1)\wedge(-f)) - (\frac{\sum\limits_{v\in V} C_{v1}}{n^2}) + (P-N)*(P+N) +$$

$$((\alpha+\beta+\theta+\rho)V) + (\frac{1}{n\,i} + \frac{x_1}{\sum\limits_{i=1}^{n} x_i}) + (\log(n) / Log(n) * \log(n))$$

We get nonlinear mathematical equations with derivatives:

$$\begin{cases} \dfrac{dQ}{dt} = Z_p Z + (C_v + C_K)Q + L_2(Q^2) + L_3(Q^3) + ... \\ \dfrac{dZ}{dt} = Y13 - Q(C_{d2} + C_{d1}) + K_2(Z^2) + K_3(Z^3) + ... \end{cases} \quad (2)$$

1. Convergence: Iterative procedures provide a gradual approximation to the exact solution, which often depends on the type of system or method.
2. The method of exceptions or the method of small deviations is used to analyze nonlinear systems when fluctuations from the initial state are small.
3. Determining the general solution of a homogeneous equation involves finding a function that satisfies the equation in the form: A(x)·f(x)=0
   where A(x) is a matrix function or operator, and f(x) is an unknown function or vector of variables.
4. The method of variation of constants is a method for finding the general solution of a non-homogeneous differential equation, which looks like this: L(y)=g(x)
   where L(y) is an operator or partial derivative, and g(x) is a function of the right-hand side of the equation.
   This method allows you to find general solutions to non-homogeneous equations, taking into account the dynamics of the change of constants depending on the variables.
5. Symbolic calculations in mathematical packages such as Mathematica, Maple or MathSad1 allow finding exact analytical solutions to differential equations.

These studies allow in practical to keep quantitative indicators of the stability of the SC and accordingly, respond to situations in real time.

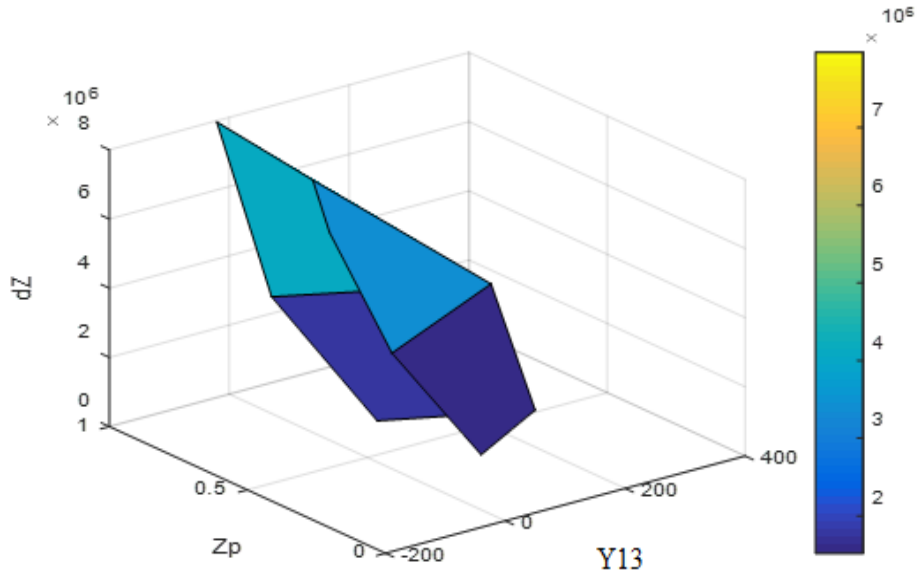


Fig.1. Differential of the cyber security function

The positive value of the differential of the cybersecurity function indicates (according to the Lyapunov theorem) the possible instability of the cybersecurity system. Additional research on this issue is required.
where: ,L1,L2 etc.K2, K3 etc. some linear operators. The system demonstrates weak nonlinearity, which facilitates finding solutions for each equation of system (2) by the method of successive approximation, assuming:

$$Q = Q_1 + Q_2 + Q_3 \cdots; \quad Z = Z_1 + Z_2 + Z_3 + \ldots \quad \text{Let at} \quad dQ = 0, \quad \frac{dQ}{dt} = 0, \text{ та } dZ = 0, \quad \frac{dZ}{dt} = 0\,0$$

$$Q = Q_0 \operatorname{Sin} \omega t, \; Z = Z_0 \operatorname{Sin} \omega t$$

We obtain a nonlinear system of mathematical equations with derivatives

$$\begin{cases} \dfrac{dQ}{dt} = Z_p Z + (C_v + C_K)Q - L_2({Q_0}^2 \operatorname{Sin}^2 \omega t) - L_3({Q_0}^3 \operatorname{Sin}^3 \omega t) - \ldots \\ \dfrac{dZ}{dt} = Y13 - Q(C_{d2} + C_{d1}) - K_2({Z_0}^2 \operatorname{Sin}^2 \omega t) - K_3({Z_0}^3 \operatorname{Sin}^3 \omega t) - \ldots \end{cases} \tag{3}$$

Let's represent the system in the following structure:

$$\begin{cases} \dfrac{dQ}{dt} = \alpha Z + \beta_1 Q - \sum\limits_{k=2}^{\infty} L_k Q_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \tag{4}$$

where $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = Y13$

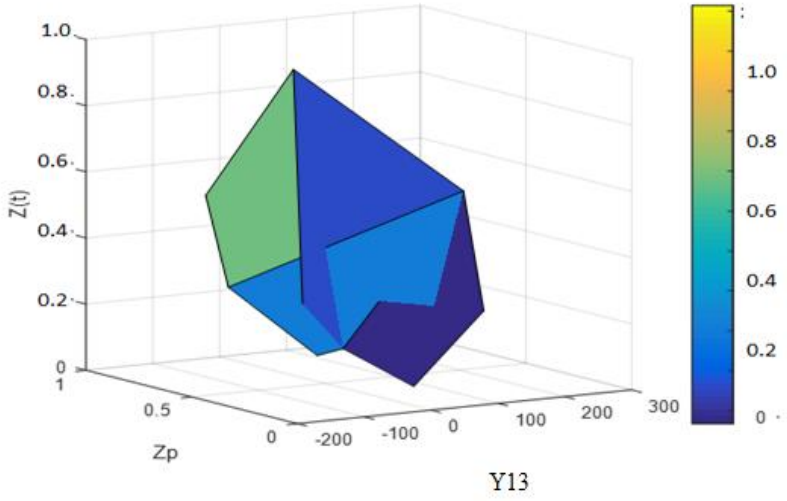


Fig. 2. Graphs of the dependence of the parameter Z(t) on the impact of threats according to expression (4)

Next, we will use the elimination method:

$$\frac{dZ}{dt} = \beta_2 Q + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \Rightarrow Q = \frac{1}{\beta_2}\left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t\right) \Rightarrow$$

$$\frac{dQ}{dt} = \frac{1}{\beta_2}\left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_k Z_0^k \sin^{k-1} \omega t \cos \omega t\right)\right) \quad (5)$$

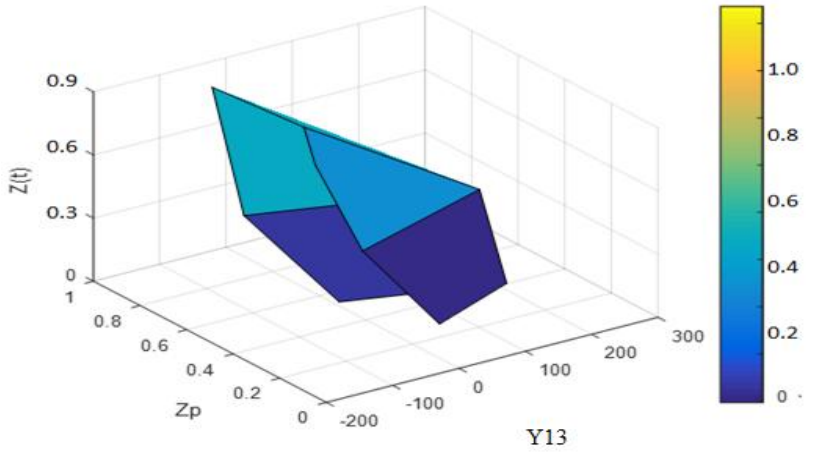


Fig. 3. Graphs of the dependence of the parameter Z(t) on the impact of threats according to expression (7)

Let us introduce expressions (5) into the first equation of the system of equations of system (4)

$$\frac{1}{\beta_2}\left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_k Z_0^k \sin^{k-1} \omega t \cos \omega t\right)\right) = \alpha Z + \frac{\beta_1}{\beta_2}\left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t\right) -$$

$$- \sum_{k=2}^{\infty} L_k Q_0^k \sin^k \omega t \quad (6)$$

or

$$\frac{d^2Z}{dt^2} - \beta_1 \frac{dZ}{dt} - \alpha\beta_2 Z = -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(kK_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t - \\ -\beta_2 \sum_{k=2}^{\infty} L_k Q_0^k \sin^k \omega t \tag{7}$$

We determine the common solution of the homogeneous equation

$$Z'' - \beta_1 Z' - \alpha\beta_2 Z = 0 \tag{8}$$

The form of the characteristic equation is as follows $\lambda^2 - \beta_1 \lambda - \alpha\beta_2 = 0$.
Let us consider the situation with a positive value of the discriminant of this equation

$$D = \beta_1^2 + 4\alpha\beta_2 > 0 \Rightarrow \lambda_{1,2} = \frac{\beta_1 \pm \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} \tag{9}$$

Where $Z_{одн}(t) = c_1 e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} + c_2 e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t}$ - the general solution to this equation.
The method of variation of constants is used to find the general solution of a non-homogeneous equation

$$Z_{одн}(t) = c_1(t) e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} + c_2(t) e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t}$$

де $c_1'(t), c_2'(t)$ знаходяться із системи:

$$\begin{cases} c_1'(t) e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} + c_2'(t) e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} = 0, \\ c_1'(t) \frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} + c_2'(t) \frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} = N(t), \end{cases} \tag{10}$$

where

$$N(t) = -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(kK_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} \left(K_k Z_0^k \sin^k \omega t \right) - \\ -\beta_2 \sum_{k=2}^{\infty} \left(L_k I_0^k \sin^k \omega t \right). \tag{11}$$

From equations (10, 11) we deduce

$$c_1'(t) e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} = -c_2'(t) e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} \Rightarrow$$

$$\Rightarrow c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\left(-\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}+\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}\right)=N(t) \quad (12)$$

або

$$c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\sqrt{\beta_1^2+4\alpha\beta_2}=-N(t) \quad (13)$$

from where we will have:

$$c_2(t)=-\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt \quad (14)$$

$$c_1(t)=\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt \quad (15)$$

Applying equations (13, 14, 15), we obtain

$$Z(t)=\int N(t)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}dt-\int N(t)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}dt \quad (16)$$

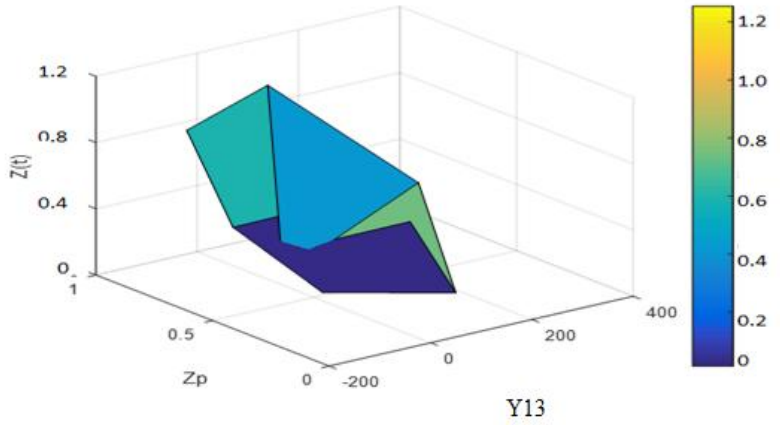


Fig. 4. Graphs of the dependence of the parameter Z(t) on the impact of threats according to expression (16)

Let's explore the phase portrait of data cybersecurity

The initial equation

$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2 Z=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1\gamma+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-$$
$$-\beta_2\sum_{k=2}^{\infty}L_kQ_0^k\sin^k\omega t \quad (17)$$

The research will be conducted in the MatLab/Multisim package. We will develop a data processing module (Fig. 8), which allows you to create a model and analyze cyber protection systems in Multisim taking into account external influences.

The results of the program are presented in Fig. 5 -7, 9-12

The closed ellipse demonstrates a phase portrait, indicating the integrity of the cyber data protection system.

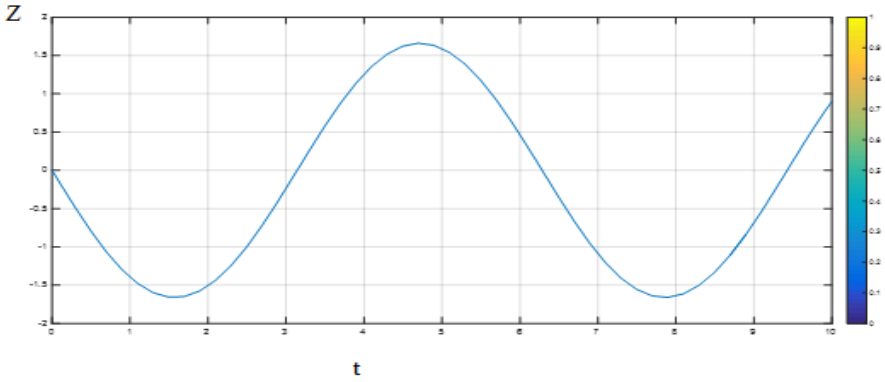


Fig. 5. Harmonic deviations in a cybersecurity system with respect to time Z=f(t)

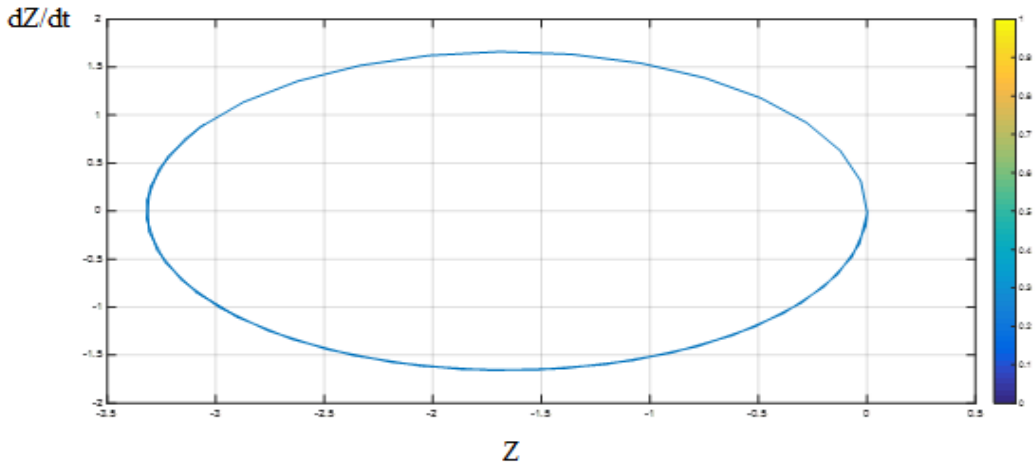


Fig. 6. Phase portrait of SC from SD

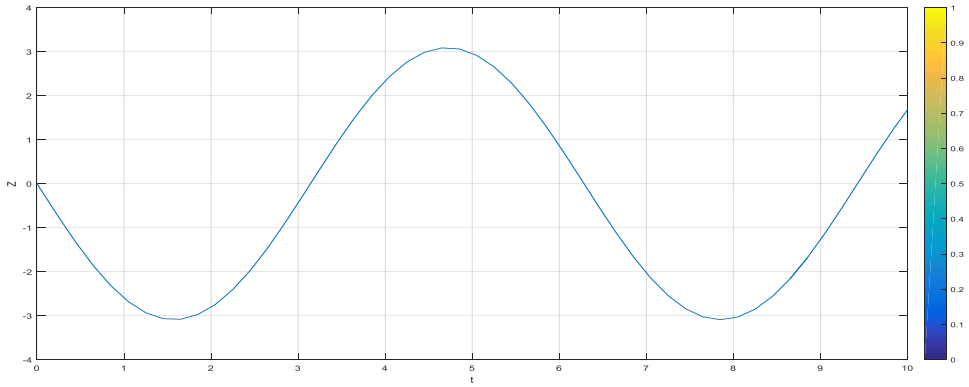


Fig. 7. Harmonic deviations in the cybersecurity system with respect to time Z=f(t)

We note a slight increase in the amplitudes of oscillations (graph z(t)) in the presence of minimal attacks by 3%

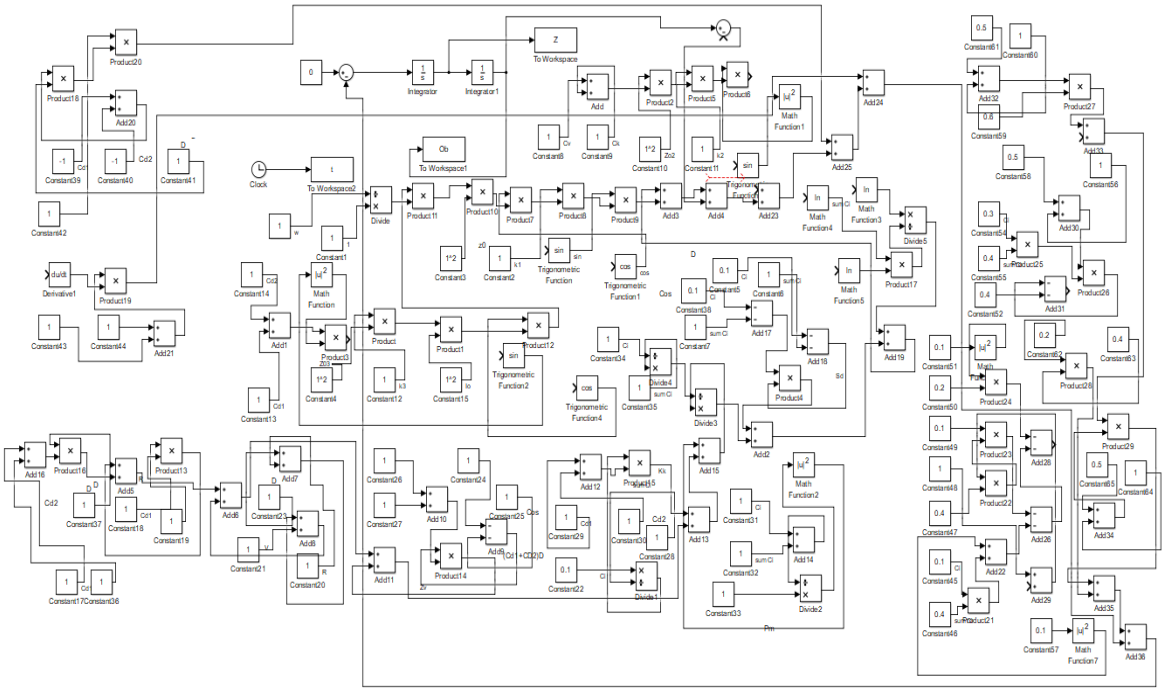


Fig. 8. Data Processing Module: Collecting Data from the System and Calculating the Phase Portrait in Multisim.

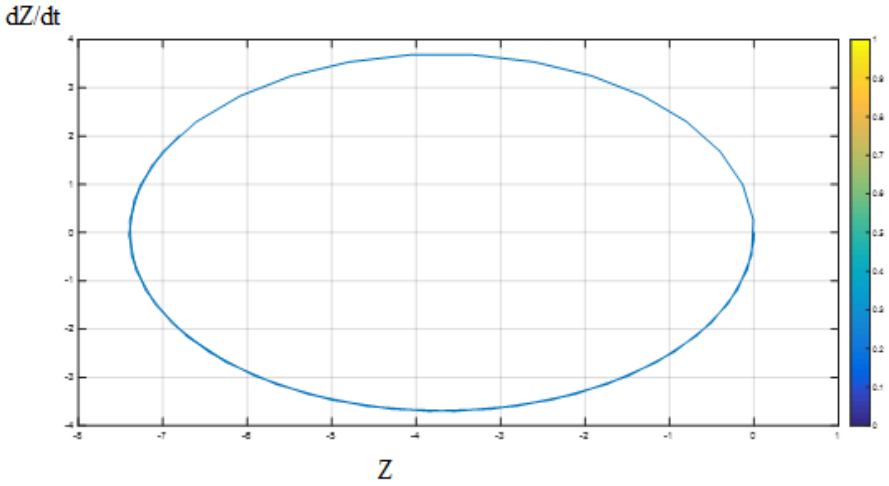


Fig. 9. Phase portrait of SC from SD

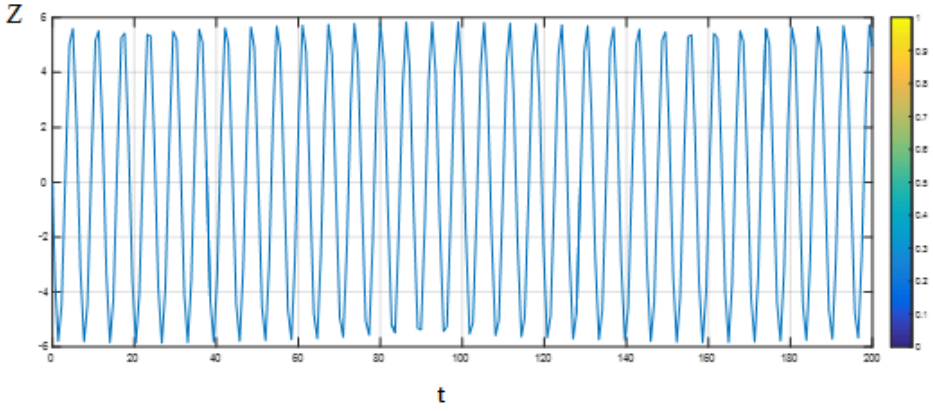


Fig. 10. Transient process in a cybersecurity system during maximum attacks with all cybersecurity parameters equal to unity

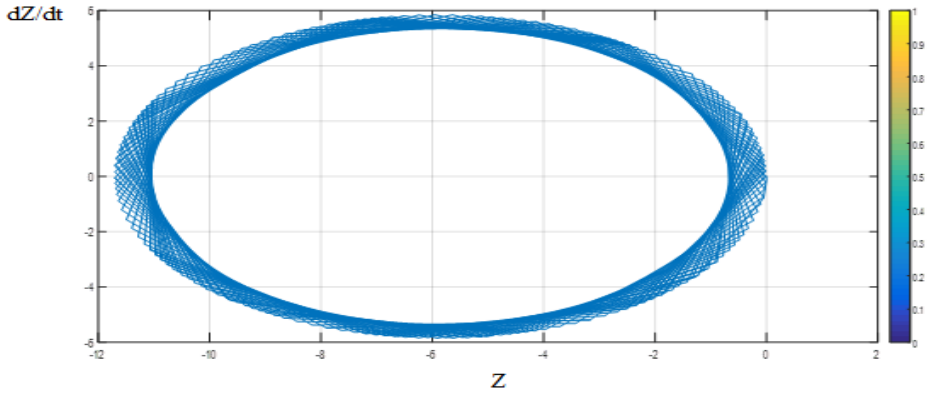


Fig. 11. Phase portrait of the SC at the maximum value of influences and the value of all cybersecurity parameters – 1

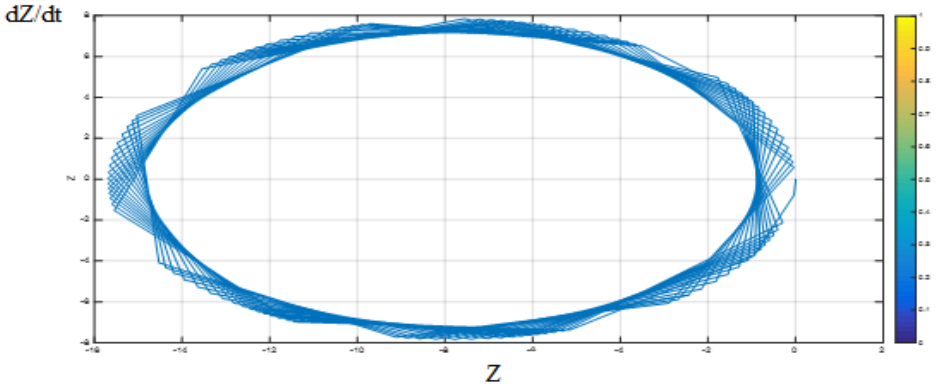


Fig. 12. Phase portrait of the SC at the attack value and the value of all cybersecurity parameters – 0.1
Conclusion: the cyber defense system remains stable during attacks

6. Exchange of views on the Consequences of the analysis of the SC in Communication Networks from the Action of the SD.

The use of probable parameters and SD in the process of analyzing the SC led to the receipt of quantitative indicators (1, 2, 4, 16) (Fig. 2-4). The symbolic basis, a substantiated plan, and a model, confirmed by simulation modeling of threats, serve as the foundation for approving the methodology. Based on the study of SC reliability (17) (Fig. 5-7, 9-10) and phase portraits (Fig. 11, 12), conclusions can be drawn about the stability and effectiveness of the protection system. The method allows for determining the numerical parameters of the SC based on the characteristics of the SD and external attacks. Today, existing methods do not allow for obtaining accurate quantitative indicators. Providing MS administrators with tools for calculating the quantitative activity of the SD and external attacks on SC parameters has economic (applied) value. This functionality will enable MS defenders to take rapid action regarding cybersecurity system parameters. Research should focus on finding new unique MS parameters to more accurately determine their impact.

7. Analysis of results and their Discussion

The use of probable parameters and SD in the process of analyzing the SC led to the receipt of quantitative indicators (1, 2, 4, 16) (Fig. 2-4). The symbolic basis, a substantiated plan, and a model, confirmed by simulation modeling of threats, serve as the foundation for approving the methodology. Based on the study of SC reliability (17) (Fig. 5-7, 9-10) and phase portraits (Fig. 11, 12), conclusions can be drawn about the stability and effectiveness of the protection system. The method allows for determining the numerical parameters of the SC based on the characteristics of the SD and external attacks. Today, existing methods do not allow for obtaining accurate quantitative indicators. Providing MS administrators with tools for calculating the quantitative activity of the SD and external attacks on SC parameters has economic (applied) value. This functionality will enable MS defenders to take rapid action regarding cybersecurity system parameters. Research should focus on finding new unique MS parameters to more accurately determine their impact.

8. Analysis of results and Discussion

A system of mathematical equations with derivatives (1-4) describing MS cybersecurity has been developed. Analyzing SC characteristics through simulation of SD influence and measures regarding data leakage speed and data loss allows for recording numerical indicators (4, 16) (Fig. 2-4). The explanation lies in the application of mathematical modeling tools, which made it possible to theoretically justify the data protection process in communication networks, considering malicious influence. The stability of the SC was analyzed by registering the influence of malicious objects in accordance with (17). Studying SC stability in communication networks under attacks and without attacks allowed for obtaining graphical dependencies of fluctuations over time (Fig. 5, 7, 10) and phase portraits of system activity (Fig. 6, 9, 11, 12). Closed curves of phase portraits without bifurcation points indicate the stability of the SC according to Lyapunov's theorem, even under the greatest influences. The obtained method and its results are evaluated in terms of numerical cybersecurity indicators, taking into account specialized determinants. Traditional analysis methods do not allow for achieving such results. The difference between previous research and the obtained results lies in the nonlinear data protection in MS. SC in MS demonstrated high resilience even against maximum external attacks and takes into account the specifics of SD in working conditions. Providing MS administrators with tools for calculating the quantitative activity of SD and external attacks on SC parameters has economic (applied) value. This functionality will allow MS defenders to take prompt action regarding cybersecurity system parameters. Research should focus on finding new unique communication network parameters to more accurately determine their impact.

9. Numerical reasoning

The SC differential (Fig. 1) has a positive value, contradicting Lyapunov's theorem. However, further analysis (Fig. 7, 9, 11, 12) proved the reliability and stability of the cybersecurity system. SC indicators vary from 0 to 1, demonstrating the significant influence of SD (Fig. 1a, 1b, 2a, 2b, 3a, 3b, 4a, 4b). An increase in attack escalation leads to an increase in the acceleration of cybersecurity system vibrations (Fig. 10, 12). Solid curves without branching spots (Fig. 11, 12) indicate the stability and reliability of the system despite the variable nature of oscillations. Research on illustrations shows the significant weight of SD parameters relative to cybersecurity system parameters.

10. Conclusions

For the first time, a study of the SC dynamic model in communication networks was conducted, considering the specifics of social determinants of networks. The model study allowed for obtaining numerical summaries of the influence of social determinants (see Fig. 2-12) and external attacks (see Fig. 10-12) on SC parameters and their interpretation. These results provide an understanding of the impact of various factors on communication network security and help in forming effective threat protection strategies. A nonlinear system of cybersecurity equations was identified. It was shown that the speed of protection changes depending on mutual influence. Phase portraits demonstrate the system's stability against external influences and social determinants in communication networks. The maximum level of social determinants' influence on the cybersecurity system is 100%. The method of forming SC phase portraits in communication networks for various threats was carried out using the data processing module in the Multisim system. It can be stated that the study of social determinants' influence on the cybersecurity system is effective. Future research should focus on finding new unique communication network parameters to more accurately determine their impact. Providing communication network administrators with tools for calculating the quantitative activity of social determinants and external attacks on SC parameters has economic (applied) value. This functionality will allow communication network defenders to take timely action regarding cybersecurity system parameters. Detecting anomalies in SC fluctuation sizes will allow for assessing the presence or absence of a threat and its degree. This will enable communication network specialists to take specific measures regarding SC parameters in real-time. Quantitative dependencies between specialized determinant parameters and external attacks, including SC criteria, were established for the first time, which is an important result of this work. The model will be useful for developing skills in the field of cybersecurity in communication networks, enhancing information security levels in communication networks, and contributing to the professional development of researchers, network administrators, and other specialists in this field. The research group is working on developing models in the field of communication networks. The advantages of the proposed model are outlined in paragraphs 1-6 of this section.

References

[1] Lukova-Chuyko N.V., Laptev O.A., Barabash O.V., Musienko A.P., Akhramovich V.M. Method for calculating personal data protection taking into account a complex of specific parameters of social networks. Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv. Kyiv: VIKNU, 2022. No. 76. P. 54 – 68.

https://doi.org/10.17721/2519-481X/2022/76-05.
[2] Albert R., Barabási A.-L. Statistical mechanics of complex networks // Review of Modern Physics, 2002. – 74. – P. 47-97.
[3] Bonacich P. F. Simultaneous group and individual centralities // Soc. Networks. 1991. V. 13. P. 155-168.
[4] Friedkin N.E. Theoretical foundations for centrality measures // Amer. J. Sociol. 1991. V. 96. P. 1478-1504.
[5] Valente T. W., Foreman R. K. Integration and radiality: measuring the extent of an individual's connectedness and reachability in a network // Soc. Networks. 1998. V. 20. P. 89-105.
[6] Wang Yu; Gumare, Eshwar; Vandenberghe, Rick; Dupont, Patrick (2017). "Comparison of various generalized clustering coefficients and local efficiency for weighted undirected graphs". Neural calculations. 29 (2): 313–331. doi: 10.1162/NECO_a_00914. Checked on August 8, 2020.
[7] Vasenin V. A., Afonyn S. A., Panyushkin D. WITH. Models of information dissemination in social networks. Software engineering.-2012.-№2 c. 33–42
[8] Horkovenko D.K. Comparative analysis of epidemic models and cellular automata when modeling the spread of information in social networks // Scientific and technical bulletins of SPbHPU. Informatics. Telecommunications. Administration. 2017. T. 10. No. 3. S. 103–113.
[9] Gubanov D. AND. Overview of online reputation/trust systems. – 2009. – M.: IPU RAS, Internet conference on management problems (www.mtas.ru/forum). - 25 p.
[10] Gubanov D.A., Novikov D.A., Chkhartishvili A.G. "Social networks: models of informational influence, control and struggle", 2010 - 228 pages.
[11] Machueva D. A., Azhmukhamedov I. M. Modeling the process of information interaction in social systems. Systems of management, communication and security No. 2, 2018, p. 18-39.
[12] Naydenov N.D., Spiryagin I.V., Novokshonova E.N. Economic and mathematical models of the cluster. Modern research of social problems (electronic scientific journal), Modern Research of Social Problems, No. 9(53), 2015. p. 415-432.
[13] Pavlov Yu. L., Cheplyukova I. AND. On the asymptotics of the power structure of configuration graphs with restrictions on the number of edges // Diskretnaya mathematica, 2018. Vol. 30. Issue 1. S. 77–94.
[14] Podlazov A.V. Zipf's law and models of competitive growth // New in synergetics. Nonlinearity in modern natural science / Ed. H.G. Malynetsky / Synergetics: from the past to the future. - M.: LIBROKOM, 2009. P.229-256.
[15] Podlazov A.V., Shchetinina D.P. A model of the growth of the social network // Preprints of the IPM named after M.V. Keldysha. 2013. No. 95. 16 p. URL: http://library.keldysh.ru/preprint.asp?id=2013-95
[16] Raigorodsky A.M. Models of random graphs and their application // Tr. MIFT 2010. Vol. 2, No. 4. P. 130–140.
[17] Trubetskov D.I. Introduction to synergy. Chaos and structure. Ed. 2nd expt. And add. – M. Editorial. URSS 2004. 240 p.
[18] D. Salnikov, D. Karaman, and V. Krylova, “Highly reconfigurable soft-cpu based peripheral modules design”, Advanced Information Systems, vol. 7, no. 2, pp. 92–97, 2023, doi: https://doi.org/10.20998/2522-9052.2023.2.13
[19] A. Podorozhniak, N. Liubchenko, V. Oliinyk, and V. Roh, “Research application of the spam filtering and spammer detection algorithms on social media and messengers ”, Advanced Information Systems, vol. 7, no. 3, pp. 60–66, 2023, doi: https://doi.org/10.20998/2522-9052.2023.3.09
[20] I. Petrovska, and H. Kuchuk, “Adaptive resource allocation method for data processing and security in cloud environment”, Advanced Information Systems, vol. 7, No. 3, pp. 67–73, 2023, doi: https://doi.org/10.20998/2522-9052.2023.3.10
[21] N. Dzheniuk, S. Yevseiev, B. Lazurenko, O. Serkov, and O. Kasilov, “A method of protecting information in cyber-physical space”, Advanced Information Systems, vol. 7, no. 4, pp. 80–85, 2023, doi: https://doi.org/10.20998/2522-9052.2023.4.11
[22] Valentyn Sobchuk, Inna Kal’chuk, Galyna Kharkevych, Oleksandr Laptiev, Yurii Kharkevych, Andriy Makarchuk. Solving the Problem of Convergence of the Results of Analog Signals Conversion in the Process of Aircraft Control. 2021 IEEE 6 th Internaional Conference. Actual Problems of Unmanned Aerial Vehicles development (APUAVD). October 19-21. 2021. Kyiv. Ukraine. P.29-33, ISBN: 978-1-6654-3821-6. IEEE Catalog Number: CFP2129V-USB.
[23] 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
[24] Serhii Yevseiev & Yuliia Khokhlachova & Serhii Ostapov & Oleksandr Laptiev et al, 2023. "Models of socio-cyber-physical systems security," Monographs, PC TECHNOLOGY CENTER, number 978-617-7319-72-5.redif, December. DOI: https://doi.org/10.15587/978-617-7319-72-5
[25] O. Laptiev, I. Parkhomenko, A. Musienko, A. Makarchuk, A. Mishchuk and D. Shapovalov, Weierstrass Method of Analogue Signal Approximation, 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek) ", Kharkiv, Ukraine, 02-06 October 2023, pp. 1-6. https://doi.org/10.1109/KhPIWeek61412.2023.10311583
[26] F. K. Mammadov, “New approach to book cipher: web pages as a cryptographic key”, Advanced Information Systems, vol. 7, no. 1, pp. 59–65, 2023, doi: https://doi.org/10.20998/2522-9052.2023.1.10
[27] S. Datsenko, and H. Kuchuk, “Biometric authentication utilizing convolutional neural networks”, Advanced Information Systems, vol. 7, no. 2, pp. 87–91, 2023, doi: https://doi.org/10.20998/2522-9052.2023.2.12

Authors' Profiles



Volodymyr Akhramovych, Doctor of Technical Science, Professor , Department of Cybersecurity of the State University "Kiev Aviation Institute", Kyiv, Ukraine.
Teaches the following disciplines:
- Methods of transmission in information security systems;
- Methods of receiving and processing signals in information security systems;
- Cyber security of banking and commercial structures;
- Theory of information resources protection with limited access;
- Licensing, certification and certification in the security field of information activity objects;
- Organization of science and research.

Over 200 scientific papers have been published, 13 of it are the USSR copyright certificates, 14 patents of Russia.
The sole author of four textbooks, co-authored with two textbooks and three workshops.
He has been working in the field of higher education for more than thirty years.



Vadym Akhramovych Head of the Computing Center of the National Academy of Statistics, Accounting and Auditing, Kyiv, Ukraine.
Teaching the following disciplines:
- Cybersecurity and Information Security
- World of Programming
- Technical Information Protection

Author of 12 scientific papers.



Alla Kobozieva Dr. Sci. (Technical),
Professor of the Department of Technical Cybernetics and Information Technology named after prof. R.V.Merkt Educational and Scientific Institute of Information Technologies and Innovative Entrepreneurship, Odesa National Maritime University
Research interests: steganography, steganalysis, digital content integrity expertise, perturbation theory, matrix analysis, numerical methods / Information about the availability of printed papers in national and international databases: monographs–8, textbooks and manuals – 1, scientific papers–178.



Oleksandr Laptiev Dr. Sci. (Technical), Senior Researcher
Associate Professor the Department of Cyber Security and Information Protection
Faculty of Information Technology, Taras Shevchenko National University of Kyiv
Research interests: protection of information resources of enterprises, blocking of information leakage channels, search and blocking of means of illegal obtaining information/ Information about the availability of printed papers in national and international databases: monographs–5, textbooks and manuals – 7, scientific papers–117.

How to cite this paper: Volodymyr Akhramovych, Vadym Akhramovych, Alla Kobozieva, Oleksandr Laptiev, "Methodological Foundations of Calculating Cybersecurity from Specialized Determinants of Communication Networks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.2, pp. 1-15, 2026. DOI:10.5815/ijwmt.2026.02.01