The methodology for researching the cybersecurity of social platforms in relation to the number of communities*

Volodymyr Akhramovych[1,*,†], Vadym Akhramovych[2,†], Anna Ilyenko[1,†], Liliia Halata[1,†], Tetiana Okhrimenko[1,3,†], Olesia Yakovenko[1,†] and Yevheniia Halych[1,†]

[1] *State University "Kyiv Aviation Institute", 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine*
[2] *National Academy of Statistics, Accounting and Auditing, 1 Pidhirna str., 04107 Kyiv, Ukraine*
[3] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3/6 Maksym Zalizniak str., 03142 Kyiv, Ukraine*

Abstract

The differential dependencies of the cybersecurity space (CS) in social platforms (SP) have been considered, taking into account the number of communities (P), and its stability has been assessed. An indicator for accounting the conditions of P has been implemented in SP. Modern approaches, technologies, and methodologies based on the principle of non-specificity have been implemented in the CS. The conditions of fixed preconditions in the time system allow for a detailed description of the changes in previous transformations, considering the elapsed time. SP is a set of clients, their methods of interaction, and C. It is asserted that there is a tendency according to which, if two individuals are close to each other in terms of views, they are most likely to take a coordinated position on any third individual, subject, or event. Based on such discoveries, researchers could build models of systematic relationships between communities adhered to by different individuals within a single group. From a mathematical perspective, an example of CS built on differential equations with variable characteristics (DEVC) has been studied, and its mathematical analysis has been performed. The results of the analysis of nonlinear models of CS in SP showed that the influence of characteristics (P) on the CS indicator can reach 100%. The portraits on the phase plane (PPP) of CS, which confirm the stability of CS even under peak levels of impactful factors, have been studied. An analysis of the developed CS structures has been conducted, and numerical dependencies between the capabilities of P and the characteristics of CS have been obtained, reflecting a high scientific level of the research.

Keywords

social platforms, models, cyber space indicator

1. Introduction

The key indicator (KI) is formed according to recommendations when the system's characteristics align with real conditions [1, 2]. In this case, emphasis is placed on the exact class of the system, and the identified interdependencies provide a complete understanding of the process of transition from the previous state to the current one [3–6]. Deviations in the value of Z are recorded using the prototype of differential equations with variable characteristics (DEVC). The relationship between the placement of system parameters and its characteristics allows for solving DEVC based on existing data. In further calculations, the parameters listed in Table 1 are used.

The previous studies are presented in [7–12]. In article [7], a mathematical model (linear differential dependency scheme) is constructed, and a privacy security model is studied based on the number of communities in social media (SM). The paper examines linear security schemes for information in social media. When describing the linear model, the object should be at least

* *CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine*
* Corresponding author.
† These authors contributed equally.
12z@ukr.net (V. Akhramovych); 12zstzi@gmail.com (V. Akhramovych); anna.ilienko@npp.kai.edu.ua (A. Ilyenko); liliia.halata@npp.kai.edu.ua (L. Halata); t.Okhrimenko@npp.kai.edu.ua (T. Okhrimenko); olesia.yakovenko@npp.kai.edu.ua (O. Yakovenko); 7405781@stud.kai.edu.ua (Y. Halych)
0000-0002-0086-9131 (V. Akhramovych); 0009-0003-2787-8745 (V. Akhramovych); 0000-0001-8565-1117 (A. Ilyenko); 0000-0002-7978-3954 (L. Halata); 0000-0001-9036-6556 (T. Okhrimenko); 0000-0003-2998-9767 (O. Yakovenko); 0009-0008-2610-1439 (Y. Halych)

approximately linear. This approach significantly simplifies the consideration of mathematical models. If linearity is not observed, the linearity of the security scheme should be studied. The research showed that the security scheme in social media is nonlinear.

Table 1
The List of Parameters Used in This Paper

Parameter	Description of the parameter:
Z	Cybersecurity indicator (KI)
S	Amount of information in the system
Z_p	Coefficient reflecting the impact of information protection measures
C_v	Coefficient reflecting the impact of the speed of personal data leakage
C_k	Coefficient reflecting the impact of the amount of personal data on its leakage
C_{d2}	Coefficient reflecting the impact of system size on cybersecurity
C_{d1}	Coefficient reflecting the impact of cybersecurity on data leakage
P	Number of communities
n	Number of nodes in social platforms (SP)
m	Number of connections in SP
L_2	Linear operators
L_3	Linear operators
K_2	Linear operators
K_3	Linear operators
α_i	Coefficient used in the division of the network into communities

In article [8], a graph model is presented, which is randomly generated with specified parameters for internal and external connections between vertices, while communities are considered to be extraordinary. A method for identifying community structures based on the maximum likelihood method is proposed, and a numerical random search algorithm is described. Graphs representing real social and communication networks change rapidly. Moreover, random graphs are an effective tool for studying these networks. An important task is to detect the structure of communities in networks.

Articles [9–11] explore the dynamic mathematical regularity Z in SP, along with characteristics such as relationships, client interaction, the number of transitions, network expansion, and their impact on the structure of Z.

In articles [12–31], there was no analysis of the quantitative interdependence between client characteristics, SP, and Z indicators, which can be considered their main disadvantage.

Justification for the research plan:

- Study of quantitative interdependencies between parameters P and characteristics Z. This involves analyzing functional or empirical dependencies to determine their correlation or consistency.
- Analysis of system stability (CS) in the context of SP using phase diagrams. This focuses on studying the impact of external or internal factors on the dynamic behavior of the system using phase analysis methods.

Providing access to operational and relevant information, as well as implementing practical measures and methods for analyzing the quantitative impact of P characteristics on Z characteristics, is an applied advantage for information security professionals within the framework of SP. The study of the amplitude of fluctuations in Z characteristics and phase diagrams allows for identifying existing threats and assessing their intensity in real time. This enables information security professionals to make informed decisions based on current Z characteristics.

2. References survey and problem statement

In article [7], a mathematical model (a scheme of linear differential dependencies) is built, and a privacy security model is studied depending on the number of communities in social media. The article considers linear security schemes for information in social media. When describing the linear model, the object must be at least approximately linear. This approach significantly simplifies the consideration of mathematical models. If linearity is not observed, the linearity of the security scheme should be investigated. The research showed that the security scheme in social media is nonlinear.

A drawback of the article is the absence of a study on the dependence of Z on P under nonlinear changes, as well as the lack of studies on the stability of the CS system.

In article [8], a model of a graph is presented, which is randomly generated with given parameters for internal and external connections between vertices, and the communities are considered extraordinary. A method for identifying the community structure based on the maximum likelihood method is proposed, and a numerical random search algorithm is described. Graphs representing real social and communication networks change rapidly. Moreover, random graphs are an effective tool for studying these networks. An important task is to detect the community structure in networks.

In articles [9–11], the dynamic mathematical regularity Z in SP is examined, along with characteristics such as relationships, client interaction, the number of transitions, network expansion, and their impact on the structure of Z. Quantitative characteristics of the parameters are calculated.

In article [12], techniques for studying the structure and behavior of groups are presented. Empirical research on the impact of structure in small groups is conducted. Focusing on communication structure, laboratory studies, in which structures are experimentally imposed on groups, are examined to determine their impact on performance.

In article [13], the cognition of a person (their thoughts and beliefs) about the situation in which they exist, as well as their evaluation of what they are capable of (self-assessment of abilities), will collectively influence their behavior. Adherence to incorrect thoughts and/or inaccurate evaluations of one's abilities can be punitive or even fatal in many situations. Abilities manifest only through performance, which is expected to depend on specific abilities.

In research [14], the dynamics of interpersonal relationships leading to stable states in a fully connected network are discussed. This approach is applied to directed networks with asymmetric relationships, and it is generalized to include self-assessment of actors according to the "Mirror" theory. A new self-acceptance index is proposed: an actor's attitude toward themselves is positive if the majority of their positive relationships with others are reciprocal. The sets of stable relationship configurations are obtained under dynamics, where the self-assessment of some actors is negative. Within each set, all configurations share the same structure.

In article [15], a conceptual model of an intelligent network is discussed, which is proposed for use in synthesizing network control in information transmission systems within intelligent info communications management systems. It is shown that during the synthesis of intellectual control systems (ICS), certain features must be taken into account: the processing speed at the upper levels of the conceptual model decreases as the "intelligence" increases, which, in turn, falls as we move down to the transport level of the proposed model. The principles include the design and architecture of ICS, considering current measurement data and information sources.

In article [16], a proposed model differs from well-known computer systems with specialized information platforms that allow testing of security, enabling the evaluation of the penetration test execution time within a specified probability interval. The proposed penetration testing process for computer systems has been further developed (modified). A distinctive feature of the modified model is the Erlang distribution as the main mathematical formalization for state transition processes. This has allowed, on one hand, the unification of the mathematical model and the presentation of the testing process at a higher level in the testing hierarchy, and, on the other hand, simplified it by 1.7 times. A mathematical model for security testing based on the well-known approach to the simplification and modification of GERT networks was developed to assess the accuracy of simulation results.

In research [17], a deterministic model for online social networks (OSN) is presented, based on transitivity and local knowledge in social interactions. In repeated local transitivity (ILT), at each time step, and for every existing node x, a new node appears and joins the closed neighborhood set of x. The ILT model has been shown to satisfy a range of local and global properties that have been observed in OSN and other real-world complex networks, such as the power-law compression, reduced average distance, and higher clustering than in random graphs with the same average degree. Experimental studies on social networks demonstrate poor expansion properties as a result of the existence of communities with few inter-community edges. Boundaries for the proven spectral gap, both for the adjacency matrix and the normalized Laplacian matrix of graphs arising from the ILT model, indicate these poor expansion properties. It is shown that the number of police officers and domination remain the same as in the graph from the initial time step G0, and the group of automorphisms G0 is a subgroup of the automorphism group of graphs created at all later time steps. A randomized version of the ILT model is presented, demonstrating a tunable power-law exponent and maintaining several properties of the deterministic model.

In article [18], it is noted that the structure of social networks is usually derived from limited sets of observations through appropriate network sampling schemes. It is well-known in the literature that using degree constraints generates methodologically undesirable features because it discards information about network connections. A mathematical model of this sampling procedure is discussed, and analytical solutions are found to recover some of the lost information about the underlying network. A closed-form expression is obtained for several network statistics, including the first and second moments of the degree distribution, network density, number of triangles, and clustering.

In article [19], it is shown that when groups compete for members, the resulting dynamics of human social activity can be understood using simple mathematical models. Methods of dynamic systems and perturbation theory are applied to analyze the theoretical basis for the growth and decline of competing social groups. A new approach to the competition for followers between religious and non-religious segments of modern secular societies is presented, and a new international dataset tracking the rise of religious disaffiliation is collected. The data indicate a specific case of a general growth law that provides clear predictions for possible future trends in society.

In study [20], it is noted that one of the most important and integral components of modern computer security is access control systems. The task of an access control system (ACS) is often described in terms of protecting system resources from unauthorized or undesirable user access. However, the high degree of sharing can hinder the protection of resources, so a sufficiently detailed policy should allow selective information sharing when, in its absence, sharing might be considered too risky in general. Incorrect configurations, faulty policies, and software implementation flaws can lead to global security risks.

In the article [21], an analysis of social networks is presented, suggesting it as a tool for linking micro- and macro-levels of sociological theory. The procedure is illustrated by developing macro-consequences of one aspect of small-scale interaction: the strength of dyadic ties. It is argued that the degree of intersection of the friendship networks of two individuals directly changes depending on the strength of their connection to each other. The influence of this principle on the spread of influence and information, mobility opportunities, and community organization is explored. Emphasis is placed on the cohesive power of weak ties. Most network models implicitly deal with strong ties, thus limiting their applicability to small, well-defined groups. The focus on weak ties invites discussion of relationships between groups and the analysis of segments of the social structure that are difficult to define in terms of primary groups.

In the article [22], an analysis of social networks is conducted, considering social relationships from the perspective of network theory, which consists of nodes and links (also called edges, connections, or ties). In this work, the authors attempt to explore the mathematical explanation of social networks. The research provides guidelines for researchers on how to optimize the parameters of social networks.

In the article [23], an analysis of the limiting behavior of the degree distribution in the partial duplication model, a random network growth model in the duplication and divergence family, which is popular in the study of biological networks, is presented. The probability of selecting a model is a phase transition for the expected proportion of isolated nodes, which tends toward 1. Asymptotic bounds on the speed of convergence of the degree distribution are obtained. A subgraph consisting of all non-isolated nodes contained in networks generated by the partial duplication model is examined, and it is shown that there is again a phase transition for the limiting behavior of its degree distribution.

The study in [24] investigates the structures of online networks, focusing on the growth mechanisms by which they develop. Growth models based on preferential attachment—the tendency of a node to connect to a node with a higher degree—are considered. Using Facebook as a dataset, a mechanism for modeling the Facebook network in a simple structure is developed.

In the article [25], a mathematical model of dynamic networks is developed, which is based on closed rather than open sets. For social networks, it seems appropriate to use the concept of adjacency to establish these sets. A concept of continuous change is then defined, which has some properties related to the continuity of counting. It is demonstrated that continuity has a local nature, meaning that if a network change is discontinuous, it will occur at a specific point, and the discontinuity will be apparent near that point. Necessary and sufficient continuity criteria are provided when the change involves only the addition or removal of individual nodes or connections (edges). To illustrate large-scale continuous changes, a practical process is chosen that reduces a complex network to its fundamental cycles, during which most of the triad-closed parts are removed. Finally, several variants of the adjacency concept are examined, and it is proved that the notion of fuzzy closure can be defined.

In article [26], a mathematical model is extended, representing social networks as tripartite hypergraphs, defining additional quantities such as edge distribution, vertex similarity, correlations, and clustering, and empirically measuring these quantities on two real-world taxonomic systems.

A drawback of these works is the lack of research on the quantitative dependencies of *Z* on *P*, including under conditions of nonlinear changes and the absence of studies on the stability of SP.

3. Concept and objectives of analysis

Main directions of research includes:

- Analysis of the quantitative relationship between the characteristics of *P* and the characteristics of *Z*.
- Study of the impact of potential factors in SP based on *P*.

The paper examines the definitions and analysis of *Z* in SP, taking into account their characteristics and parameters of *P*. To compute *Z*, an uncertain cognitive simulation approach is applied. The development and research are based on the conceptual foundations of scientific thought and the modeling of imprecise dependencies. This has allowed for a deeper understanding and formation of insights into little-known technological processes. To study KI in SP, DEVC systems were created that demonstrate *Z*. Methods for solving DEVC are proposed (including the exclusion method, joint solutions of homogeneous and non-homogeneous equations, collective search for relevant dependencies, etc.). The study of the impact on Z was carried out through the analysis of DEVC and a specially developed module in MATLAB/MULTISIM.

4. Proposed methodology

The methodology continues and develops the work presented in [9–11], allowing for the creation of an approach to determine the quantitative indicators of *Z* in SP under the influence of *P* and external factors.

4.1. Features of P in SP

A graphical dependence of the differential of P is presented in Figure 1.

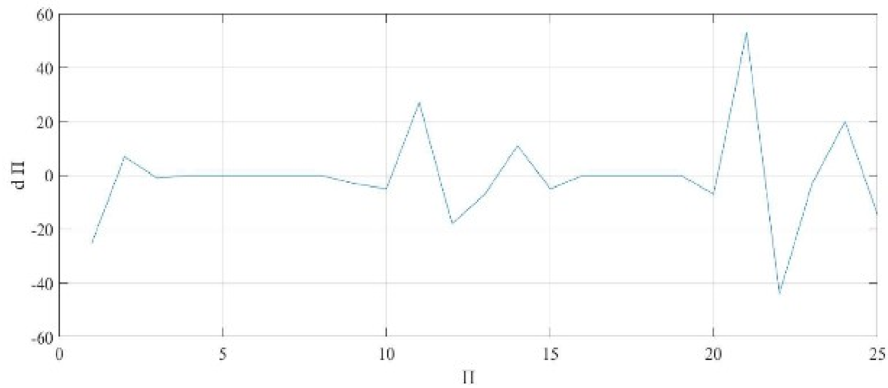


Figure 1: Differential of function *P*

The first step is the application of the system of equations [8–11].

4.2. Analysis and modeling of a nonlinear system considering P in SP

Since the nonlinearity of *Z* is insignificant, the method of successive approximations was chosen to solve the dependencies, assuming:

$$S = S_1 + S_2 + S_3 \ldots,$$
$$Z = Z_1 + Z_2 + Z_3 + \ldots.$$

Assume that

$$dS = 0, \frac{dS}{dt} = 0, \text{ and } dZ = 0, \ \frac{dZ}{dt} = 0, S = S_0 \sin \omega t, Z = Z_0 \sin \omega t.$$

The analysis of the graphical dependencies of the linear system presented in [7] indicates its nonlinear nature. To account for this feature, nonlinear components are added to the system of equations (1), as stated in expression (2):

$$\begin{cases} \frac{dS}{dt} = Z_p Z + (C_v + C_K) S \\ \frac{dZ}{dt} = \sum_{k=1}^{K} m_k - \frac{1}{2} \sum_{k=1}^{K} n_k^2 \alpha_i - S(C_{d2} + C_{d1}) \end{cases} \quad (1)$$

$$\begin{cases} \frac{dS}{dt} = Z_p Z + (C_v + C_K) S - L_2 S_0^2 \sin^2 \omega t - L_3 S_0^3 \sin^3 \omega t - \ldots \\ \frac{dZ}{dt} = \sum_{k=1}^{K} m_k - \frac{1}{2} \sum_{k=1}^{K} n_k^2 \alpha_i - S(C_{d2} + C_{d1}) - K_2 Z_0^2 \sin^2 \omega t - K_3 S_0^3 \sin^3 \omega t - \ldots \end{cases} \quad (2)$$

Let's rewrite the system of equations and present it in the proposed format:

$$\begin{cases} \dfrac{dS}{dt} = \alpha Z + \beta_1 S - \sum\limits_{k=2}^{\infty} L_k S_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 S + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \tag{3}$$

where: $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -(C_{d2} + C_{d1})$, $\gamma = \sum\limits_{k=1}^{K} m_k - \dfrac{1}{2}\sum\limits_{k=1}^{K} n_k^2 \alpha_i$.

Graphs based on dependency (3) are shown in Figure 2.

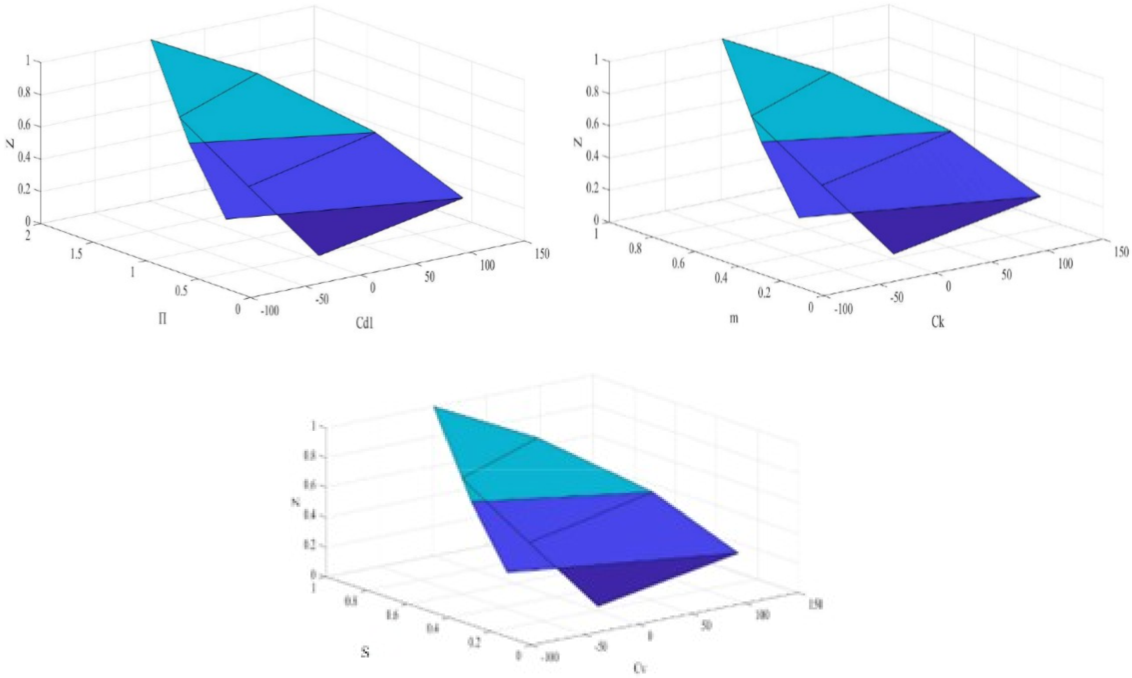


Figure 2: Graphs based on dependency (3)

We use the method of elimination:

$$\begin{cases} \dfrac{dZ}{dt} = \beta_2 S + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \Rightarrow \\ S = \dfrac{1}{\beta_2}\left(\dfrac{dZ}{dt} - \gamma + \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t\right) \Rightarrow \end{cases}$$

$$\frac{dS}{dt} = \frac{1}{\beta_2}\left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega}\sum_{k=2}^{\infty} k K_k Z_0^k \sin^{k-1} \omega t (\cos \omega t)\right) \tag{4}$$

We substitute the obtained expressions (4) into the first equation of the system (3).

$$\begin{aligned} &\frac{1}{\beta_2}\left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega}\sum_{k=2}^{\infty}\left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t\right)\right) = \\ &= \alpha Z + \frac{\beta_1}{\beta_2}\left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t\right) - \sum_{k=2}^{\infty} L_k S_0^k \sin^k \omega t, \end{aligned} \tag{5}$$

or:

$$\begin{cases} \frac{d^2 Z}{dt^2} - \beta_1 \frac{dZ}{dt} - \alpha \beta_2 Z = \frac{-1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^{k-1} \sin^k \omega t \cos \omega t \right) \\ \quad - \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t - \beta_2 \sum_{k=2}^{\infty} L_k S_0^k \sin^k \omega t, \end{cases} \tag{6}$$

Graphs based on dependency (3) are shown in Figure 3.

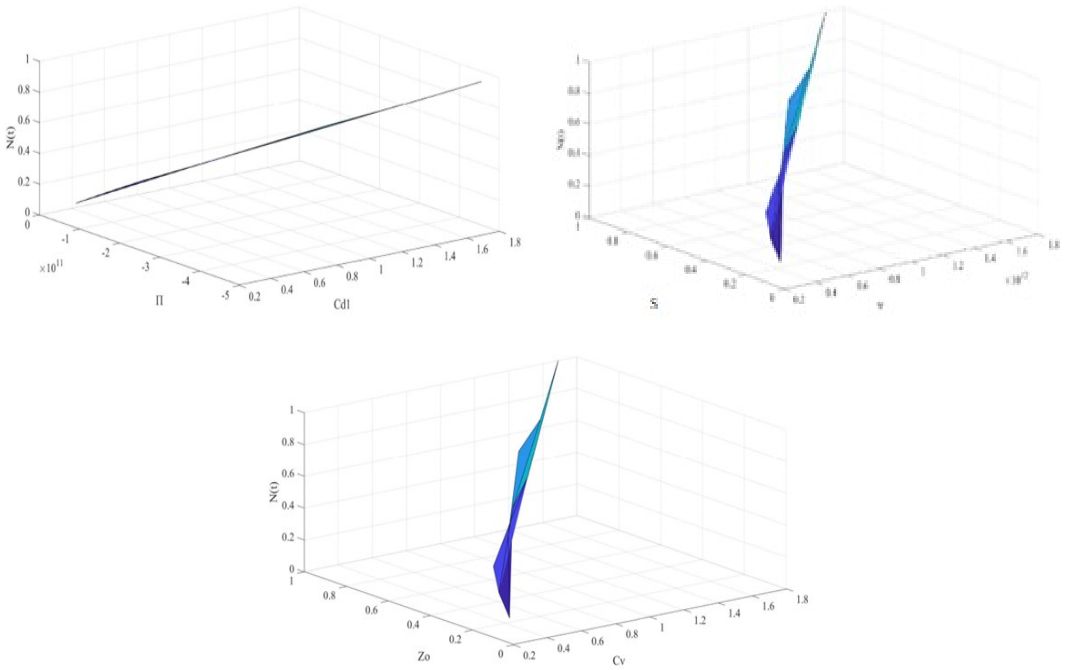


Figure 3: Dependencies according to equation (6)

We determine the general solution of the homogeneous expression:

$$Z'' - \beta_1 Z' - \alpha \beta_2 Z = 0. \tag{7}$$

The main equation looks as follows: $\lambda^2 - \beta_1 \lambda - \alpha \beta_2 = 0$.

Let us consider the case with a positive discriminant of the given equation.

$$D = \beta_1^2 + 4 \alpha \beta_2 > 0 \Rightarrow \lambda_{1,2} = \frac{\beta_1 \pm \sqrt{\beta_1^2 + 4 \alpha \beta_2}}{2}. \tag{8}$$

where:

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

We apply the method of variation of parameters to solve the non-homogeneous equation.

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

where $c_1'(t), c_2'(t)$ are determined from the expressions:

$$\begin{cases} c_1'(t) e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4 \alpha \beta_2}}{2} t} + c_2'(t) e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4 \alpha \beta_2}}{2} t} = 0, \\ c_1'(t) \frac{\beta_1 + \sqrt{\beta_1^2 + 4 \alpha \beta_2}}{2} e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4 \alpha \beta_2}}{2} t} + c_2'(t) \frac{\beta_1 - \sqrt{\beta_1^2 + 4 \alpha \beta_2}}{2} e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4 \alpha \beta_2}}{2} t} = N(t), \end{cases} \tag{9}$$

where:

$$\begin{cases} N(t)=\frac{-1}{\omega}\sum_{k=2}^{\infty}(kK_k Z_0^k \sin^{k-1}\omega t\cos\omega t) \\ -\beta_1\gamma+\beta_1\sum_{k=2}^{\infty}K_k Z_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_k Z_0^k\sin^k\omega t. \end{cases} \tag{10}$$

From the dependencies (9, 10), we will determine:

$$c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=-c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\Rightarrow, \tag{11}$$

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

or:

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

From which we will obtain:

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

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

Considering (11, 12, 13) we have:

$$\begin{aligned} Z(t)=&\int N(t)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}dt- \\ &-\int N(t)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}dt, \end{aligned} \tag{16}$$

4.3. Analyzing the behavior of the data protection system in the phase space

The initial equation:

$$\begin{aligned} \frac{d^2Z}{dt^2}=&\frac{-1}{\omega}\sum_{k=2}^{\infty}\left(kK_k Z_0^k\sin^{k-1}\omega t\cos\omega t\right)^k\omega t-, \\ &-\beta_1\gamma+\beta_1\sum_{k=2}^{\infty}K_k Z_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_k I_0^k\sin ¿ \end{aligned} \tag{17}$$

The study will be conducted in the MatLab/Multisim environment. We will build a schematic of the solution search module (Figure 4).

The results of the module's work are shown in Figures 5 and 6.

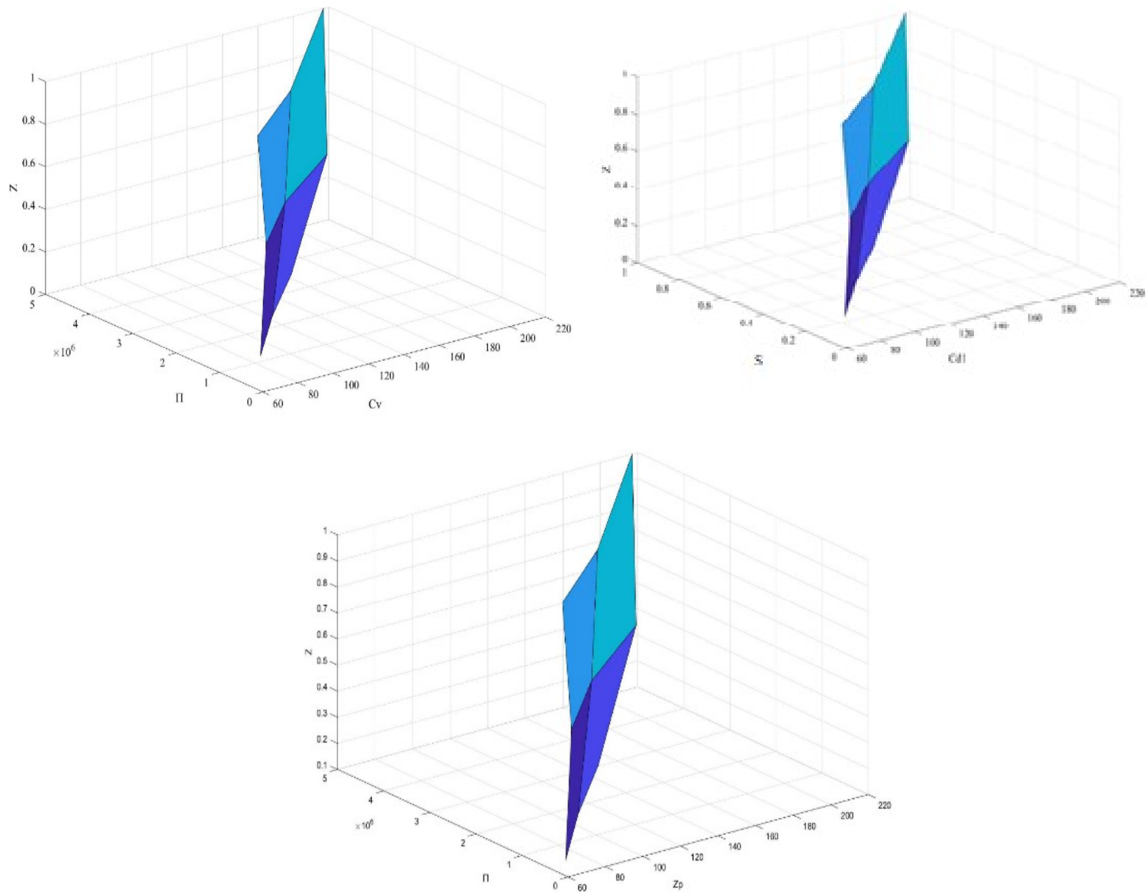


Figure 4: Graphs based on dependency (16)

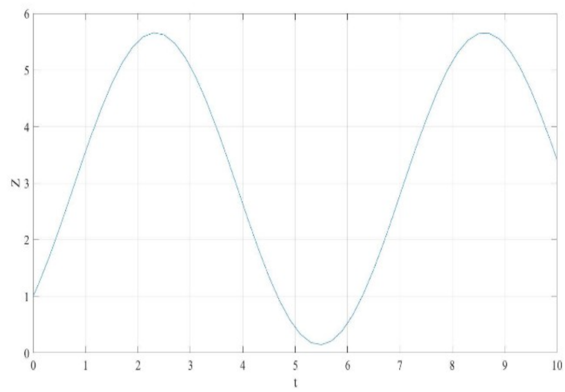


Figure 5: Periodic changes of the protection system as a function of time *Z=f(t)Z*

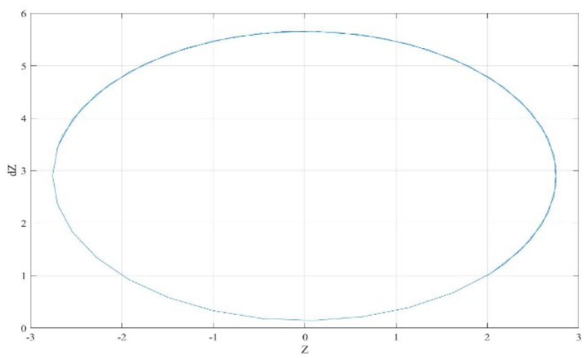


Figure 6: Phase portrait of the protection system based on parameters *P*

4.4. Creation of the phase diagram of the CPS system considering attacks

Consider a system that models an attack on the system and its immune response. It is assumed that the dynamics of the harmful agent are described by the logistic model (18). The growth of the infection is determined by its initial state, the decay caused by the immune response, and the effect of density. In turn, the change in the immune response depends on the initial state, natural decay, stimulation that enhances the response, and the damage caused by the harmful agent, as shown in Figures 7 and 8. Finally, the condition of the affected organ depends on the density of the harmful agent and its natural degeneration. Thus, the dynamics of the system can be expressed through the following system of differential equations:

$$\frac{dP}{dt} = \beta P - \gamma IP - \beta_0 P^2, \qquad \frac{dI}{dt} = \mu - \alpha I + bIP - \eta \gamma IP \tag{18}$$

where: $P(t)$ is the concentration of malicious agents; $I(t)$ is the state of the immune system; β is the growth rate coefficient of malicious agents; γ is the coefficient of decrease in malicious agents due to their interaction with the network's immune system; θ is the parameter of intraspecific competition between malicious agents; μ is the rate of activation of the immune system; a—natural decay rate of the immune system; b is the rate of immune system stimulation due to interaction with malicious agents; η is the decay rate of the immune system due to interaction with malicious agents; α is the coefficient of increased node damage under the influence of malicious agents.

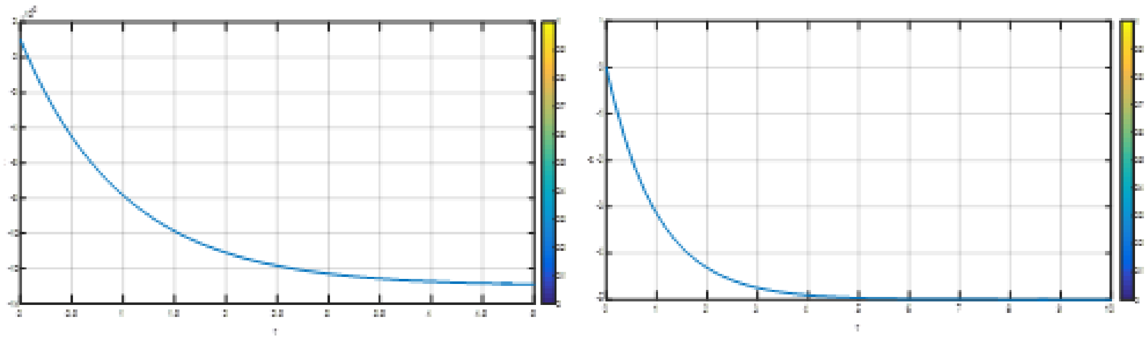
For the initial investigation, we will design a block diagram of the system according to the equations (18). We will set the initial conditions:

$$P = 0,\ I = \beta/\gamma,\ \gamma = 0.4,\ \beta = 0.6,\ \beta_0 = 0.2,\ \alpha = 0.3,\ \eta = 0.2,\ b = 0.4,\ \mu = 0.5.$$

The modeling process will include variation of attack parameters and the level of protection to determine the stability zone of the system in response to threats (Figures 7 and 8).

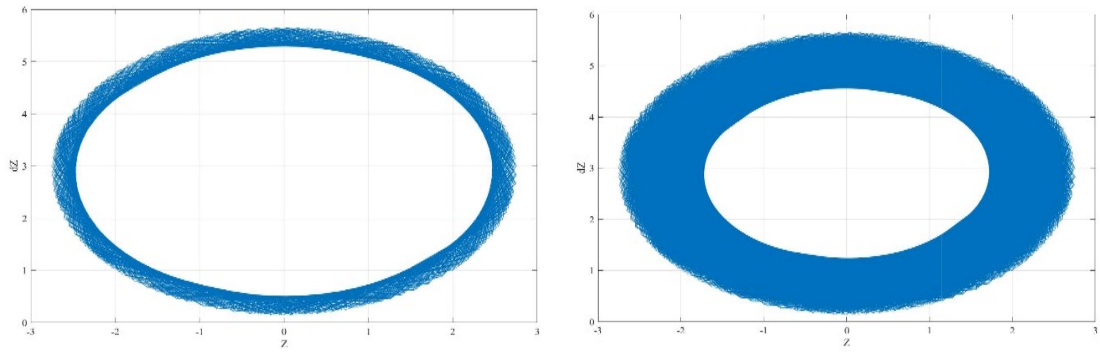
The conclusions of the research on the stability of the protection system in social media highlight its effectiveness at maximum amplitudes of impacts under operational parameters and various network specifics according to Lyapunov's theorem. This ensures secure information protection and minimizes attack risks.

Solution search module in the Multisim program is shown in Figure 9.



a b

Figure 7: The minimum attack amplitude value considering the attack duration—a) (all parameters are equal to 0.1), and the maximum attack amplitude value—b) (all parameters are equal to 1)



a b

Figure 8: Phase portrait of the protection system a) from impact parameters—0.5, and b) the maximum value of impact amplitude

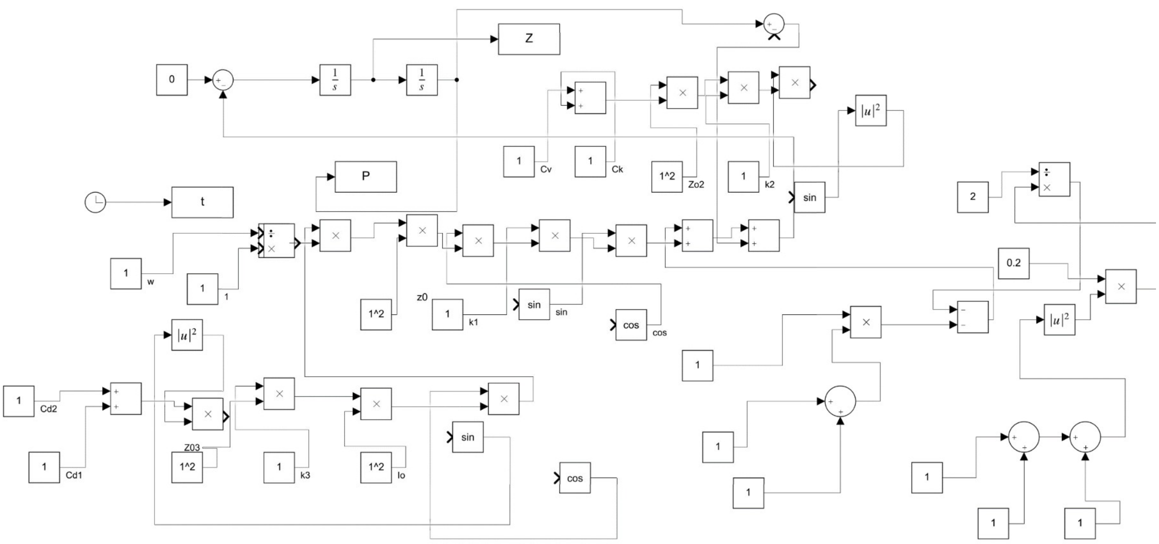


Figure 9: Solution search module in the Multisim program

4.5. Exchange of expressed considerations from the study of Z in SP taking into account P

The analysis of *Z* using probabilistic characteristics and *P* characteristics allowed for the acquisition of numerical evidence regarding the crucial isolated characteristics of the CS, which include the impact of *P* on *Z* (1, 2, 16) (Figures 2–4). The evaluation of fundamental approaches, models, and scientific concepts, assessed through simulation modeling of Z considering the influences, confirmed the validity of the methodology.

The study of the stability of *Z* (17) (Figures 5—8) demonstrates high reliability and stability. The chosen method allows obtaining quantitative characteristics of *Z* using SP and *P* characteristics. At the same time, there is no alternative method with the same result.

The positive thing that *Z* withstands maximum loads, including the influence of *P*. To provide information to security personnel in SP with convenient, "at-hand" information, tools, and methods for analyzing the quantitative impact of *P* characteristics on *Z* characteristics is considered a significant advantage.

The study of *Z* oscillation amplitudes and phase diagrams reveals current threats in real-time along with their intensity. This enables information security personnel to make real-time decisions based on *Z* characteristics. The next stage of the scientific work will involve investigating other SP parameters and their influence on *Z*.

5. Numerical expression

Phase portraits on the phase plane of CS, which confirming its stability even under peak levels of impact factors, have been studied. This was further validated by subsequent research (Figure 9).

The values of *Z* characteristics range from 0 to 1, indicating a strong influence of *P* characteristics (see Figures 3, 4). Closed curves without bifurcations (Figure 8) under varying impact levels confirm the high stability of *Z*.

Conclusions

Analysis of the model that reproduces Z reveals quantitative results of the impact of the characteristics of SP and characteristics of P on KP in SP and their awareness. The influence characteristics of P on Z range from zero to one hundred percent, which enabled further research into other attacks.

Research in SP based on different indicators of the impact of harmful elements on Z was conducted using the solution search module in the Multisim program. The study of Z's oscillation graphs and phase diagrams confirms the stability of KP under various impacts of harmful elements. Based on the analysis, it can be concluded that the study of the impact of P on Z is accurate. The next research will focus on the study and use of other unique characteristics of SP to determine their influence on Z. Research into the amplitudes of oscillations of Z and phase diagrams demonstrates existing threats and their strength in real-time. This allows information security staff to make decisions based on Z characteristics in real-time.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] O. Milov et al., Development of Methodology for Modeling the Interaction of Antagonistic Agents in Cybersecurity Systems, Eastern-European J. Enterp. Technol. 2.9 (98) (2019) 56–66. doi:10.15587/1729-4061.2019.164730

[2] V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.

[3] R. Marusenko, V. Sokolov, P. Skladannyi, Social Engineering Penetration Testing in Higher Education Institutions, Advances in Computer Science for Engineering and Education VI, vol. 181 (2023) 1132–1147.

[4] V. Buhas, et al., AI-Driven Sentiment Analysis in Social Media Content, in: Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 (2024) 12–21.

[5] R. Marusenko, V. Sokolov, I. Bogachuk, Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation, Advances in Artificial Systems for Logistics Engineering, vol. 135 (2022) 583–594. doi: 10.1007/978-3-031-04809-8_53.

[6] Z. B. Hu, V. Buriachok, V. Sokolov, Implementation of social engineering attack at institution of higher education, in: 1st Int. Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), vol. 2654 (2020) pp. 155–164.

[7] V. Akhramovych, V. Akhramovych, R. Prydybailo, S. Chuprun, Method for Information Security Research based on the Number of Communities in Social Media, Measuring Comput. Devices Technol. Processes 2 (2024) 96–106. doi:10.31891/2219-9365-2024-78-11

[8] V. Akhramovych, S. Lazarenko, H. Martynyuk, Y. Balanyuk, Model for Searching Communities in Social Networks, Inform. Secur. 26(1) (2020) 35–41.
[9] V. Akhramovych, G. Shuklin, Y. Pepa, T. Muzhanova, S. Zozuli, Devising a Procedure to Determine the Level of Informational Space Security in Social Networks Considering Interrelations among Users, Eastern European J. Adv. Technol. 1/9 (115) (2022) 63–74. doi:10.15587/1729-4061.2022.252135
[10] V. Akhramovych, Y. Pepa, A. Zahynei, V. Akhramovych, T. Dzyuba, I. Danylov. Method for Calculating the Information Security Indicator in Social Media with Consideration of path Duration between Clients, Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska – IAPGOS 14 (1) (2024) 71–77. doi:10.35784/iapgos.5720.2024.03.31
[11] V. Akhramovych, S. Lehominova, O. Stefurak, V., Akhramovych, S. Chuprun, Methodology for Searching for the Dependence between Data Defensiveness and Volume of Social Network Evolution, Int. J. Comput. Netw. Inf. Secur. 16(6) (2024) 1–19. doi:10.5815/ijcnis.2024.06.01
[12] A. Bavelas, Communication Patterns in Task-oriented Groups, J. Acoustical Soc. America 22 (1950) 725–730. doi:10.1121/1.1906679
[13] L. Festinger,. A theory of Social Comparison Processes, J. Human Relations 7 (2) (1954) 117–140. doi:10.1177/001872675400700202
[14] F. Heider, Attitudes and Cognitive Organization, J. Psychol. 21 (1946) 107–112. doi:10.1080/00223980.1946.9917275
[15] L. Berkman, et al., The Intelligent Control System for Infocommunication Networks, Int. J. Emerging Trends Eng. Res. 8 (5) (2020) 1920–1925.
[16] S. Semenov, C. Weilin, Testing Process for Penetration into Computer Systems Mathematical Model Modification, Adv. Inf. Syst. 4 (3) (2020) 133–138. doi:10.20998/2522–9052.2020.3.19
[17] A. Bonato, N. Hadi, P. Horn, P. Pralat, C. Wang, Models of Online Social Networks, Internet Math. 6 (3) (2020) 285–313.
[18] B. Fotouhi, S. Rytina, Mathematical Modeling and Inference for Degree-Capped Ego-Centric Network Sampling. https://scholar.harvard.edu/files/babak_fotouhi/files/main.pdf
[19] D. M. Abrams, J. Richard, A. Haley, A Mathematical Model of Social Group Competition with Application to the Growth of Religious Non-Affiliation. https://www.arxiv-vanity.com/papers/1012.1375/
[20] G. Cherneva, P. Khalimov, Mutation Testing of Access Control Policies, Adv. Inf. Syst. 5(1) (2021) 118–122. doi:10.20998/2522–9052.2021.1.1.7
[21] M. S. Granovetter, The Strength of Weak Ties, American J. Sociology (1973) 1360–1380.
[22] M. K. Srivastav, A. Nath, Study on Mathematical Modeling of Social Networks, Int. J. Emerging Technol. Adv. Eng. 5 (3) (2015) 611–618.
[23] S. Li, K. P. Choi, T. Wu,. Degree Distribution of Large Networks Generated by the Partial Duplication Model, Theoretical Comput. Sci. 476 (2013) 94–108.
[24] O. Mandelshtam, Growth Models of Social Networks. SURF 2007 Final Report.
[25] J. L. Pfaltz, A Mathematical Model of Dynamic Social Networks, Social Network Analysis and Mining 3(4) (2013) 1–16. doi:10.1007/s13278-013-0109-9
[26] V. Zlatić, G. Ghoshal, G. Caldarelli, Hypergraph Topological Quantities for Tagged Social Networks. Physical Review E 80 (2009). doi:10.1103/PhysRevE.80.036118