Linear and dynamic models of the system of information security in social networks, taking into consideration the relationships between users, were studied and the resistance of the security system was analyzed.

There is a practical interest in studying dependence of the behavior of the system of social network security on the parameters of users' interaction. Dynamic systems of information security in social networks in the mathematical sense of this term were considered. A dynamic system refers to any object or process, for which the concept of state as a totality of certain magnitudes at a given time is unambiguously defined and the law that describes a change (evolution) of the initial state over time was assigned.

The network of social interactions consists of a totality of social users and a totality of the relations between them. Individuals, social groups, organizations, cities, countries can act as users. Relations imply not only communication interactions between users but also relations of the exchange of various resources and activities, including conflict relations.

As a result of research, it was found that the security systems of a social network are nonlinear. Theoretical study of the dynamic behavior of an actual object requires the creation of its mathematical model. The procedure for developing a model is to compile mathematical equations based on physical laws. These laws are stated in the language of differential equations.

Phase portraits of the data security system in the MATLAB/Multisim program, which indicate the stability of a security system in the working range of parameters even at the maximum value of the impacts, were determined.

Thus, the influence of users' interaction parameters on the parameters of the system of social network security was explored. Such study is useful and important in terms of information security in the network, since the parameters of users' interaction significantly affect, up to 100 %, the security indicator

Keywords: social network, users' relationships, security system, nonlinearity, differential equations, procedure

UDC 004.738.5
DOI: 10.15587/1729-4061.2022.252135

DEVISING A PROCEDURE TO DETERMINE THE LEVEL OF INFORMATIONAL SPACE SECURITY IN SOCIAL NETWORKS CONSIDERING INTERRELATIONS AMONG USERS

Volodymyr Akhramovych
Corresponding author
Doctor of Technical Sciences,
Senior Researcher, Professor*
E-mail: 12z@ukr.net
German Shuklin
PhD, Associate Professor, Head of Department*
Yuriy Pepa
PhD, Associate Professor*
Tetiana Muzhanova
PhD, Associate Professor
Department of Information
and Cyber Security Management**
Serhii Zozulia
Postgraduate Student*
*Department of Information
and Cyber Defense Systems**
**State University of Telecommunications
Solomianska str., 7, Kyiv, Ukraine, 03110

Received date 30.12.2021
Accepted date 10.02.2022
Published date 28.02.2022

How to Cite: *Akhramovich, V., Shuklin, G., Pepa, Y., Muzhanova, T., Zozulia, S. (2022). Devising a procedure to determine the level of informational space security in social networks considering interrelations among users. Eastern-European Journal of Enterprise Technologies, 1 (9 (115)), 63–74. doi: https://doi.org/10.15587/1729-4061.2022.252135*

1. Introduction

In the modern world, information needs reliable protection: from unauthorized access and distribution, accidental deletion, or change. All developed countries of Europe are concerned about the problem of information security, as well as the security of the personal information of citizens. This is due to the fact that informatization and digitization of information have become widespread in all spheres of human activity, including the storage of personal and working data.

Social networks (SN) are one of the main methods of communication, search for relations, and exchange of both public and confidential information. Social networks make up an ever-growing share among general networks. In addition, a network itself acquires new properties, acting as an independent factor.

This problem is especially exacerbated by strengthening the digital humanistic nature of education, the growing role of social networks in human life as a whole.

Security of personal information under conditions of modern information life is perhaps the most important aspect in satisfying the safe use of all the capabilities of current technologies. That is why the problem of studying the parameters of social networks for their further use in solving the problems of security of information and personal data is important and relevant.

In paper [1], it is argued that there is a tendency that if two individuals are close to each other in views, they are

likely to take a coordinated position to any third individual, subject, or event. Based on similar discoveries, the researchers could construct models of systematic interdependence between the settings followed by different individuals within the same group. This statement was summarized in the theoretical concept [2]. The attempt to apply mathematics to the structure of group relationships was certainly not a new idea. Such attempts were made in the late 1950s [3–5]. Article [6] developed powerful models of group cohesion, social pressure, cooperation, power, and leadership. In the UK, two methods were used to study social structure – morphological and physiological study of social systems. The functions of the first include definition, comparison, and classification of different structures. The task of the physiological method is to study the mechanisms that support the existence of a system.

The author of [7] is considered the founder of the theory of cognitive balance – the motivational theory of changing attitudes. It conceptualizes the cognitive coherence of motives as the cause of psychological balance. The consistency of motives seeks to maintain someone's values and beliefs over time. Heider suggested that «dispositions» or relationships are balanced if their impact multiplies the positive outcome of a system.

Scientists explored networks in terms of their physical nature and possible impact on the protection of information [8–10], access to information policy [11–13], protection of personal information from the point of view of law [14], protection against outside electromagnetic radiation [15].

The methodology of social networks was evaluated using two pilot cases [16], the user profile was described [17, 18]. It is proposed to use the «interaction graphs», to give importance to social online links by quantifying users' interaction [19]. The approach of checking the model for managing relationships with users in a social network [20]. The processes of the development of social communication and social relations in virtual communities are studied, and processes themselves are considered and analyzed [21, 22]. The elements of users' relationships in social networks were considered. It was shown that the social relations of network users are a coherence table; an intersection of matrices of social relations and coherence. The composition of relationships contains elements and types of network graphs; a set of statistics for social relations; the intensity of interaction of groups, a degree of centrality of different users. Characteristics of the network of social interactions contain balance and transitivity; force of a user's structural position; states of dyads; the influence of the network structure on model p; probability of the existence of relations between users; dependent and independent edges of the graph; evaluation of parameters of a model; logit models [23]. Scientists gradually approached determining the parameters of information security in social networks, in particular, articles [24, 25] study the parameters of trust, papers [26, 27] deal with joint filtering based on the construction of associative networks of users similarity.

Some researchers have moved to studying the impact of specific social network parameters directly on information security parameters where it is proved that the protection system is nonlinear [28]. They studied the dependence of nonlinear parameters of the security system against specific parameters of social networks, including trust between users [29].

Information security in social networks uses traditional methods of protection (identification, authentication [30–32], firewalls, security subnets, etc.). However, they do not take into consideration the impact of specific parameters of the network itself, including users' interaction parameters, which is of practical importance, because the impact of these parameters on security is significant.

That is why the studies devoted to the development of a procedure for taking into consideration the influence of specific parameters on information security in social networks, including users' interaction, are relevant.

2. Literature review and problem statement

Article [1] states that there is a tendency that if two individuals are close to each other in views, it is likely that they will take a consistent position to any third individual, object, or event. The interaction of users is not brought to mathematical dependences.

Paper [2] considers the generalization of the theory of Haider's equilibrium using the concepts from the mathematical theory of linear graphs. In Haider's theory, there was no creation of and research into a model for the protection of personal data from users' interaction and the intensity of data transmission in social networks.

In paper [8], it was shown that the dynamic distribution of information flows is one of the effective ways to increase the use of network resources in emergencies. To ensure the dynamic distribution of flows in the network of transmission of guiding information, it is proposed to use a dynamic system for managing the flows distribution, which is a subsystem of the information system of control. It was shown that dynamic routing is effective only with average use of the channel. The method for automated penetration testing with the use of deep machine learning technology was developed. The main goal of the development is to enhance the security of computer systems. The «classic» parameters of a network were studied. Specific parameters, such as interaction and their impact on security systems were not considered.

Article [11] shows that as a result of the policy of access, specifications, the presented models must undergo rigorous verification and legalization through systematic inspections and tests to make sure that the policy specifications do meet the wishes of developers. The verification of the policy of access control and agreement of models is not a trivial and crucial task, but one of the important aspects of such verification is a formal check if the model is inconsistent and incomplete or if it meets well the requirement of security policy. The analysis and comparative studies of the methods of testing for software penetration were carried out. This procedure facilitates the assessment of the sufficiency of accumulation of diagnostic information structure of a wireless sensor network to further determine the technical condition of sensor networks. In addition, the proposed function of sufficient diagnostic information with its subsequent decryption makes it possible to limit the accumulation of audit results in the network. The «classic» parameters of network security are studied, but specific parameters, for example, interaction and their impact on security systems, are not explored.

Article [14] outlined the possibility and special conditions for concluding an agreement, that is, acceptance of the terms of a confidentiality agreement as a separate agreement without proper preliminary conditions. The legal aspects of information security of a network are considered, rather than specific parameters, for example, interaction.

Paper [17] proposed the assembly model for the data set to find out the user's profile. Based on experimental results, it was noticed that several data sources complement each other,

and their corresponding merging increases the performance of users' profiling. Openness is mainly associated with location-based variables (the average distance between visited sites, the site popularity, the number of registrations in social places). The paper does not contain any mathematical dependences on users' relationships.

The reported [20] implicit methodology of social networks was evaluated using two pilot cases: implicit social networks based on the SmartSocial platform; and implicit social networks of IP-TV users. The generalization of implicit social networks is demonstrated on an additional example aimed not at external stakeholders of a company (for example, company's consumers), but rather at internal stakeholders (that is, the company's employees). The «classic» parameters of network security are studied, but specific parameters, for example, interaction and their impact on security systems, are not explored.

Important specific parameters of a social network, such as the average distance between the visited sites, the site popularity, the number of registrations on social sites were explored, but the impact of these parameters on the security system was not studied. In addition, the users' interaction was not explored.

In article [22], the study was aimed at understanding the impact of using social networks on conflicts in romantic relationships through intermediary variables of jealousy, infidelity, and monitoring. The article attempts to clarify the parameters of users' interaction and their impact on the performance of a social network, but the issues of the quantitative impact of interaction on the security system were not considered.

In paper [26], a detailed study of users' interaction in a social network was carried out. Mathematical dependences of users' interaction on other parameters were shown. An important specific parameter of a social network, such as the users' interaction, was studied, but the influence of this parameter on the security system was not dealt with.

Paper [24] indicates that trust in nodes can be an important indicator of their impact, and trusted nodes can also affect other nodes. This study proposes the SNtrust model to find node trust in the network through local and global trust and explores trust, impact, and interrelations in the SN communities. An important indicator of a social network, such as trust between users, was explored, but research into quantitative indicators of the relationship between trust and the protection system was not performed.

In article [26], the method for joint filtering based on the construction of associative networks of users' similarity was developed. To implement this method, the software was developed, experiments were conducted using the developed software to taste testing the developed method, as well as the method for identifying the bot profiles based on neural networks in recommendation systems. The «classic» parameters of traffic filtering were studied, while the specific parameters of social networks were not. Paper [28] developed a linear mathematical model and conducted a study of the model of personal data security depending on the reputation of users and the intensity of data transmission in social networks. However, there remained unresolved issues related to the impact on the system of protection of user interaction parameters in a linear mathematical model.

In paper [29], mathematical modeling of nonlinear dependences of personal data security on the parameters of trust among users was carried out. However, there remained unresolved issues related to the impact of parameters of users' interaction on the security system. The study is important in terms of determining quantitative indicators of the impact on the security system of a specific parameter of the social network, which is trust among users, but it does not consider users' interaction.

Paper [30] considered the functioning of social networks (SN) in accordance with four main user properties: the geographical location of a user, the weight of a user, the number of interactions with a user, and the life expectancy of a user. In the research, the ratio between the specific parameters of a social network, for example, interaction and information security indicator, was not brought to qualitative characteristics.

Article [31] proposed a method to determine the weight of a user based on a new metric for determining time intervals. The metric for determining time intervals is based on standard deviation and determines that the user's weight is based on a simple exponential smoothing model. An attempt is made to determine the interaction of users through their weight indicators, but the impact of interaction on the security system is not studied.

Our review of data from the literature [1–32] revealed that at the moment there is no study related to the impact of parameters of user's interaction on the security system.

Analysis of the nonlinear dynamic security system and obtaining security indicators would be of practical and theoretical significance.

The reason for this may be difficulties in taking into consideration the interaction parameters, nonlinearity itself, and its compliance with the security system.

The option of overcoming the relevant difficulties may be the creation of a mathematical model of the nonlinear security system and researching it, as well as studying the resistance of the system of social network security.

3. The aim and objectives of the study

The aim of the study is to develop a procedure for the level of security of the information space of social networks, taking into consideration users' relationships. This makes it possible to determine quantitative indicators of the impact of parameters of users' interaction and other specific parameters of a social network on the parameters of information security. The study will enable taking into consideration these indicators when planning and implementing the systems of social network security.

To achieve the aim, the following tasks were set:

– to research the linear model of interaction among users in the SN;

– to verify the linearity of the information security system;

– to perform modeling of the nonlinear security system taking into consideration the impact of specific parameters and parameters of users' interaction;

– to explore the resistance of the security system in the SN without impacts and in the presence of impacts on the security system.

4. The study materials and methods

The current research deals with a dynamic nonlinear system of information in a social network (SN) depending on the specificity of its parameters and parameters of users' relationships.

Ensuring information security based on fuzzy cognitive modeling was considered. The cognitive models and methods based on mathematical formalism, the theory of fuzzy sets, and procedures of fuzzy logic were considered. The problems of expanding the arsenal of the classical theory of systems were solved through the use of the methods, which made it possible to adequately model poorly formalized processes. This significantly depended on the influence of hard-to-predict factors and solved the problems of analysis, that is, assessing information security (vulnerability), and synthesis, that is, optimization of the distribution of resources allocated for security.

The systems of non-linear differential equations describing the security system were adopted as the tools to study a dynamic system of information security in the SN. The equations took into consideration: (Z – the indicator of the security of the information system; I – the amount of information in the system; Z_p – the coefficient that reflects the impact of information security measures; C_v – the coefficient that reflects the impact of the rate of personal data leakage; C_k – the coefficient that reflects the impact of the amount of personal data on their leakage; C_{d2} – the coefficient that reflects the impact of the system size on its security; C_{d1} – the coefficient that reflects the impact of security of the data leakage. According to [26], it was accepted: V_i is the coefficient that reflects the impact of threats to personal data security from users' interaction on the information system security, parameter α described the subject's tendency to set interaction, parameter β describes attractiveness and popularity, Θ describes the graph density (evaluation – the number of edges L), p – is the characteristic of the model's tendency to dyads symmetry). The following were also used as the tools: methods of solving a nonlinear system of differential equations (method of exceptions, a joint solution to the relevant homogeneous characteristic equation, etc.); mathematical modeling of processes in the MATLAB system. Resistance of the security system to attacks on it was studied using analysis of nonlinear equations and a special block diagram created in the MATLAB/Multisim system.

5. Results of studying the security level of information space of social networks, taking into consideration users' relationships

5. 1. Study of a linear model of users' interaction in a social network

In the classical approach to personal data security:

$$T_i = \left[V_i, V_j\right], \tag{1}$$

where T_i is the set of threats from users' relationships, V_i is the positive interaction among users, V_j is the negative interaction among users.

The loss of such quality as relationships is a process that has a time interval. Let the $I(t)$ function be the information flow. If we assume that the information flow occurs continuously during the period that is an observation cycle, then $I(t)$ is a continuous deterministic magnitude. Then the rate of a change of this flow is determined as a derivative of function $I(t)$, that is, dI/dt.

It is logical that if the flow and the rate of flow change are equal to zero, there is no information leakage:

$$dI = 0;\ \frac{dI}{dt} = 0. \tag{2}$$

The capability of taking measures of unauthorized access to personal information (information leakage) is directly possible at the insufficient level of the information security system that neutralizes threats to personal data security. Let us assume that Z is the indicator of information system security. Then:

$$\frac{dI}{dt} = Z_p Z + \left(C_v + C_k\right) I, \tag{3}$$

where Z_p is the coefficient that reflects the impact of information security measures; C_v is the coefficient that reflects the impact of the rate of personal data leakage; C_k is the coefficient that reflects the impact of the amount of personal data on their leakage.

The content of equation (3) is as follows. The information leakage depends on:

– the size of an information system (therefore, to some extent, on the amount of personal data);

– the rate of personal data leakage;

– information leakage is blocked by system security (measures to neutralize information security threats).

Next, we consider what determines the system security – Z. The system security is defined as the ability of a system to resist unauthorized access to confidential personal data. Therefore, the system security will depend on:

– the size of a system (as well as on the amount of personal information);

– the threats to information security from users' relationships.

The equation was built:

$$\frac{dZ}{dt} = \left(\alpha + \beta + \theta + \rho\right) V_i - I\left(C_{d2} + C_{d1}\right), \tag{4}$$

where, according to [23], it is accepted: V_i is the coefficient reflecting the impact of threats to personal data security from the interaction between users on the information system security, parameter α describes the subject's tendency to establish interaction, parameter β describes attractiveness or popularity, Θ – the density of the graph (estimate – the number of edges L), p is the characteristic of the model's tendencies to dyads symmetry.

Equations (3) and (4) are combined into a system:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + \left(C_v + C_K\right) I, \\ \dfrac{dZ}{dt} = \left(\alpha + \beta + \theta + \rho\right) V_i - I\left(C_{d2} + C_{d1}\right). \end{cases} \tag{5}$$

Find a stationary position of the system, described by equations (5). Conditions of stationarity are as follows:

$$dI = 0;\ \frac{dI}{dt} = 0.$$

Thus:

$$\begin{cases} Z_p \bar{Z} \lim\limits_{x \to \infty} + \left(C_v + C_K\right) \bar{I} = 0, \\ \left(\alpha + \beta + \theta + \rho\right) V_i - I\left(C_{d2} + C_{d1}\right) = 0. \end{cases} \tag{6}$$

From another equation, we obtained:

$$\bar{I} = \frac{\left(\alpha + \beta + \theta + \rho\right) V_i}{\left(C_{d2} + C_{d1}\right)}. \tag{7}$$

Then from the first equation of the system of equation (6), we found $\bar{Z}$:

$$Z_p\bar{Z}-\frac{(\alpha+\beta+\theta+\rho)V_i(C_v+C_k)}{(C_{d2}+C_{d1})}=0. \quad (8)$$

$$\bar{Z}=\frac{(\alpha+\beta+\theta+\rho)V_i(C_v+C_k)}{(C_{d2}+C_{d1})Z_p}. \quad (9)$$

Thus, the conditions of the system's stationarity position are:

$$\begin{cases}\bar{I}=\dfrac{(\alpha+\beta+\theta+\rho)V_i}{(C_{d2}+C_{d1})},\\ \bar{Z}=\dfrac{V_i(\alpha+\beta+\theta+\rho)(C_v+C_k)}{(C_{d2}+C_{d1})Z_p}.\end{cases} \quad (10)$$

The system of equations (5) was solved using the method of «small deviations» $I=\bar{I}+I;\ Z=\bar{Z}+Z$, thus, the system of equations takes the form:

$$\begin{cases}\dfrac{dI}{dt}=Z_p(\bar{Z}+Z)+(C_v+C_K)(\bar{I}+I),\\ \dfrac{dZ}{dt}=V_i(\alpha+\beta+\theta+\rho)(C_v+C_k)-(\bar{I}+I)(C_{d2}+C_{d1}).\end{cases} \quad (11)$$

$$\begin{cases}\dfrac{dI}{dt}=(C_{d1}+C_{d2})Z-(C_v+C_K)I,\\ \dfrac{dZ}{dt}=-I(C_{d2}+C_k)+V_i(\alpha+\beta+\theta+\rho)(C_v+C_k).\end{cases} \quad (12)$$

By differentiating the first equation of the system (12), we obtained:

$$\frac{d^2I}{dt^2}=-IV_i(C_{d1}+C_{d2})\times$$
$$\times(Z_p+(\alpha+\beta+\theta+\rho))-(C_v+C_K)\frac{dI}{dt}, \quad (13)$$

$$\frac{d^2I}{dt^2}+(C_v+C_K)\frac{dI}{dt}+$$
$$+IV_i(C_{d1}+C_{d2})(Z_p+(\alpha+\beta+\theta+\rho))=0. \quad (14)$$

Equation (14) is an equation of harmonic oscillator with fading amplitude where:

$$\omega_0=\sqrt{(C_{d1}+C_{d2})(Z_p+(\alpha+\beta+\theta+\rho)V_i)}. \quad (15)$$

$$\omega=\sqrt{(C_{d1}+C_{d2})(Z_p+(\alpha+\beta+\theta+\rho)V_i)-\frac{(C_v+C_K)^2}{4}}. \quad (16)$$

$$T=\frac{2\pi}{\sqrt{(C_{d1}+C_{d2})(Z_p+(\alpha+\beta+\theta+\rho)V_i)-\frac{(C_v+C_K)^2}{4}}}. \quad (17)$$

$$\beta=\frac{(C_v+C_K)}{2}. \quad (18)$$

The solution of the equation of harmonic oscillator equation broke down into three cases:

1. $\beta\prec\omega_0: I=$
$$=A_0\exp\left(-\frac{(C_v+C_K)}{2}\times\right.$$
$$\left.\times\cos\left(\sqrt{C_{d1}+C_{d2}+Z_p+\left(\alpha+\beta+\theta+\rho\right)V_i-\frac{(C_v+C_K)^2}{4}}\,t\right)+\varphi_0\right). \quad (19)$$

2. $\beta=\omega_0: I=A_0+B_0t\exp\left(-\frac{C_v+C_K}{2}\right)t.$ (20)

3. $\beta\succ\omega_0: I=A_0\exp(-y_1t)+B_0\exp(-y_2t),$ (21)

where

$$y_{1,2}=\beta\mp\sqrt{\frac{(C_v+C_K)^2}{4}\mp\left(C_{d1}+C_{d2}+Z_p+(\alpha+\beta+\theta+\rho)V_i\right)}. \quad (22)$$

Thus, a linear model of the users' interaction in a social network and its impact on the security system was studied. The dependences of the harmonic oscillator with fading amplitude were obtained. The main parameters of the security system were determined: oscillation frequency (15), (16), oscillation period (17), damping coefficient (18). The solution of the equation of harmonic oscillator, depending on the value of the β parameter, has one of three representations: (19) to (21).

5. 2. Verification of linearity of the information security system

Three options to solve the equation near the stationary state of the system were considered, and the following conclusion was made. Based on the conditions of the ratio of dissipation and its proper frequency of oscillations of magnitude, fading of the latter to a certain value was carried out periodically. The amplitude of oscillations is fading under an exponentially fading law. A more visual analysis of the behavior of the system was made by the transition from the differential form of equations (5), (6) to discrete and modeling forms and by modeling a certain interval of the system existence. Specifically:

$$\begin{cases}\dfrac{I_{n+1}-I_n}{\Delta t}=(C_{d1}+C_{d2})Z_n-(C_v+C_K)I_n,\\ \dfrac{Z_{n+1}-Z_n}{\Delta t}=Z_p-(C_{d2}+C_{d1})I_n-\\ -(Z_p+(\alpha+\beta+\theta+\rho)V_i)(C_v+C_k)I_n.\end{cases} \quad (23)$$

$$\begin{cases}I_{n+1}=I_n+\left((C_{d1}+C_{d2})Z_n-(C_v+C_K)I_n\right)\Delta t,\\ Z_{n+1}=Z_n+\left(\begin{matrix}Z_n-I_nV_i\left(\begin{matrix}C_{d2}+C_{d1}+Z_p+\\+(\alpha+\beta+\theta+\rho)\end{matrix}\right)\times\\ \times(C_v+C_k)\end{matrix}\right)\Delta t.\end{cases} \quad (24)$$

Table 1 with parameters of modeling was created. Following the condition of the stationary position of the system, accepted values for I and Z will be equal to 0.5 and 0.5. The modeling pitch of 0.1 was accepted for all modeling iterations, so it is not shown in the Table.

Table 1

Parameters of modeling

No. by order	Z_p	I	Z	C_v	C_{d1}	V_i	C_{d2}	C_k	α	β	Θ	p	Parameters
1	0.8	0.5	0.5	1	1	0.1	0.5	1	0.8	0.5	0.2	0.5	$\beta<\omega_0$
2	0.8	0.5	0.5	2	1	0.1	1	2	0.8	0.5	0.2	0.5	$\beta=\omega_0$
3	1	0.5	0.5	4	1	1	1	5	1	0.5	0.2	0.5	$\beta>\omega_0$

Magnitudes I_{sp}, Z_{sp} display stationary values of parameters, if there were any within the final number of iterations. Next, simulation for values $\beta \prec \omega_0$, $\beta = \omega_0$, $\beta \succ \omega_0$ with a deviation from the stationary position of the system was performed. The data are shown in Table 1.

Results visualization (Fig. 1–3).

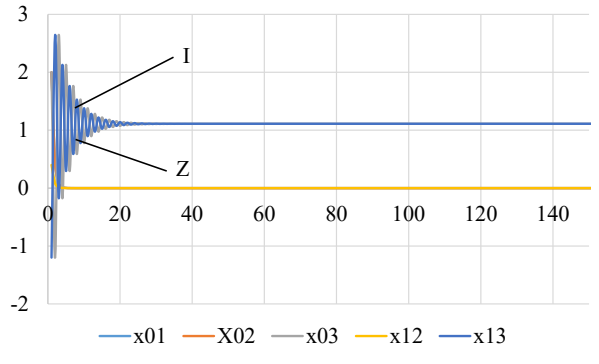

Fig. 1. Dependence of intensity and data security on the number of iterations (140). The data of components were taken from Table 1. $\beta \prec \omega_0$ and the number of iterations was specified

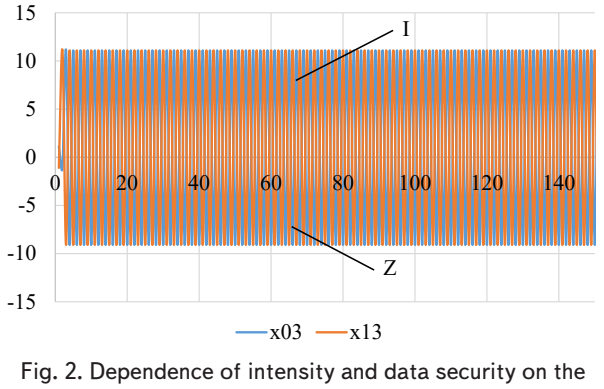

Fig. 2. Dependence of intensity and data security on the number of iterations (140), $\beta=\omega_0$, Di=0.5

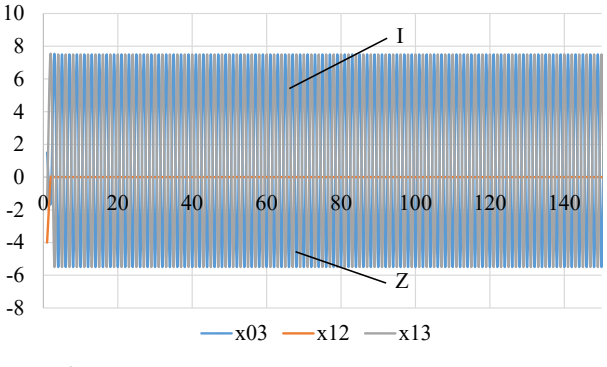

Fig. 3. Dependence of intensity and data security on the number of iterations (140), $\beta \succ \omega_0$, Di=0.1

Analysis of the data in Fig. 3 indicates the nonlinearity of the information security system [1, 12].

5. 3. Modeling a nonlinear security system taking into consideration the impact of specific parameters and parameters of users' interaction

A dynamical system is considered to be assigned if the coordinates of a system, which make it possible to determine its state were entered, and the operator that describes the evolution of the initial state over time was assigned. The mathematical representation of dynamical systems allows great differentiation. The evolution of the state can be described using discrete systems, systems of differential equations, equations in partial derivatives, integral, integral and differential equations, systems with impulse influence, hybrid systems, Markovian chains, that is why we will introduce nonlinear components (25) into the system of equations (24):

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I, \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1}), \end{cases} \quad (25)$$

where V_i is the coefficient that reflects the impact of data security threats from the users' interaction on the security of an information system, parameter α describes the subject's tendency to establish interaction, parameter β describes attractiveness or popularity, Θ – graph density (estimate – number of edges L), ρ is the characteristic of the model's tendencies to dyads symmetry.

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I + L_2 I^2 + L_3 I^3 + ..., \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - \\ -I(C_{d2} + C_{d1}) + K_2 Z^2 + K_3 Z^3 ..., \end{cases} \quad (26)$$

where L_2, L_3, etc. K_2, K_3 etc. are some linear operators. We consider that nonlinearity of the system is weak, which made it possible to look for solutions for each equation of the system (26) using the method of sequential approximation, assuming that:

$$I = I_1 + I_2 + I_3 ...,$$

$$Z = Z_1 + Z_2 + Z_3 + ...$$

It was accepted that at:

$$dI = 0, \ \frac{dI}{dt} = 0, \text{ and } dZ = 0, \ \frac{dZ}{dt} = 0,$$

$$I = I_0 \sin \omega t, \ Z = Z_0 \sin \omega t.$$

Derive the system of equations:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I - \\ -L_2 \left(I_0^{\,2} \operatorname{Sin}^2 \omega t\right) - L_3 \left(I_0^{\,3} \operatorname{Sin}^3 \omega t\right) - \ldots \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I (C_{d2} + C_{d1}) - \\ -K_2 \left(Z_0^{\,2} \operatorname{Sin}^2 \omega t\right) - K_3 \left(Z_0^{\,3} \operatorname{Sin}^3 \omega t\right) - \ldots \end{cases} \quad (27)$$

The system was rewritten and represented in the following form:

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \quad (28)$$

where $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -(C_{d2} + C_{d1})$, $\gamma = (\alpha + \beta + \Theta + \rho)$. Graphic dependence – (Fig. 4).

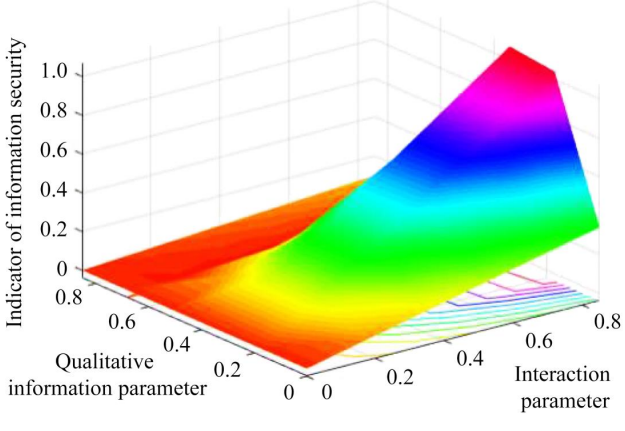

Fig. 4. Plots of dependence (28)

The plot (Fig. 4) indicates that not all information can be secured (due to the bandwidth of the security system).

Then we used the method of exceptions:

$$\frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \Rightarrow$$

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

$$\Rightarrow \frac{dI}{dt} = \frac{1}{\beta_2} \left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) \right). \quad (29)$$

All found expressions (5) were substituted in the first equation of system (4):

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

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

$$- \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t. \quad (30)$$

or

$$\frac{d^2 Z}{dt^2} - \beta_1 \frac{dZ}{dt} - \alpha \beta_2 Z =$$

$$= -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) -$$

$$- \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t - \beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t. \quad (31)$$

A joint solution to the corresponding homogeneous equation is:

$$Z'' - \beta_1 Z' - \alpha \beta_2 Z = 0. \quad (32)$$

The characteristic equation took the form of $\lambda^2 - \beta_1 \lambda - \alpha \beta_2 = 0$. The case of a positive discriminant of this equation was considered:

$$D = \beta_1^2 + 4\alpha\beta_2 > 0 \Rightarrow \lambda_{1,2} = \frac{\beta_1 \pm \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}. \quad (33)$$

hence:

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

– joint solution to a homogeneous equation.

To find the general solution to the heterogeneous equation, we used the method of variation of arbitrary constants:

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

where $c_1'(t)$, $c_2'(t)$ were found from the system:

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

where

$$N(t) = -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) -$$

$$- \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} \left(K_k Z_0^k \sin^k \omega t \right) - \beta_2 \sum_{k=2}^{\infty} \left(L_k I_0^k \sin^k \omega t \right). \quad (34)$$

Finally:

$$Z(s) = \int_{t_0}^{t} \left(N(s) - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} s} \frac{e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} s}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \right) ds -$$

$$- \int_{t_0}^{t} \left(N(s) - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} s} \frac{e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} s}}{\sqrt{s\beta_1^2 + 4\alpha\beta_2}} \right) ds. \quad (35)$$

Dependence (35) of the indicator of information security of a social network on the specific parameters of a network, including the parameters of interaction.

5. 4. Studying the robustness of security system in a social network without impact and in the presence of impact on the security system

Considering the positive value of differential of the security function (Fig. 5), a study of the phase portrait of the information security system was carried out.

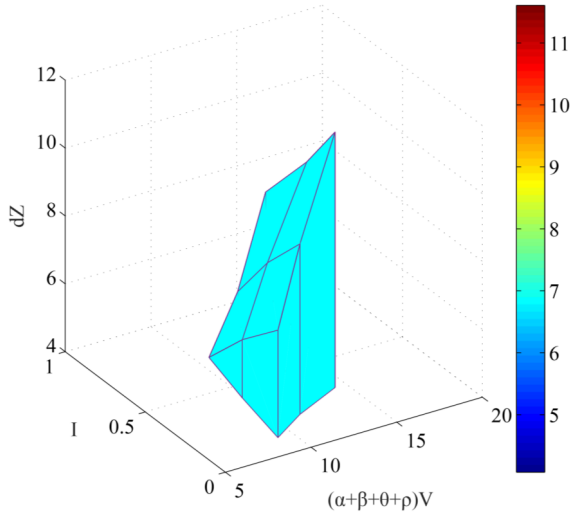

Fig. 5. The differential of a security function

In essence, the trajectory of the system is a projection of the integration curve of this system onto phase space. Since there are some conditions of existence and uniformity of solving the Cauchy problem, each solution of the equation (36) matches one trajectory and only one trajectory passes through each point of phase space. Therefore, the intersection of two different trajectories is impossible.

The output equation is:

$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2 Z=$$

$$=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1\gamma$$

$$+\beta_1\sum_{k=2}^{\infty}\left(K_kZ_0^k\sin^k\omega t\right)-\beta_2\sum_{k=2}^{\infty}\left(L_kI_0^k\sin^k\omega t\right)-$$

$$-\beta_2\sum_{k=2}^{\infty}\left(L_kI_0^k\sin^k\omega t\right). \qquad (36)$$

The second-degree differential equation (36) is nonlinear. To solve this equation, the block diagram (Fig. 6) in the MATLAB/Multisim program [1] was applied.

The results of the program are shown in Fig. 7, 8.

The resistance of the SN security system in the presence of impact on it was studied.

The behavior of SN resembles the behavior of a biological object. Assumption: the amplitude of impact is nonlinear in time. That is why the following considerations are permissible.

We considered the system in which the impact of harmful objects on it and the immune response of the system were modeled.

It is accepted that the dynamics of a harmful object corresponds to the logistic model. An increase in a harmful infection depends on its initial status, an increase caused by the immune response, and its own density effect, while a change in the immune response depends on its original status, natural decline, stimulation, which leads to the increased response, and the damage caused by a harmful object. Finally, the relative characteristic of the damaged organ depends on the density of a harmful object and its natural degeneration.

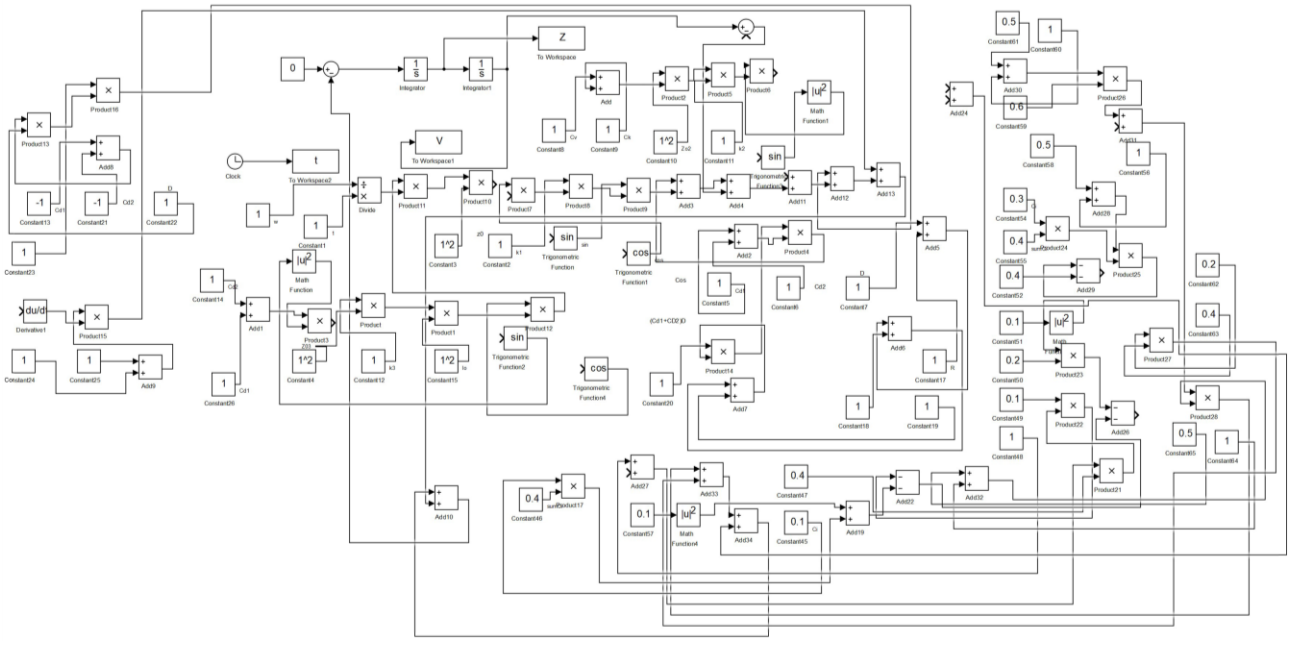

Fig. 6. Block diagram of the phase program in the Multisim program, taking into consideration the attack unit

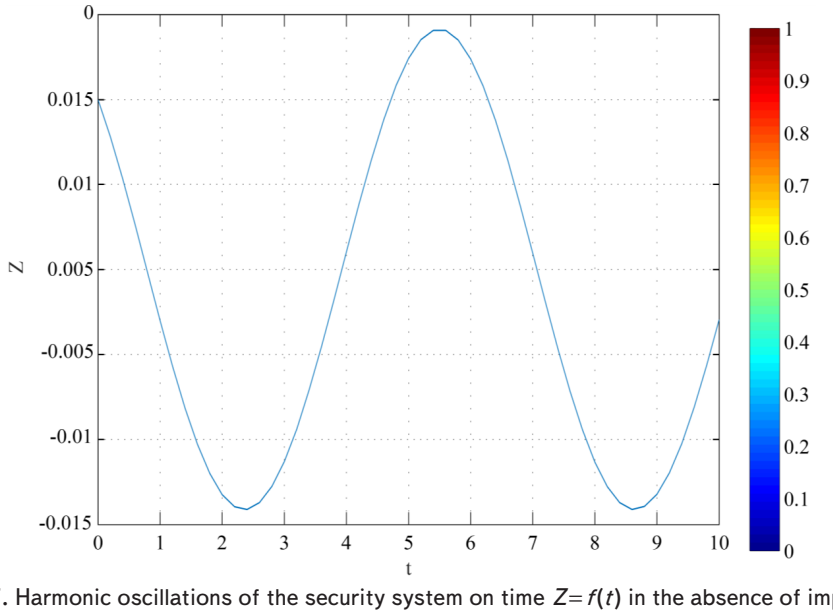

Fig. 7. Harmonic oscillations of the security system on time $Z = f(t)$ in the absence of impact

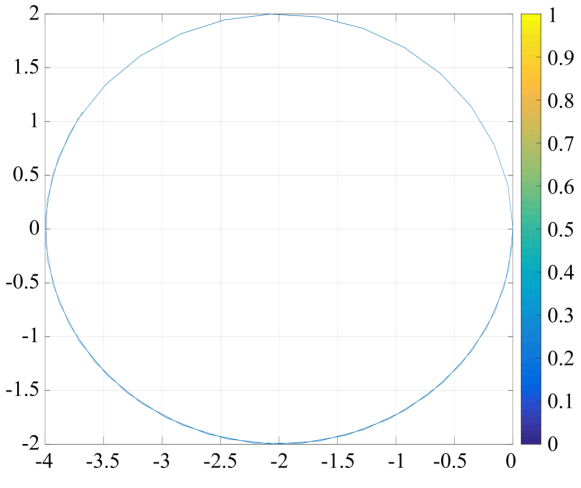

Fig. 8. Phase portrait of the system of protection against users' interaction parameters in the absence of impact

Then the dynamics of the system can be described using the following system of differential equations [29]:

$$\begin{cases} dP/dt = \beta P - \gamma IP - \beta_0 P^2, \\ dI/dt = \mu - \alpha I + bIP - \eta\gamma IP, \end{cases} \quad (37)$$

where $P(t)$ is the density of harmful objects, $I(t)$ is the immune status of the system, β is the coefficient of the rate of a harmful object increase, γ is the coefficient of the rate of decomposition of a harmful object through its interaction with the immune system of a network, β_0 is the coefficient of intraspecific interference of harmful objects, μ is the rate of the growth of the immune system, a is the coefficient of the natural rate of its decomposition, b is the stimulating rate of the growth of immune system through its interaction with harmful objects, η is the coefficient of its decomposition through the interaction with a harmful object, α is the coefficient of the rate of growth of the damaged node through the harmful object.

This is nothing else but a «predator-prey» equation system. Graphic interpretation is shown in Fig. 9, 10. Phase portraits of the security system are shown in Fig. 11.

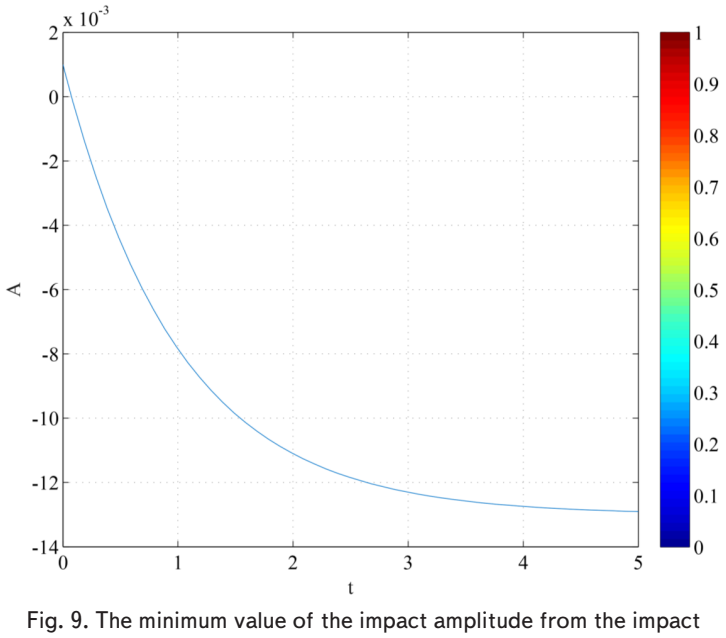

Fig. 9. The minimum value of the impact amplitude from the impact time — all parameters (36) are equal to 0.1 a.u.

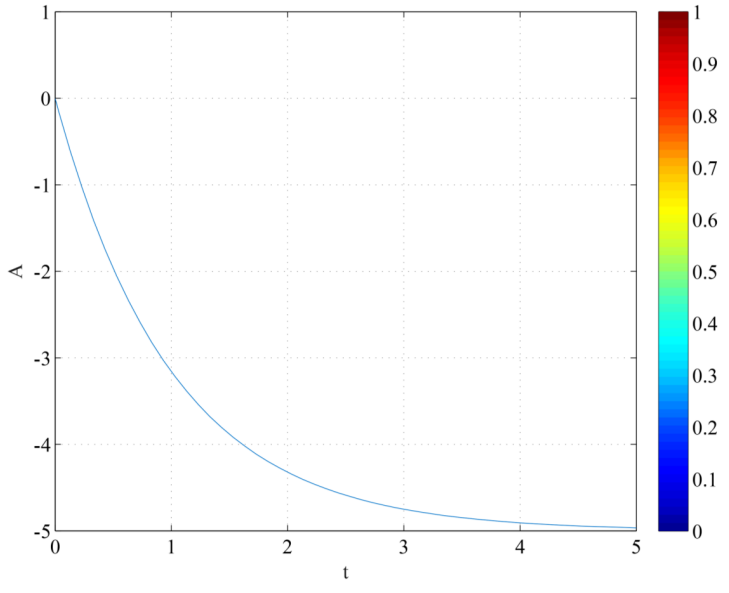

Fig. 10. Maximum value of the impact amplitude from the impact time — all parameters (36) are equal to 1 a.u.

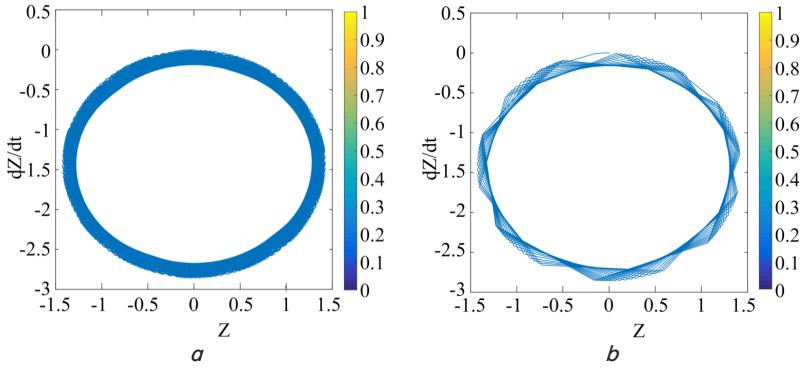

Fig. 11. Phase portrait of the security system:
a — from the parameters of impacts — 0.5 according to (36); *b* — the maximum value of the impact amplitude

The above results of the study of the resistance of the security system in the SN make it possible to assert that it is resistant even at the maximum value of the impact amplitudes in the operation range of parameters and at different values of the specific parameters of the network – users' interaction. That is, there opens the ability to ensure reliable information security.

6. Discussion of results of studying the security level of information space of social networks, taking into consideration users' relationships

Dependence (1) shows the classic approach to personal data security. The system of linear differential equations (5), which described the system of social network security, was obtained. The stationary position of the system described by systems of equations (6), (10) was found. The solution to the system of equations (5) was obtained by the method of «small deviations» (12). The equation of harmonic oscillator was obtained by differentiating the first equation of the system (12). The solution to the harmonic oscillator equation was divided into three cases, depending on the ratio of the system frequency and the fading coefficient (19) to (21).

It was found that the information security system is nonlinear. This is due to the fact that unfading oscillations of the security system were found beyond the resonant area (Fig. 3). This caused further studies of the nonlinear security system.

Modeling the nonlinear security system, taking into consideration the impact of specific parameters and parameters of users' interaction, making it possible to obtain quantitative indicators of the impact of specific parameters of the social network, including interaction, on the security indicator (29), (36) (Fig. 4). This is due to the fact that modeling correctly used mathematical apparatus, substantiated theoretical statements, as well as proved the theoretical results by the results of modeling the process of information security in social networks during the external impact on the system.

Owing to (36), further studies of the resistance of the nonlinear system, taking into consideration the action of harmful objects, were carried out. The study of the resistance of the security system in the social network without the impact and in the presence of impact on the security system made it possible to obtain graphical representations of oscillations in the security system depending on time (Fig. 7) and behavior of the system in the phase plane (phase portraits) (Fig. 11). This is due to the fact that the obtained phase portraits are closed curves and have no bifurcation points. Due to this, it was concluded that the security system is stable, taking into consideration the existence of the greatest impacts.

The specific features of the proposed method and the obtained results include obtaining quantitative indicators of information protection from specific parameters of the social network, including those from the parameters of users' interaction. The existing research methods do not make it possible to obtain such indicators. Unlike previous studies, the obtained results indicate the nonlinearity of the security system of the SN. It was proved that the security system of the SN is resistant even to external maximum influences and specific interaction parameters in the operation range of parameters. However, it should be noted that it is desirable to obtain a mathematical model of the impact of a complex of specific network parameters on the security system.

The practical result of the research is that according to the graphs of the oscillations of the actual system of social network security and phase portraits, it is possible to track the existence of impacts on the security system and their intensity. This will make it possible to apply appropriate security measures in real time.

This study can be subsequently developed by using the known specific parameters of social networks (mutual influence, average distance between users, network expansion, clustering coefficient, coefficient of information spread, network centrality, etc.) and by identifying new factors and parameters.

7. Conclusions

1. The study of the linear model of interaction between users in the SN made it possible to proceed from the classical approach to systems of differential equations, which made it possible to obtain mathematical dependences between the specific parameters of a social network, including interaction and security indicator. As a result of the study, the equations of a harmonic oscillator with a fading amplitude were obtained. This allowed determining the frequency of oscillations, the period, and the coefficient of fading of the security system. Mathematical dependences of the behavior of the security system in the pre-resonance, resonance, and post-resonance areas were obtained. This approach enables proceeding to the study of the linearity of the security system.

2. Verification of linearity of the system of information security indicated its nonlinearity. This was proved by considering three options for solving the oscillator equation near the stationary state of the system and made it possible to note that based on the conditions of the ratio of dissipation and proper frequency of oscillation of magnitude, the fading of the latter, to a certain value, happens periodically. The amplitude of oscillations is a fading amplitude under an exponentially fading law. A more visual analysis of the behavior of the system was performed by moving from the differential form of equations to discrete form and modeling a certain interval of the system's existence. Analysis of iterations of oscillations of the security system revealed its nonlinearity. This made it possible to proceed to the study of a nonlinear protection system.

3. The system of nonlinear equations was constructed, which made it possible by analysis and solution to obtain mathematical quantitative results of the impact of specific parameters and parameters of users' interaction on the system of social network security and their graphic interpretation. The parameters of the impact of users' interaction on the security system show a significant impact on the security indicator of up to 100 %. This approach to the research enabled us to proceed to studying the resistance of the security system.

4. The study of the resistance of the security system in a social network without any impact and in the presence of impact on the security system was carried out using a block diagram created in the MATLAB/Multisim program. Due to the obtained graphic interpretations of the oscillations of the security system and phase portraits, the resistance of the security system was proved even in the presence of maximum impact.

References

1. Newcomb, T. M. (1953). An approach to the study of communicative acts. Psychological Review, 60 (6), 393–404. doi: https://doi.org/10.1037/h0063098
2. Cartwright, D., Harary, F. (1956). Structural balance: a generalization of Heider's theory. Psychological Review, 63 (5), 277–293. doi: https://doi.org/10.1037/h0046049
3. Glaser, W. A. (1959). Job Mobility between Government and other Social Structures. Political Research, Organization and Design, 3 (3), 20–23. doi: https://doi.org/10.1177/000276425900300307
4. Bavelas, A. (1950). Communication Patterns in Task-Oriented Groups. The Journal of the Acoustical Society of America, 22 (6), 725–730. doi: https://doi.org/10.1121/1.1906679
5. Festinger, L. (1954). A Theory of Social Comparison Processes. Human Relations, 7 (2), 117–140. doi: https://doi.org/10.1177/001872675400700202
6. Radcliffe-Brown, A. R. (1935). On the Concept of Function in Social Science. American Anthropologist, 37 (3), 394–402. doi: https://doi.org/10.1525/aa.1935.37.3.02a00030
7. Heider, F. (1946). Attitudes and Cognitive Organization. The Journal of Psychology, 21 (1), 107–112. doi: https://doi.org/10.1080/00223980.1946.9917275
8. Berkman, L. (2020). The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research, 8 (5), 1920–1925. doi: https://doi.org/10.30534/ijeter/2020/73852020
9. Semenov, S., Weilin, C. (2020). Testing process for penetration into computer systems mathematical model modification. Advanced Information Systems, 4 (3), 133–138. doi: https://doi.org/10.20998/2522-9052.2020.3.19
10. Semenov, S., Weilin, C., Zhang, L., Bulba, S. (2021). Automated penetration testing method using deep machine learning technology. Advanced Information Systems, 5 (3), 119–127. doi: https://doi.org/10.20998/2522-9052.2021.3.16
11. Cherneva, G., Khalimov, P. (2021). Mutation testing of access control policies. Advanced Information Systems, 5 (1), 118–122. doi: https://doi.org/10.20998/2522-9052.2021.1.17

12. Liqiang, Z., Weiling, C., Rabčan, J., Davydov, V., Miroshnichenko, N. (2021). Analysis and comparative studies of software penetration testing methods. Advanced Information Systems, 5 (2), 136–140. doi: https://doi.org/10.20998/2522-9052.2021.2.20
13. Mashkov, V. A., Barabash, O. V. (1998). Self-checking and self-diagnosis of module systems on the principle of walking diagnostic kernel. Engineering Simulation. Amsterdam: OPA, 15 (1), 43–51.
14. Radkevych, O. P. (2012). Konfidentsiynist personalnoi informatsiyi v sotsialnykh merezhakh. Visnyk Vyshchoi rady yustytsiyi, 3 (11), 215–224.
15. Laptiev, O., Shuklin, G., Savchenko, V., Barabash, O., Musienko, A., Haidur, H. (2019). The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), 8 (6), 2840–2846. doi: https://doi.org/10.30534/ijatcse/2019/26862019
16. Podobnik, V., Lovrek, I. (2015). Implicit Social Networking: Discovery of Hidden Relationships, Roles and Communities among Consumers. Procedia Computer Science, 60, 583–592. doi: https://doi.org/10.1016/j.procs.2015.08.185
17. Farseev, A., Nie, L., Akbari, M., Chua, T.-S. (2015). Harvesting Multiple Sources for User Profile Learning. Proceedings of the 5th ACM on International Conference on Multimedia Retrieval. doi: https://doi.org/10.1145/2671188.2749381
18. Chorley, M. J., Whitaker, R. M., Allen, S. M. (2015). Personality and location-based social networks. Computers in Human Behavior, 46, 45–56. doi: https://doi.org/10.1016/j.chb.2014.12.038
19. Wilson, C., Sala, A., Puttaswamy, K. P. N., Zhao, B. Y. (2012). Beyond Social Graphs. ACM Transactions on the Web, 6 (4), 1–31. doi: https://doi.org/10.1145/2382616.2382620
20. Souri, A., Nourozi, M., Rahmani, A. M., Jafari Navimipour, N. (2019). A model checking approach for user relationship management in the social network. Kybernetes, 48 (3), 407–423. doi: https://doi.org/10.1108/k-02-2018-0092
21. Grevtsov, V. E. (2010). Razvitie sotsial'nyh svyazey i otnosheniy v virtual'nyh soobschestvah. Sotsiosfera, 1, 59–61.
22. Kaltenbrunner, A., Scellato, S., Volkovich, Y., Laniado, D., Currie, D., Jutemar, E. J., Mascolo, C. (2012). Far from the eyes, close on the web. Proceedings of the 2012 ACM Workshop on Workshop on Online Social Networks – WOSN '12. doi: https://doi.org/10.1145/2342549.2342555
23. Akhramovych V. M. (2019). Model of Mutual Relationship of Users in Social Networks. Modern Information Security, 3, 42–50. doi: https://doi.org/10.31673/2409-7292.2019.034250
24. Asim, Y., Malik, A. K., Raza, B., Shahid, A. R. (2019). A trust model for analysis of trust, influence and their relationship in social network communities. Telematics and Informatics, 36, 94–116. doi: https://doi.org/10.1016/j.tele.2018.11.008
25. Bouffard, S., Giglio, D., Zheng, Z. (2021). Social Media and Romantic Relationship: Excessive Social Media Use Leads to Relationship Conflicts, Negative Outcomes, and Addiction via Mediated Pathways. Social Science Computer Review, 089443932110135. doi: https://doi.org/10.1177/08944393211013566
26. Meleshko, Y. (2018). Method of collaborative filtration based on associative networks of users similarity. Advanced Information Systems, 2 (4), 55–59. doi: https://doi.org/10.20998/2522-9052.2018.4.09
27. Barabash, O., Lukova-Chuiko, N., Sobchuk, V., Musienko, A. (2018). Application of Petri Networks for Support of Functional Stability of Information Systems. 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC). doi: https://doi.org/10.1109/saic.2018.8516747
28. Akhramovich, V., Hrebennikov, A., Tsarenko, B., Stefurak, O. (2021). Method of calculating the protection of personal data from the reputation of users. Sciences of Europe, 80, 23–31. doi: https://doi.org/10.24412/3162-2364-2021-80-1-23-31
29. Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), 13 (1), 15–21. Available at: https://www.ijcnis.org/index.php/ijcnis/article/view/4882
30. Mahmoudi, A., Yaakub, M. R., Bakar, A. A. (2019). The Relationship between Online Social Network Ties and User Attributes. ACM Transactions on Knowledge Discovery from Data, 13 (3), 1–15. doi: https://doi.org/10.1145/3314204
31. Mahmoudi, A., Yaakub, M. R., Abu Bakar, A. (2018). New time-based model to identify the influential users in online social networks. Data Technologies and Applications, 52 (2), 278–290. doi: https://doi.org/10.1108/dta-08-2017-0056
32. Meleshko, Y., Drieiev, O., Drieieva, H. (2020). Method of identification bot profiles based on neural networks in recommendation systems. Advanced Information Systems, 4 (2), 24–28. doi: https://doi.org/10.20998/2522-9052.2020.2.05