http://doi.org/10.35784/iapgos.5720

received: 25.12.2023 | revised: 18.01.2024 | accepted: 11.02.2024 | available online: 31.03.2024

METHOD FOR CALCULATING THE INFORMATION SECURITY INDICATOR IN SOCIAL MEDIA WITH CONSIDERATION OF THE PATH DURATION BETWEEN CLIENTS

Volodymyr Akhramovych[1], Yuriy Pepa[2], Anton Zahynei[1], Vadym Akhramovych[3], Taras Dzyuba[4], Ihor Danylov[1]

[1]State University of Information and Communication Technologies, Department of Information and Cybersecurity Systems, Kyiv, Ukraine, [2]State University of Information and Communication Technologies, Department of Robotics and Technical Systems, Kyiv, Ukraine, [3]National Academy of Statistics, Accounting and Auditing, Computing Center, Kyiv, Ukraine, [4]State University of Information and Communication Technologies, Department of Information and Cybersecurity Management, Kyiv, Ukraine

Abstract. *Heterogeneous differential dependencies of the information security indicator (HDISI) in social media (SM) were analyzed, taking into account the duration of the path between clients (UDPC). The resilience of the information security indicator system (RSIIS) was also determined. The HDISI in SM was developed based on UDPC conditions. It uses modern methods and techniques, including a non-specific method. The conditions of a fixed precondition were formed according to the time grid. This dependency provides a comprehensive explanation of how the previous transformation is replaced by the elapsed period. SM is a set of clients and their types of communication. Clients can be individuals, populations, settlements, or countries. Communication is understood as more than just the transmission and receipt of information. It also includes interaction, the exchange of knowledge and expertise, and discussion. Under the angle of mathematics, the HDISI model based on non-homogeneous differential equations (NDE) was analyzed and its transcendental study was done. The transcendental study of nonlinear HDISI models in SM showed that the characteristics of UDPC significantly affect the information security indicator (ISI) - up to one hundred percent. Phase diagrams (PDs) of ISI were studied, which indicate the highest ISI even at the maximum parameters of malicious actions. For the first time, the analysis of designed HDISI structures was carried out and numerical criteria between the capabilities of UDPC and the measures of ISI, as well as the highest ISI, were obtained, which shows the scientific content of this article.*

Keywords: social media, mathematical models, information security indicator

METODA OBLICZANIA WSKAŹNIKA BEZPIECZEŃSTWA INFORMACJI W MEDIACH SPOŁECZNOŚCIOWYCH Z UWZGLĘDNIENIEM DŁUGOŚCI ŚCIEŻKI MIĘDZY KLIENTAMI

Streszczenie. *Przeanalizowano niejednorodne zależności różnicowe wskaźnika bezpieczeństwa informacji (HDISI) w mediach społecznościowych (SM), biorąc pod uwagę długość ścieżki między klientami (UDPC). Określono również odporność systemu wskaźników bezpieczeństwa informacji (RSIIS). HDISI w SM został opracowany w oparciu o warunki UDPC. Wykorzystuje on nowoczesne metody i techniki, w tym metodę niespecyficzną. Warunki stałego warunku wstępnego zostały utworzone zgodnie z siatką czasową. Ta zależność zapewnia kompleksowe wyjaśnienie, w jaki sposób poprzednia transformacja jest zastępowana przez upływający okres. SM to zbiór klientów i ich rodzajów komunikacji. Klientami mogą być jednostki, populacje, osady lub kraje. Komunikacja jest rozumiana jako coś więcej niż tylko przekazywanie i odbieranie informacji. Obejmuje również interakcję, wymianę wiedzy i doświadczenia oraz dyskusję. Pod kątem matematyki przeanalizowano model HDISI oparty na niejednorodnych równaniach różniczkowych (NDE) i przeprowadzono jego transcendentalne badanie. Transcendentalne badanie nieliniowych modeli HDISI w SM wykazało, że charakterystyka UDPC znacząco wpływa na wskaźnik bezpieczeństwa informacji (ISI) – nawet do stu procent. Zbadano diagramy fazowe (PDs) ISI, które wskazują na najwyższy ISI nawet przy maksymalnych parametrach złośliwych działań. Po raz pierwszy przeprowadzono analizę zaprojektowanych struktur HDISI i uzyskano kryteria liczbowe między możliwościami UDPC a miarami ISI, a także najwyższym ISI, co pokazuje naukową treść tego artykułu.*

Słowa kluczowe: media społecznościowe, modele, wskaźnik bezpieczeństwa informacji

Introduction

Subject of research: To analyze the information security indicator (ISI) based on the HDISI.

In the future, the characteristics from table 1 will be used in the dependencies.

HDISI is deployed as recommended when the system characteristics correspond to reality, then attention is paid to its non-approximate class, and the identified interdependencies give a complete understanding of the replacement of the previous state from that time for this time. The variation of the ISI value is detected by prototypical NDE. The position of the system's values and its characteristics are interdependent, which makes it possible to solve NDE with the existing characteristics.

The closest in meaning, works [1, 2, 5, 8, 9]. In work [2], the analysis of the impact, taking into account the duration of the path between clients and other characteristics of the SM on the ISI was performed. It was concluded that the pattern is nonlinear. In the works [1, 5, 8, 9], the mathematical pattern of the ISI in the SM is considered and analyzed, and the characteristics are also taken into account: client interaction, media clustering parameters, information dissemination in media, client relationships and their impact on the ISI pattern.

In the works [3, 4, 6, 7, 10–18], the digital relationships between the characteristics of clients and the media itself and the characteristics of ISI have not been analyzed. This is a key flaw in the cited works.

Table 1. Characteristics that are in use

Characteristic	Description of a characteristic
Z	ISI metric
R_z	characteristic that shows numerical characteristics of the RSIIS
U_v	characteristic that shows the speed of numerical information conversions that are transmitted
U_k	characteristic that shows the speed of numerical information conversions between the information size and its extraction
n_i	unmetrical value of the vertices that are present in the media over time t
P	information volume in the SM
U_{d1}	characteristic that shows the activity of the ISI before information extraction
U_{d2}	characteristic that shows the activity of taking into account the path length between clients on the ISI
S, Q, P_0, C_0	linear gradients
E	density of harmful entities
W	unsusceptible system rank
δ	prudence indicator of the spread of harmful entities
Characteristic	Description of a characteristic
φ	prudence indicator of harmful entity removal in interaction with the media's immune system
λ_0	interspecies interference indicator of harmful entities
ϑ	growth rate of the immune system
ρ	natural decomposition rate indicator of the immune system
ς	compelling elasticity of immune system increase upon interaction with harmful entities
ξ	indicator of elasticity of immune system removal upon interaction with harmful entities
A	amplitude of oscillations

The justified survey project:

- survey of the quantitative correspondence between the characteristics of the path duration between UDPC and the characteristics of ISI;
- survey of the resilience of the ISI system in the SM from potential impacts in the analysis of phase diagrams.

The addition of adequate "at your fingertips" information, activities and methods for analyzing the quantitative effect of the characteristics of UDPC on the characteristics of ISI to information security workers in the SM is seen as an applied benefit.

The study of the amplitudes of the oscillations of ISI and phase diagrams shows the existing threats and their strength in real time. This will provide the ability for information security workers to make decisions based on the characteristics of ISI in real time.

1. Literature survey and problem statement

In [1], the effects of the path duration between clients and other components of social media characteristics on the information security indicator were analyzed. The model status is nonlinear. The disadvantage is that a nonlinear model for calculating the information security indicator (NMISI) in social media taking into account the path duration between clients has not been developed and investigated.

A general shortcoming of the works [1, 3–18] is that the dependence of NMISI in social media, taking into account UDPC, has not been developed and investigated.

In [5], the effects of ISI were analyzed taking into account the characteristics of client interaction

In [8], the effects of ISI were analyzed taking into account the characteristics of media clustering and the amount of information in social media.

In [9], the effects of ISI were analyzed taking into account the characteristics of propagation and the amount of information in social media

In [1], the effects of ISI were analyzed taking into account the characteristics of client relationship parameters and the amount of information in social media.

In [15], it is pointed out that the storage and exchange of large amounts of information poses privacy problems for the clients of these websites. To prevent these problems, it is necessary to provide a strict privacy policy, data protection mechanisms, reliable and built-in programs that help protect the privacy of clients by limiting the people who have access to the client's personal information. A program is proposed that offers social media users a trust architecture based on reputation. It creates and tracks social reputation, finds circles of communication, and helps users easily, meaningfully, and automatically group their friends to protect their privacy. This system provides grouping of clients through an automated system into different social circles by analyzing the client's social connections and depending on what common information or application they share that other users should not have access to.

In [3], a conceptual approach to the analysis of online social media is developed. The issues of social media management are considered.

In [6, 14], it is pointed out that analysts note that the main causes of incidents in Internet resources are related to human factor, mass hacking of IoT devices and cloud services. This problem is especially exacerbated by the strengthening of the digital humanistic nature of education, the growing role of social media in human life in general. Therefore, the issue of protecting personal information is constantly growing. To solve this problem, we propose a methodology for evaluating the dependence of personal data protection on the volume of information in the system and trust in social media.

In [11], programs are modelled as finite automates and the required profile attributes of the client are used as the conditions that govern the execution of the program. The problems of generalizing the minimum attributes are formulated, and a solution is proposed that reflects the shortest path problem in order to find the minimum set of generalization attributes required to access the program services. The feasibility of this approach is evaluated under the conditions of verifying the implementation of the concept and conducting customer research.

In [4], it is pointed out that the protection of location privacy of clients still remains an open task for social media service providers. It has been shown that hiding the real person and choosing a pseudonym does not guarantee the protection of the client's privacy, since privacy can be violated only by analyzing location data. This is indeed a big problem, since other personal information of clients can be disclosed by analyzing their location data (for example, home address, health status, interests, etc.). In this regard, a distance-based privacy protection mechanism (DBLP2) is developed, a customized location privacy protection approach that is uniquely designed for social media clients. It uses the concept of social distance to generalize client location data before publishing it on social media. The level of generalization is determined taking into account the social distance between clients. Secondly, cryptographic methods for protecting location privacy in geolocation services (LBS) and social networks are considered.

In [7], computer viruses are studied in the form of theory and experiments, as well as security. An epidemiological model of virus spread and cleaning.

In [10], it is reported that if A tells B, and B tells C (and A does not tell C), then clients A and C are at a distance of two. How many clients are at different distances from each client can be important for understanding the differences between clients in the constraints and opportunities they have as a result of their position. That is, can actor A reach client B in several ways? Sometimes multiple links can indicate a stronger connection between two clients than one link.

In [17], the distance between clients in media can be an important macro-characteristic of the media as a whole. Where distances are large, it may take a long time for information to spread among the population. It may also be that some clients are completely unaware of it and are under the influence of others – even if they are technically available, the costs may be too high to conduct the exchange. The variability between clients in the distances they have from other clients can be the basis for differentiation and even stratification. Those clients who are closer to others may have more power than those who are more distant.

In [13], it is noted that one of the most acute problems of social media is the disclosure and unauthorized access to information, data and communication between clients, which is a kind of violation of their privacy, which can be done by social media providers, especially unauthorized clients. One way to protect privacy is to use encryption.

In [16, 18], it is proposed, in particular, to use the distance between two clients to predict whether they are friends. It is first shown that distance is a useful indicator for dividing into friends and strangers. Taking into account the popularity of the location together with the distance, the difference between friends and strangers becomes even greater. It is further shown that distance can be used for effective link prediction. A machine learning classifier is used to further improve the prediction efficiency.

In the work [12], presents nonlinear models, their characteristics, and methods of determination. The results of calculations are presented.

2. Concept and objectives of analysis

The purpose of the analysis is to improve the methodology of ISI in SM, taking into account the characteristics of the UDPC.

The most closely related works are [1, 2, 5, 8, 9], which analyze the impact of parameters such as the size of social media development, user interactions and relationships, network clustering, the spread and volume of information, and their actions on ISI. In [2] analyzed the impact of the duration of the path between clients and other components of the characteristics of social media on the information security indicator. It was shown that the model is nonlinear. The error is that a nonlinear ISI model has not been developed or analyzed. This article investigates the indicated problem.

The scientific article explores the relationship between the characteristics of UDPC and the characteristics of ISI in the analysis and rationalization of ISI in SM.

The main research perspectives are:

- investigating the numerical correspondence between the characteristics of UDPC and the characteristics of ISI;
- investigating the RSIIS in SM from potential impacts based on PD.

Motivations and methods of testing

The paper is devoted to the definition and analysis of the HDISI in SM, with the processing of its characteristics and characteristics of the UDPC. ISI is calculated using indefinite cognitive imitation. The development and investigation were carried out on the basis of scientific thought, the plan of non-precise dependencies. This provided an opportunity to understand and nurture almost unfamiliar technological actions.

To master the HDISI in SM, NDE systems that depict ISI were developed.

The following were adopted: methods for obtaining the solution of NDE (cut-out technique, group search for the corresponding native dependence, etc.); finding characteristics in the MATLAB program. RSIIS from influences on ISI was carried out through the study of NDE and the electronic circuit developed in MATLAB/MULTISIM.

3. Proposed methodology

This methodology is a continuation of the developments outlined in [1, 5, 8, 9], which allowed us to develop these models in the direction of creating a methodology for determining quantitative indicators of information protection in social media from the influence of the distance between users and other media parameters.

3.1. Features ISI in SM considering characteristics UDPC

The graphical dependence of the differential [2] of the UDPC (Fig. 1), the differential of the ISI (Fig. 2) [2] are presented.

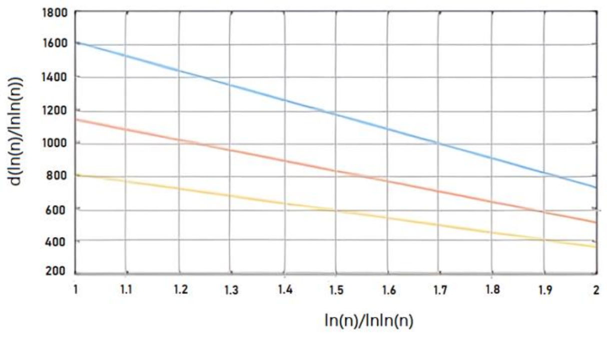

Fig. 1. Differential of the path duration function between clients

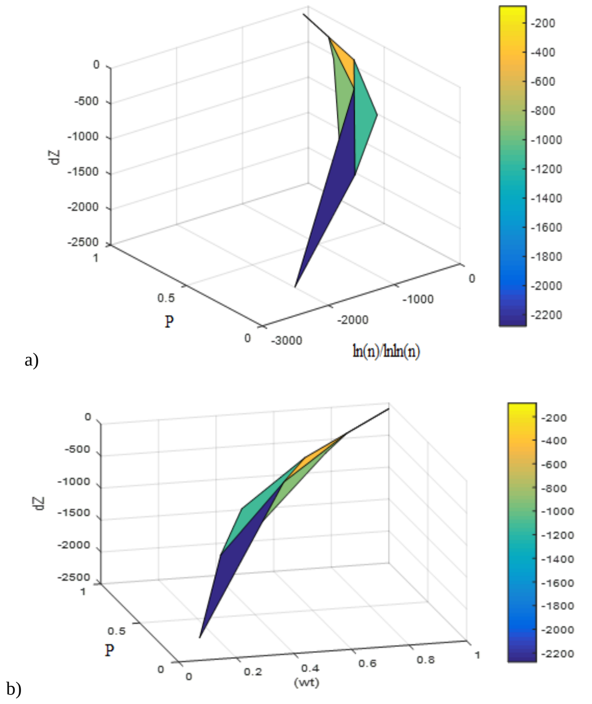

Fig. 2. Differential ISI: a) $dZ = f(P, \ln(n)/\ln\ln(n))$; b) $dZ = f(P, wt)$

To start, we will use a system of equations [1, 5, 8, 9].

The illustrated relationships show that the derivative of ISI is negative. Therefore, according to the Lyapunov theorem, the protection system is reliable and stable.

The ISI nonlinearity is negligible, which suggests that we can solve the dependencies using a successive approximation method.

$$P = P_1 + P_2 + P_3 + \ldots$$

$$Z = Z_1 + Z_2 + Z_3 + \ldots$$

We believe that when

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

$$P = P_0 \sin \omega t\ ,\ Z = R_0 \sin \omega t\ .$$

The equation can be expressed as follows:

$$\begin{cases} \frac{dP}{dt} = R_z Z + P\left(U_v + U_k\right) - S_2\left(P_0^2 \sin^2 \omega t\right) - \\ -S_3\left(P_0^3 \sin^3 \omega t\right) - \ldots \\ \frac{dZ}{dt} = \frac{\ln\ln n - n}{n(\ln\ln n)^2} - P\left(U_{d2} + U_{d1}\right) - Q_0\left(C_0^2 \sin^2 \omega t\right) - \\ -Q_0\left(C_0^3 \sin^3 \omega t\right) - \ldots \end{cases} \tag{1}$$

Let's generalize the equation:

$$\begin{cases} \frac{dP}{dt} = \alpha Z + \beta_1 P - \sum_{k=2}^{\infty} S_k P_0^k \sin^k \omega t \\ \frac{dZ}{dt} = \beta_2 P + \gamma - \sum_{k=2}^{\infty} Q_k C_0^k \sin^k \omega t \end{cases} \tag{2}$$

where

$$\alpha = R_z\ ,\ \beta_1 = U_v + U_k\ ,\ \beta_2 = -\left(U_{d2} + U_{d1}\right),\ \gamma = \frac{\ln\ln n - n}{n(\ln\ln n)^2}$$

We will use the process of elimination:

$$\frac{dZ}{dt} = \beta_2 P + \gamma - \sum_{k=2}^{\infty} Q_k C_0^k \sin^k \omega t \Rightarrow$$

$$\Rightarrow I = \frac{1}{\beta_2}\left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} Q_k C_0^k \sin^k \omega t\right) \Rightarrow$$

$$\Rightarrow \frac{dP}{dt} = \frac{1}{\beta_2}\left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega}\sum_{k=2}^{\infty}\left(kQ_k C_0^k \sin^{k-1} \omega t \cos \omega t\right)\right) \tag{3}$$

We substitute (3) into the first equation (2):

$$\frac{1}{\beta_2}\left(\frac{d^2Z}{dt^2}+\frac{1}{\omega}\sum\nolimits_{k=2}^{\infty}\left(kQ_kC_0^k\sin^{k-1}\omega t\cos\omega t\right)\right)=$$
$$\alpha Z+\frac{\beta_1}{\beta_2}\left(\frac{dZ}{dt}-\gamma+\sum\nolimits_{k=2}^{\infty}Q_kC_0^k\sin^k\omega t\right)-$$
$$-\sum\nolimits_{k=2}^{\infty}Q_kC_0^k\sin^k\omega t, \tag{4}$$

we will get:

$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2 Z=$$
$$=-\frac{1}{\omega}\sum\nolimits_{k=2}^{\infty}\left(kQ_kC_0^k\sin^{k-1}\omega t\cos\omega t\right)-$$
$$-\beta_2\sum\nolimits_{k=2}^{\infty}S_kP_0^k\sin^k\omega t \tag{5}$$

The general form of a homogeneous equation is:

$$Z''-\beta_1 Z'-\alpha\beta_2 Z=0 \tag{6}$$

eigenvalue equation: $\lambda^2-\beta_1\lambda-\alpha\beta_2=0$

This equation has a positive discriminant:

$$D=\beta_1^2+4\alpha\beta_2>0\Rightarrow\lambda_{1,2}=\frac{\beta_1\pm\sqrt{\beta_1^2+4\alpha\beta_2}}{2} \tag{7}$$

We will obtain:

$$Z_{od}(t)=c_1e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}+c_2e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}$$

common solution of homogeneous equation.

The calculation of the general inhomogeneous equation will be performed by the method of separation of arbitrary constants, where $c_1'(t)$, $c_2'(t)$ is established as:

$$\begin{cases} c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}+c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}=0 \\ c_1'(t)\dfrac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}+ \\ +c_2'(t)\dfrac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}=N(t) \end{cases} \tag{8}$$

Thereafter:

$$N(t)=-\frac{1}{\omega}\sum\nolimits_{k=2}^{\infty}\left(kQ_kP_0^k\sin^{k-1}\omega t\cos\omega t\right)-$$
$$-\beta_1\gamma-\beta_1\sum\nolimits_{k=2}^{\infty}Q_kP_0^k\sin^k\omega t$$

$$Z(s)=\int_{t_0}^{t}\left(N(s)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}\frac{e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\right)ds \tag{9}$$

From equations (8, 9) we will expand:

$$c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}=-c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}}\Rightarrow$$
$$\Rightarrow c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\left(-\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}+\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}\right)= \tag{10}$$
$$=N(t)$$

or:

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

Now we will expose:

$$c_2(t)=-\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt \tag{12}$$

$$c_1(t)=\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt \tag{13}$$

By carrying out an analysis of equations (7–9) together, we will obtain:

$$Z(s)=\int_{t_0}^{t}\left(N(s)-e^{\frac{-\beta_1-\sqrt{\beta_1^2}+4\alpha\beta_2}{2}s}\frac{e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\right)ds-$$
$$-\int_{t_0}^{t}\left(N(s)-e^{\frac{-\beta_1-\sqrt{\beta_1^2}+4\alpha\beta_2}{2}s}\frac{e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}}{\sqrt{s\beta_1^2+4\alpha\beta_2}}\right)ds \tag{14}$$

To confirm the assessment taking into account the UDPC on the ISI, we will conduct modeling. Graphical dependencies of the ISI are presented in Fig. 3.

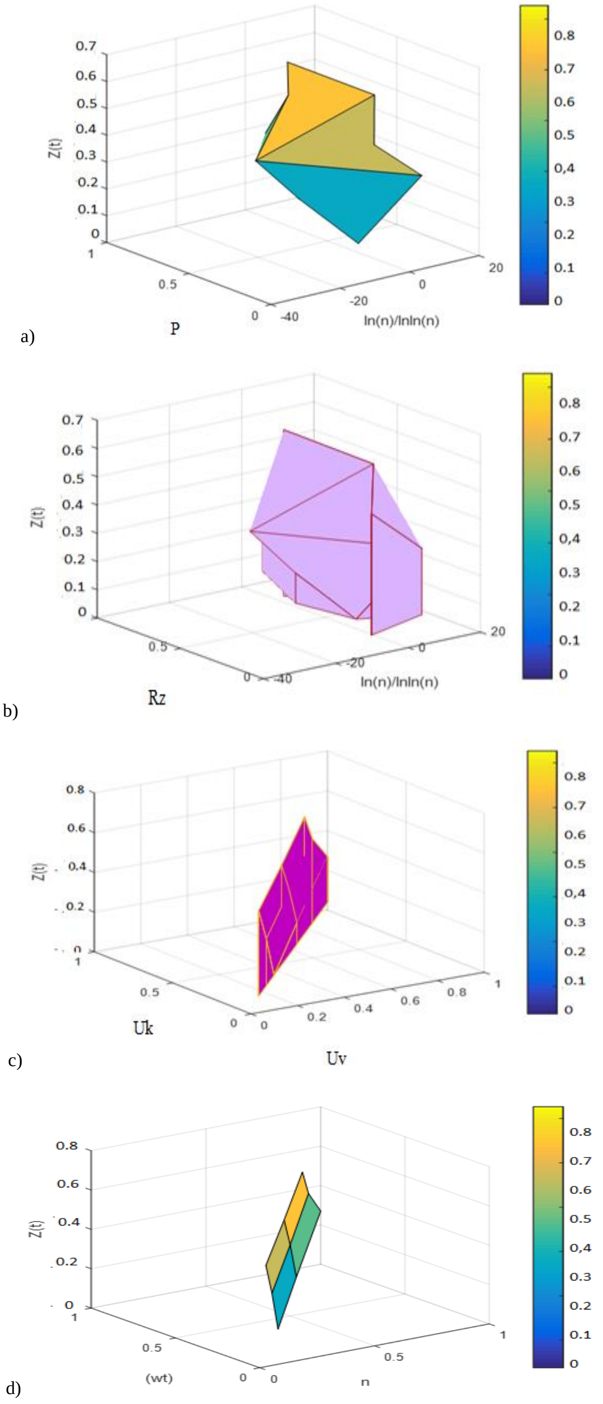

Fig 3. Dependences ISI: a) $Z(t)=f(P,\ln(n)/\ln\ln(n))$ *, b)* $Z(t)=f(R_z,\ln(n)/\ln\ln(n))$ *, c)* $Z(t)=f(U_k,U_v)$ *, d)* $Z(t)=f(wt,n)$

3.2. Formation PD ISI

Output dependency similar to [4, 7, 10, 11, 15]:

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

$$=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kS_kP_0^k\sin^{k-1}\omega t\cos\omega t\right)-$$

$$-\beta_1\left(\frac{\ln\ln n-n}{n(\ln\ln n)^2}\right)+\beta_1\sum_{k=2}^{\infty}S_kP_0^k\sin^k\omega t-$$

$$-\beta_2\sum_{k=2}^{\infty}Q_kC_0^k\sin^k\omega t \qquad (15)$$

The illustrated phase diagrams are elliptical and closed, which indicates that the ISI system is reliable and stable.

Electronic circuit components identification for Fig. 5.

The analysis of the dependence was performed in the Multisim system. An electronic circuit was developed (Fig. 6). The results of the system's operation are presented in Fig. 4.

Thanks to the developed phase diagram, it was possible to model the behavior of the social media information protection system depending on various parameters and media loads. The graphical results are shown in Figs. 4b, c.

The results obtained in Figs. 4b, c are closed oscillating curves resembling a closed ellipse, indicating that the social media information protection system is resistant to various types of influences in the operating range of parameters. Fig. 4a shows the oscillations of the protection system without external influences.

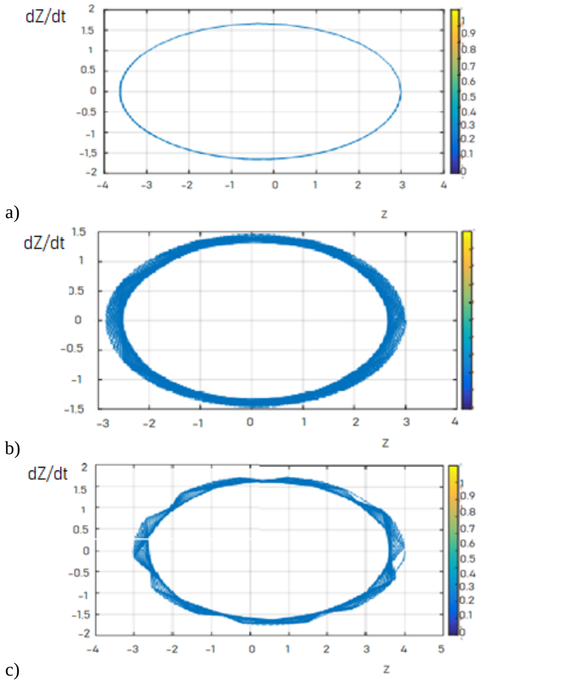

Fig. 4. Phase diagrams of ISI: a) in the absence of influences; b) when the influence is half its maximum value; c) at its maximum value

$\frac{1}{s}$	Integrator	+ +	Variable or constant adder
z	Data transfer element to workspace	x́	Multiplication or division of variables or constants
c	Constant	Sin	Trigonometric functions
dU/dt	Derivative	|U|	Ascension to a power or logarithm

Fig. 5. Electronic circuit components

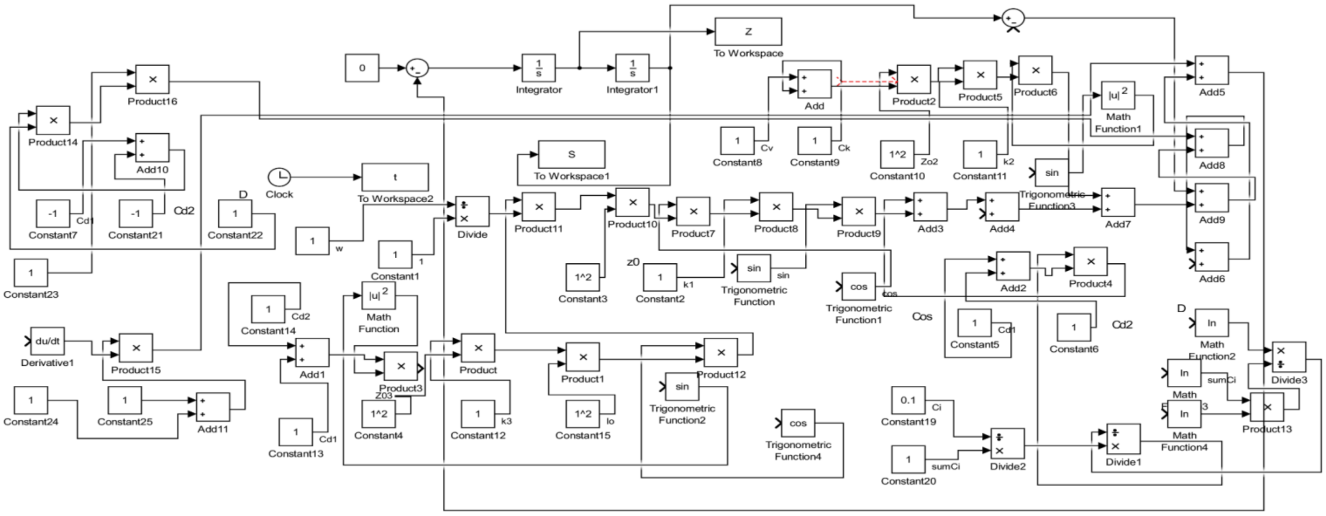

Fig. 6. Phase diagram circuit in Multisim

3.3. Load simulation for ISI

We are developing a system to simulate the impact on the system and the immune resistance of the system. We assume that the dynamics of harmful actions behaves in a logistic pattern. The growth of harmful infection depends on its initial state, weakening caused, including, by immune influence, and the effect of density, while the mutation of the immune response depends on its initial state, natural reduction, activation that leads to the increase of the response, and damage from harmful actions. The comparative characteristic of the injured subject depends on the density of the harmful object and its natural reduction. We will reproduce such a dynamic system with the support of a further system of differential dependencies:

$$\begin{cases}\dfrac{dE}{dt}=\delta E-\varphi WE-\lambda_0E^2\\[2mm] \dfrac{dW}{dt}=\vartheta-\rho W+\varsigma WP-\xi\varphi WE\end{cases} \qquad (16)$$

This is a predator-prey system. Graphical dependencies of the amplitude of influence according to equation (16) are presented in Figs. 7, 8.

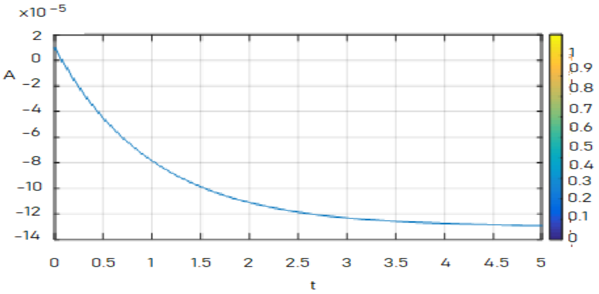

Fig. 7. The smallest amplitude of the force of action of a destructive object. All characteristics (16) are equal to 0.1 relative units

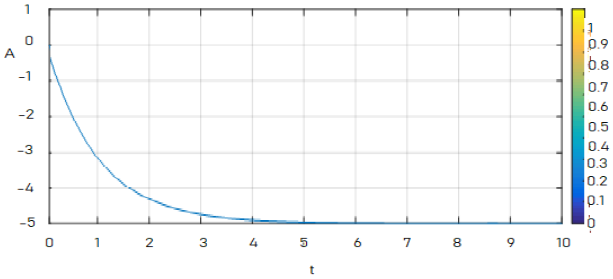

Fig. 8. The greatest amplitude of the force of action of a destructive object. All characteristics (16) are equal to 1.0 relative units

3.4. Exchange of expressed considerations from the study of ISI in SM taking into account UDPC

The analysis of the HDISI using the probability characteristics and the characteristics of the UDPC provided the opportunity to obtain numerical evidence of extremely important isolated characteristics of SM which include the effect of UDPC on the ISI (1, 2, 14) (Figs. 2, 3). A reasoned assessment of the fundamental approaches, introduced scientific thoughts, models that have been evaluated by simulation modeling of the ISI taking into account the effects of influences, approved the methodology.

The analysis of the RSIIS (14) (Fig. 2) and the PD (Fig. 4) shows the reliability and stability of the ISI.

The method allows obtaining quantitative characteristics of the ISI from the characteristics of the SM and UDPC. To date, there is no method that allows obtaining such an achievement.

It is satisfactory that the ISI withstands the maximum loads, including those to UDPC.

Adding to the information security workers in the SM adequate "at your fingertips" information, activities and methods for analyzing the quantitative effect of UDPC characteristics on ISI characteristics, this is seen as an applied benefit.

The study of the amplitudes of the ISI oscillations and the phase diagrams shows the existing threats in real time, their strength. This will provide the opportunity for information security workers to make decisions in real time based on the characteristics of the ISI.

The prospect in further scientific work lies in the identification of other SM parameters and the identification of their impact on the ISI.

4. Numerical expression

The illustration of the ISI differential in Fig. 2 indicates that it has negative values in the entire operating range, which corresponds to Lyapunov's theorem, which means that the RSIIS is ensured. This is confirmed by further studies (Fig. 4).

The values of the ISI characteristics lie within the range from 0 to 1, which indicates a strong influence of the UDPC characteristics (Figs. 3 a, 3 b).

Closed curves without bifurcation points (Fig. 4) at different values of influences indicate ISI stability indicators.

5. Summary

1) The analysis of the model, which is reproduced by the HDISI, shows that quantitative results of the activity of SM characteristics and characteristics of UDPC on ISI in SM and their understanding were obtained. Characteristics of the UDPC action on ISI are in the range from zero to one hundred percent, which made it possible to further conduct research on the RSIIS.
2) The acquisition of RSIIS in SM at different indicators of the action of harmful elements on ISI was performed according to the electronic circuit, in the program MULTISIM. The study of illustrations with oscillations of ISI and phase diagrams confirms RSIIS at different influences of harmful elements.

As a result of the analysis, it can be recognized that the study of the impact of the UDPC on the ISI is accurate. Further scientific work, from our point of view, consists in exploring and using other unique characteristics of SM to establish their impact on ISI.

The study of the amplitudes of ISI oscillations and PD shows the existing threats and their strength in real time. This will provide the opportunity for information security workers to make decisions based on ISI characteristics in real time.

References

[1] Akhramovych V. et al.: 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)), 2022, 63–74.

[2] Akhramovych V.: Method of Calculation of Protection of Information from the Average Length of the Road Between Users in Social Networks. Collection Information Technology and Security 10(2), 2022, 153–164.

[3] Gubanov D., Chkhartishvili A.: A Conceptual Approach to the Analysis of Online Social Networks. Large-Scale Systems Control 45, 2013, 222–236.

[4] Hanneman R., Riddle M.: Introduction to Social Network Methods [https://faculty.ucr.edu/~hanneman/nettext/C7_Connection.html#distance].

[5] Khrashchevskyi R. et al.: Method of Calculating Information Protection from Mutual Influence of Users in Social Networks. International Journal of Computer Network and Information Security – IJCNIS 15(5), 2023, 27–40 [https://doi.org/10.5815/ijcnis.2023.05.03].

[6] Nosouhi M. R.: Location Privacy Protection in Social Networks. Ph.D. thesis. University of Technology Sydney, Sydney 2020 [http://hdl.handle.net/10453/143934].

[7] Rohloff K.: Stochastic Behavior of Random Constant Scanning Worms. The 14th ICCCN, 2005, 339–344.

[8] Savchenko V. et al.: Method of Calculation of Information Protection from Clusterization Ratio in Social Networks. Proceedings of the 3rd International Conference on Information Security and Information Technologies – ISecIT 2021, 24–31.

[9] Savchenko V. et al.: Methodology for Calculating Information Protection from Parameters of its Distribution in Social Networks. 3rd International Conference on Advanced Trends in Information Theory – ATIT, 99–105.

[10] Seyyed M. S. et al.: Privacy Protection Scheme for Mobile Social Network. Journal of King Saud University – Computer and Information Sciences 34(7), 2022, 4062–4074.

[11] Shehab M. et al.: Access Control for Online Social Networks Third Party Applications. Computers & Security 31(8), 2012, 897–911.

[12] Trubetskoy D. I.: Introduction to Synergetics. Chaos and structures. Editorial, Moscow 2004.

[13] Yating L. et al.: Intelligent Privacy Protection of End User in Long Distance Education. Mobile Networks and Applications 27, 2022, 1162–1173.

[14] Yevseiev S. et al.: Modeling the Protection of Personal Data from Trust and the Amount of Information on Social Networks. Eureka Physics and Engineering 13(1), 2021, 24–31.

[15] Yüksel A. S., Halim Zaim A.: A Reputation-based Privacy Management System for Social Networking Sites. Turkish Journal of Electrical Engineering and Computer Sciences 21(3), 2015, 766–784.

[16] Zan Y., Wu J., Li P., Yu Q.: SICR Rumor Spreading Model in Complex Networks: Counterattack and Self-resistance. Physics A: Statistical Mechanics and its Applications 405, 2014, 159–170.

[17] Zhang Y., Pang J.: Distance and Friendship: A Distance-based Model for Link Prediction in Social Networks [https://satoss.uni.lu/members/jun/papers/APWeb15.pdf].

[18] Zhang Y., Zhu J.: Stability Analysis of I2S2R Rumor Spreading Model in Complex Networks. Physics A: Statistical Mechanics and its Applications 503, 2018, 862–881.

Prof. Volodymyr Akhramovych
e-mail: 12z@ukr.net

Doctor of Technical Science, Professor, Associate Professor, Department of Information and Cybersecurity Systems of the State University of Information and Communication Technologies, Kyiv, Ukraine.
Over 200 scientific papers have been published, 13 of it are the USSR copyright certificates, 14 patents of Russia. The sole author of four textbooks, co-authored with two textbooks and three workshops.
He has been working in the field of higher education for more than thirty years.

https://orcid.org/0000-0002-6174-5300

Ph.D. Yuriy Pepa
e-mail: yurka14@ukr.net

Candidate of technical sciences, Head of the Department of Robotics and Technical Systems, State University of Information and Communication Technologies, Kyiv, Ukraine.

https://orcid.org/0000-0003-2073-1364

Anton Zahynei
e-mail: Antonio.com237@gmail.com

Postgraduate student, senior lecturer. Department of Information and Cybersecurity Systems of the State University of Information and Communication Technologies, Kyiv, Ukraine. Interested in: cloud computing, fog computing, comprehensive information security systems.

https://orcid.org/0000-0002-0303-8501

Vadym Akhramovych
e-mail: 12zstzi@gmail.com

Head of the Computing Center of the National Academy of Statistics, Accounting and Auditing, Kyiv, Ukraine.

https://orcid.org/0009-0003-2787-8745

Ph.D. Taras Dzyuba
e-mail: iwartar@gmail.com

Ph.D. in Technical Science, associate professor of the Department of Information and Cybersecurity Management, State University of Information and Communication Technologies, Kyiv, Ukraine.
He has been working in the field of higher education more than twenty years.

https://orcid.org/0000-0001-6607-2507

Ihor Danylov
e-mail: danylovihor@gmail.com

Postgraduate student of Department of Information and Cybersecurity Systems of the State University of Information and Communication Technologies, Kyiv, Ukraine.

https://orcid.org/0009-0000-1426-6414