Methodology for assessing computer security levels*

Volodymyr Akhramovych[1,*,†], Vadym Akhramovych[2,†], Anna Ilyenko[1,†], Olha Kryvokulska[1,†], and Viktoriia Zhebka[3,†]

[1] The State University "Kyiv Aviation Institute," 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine
[2] Computer Center of the National Academy of Statistics, Accounting and Audit, 1 Pidhirna str., 04107 Kyiv, Ukraine
[3] State University of Information and Communication Technologies, 7 Solomyanska str., 03110 Kyiv, Ukraine

Abstract

This article examines a dynamic model of a computer information security system, taking into account factors that affect its stability. The stability of the protection system is analyzed, and the dependence of its behavior on parameters that affect the level of security is considered. The protection system is presented as a dynamic system in a mathematical sense, the state of which changes according to the given laws of evolution. Theoretical research was carried out using mathematical models formulated in the form of differential equations, with their subsequent implementation in the MATLAB/Multisim environment. The phase portraits of the system indicate its stability in the working range of parameters even under conditions of maximum external influence. The scientific novelty of the work lies in the presentation of a computer security assessment system in the form of a nonlinear dynamic model that takes into account the relationships between key security parameters. Unlike existing studies that focus on individual aspects (antivirus protection, cryptographic algorithms, access policies), the proposed approach allows for a quantitative assessment of the impact of a set of internal and external factors on the stability of the system, as well as determining the dynamics of its behavior in real time.

Keywords

computer, protection system, influencing factors, dynamic system, nonlinearity, differential equations, stability

1. Introduction

The problem of protecting information from unauthorized access and unwanted influence has existed for as long as the concept of valuable information itself. With the development of automated control systems, network technologies, and personal computers, the issue of data protection has taken on new relevance.

The problem of ensuring computer security has become increasingly complex in recent decades, as information technologies have deeply penetrated into all spheres of human activity. Modern information systems are exposed to a wide spectrum of threats, ranging from hardware and software failures to sophisticated cyberattacks aimed at disrupting the confidentiality, integrity, and availability of information. According to recent reports by ENISA and ISO/IEC 27001 standards, the number and diversity of threats are steadily increasing, requiring more advanced and adaptive protection mechanisms.

Traditional approaches to computer security mainly rely on separate tools such as antivirus software, firewalls, cryptographic protocols, and access control policies. While these methods remain effective for mitigating specific types of threats, they do not provide a holistic view of the system's resilience, particularly when complex interdependencies between parameters are considered. In this context, mathematical modeling of computer security systems as dynamic nonlinear systems has gained importance, since it allows for the quantitative evaluation of

* CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
12z@ukr.net (V. Akhramovych); 12zstzi@ukr.net (V. Akhramovych); anna.ilienko@npp.kai.edu.ua (A. Ilyenko); olha.kryvokulska@npp.kai.edu.ua (O. Kryvokulska); viktoria_zhebka@ukr.net (V. Zhebka)
0000-0002-0086-9131 (V. Akhramovych); 0009-0003-2787-8745 (V. Akhramovych); 0000-0001-8565-1117 (A. Ilyenko); 0009-0003-8518-6915 (O. Kryvokulska); 0000-0003-4051-1190 (V. Zhebka)

challenges, the present study aims to develop and analyze a nonlinear differential model of a computer protection system, focusing on its stability and the dynamic impact of both internal and external parameters. Such an approach not only complements existing studies but also provides a universal framework for quantitative assessment of information security at the level of an individual computer [1, 2].

Factors contributing to increased information security requirements include: growth in data volumes and their concentration in shared databases; multitasking and real-time operation; automation of data exchange over long distances; the development of global networks and financial systems, which have become targets of cybercrime [3, 4].

Therefore, studying the impact of computer system parameters on the effectiveness of information protection is a task of both practical and theoretical importance.

2. Problem statement

Recent studies on computer and information security can be divided into two major directions. The first group focuses on practice-oriented solutions, including protection against hardware and software failures, recovery of lost data, and methods of countering malicious software and fraud [5–11]. These works provide valuable insights for practitioners, yet they often lack a systemic view of the computer as an interconnected dynamic system.

Article [12] examines the issue of quantitatively determining the level of information security on a personal computer depending on the impact of internal and external threats. Factors such as user identification and authentication, data integrity and authenticity control, backup, access control, firewall operation, auditing, antivirus protection, as well as risks associated with software and hardware failures are considered [13]. The impact of the speed and volume of data leakage, loss of trust between users, and system scale on the level of security is analyzed separately. decay; as well as fluctuations taking into account dissipative characteristics. At the same time, the study does not consider the behavior of the system in nonlinear coordinates, which limits the completeness of the analysis.

Articles [14–17] develop mathematical models based on nonlinear systems of equations to assess the impact of dynamic parameters, in particular network centrality indicators, distance, and interaction between social network users, on the level of information security. These works demonstrate the significant potential of nonlinear modeling for assessing security, but they do not directly address computer systems as objects of study.

Work [5] provides practical recommendations for protecting computers from hardware and software failures and virus attacks, and also discusses means of diagnostics, detection of operating system errors, recovery of lost data, and improvement of operational reliability. A similar example is given in study [6], which focuses on detecting and countering hacking techniques, methods of protection against malicious software, combating Internet fraud and spam, and ensuring parental control of access to unwanted resources.

Further analysis [7–11] indicates the existence of a significant body of practice-oriented work investigating the reliability and security of personal computers. In particular, [7] presents recommendations for preventing technical failures, ranging from software installation errors to local network construction problems. The study [8] emphasizes the growing role of the computer as a universal tool for work, study, leisure, and creativity, while drawing attention to the multifactorial nature of the hardware selection process. Article [9] provides a detailed overview of measures to counter viruses, spyware, and fraudulent practices, as well as methods for ensuring data confidentiality.

The work [10] consistently highlights the evolution of approaches—from the basic concepts of "computer virus" and "software protection" to specific methods of countering information destruction. Work [11] focuses on the most common technical malfunctions, methods of their elimination, and data recovery. At the same time, these studies lack a systematic analysis of the computer as a dynamic nonlinear system, which reduces the possibility of quantitatively assessing its level of protection. Article [18] discusses the specifics of managing shared computers in educational laboratories, with a particular focus on advanced access control mechanisms in the Microsoft Windows SteadyState operating system.

The study [19] emphasizes the need for strict validation of access policies through formal checks, penetration testing, and analysis of the adequacy of diagnostic information in wireless sensor networks. At the same time, the "classic" parameters of network protection have been studied, but specific aspects of interaction between system elements remain insufficiently researched.

The practical effectiveness of antivirus solutions is assessed in [20], where laboratory tests and real-world examples establish the advantages of Bitdefender Antivirus Plus and Norton AntiVirus Plus, recognized as the "editor's choice." At the same time, the authors note that the market is not limited to these products.

Article [21] presents a broader approach to security policy analysis based on process algebra (Communicating Sequential Processes), bi-modeling, and generalization of formal methods for modeling non-interference policies.

The growth in cyber threats has necessitated mathematical modeling of the behavior of malicious objects, as emphasized in article [22]. The proposed stochastic model for designing a cyber defense system is based on probability theory methods and a system of differential equations for describing attacks. The study [23] considers another direction—the construction of a data encryption system based on nonlinear differential equations with partial derivatives. An architecture using the DES algorithm and "onion" encryption of databases is proposed, which provided a 25% increase in the level of protection compared to traditional solutions.

In [24], the authors proposed a model predictive control (MPC) model for nonlinear cyber-physical systems, taking into account deception attacks and constraints on executive mechanisms. The model guarantees the root mean square stability of the system and demonstrates effectiveness in counteracting destabilizing factors. This study is similar to the proposed approach, as it also analyzes the dynamics of systems with nonlinear parameters, but the emphasis is on CPS control rather than on a single computer.

In [25], a multi-level model of situational awareness was created using machine learning methods (Random Forest), which allows nonlinear patterns in network security to be taken into account. Although the model is more focused on big data analytics, the approach confirms the relevance of integrating nonlinear methods into cybersecurity assessment tasks.

Article [26] creates a model for assessing cyber threats in microcontrollers, which takes into account various factors of information influence and optimizes threat parameters. This approach is relevant because it expands the application of mathematical models to internal hardware components, which is related to your topic (hardware failures and malfunctions).

The work [27–31] proposes a security model for socio-cyber-physical systems that takes into account not only technical but also social factors, including the influence of social engineering. The mathematical basis is based on a modification of the Lotka–Volterra equations. This confirms the trend toward using nonlinear system models to describe security in conditions of complex interrelationships. The study in [28] presents a systematic review of modern ML/DL methods for ensuring security in cloud environments. It emphasizes the importance of adaptive protection systems capable of operating in dynamic environments, which has parallels with the approach of modeling computer resilience as a nonlinear system.

Current research confirms that nonlinear mathematical models and machine learning methods are the dominant approaches to assessing cybersecurity. Summarizing the results of the analysis of literary sources [5–28], we can conclude that there is significant scientific and practical work in the field of information security and computer system functioning. At the same time, existing studies mostly focus on individual aspects—antivirus protection, technical reliability, access control, or cryptographic methods. However, there are no studies in which a computer is considered as an integral dynamic nonlinear system with complex interrelationships between parameters, which significantly limits the possibilities for developing universal quantitative models for assessing the level of information security.

The analysis of existing studies highlights both the achievements and the limitations of current approaches in assessing computer security. While practice-oriented works provide valuable recommendations for addressing software failures, malware protection, and access control, and mathematical models demonstrate the potential of nonlinear and stochastic methods, the literature still lacks an integrated approach that considers the computer as a dynamic nonlinear system with interdependent parameters. This gap defines the direction of the present research.

The aim of this work is to develop a methodology for assessing the level of security of computer systems, taking into account both external and internal influencing factors. To achieve this aim, it is necessary to: model a nonlinear system of computer protection; investigate its stability under conditions of both absence and presence of destabilizing factors.

In this study, the apparatus of nonlinear differential equations, fuzzy cognitive modeling, and fuzzy set theory was applied to describe weakly formalized processes of information security. The mathematical models were implemented in MATLAB and Multisim environments, which enabled the construction of block diagrams of the protection system, the simulation of external attacks, and the evaluation of the dynamic behavior of the system.

This methodological framework provides the foundation for the subsequent sections, where the proposed models are analyzed in detail, and their effectiveness in capturing the dynamics of computer security is evaluated.

3. Modeling of nonlinear protection system

The suggested model considers the impact of the following factors: data integrity control, access control, firewall operation, antivirus protection, auditing, backup, as well as factors related to software and hardware failures.

The system of nonlinear differential equations, which allows us to determine dynamics of the protection indicator depending on the parameters, has been obtained. Analytical solutions and numerical modeling demonstrated that even under weak nonlinearity it is possible to evaluate quantitative characteristics of the influence. Let's imagine a linear model of the computer.

A dynamic system is considered to be specified if the coordinates defining its state and the operator describing the evolution of the initial state over time are given. The mathematical representation of such systems can be implemented in the form of discrete models, systems of differential equations, partial differential equations, integral and integro-differential equations, systems with impulse effects, hybrid systems, or Markov processes. To describe the level of computer security, let us consider a linear model [12]:

$$\begin{cases} \dfrac{dl}{dt} = Z\left(Z_p + Q + W + F + V + Z_{Pl} + Z_k\right) + \left(C_v + C_{k)}\right) I \\ \dfrac{dZ}{dt} = I_d A_c \left(R + A_d\right) - \left(C_{d2} + C_{d1}\right) I \end{cases} \tag{1}$$

where Z_p—coefficient reflecting the impact of additional information protection measures (e.g., combating electromagnetic interference, physical protection, etc.); Q—coefficient reflecting data integrity and authenticity control (value 0...1); W—coefficient reflecting the separation of access to

information (value 0...1); F—coefficient reflecting the operation of a firewall (packet filter)—used to control incoming and outgoing traffic (value 0...1); V—coefficient reflecting antivirus software (value 0...1) Z_{p1}—coefficient reflecting software component failures and malfunctions (value 0 or 1); Z_k—coefficient reflecting hardware component failures and malfunctions (value 0 or 1) C_v—coefficient reflecting the impact of personal data leakage speed; C_k—coefficient reflecting the impact of the amount of personal data on its leakage; I_d—coefficient reflecting user identification (value 0 or 1); A—coefficient reflecting user authentication (value 0 or 1); R—coefficient reflecting data backup (value 0...1); A_d—coefficient reflecting auditing (used for monitoring, logging) (value 0...1);. C_{d1}—coefficient reflecting the impact of security on information leakage. C_{d2}—coefficient reflecting the impact of system size on security.

Since the linear model does not take into account the actual relationships between parameters, the system (1) is supplemented with nonlinear components: (2):

$$\begin{cases} \dfrac{dI}{dt} - Z\left(Z_p + Q + W + F + V + Z_{p1} + Z_k\right) + \left(C_v + C_k\right) I + L_2 I^2 + L_3 I^3 + \ldots \\ \dfrac{dZ}{dt} = I_d A_c \left(R + A_d\right) - \left(C_{d2} + C_{d1}\right) I + K_2 Z^2 + K_3 Z^3 \ldots \end{cases} \quad (2)$$

where L_2, L_3, etc. K_2, K_3, etc. are some linear operators.

We consider the nonlinearity of the system to be weak, which allowed us to find solutions for each equation of system (2) using the method of successive approximation, setting:

$$I = I_1 + I_2 + I_3 + \ldots, dI = 0;$$
$$Z = Z_1 + Z_2 + Z_3 + \ldots, dI = 0;$$

$$dI = 0, \frac{dI}{dt} = 0 \text{ and } dZ = 0, \frac{dZ}{dt} = 0,$$
$$I = I_0 \sin\omega t, Z = Z_0 \sin\omega t.$$

The following system of equations was obtained (3):

$$\begin{cases} \dfrac{dI}{dt} - Z\left(Z_p + Q + W + F + V + Z_{p1} + Z_k\right) + \left(C_v + C_k\right) I - L_2\left(I_0^2 \sin^2 \omega t\right) - L_3\left(I_0^3 \sin^3 \omega t\right) - \ldots \\ \dfrac{dZ}{dt} = I_d A_c \left(R + A_d\right) - \left(C_{d2} + C_{d1}\right) I + K_2\left(Z_0^2 \sin^2 \omega t\right) - K_3\left(Z_0^3 \sin^3 \omega t\right) - \ldots \end{cases} \quad (3)$$

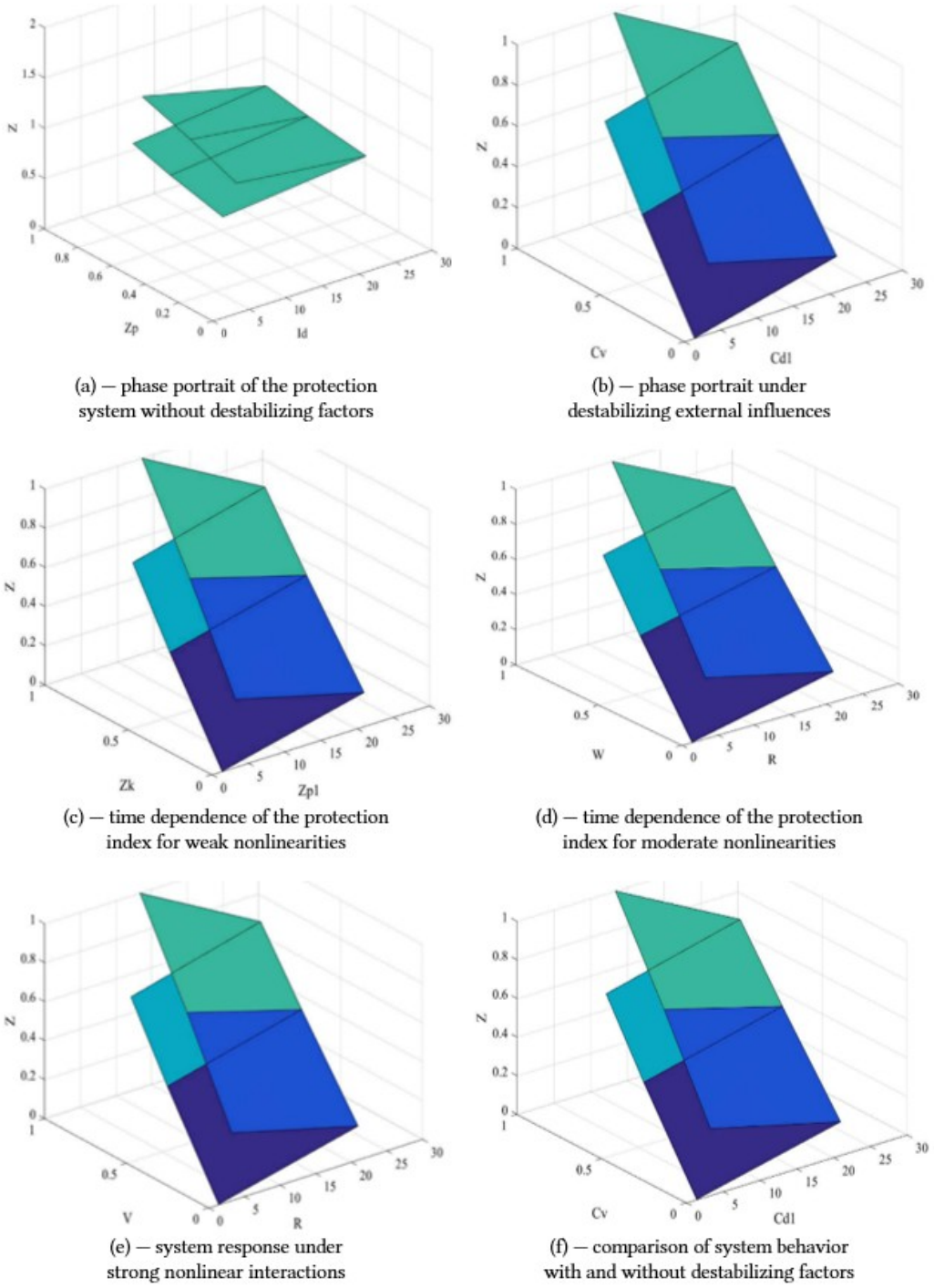
The system of equations is presented in the following form (4) (Figure 1):

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \quad (4)$$

where

$$\alpha = Z_p + Q + W + F + V + Z_{p1} + Z_k, \beta_1 = C_v + C_k,$$
$$\beta_2 = I_d\left(R + A_d\right) - \left(C_{d2} + C_{d1}\right).$$

Figure 1 illustrates the results of numerical modeling of the proposed nonlinear protection system under different parameter configurations. To provide a more detailed interpretation, the figure is divided into several subplots (a–f), each highlighting specific aspects of the system's dynamics.



(a) — phase portrait of the protection system without destabilizing factors

(b) — phase portrait under destabilizing external influences

(c) — time dependence of the protection index for weak nonlinearities

(d) — time dependence of the protection index for moderate nonlinearities

(e) — system response under strong nonlinear interactions

(f) — comparison of system behavior with and without destabilizing factors

Figure 1 (a-f): Dependencies of the protection indicator on the components of model (4)

The results illustrated in Figure 1 confirm that the proposed nonlinear differential model adequately reflects the resilience of the computer protection system. In all considered cases, including scenarios with destabilizing factors and varying degrees of nonlinearity, the system eventually converges to a stable state. This demonstrates the robustness of the methodology and its suitability for quantitative evaluation of computer security under different operating conditions.

Further transformations using the elimination method led to the following system:

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

All found expressions (5) are substituted into the first equation of system (4):

$$\frac{dI}{dt}=\frac{1}{\beta_2}\left(\frac{d^2Z}{dt^2}+\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)\right). \tag{6}$$

or:

$$\begin{aligned}\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2Z=\frac{-1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)+\\+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t.\end{aligned} \tag{7}$$

Joint solution of the corresponding homogeneous equation:

$$Z''-\beta_1Z'-\alpha\beta_2Z=0. \tag{8}$$

The characteristic equation took the form: $\lambda^2-\beta_1\lambda-\alpha\beta_2=0$. Provided that the discriminant is positive:

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

The solution to a homogeneous equation is defined as:

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

Stable oscillatory trajectories were obtained. The general solution of the inhomogeneous equation was found by the method of variation of arbitrary constants:

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

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

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

where

$$\begin{aligned}N(t)=\frac{-1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)+\\+\beta_1\sum_{k=2}^{\infty}\left(K_kZ_0^k\sin^k\omega t\right)-\beta_2\sum_{k=2}^{\infty}\left(L_kI_0^k\sin^k\omega t\right)\end{aligned} \tag{10}$$

The final dependence of the protection indicator takes into account the influence of the main system parameters (Figure 2).

$$\begin{aligned}Z(s)=\int_{t_0}^{t}\left(N(s)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\right)ds-\\-\int_{t_0}^{t}\left(N(s)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}s}}{\sqrt{s\,\beta_1^2+4\alpha\beta_2}}\right)ds\end{aligned} \tag{11}$$

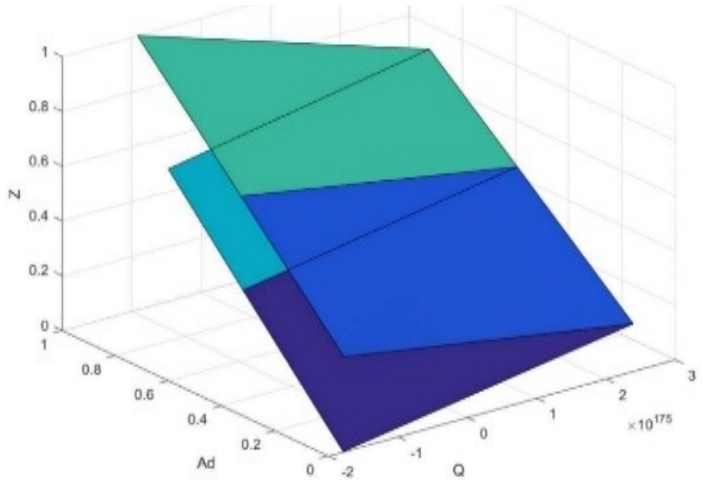


Figure 2: Dependencies of the protection indicator on the components of model (11)

A system of nonlinear differential equations was obtained, which allows determining the dynamics of the protection indicator depending on the parameters. Analytical solutions and numerical modeling showed the stability of the system even with weak nonlinearity.

3.1. Investigation of the stability of the protection system in a computer

To assess stability, the analysis of the differential of the protection function was used (Figure 3).

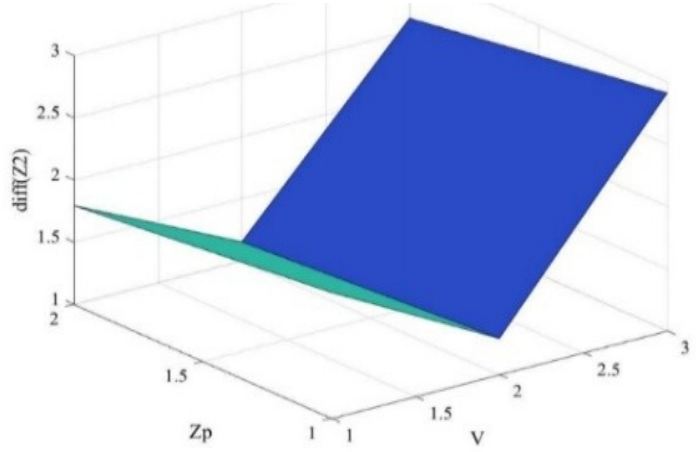


Figure 3: Differential of the protection function

Since the conditions for the existence and uniqueness of the solution to the Cauchy problem are satisfied, the trajectory of the system is the projection of the integral curve onto the phase space. The intersection of two different trajectories is impossible, which confirms the stability of the solutions.

The initial differential equation of the system:

$$\frac{d^2 Z}{d t^2} - \beta_1 \frac{dZ}{dt} - \alpha \beta_2 Z = \frac{-1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) + \\ + \beta_1 \sum_{k=2}^{\infty} \left(K_k Z_0^k \sin^k \omega t \right) - \beta_2 \sum_{k=2}^{\infty} \left(L_k I_0^k \sin^k \omega t \right) - \beta_2 \sum_{k=2}^{\infty} \left(L_k I_0^k \sin^k \omega t \right). \quad (13)$$

To solve equation (12), a block diagram in the MATLAB/Multisim environment was used (Figure 4).

The stability of the CM protection system in the presence of influences on it has been investigated.

The behavior of CM resembles the behavior of a biological object. Assumption: the amplitude of influences is nonlinear in time. Therefore, the following considerations are acceptable. A system was considered in which the impact of harmful objects on the system and the immune response of the system were modeled. It was assumed that the dynamics of the harmful object correspond to the logistic model. The growth of a harmful infection depends on its initial status, the decline caused by the immune response, and its own density effect, while the change in the immune response depends on its initial status, natural decline, stimulation leading to an enhanced response, and damage caused by the harmful object. Finally, the relative characteristic of the damaged organ depends on the density of the harmful object and its natural degeneration. Then the dynamics of the system is represented by differential equations [24]:

$$\begin{cases} \frac{dP}{dt} = \beta P - \gamma IP - \beta_0 P^2 \\ \frac{dI}{dt} = \mu - \alpha I + bIP - \eta\gamma IP \end{cases}, \tag{14}$$

where: $P(t)$—density of harmful objects, $I(t)$—immune status of the system, β—growth rate coefficient of the harmful object, γ—decay rate coefficient of the harmful object due to its interaction with the immune system of the network, and β_0–coefficient of intraspecies interference of harmful objects. μ—growth rate of the immune system, a—coefficient of its natural decay rate, b—stimulating growth rate of the immune system due to its interaction with harmful objects, η—coefficient of its decay rate due to interaction with a harmful object. α—coefficient of growth rate of the damaged node due to a harmful object. This is nothing more than a system of equations of the "predator-prey" type.

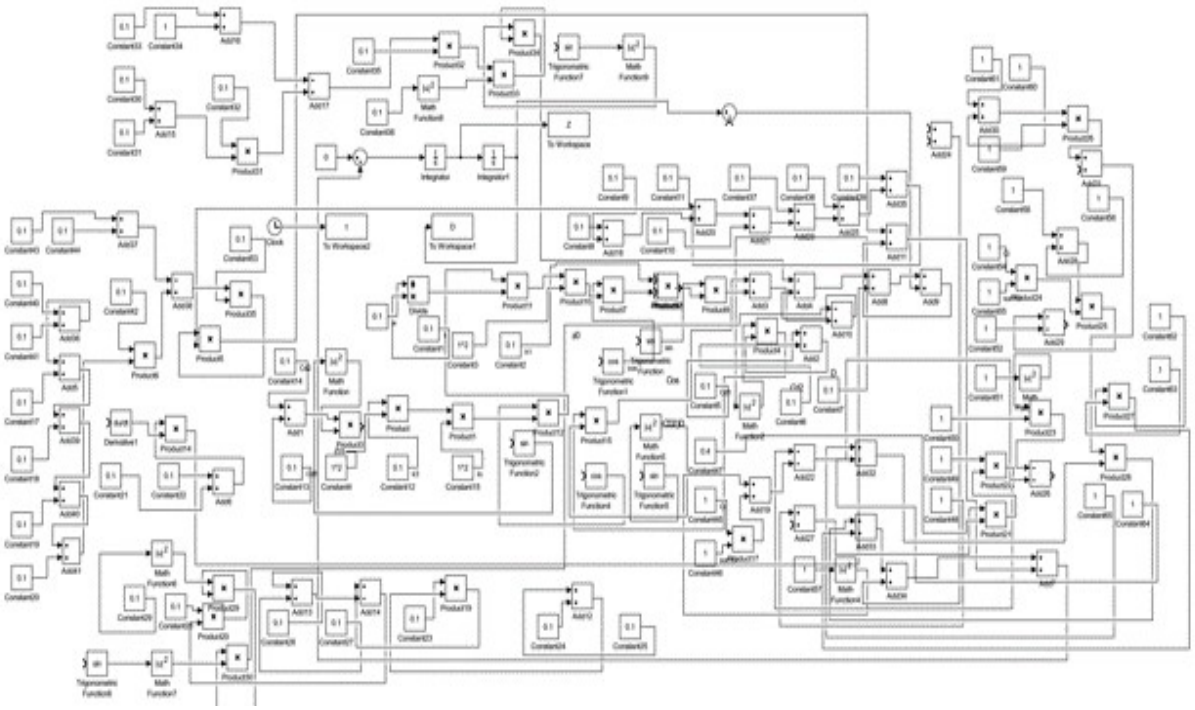


Figure 4: Block diagram of the phase portrait program in Multisim, taking into account the attack block

The results of the program are shown in Figures 4–7.

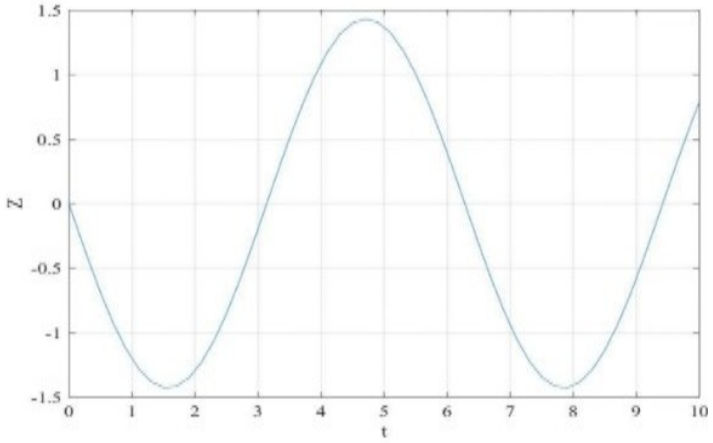


Figure 5: Harmonic oscillations of the time protection system Z=f(t) in the absence of influence

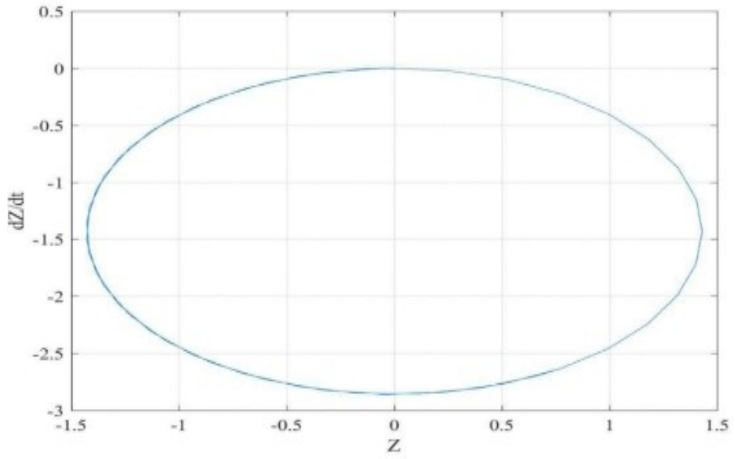
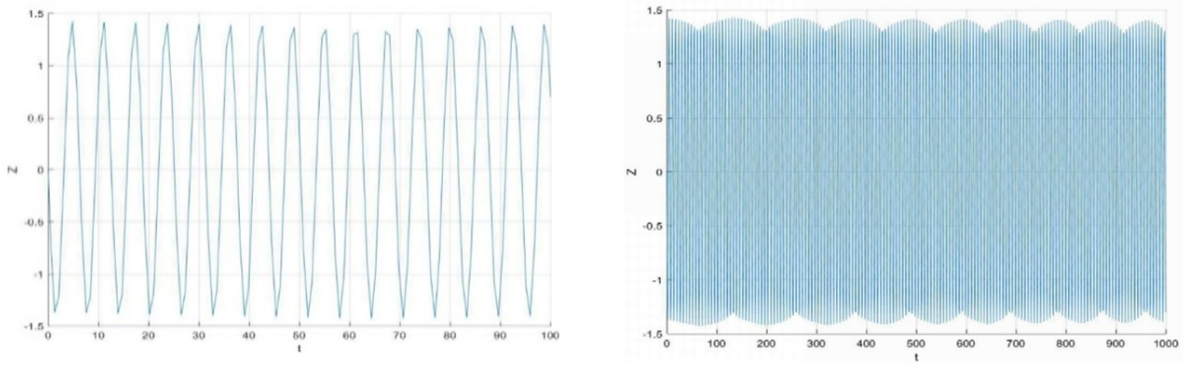


Figure 6: Phase portrait of the protection system against user interaction parameters in the absence of influence

Phase portraits of the protection system are shown in Figure 7.



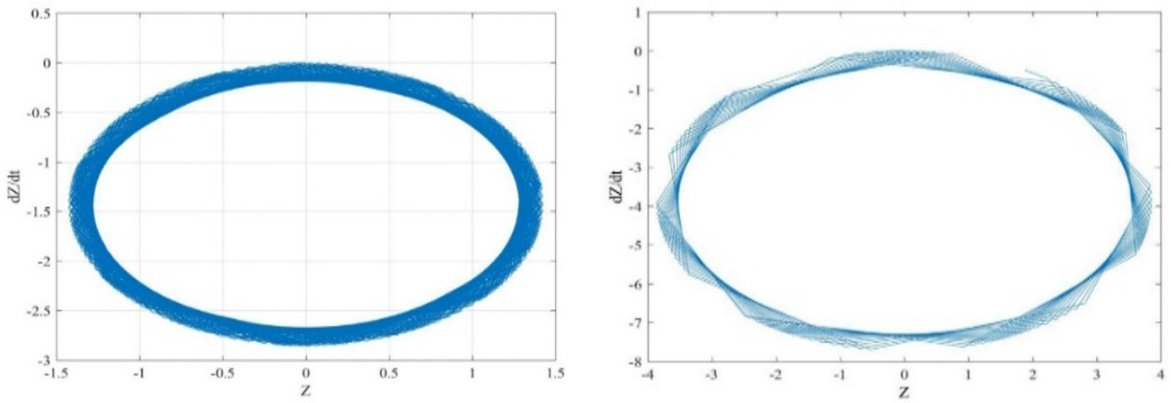
(a) — dynamics of the protection index without external attacks

(b) — dynamics of the protection index under external attacks

Figure 7: Amplitude of oscillations of the protection system in the presence of influences: a—from the parameters of influences—0.3 per (13); b—maximum value of the amplitude of influence

Phase portraits of the protection system are shown in Figure 8.

The results demonstrate the system's capability to maintain stability even in the presence of destabilizing factors.



(a) — time dependence of the protection index under weak nonlinearity

(b) — time dependence of the protection index under strong nonlinearity

Figure 8: Phase portrait of the protection system: a—from the parameters of influences—0.5 per (13); b—maximum value of the amplitude of influence

4. Discussion of the results of the study of the level of protection of the computer's information space

The proposed methodology allowed us to consider the computer protection system as a dynamic nonlinear system, where the security level is described by a system of differential equations. Unlike traditional approaches, which mostly focus on individual aspects (antivirus protection, cryptographic algorithms, or access policies), the proposed model integrates the influence of key factors, including authentication, auditing, firewall operation, backup, and software and hardware failures. The results of analytical and numerical modeling showed that even under conditions of weak nonlinearity, it is possible to obtain quantitative characteristics of the influence of factors on the level of security. The constructed phase portraits confirmed the stability of the system in the working range of parameters, as well as the absence of bifurcations, which indicates the stability of the proposed approach.

A comparison with existing works indicates the novelty of the results. In particular, studies [25] considered stochastic attacks and predictive control for cyber-physical systems, but there is no analysis of the influence of internal computer parameters on system stability. In [26], machine learning methods were applied for situational awareness, but without mathematical formalization of the interaction of factors in the form of differential equations. The proposed model allows combining mathematical rigor with the practical possibility of assessing the impact of parameters in real time, which confirms its potential for use in monitoring and adaptive protection control systems.

The obtained phase portraits confirm the stability of the system and the absence of bifurcations in the working range of parameters (Figures 5, 7). This indicates the stability of the system.

Overall, the proposed methodology not only demonstrates the feasibility of representing computer protection as a dynamic nonlinear system but also opens avenues for extending this approach. The integration of fuzzy cognitive modeling and probabilistic methods makes it possible to incorporate stochastic and weakly formalized factors, including user behavior, social engineering techniques, and random hardware or software failures. This provides a foundation for creating hybrid models capable of adaptive decision-making in real time. Consequently, the presented results can be viewed as a step toward developing universal frameworks for assessing and improving the resilience of information security systems across both standalone computers and complex network infrastructures.

5. Conclusion

The study proposed and analyzed a methodology for assessing the level of computer security by representing the system as a set of nonlinear differential equations. The developed model integrates both external and internal factors of influence, including user authentication, auditing, firewall operation, antivirus protection, software and hardware failures, and data leakage processes. Numerical modeling carried out in MATLAB and Multisim demonstrated that the system maintains stability within its operational range, even under destabilizing influences.

The main findings of the study can be summarized as follows:

1. A system of nonlinear differential equations has been developed to assess the level of computer security.
2. It has been established that the protection system remains stable even under conditions of maximum external influences within the operating range of parameters.
3. The obtained graphical interpretations (phase portraits and dependencies of the protection index on parameters) allow quantitative assessment of the influence of factors on the level of security.
4. The proposed methodology can be used to monitor and improve the effectiveness of information protection systems in personal computers and network environments.

Unlike traditional approaches that address only isolated aspects of computer security, the methodology presented in this work allows for a holistic evaluation of the computer as a dynamic nonlinear system. This novelty ensures higher diagnostic accuracy and the possibility of identifying critical parameters that most significantly affect the level of protection.

The practical significance of the study lies in its potential application for real-time monitoring of computer security, early detection of cyberattacks, and prediction of their consequences. Moreover, the model can serve as a foundation for developing intelligent decision-support systems in the field of information security.

Future research should focus on extending the model to strongly nonlinear regimes, incorporating hybrid types of threats such as combined DDoS and social engineering attacks, and integrating the proposed methodology with machine learning algorithms to enable adaptive security management.

Declaration on Generative AI

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

References

[1] S. Rzaieva, et al., Methods of Modeling Database System Security, in: Cybersecurity Providing in Information and Telecommunication System, vol. 3654, 2024, 384–390.

[2] Y. Kostiuk, et al., Effectiveness of Information Security Control using Audit Logs, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991, 2025, 524–538.

[3] S. Vasylyshyn, et al. A Model of Decoy System based on Dynamic Attributes for Cybercrime Investigation, East.-Europ. J. Enterp. Technol. 1.9(121) (2023) 6–20. doi:10.15587/1729-4061.2023.273363

[4] V. Bilous, et al., Cyber Evidence Software as the Digital Forensics Tools in the Investigation of Cybercrime, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991 (2025) 26–37.

[5] A. Ilyenko, S. Ilyenko, M. Herasymenko, A Biometric Asymmetric Cryptosystem Software Module Based on Convolutional Neural Networks, Int. J. Comput. Netw. Inf. Secur. 9(6) (2021). doi:10.5815/ijcnis.2021.06.01
[6] A. Ilyenko, S. Ilyenko, I. Kravchuk, M. Herasymenko, Prospective Directions of Traffic Analysis and Intrusion Detection based on Neural Networks, Electron. Prof. Sci. Edition Cybersecur. Educ. Sci. Tech. 1(17) (2022) 46-56. doi:10.28925/2663-4023.2022.17.4656
[7] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, M. Benbouzid, Learning-based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects, Electronics, 11(9) (2022) 1502.
[8] H. Ahmetoglu, R. Das, A Comprehensive Review on Detection of Cyber-Attacks: Data Sets, Methods, Challenges, and Future Research Directions, Internet of Things, 20 (2022) 100615.
[9] A. N. Ozalp, Z. Albayrak, Detecting Cyber Attacks with High-Frequency Features using Machine Learning Algorithms, Acta Polytechnica Hungarica, 2022.
[10] A. Oyetoro, J. Mart, U. Amah, Using Machine Learning Techniques Random Forest and Neural Network to Detect Cyber Attacks, ScienceOpen Preprints, 2023.
[11] A. Kumar, N. Saxena, B. J. Choi, Machine Learning Algorithm for Detection of False Data Injection Attack in Power System, in: Proc. 2021 Int. Conf. Inf. Netw. (ICOIN), IEEE, 2021, 385–390.
[12] S. A. Mahboub, E. S. A. Ahmed, R. A. Saeed, Smart IDS and IPS for Cyber-Physical Systems, in: Artificial Intelligence Paradigms for Smart Cyber-Physical Systems, 2021, 109–136.
[13] P. Petriv, I. Opirskyy, N. Mazur, Modern Technologies of Decentralized Databases, Authentication, and Authorization Methods, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 60–71.
[14] A. N. Jaber, S. Anwar, N. Z. B. Khidzir, M. Anbar, The Importance of IDS and IPS in Cloud Computing Environment: Intensive Review and Future Directions, in: Advances in Cyber Security: Second International Conference (ACeS 2020), 2020, 479–491.
[15] A. Aldweesh, A. Derhab, A. Z. Emam, Deep Learning Approaches for Anomaly-based Intrusion Detection Systems: A Survey, Taxonomy, and Open Issues, Knowledge-based Systems, 189 (2020) 105124.
[16] S. M. Sohi, J. P. Seifert, F. Ganji, RNNIDS: Enhancing Network Intrusion Detection Systems through Deep Learning, Comput. Secur. 102 (2021) 102151.
[17] R. Achary, Cryptography and Network Security: An Introduction. Mercury Learning and Information, 2021.
[18] D. Dwivedi, A. Bhushan, A. K. Singh, Snehlata, Detection of Malicious Network Traffic Attacks using Support Vector Machine, in: Int. Conf. Adv. Netw. Technol. Intell. Comput., Springer, Cham, 2023, 54–68.
[19] R. D. Reddy, S. Katkam, C. R. S. Rao, Cyber Attacks Detection using Machine Learning, NeuroQuantology, 20(19) (2022) 4388.
[20] P. Semwal, A. Handa, Cyber-Attack Detection in Cyber-Physical Systems using Supervised Machine Learning, in: Handbook of Big Data Analytics and Forensics, 2022, 131–140.
[21] J. Gu, L. Wang, H. Wang, S. Wang, A novel approach to intrusion detection using SVM ensemble with feature augmentation, Comput. Secur., 86 (2019) 53–62.
[22] A. Nazir, R. A. Khan, A novel combinatorial optimization based feature selection method for network intrusion detection, Comput. Secur., 102 (2021) 102164.
[23] Z. Wang, Y. Liu, D. He, S. Chan, Intrusion Detection Methods based on Integrated Deep Learning Model, Comput. Secur., 103 (2021) 102177.
[24] Y. Wu, J. Yang, et al., Robust Security-based Model Predictive Control for Nonlinear Cyber-Physical Systems under Random Deception Attacks and Actuator Saturation, Int. J. Robust Nonlinear Control, Wiley, 2024.
[25] J. He, W. Su, Establishment of Nonlinear Network Security Situational Awareness Model based on Random Forest under the Background of Big Data, Nonlinear Eng., De Gruyter, 2023.

[26] R. Malinovskyi, D. Kupershtein, V. Lukichov, Mathematical Model for Assessing Cyber Threats and Information Impacts in Microcontrollers, Inf. Technol. Comput. Eng., 59(1) (2024).
[27] S. Milevsky, Socio-Cyberphysical Systems' Security Models, Ukr. Inf. Secur. Res. J., 26(1) (2024).
[28] Y. I. Alzoubi, A. Mishra, A. E. Topcu, Research Trends in Deep Learning and Machine Learning for Cloud Computing Security: A Systematic Review, Artif. Intell. Rev., Springer, 2024.
[29] S. Kazmirchuk, et al., Improved Gentry's Fully Homomorphic Encryption Scheme: Design, Implementation and Performance Evaluation, CybHyg (2019) 72–83.
[30] O. Yudin, Y. Ziatdinov, A. Voronin, A. Ilyenko, A Method for Determining Informative Components on the basis of Construction of a Sequence of Decision Rules, Cybern. Syst. Anal., 52(2) (2016) 323–329.
[31] A. Ilyenko, S. Ilyenko, Program Module of Cryptographic Protection Critically Important Information of Civil Aviation Channels, in: Int. Conf. Comput. Sci. Eng. Educ. Appl. 2022, 235–247.