Simulation model of information system transformation to increase survivability against cyber threats

Yuriy Syvytsky[1,†] and Viktor Shevchenko[1,*,†]

[1] *Institute of Software Systems of the National Academy of Sciences of Ukraine, 40-5 Akademik Hlushkov ave., 03187 Kyiv, Ukraine*

Abstract

The paper is devoted to the topical issue of the development of methods for increasing the survivability of information systems in conditions of malicious harmful influences. The purpose of the study is to create computer simulation models of the transformation of information systems to increase their survivability in the face of cyber threats. Increasing the survivability of information systems is achieved by using models to predict the consequences of management decisions, as well as by finding optimal solutions for the survivability of information systems. The transformation of information systems is considered a necessary response to a change in the spectrum of threats, a change in the operating conditions, or a change in the functions of the information system. The connection between the current and previous research of the authors is established based on the identification of similarities in the patterns of transformation of organizational structures, technologies, and information systems. The analysis of previous studies on ensuring the survivability of information systems in the areas of management, audit, assessment of the level of information and cyber security, modeling, and optimization of measures to ensure information and cyber security was carried out. Analyzed studies on the protection of information systems of critical infrastructure objects. It was determined that information systems are an integral part of critical infrastructure facilities. Atomic (elementary) models and the construction of complex structural and logical models based on them are considered. The importance of the development of hierarchical models and the procedure for their creation by step-by-step conversion from mixed models is determined. The question of the existence of an optimal level of complexity of models is considered. Logistic models are considered the most adequate for modeling development processes. The considered model of the dynamics of structural transformation allows modeling of the transformation processes of organizations, technologies, and information systems. The results of the approbation of the model for various transformation scenarios are given. The simulation model is implemented in the MatLab algorithmic language.

Keywords

computer simulation model, information system, survivability, logistic dependence, useful effect, resource, management decision support, automation, optimization

1. Introduction

The relevance of the study is confirmed by the analysis of the state and prospects for the development of the main laws of cyber security in the world [1], which shows that threats to the survivability of information systems are growing and will continue to grow even more. The relevance of research is because today all organizations are involved in the process of digitization. And any information threats can turn into big losses for the organization.

The survivability of information systems is achieved both by timely changes in information technologies, in particular information protection technologies, and by changing the structure of the information system by new functional and security conditions. It is well known that the successful implementation of ERP systems (Enterprise Resource Planning—ERP) is possible only on condition of careful analysis and reasonable adjustment of the enterprise's business processes, taking into account the limitations and capabilities of ERP systems [2]. This entails a deep transformation of the information systems themselves. But the most acute issue of transformation of information systems is caused by the need to ensure their viability. According to the provisions of systems theory, modern information systems are complex systems. Therefore, in complex issues of transformation, their behavior cannot always be clear and predictable. Therefore, it is advisable to use mathematical and simulation models to predict the behavior of information systems in the conditions of transformation [2, 3].

Accordingly, an urgent task is to create computer simulation models of the transformation of information systems to increase their survivability in the face of cyber threats.

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
ys@intecracy.com (Y. Syvytsky);
gii2014@ukr.net (V. Shevchenko)
0009-0008-9947-6653 (Y. Syvytsky);
0000-0002-9457-7454 (V. Shevchenko)

2. Analysis of existing studies

Survivability is understood as the possibility of realizing the goal of functioning in the event of adverse effects [4]. In the conditions of war and the conditions of the existing trends of cyber threats in the world [1] adverse influences take the form of malicious destructive influences. To ensure the survivability of information systems, it is necessary to solve a complex of tasks related to ensuring cyber security, information security, choosing safe structures of information systems, as well as choosing safe organizational structures that ensure the functioning of information systems. The last two questions lead to complex problems of transformation of structures [5].

Management issues of information and cybernetic security have a complex nature [6, 7] and lie not only in the technical plane. Many security issues are regulated by relevant regulatory documents, such as NIST standards [8]. Information security management is based on an objective assessment of the state of objects and threats. This requires the use of specific methods of obtaining numerical estimates of the level of information security, which, for example, for distributed wireless systems are considered in [9], and for communication systems under conditions of cyber-attacks are considered in [10]. Adequate use of classic methods of auditing information infrastructures [11] and assessment of relevant information security risks [12, 13] is important. Cybersecurity requires the creation and implementation of appropriate complex programs [14]. Ensuring the survivability of information systems by creating information security systems, which include cyber security systems, is based on a thorough numerical assessment of information security risks [15, 16].

The considered approaches to ensuring the survivability of information systems based on classical methods of information security management and auditing, unfortunately, do not pay enough attention to prognostic modeling of the development of complex systems in conditions of structural transformation.

The creation of models of dynamic processes, to which the processes of structural transformation should be attributed, are discussed in detail in [2, 3]. The given approaches make it possible to predict the consequences of management decisions made and to find optimal solutions for single-criteria and multi-criteria problems with vector criteria. Simulation modeling methods are based on specific computational methods [17]. One of the most vivid examples of simulation modeling of dynamic processes is the task of forecasting the dynamics of the development of computer epidemics, which includes the subtask of finding optimal parameters of the cyber security system, which would ensure the containment of the epidemic within the relatively safe limits of the "controlled process" [18]. To solve multi-criteria optimization problems, approaches based on scalar convolution of vector criteria are used [2, 3, 19]. Unfortunately, the considered approaches to modeling and finding optimal solutions in the presented works are general and do not take into account many features of the task of ensuring the survivability of information systems.

Paper [20], which considers the model of cyber protection in the information system of the situational center, and paper [21] regarding dynamic models of cyber security based on a numerical assessment of the guarantee capability of information systems of critical infrastructure objects are closer to the formulation of the task of this research. The study of the structure of dangers from cyber-attacks on critical infrastructure is analyzed in [22]. Regulatory and legal provision of information security of critical infrastructure objects is considered in [23]. Approaches to cyber protection of critical infrastructure based on integrated systems at the national level are studied in [24]. The issue of protecting critical infrastructure objects from cyber-attacks by decentralizing telecommunication networks is discussed in [25].

The value of research on the protection of information systems of critical infrastructure facilities is that almost all critical infrastructure facilities use complex and functionally rich information systems to ensure their functioning. Information systems are becoming an integral part of critical infrastructure facilities. The regularities that will be revealed when modeling the development of information systems of critical infrastructure objects can be extended to other types of information systems of a similar level of complexity. However, in the reviewed publications, attention is not paid to the modeling of structural transformation processes.

One of the important criteria of structural transformation is the minimization of losses or the maximization of the useful effect. The specified values depend on the costs of information protection, which, according to world experience, should be within 10–20% of the costs of the organization's information technologies [26]. The optimization of resource costs was studied in [27]. Methods of modeling the dynamics of changes in the efficiency of resource use in various organizational structures were studied in the paper [2]. Unfortunately, at the same time, abstract organizational structures were considered without taking into account the existing experience of forming specific organizational structures within the framework of project management approaches [28, 29]. In addition, the works [2, 26, 27] did not consider the conditions of structural transformation at all.

In [5], the task of forecasting the beneficial effect of the organization in the conditions of transformation of the organization structure is considered. It was determined that over time, any organizational structure needs to be transformed to increase competitiveness, adapt to new conditions, specifics of business tasks, a new set of dangers and challenges, etc.

The need to change the structure of the organization is usually caused by very serious reasons. In simpler cases, it is enough to change the technologies used by the organization. At the same time, it should be noted that the development of the beneficial effects of organizations and the development of the beneficial effects of technologies have very similar patterns: exponential, linear, and logistic. The disadvantage of the latter work is the modeling of the structural transformation of exclusively organizational structures. At the same time, approaches to the structural transformation of information systems were not considered. The main hypothesis in the further development of the work was an assumption regarding the similarity of

patterns of structural transformations of organizational structures, technologies, and information systems.

During the analysis of existing research, a contradiction was revealed between the need for practice in methods of modeling and optimization of the processes of structural transformation of information systems and the lack of appropriate theoretical and applied approaches.

The purpose of the paper is to increase the effectiveness of the transformation of information structures by forecasting the consequences of management decisions and finding optimal solutions for the structural transformation of information systems by creating dynamic simulation models of the transformation of information systems.

3. Structural and logical models of information systems

Information systems of organizations are complex large systems, which does not allow all management decisions regarding structural transformations to be checked in practice. Because it carries the risk of stopping the system and great losses for the organization. But from time to time information systems need structural transformations, in particular, to ensure the required level of their survivability. This happens because, at the first stages of creating information systems, the organization tries to put the information system into operation as soon as possible to receive functional support from it. Setting the task of creating an information system at the first stages may not take into account all the necessary factors. In addition, at the first stages of creating an information system, all the necessary factors may simply not yet manifest themselves and, accordingly, be simply unknown to the developers of the technical task. Further, as the information system is operated, the necessary experience is gained, problem areas are identified, old and new threats are identified, etc. All this may lead to the need to transform the structure of the information system. For example, a common approach is to tie the structure of the information system to the structure of the organization. And for a quick start, that's probably true. But, for example, when creating ERP systems based on the developments of market leaders in the development of ERP systems, the structure of the information system is tied to business processes, which will not necessarily reflect the organizational structure.

Thus, there is a need for periodic structural transformations of information systems. Secondly, checking management decisions regarding transformation in practice is an expensive and dangerous measure. Therefore, it is advisable to use simulation modeling to check the consequences of management decisions and to find optimal solutions for the structural transformation of information systems.

As an atomic (elementary) model of a structure node, we define a certain functional element, at the input of which input resources are received, and at the output, the useful effect is obtained (Fig. 1). The atomic model formalizes the transformation of input resources (equipment, materials, money, personnel, information, know-how, reputation, license, experience, time, etc.) into the output useful effect (safety, profit, production volume, reputation, experience, quality, efficiency, etc.).

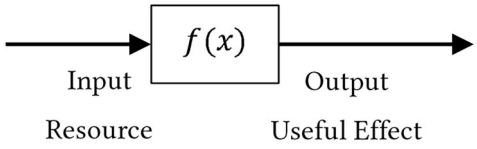

Figure 1: Atomic model of development of organizations, technologies, and information systems

The output values of one atomic model can be input to another in such a way that a complex model will be formed that is adequate for a complex real object. For example, a structural-logical model of the useful effect of the organization (profit) can have the form of a two-level hierarchy (Fig. 2), consisting of atomic models of the useful effects of personnel, production equipment, and material supply.

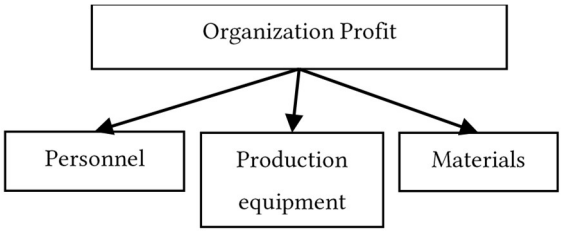

Figure 2: Structural and logical model of the organization's profit: 2 levels

As another example of a multi-level hierarchical model, we present a model for assessing the security level of an information system depending on the security characteristics of its constituent elements of the information system structure (Fig. 3).

The difficulty of creating such models is that to achieve the required level of adequacy, the complexity of the hierarchical model must be increased both vertically and horizontally. The general procedure for creating models includes:

1. Creating a set of atomic models and establishing a connection between them.
2. Analysis of the results of the current modeling on the primary model, comparison with the results of statistical and expert data on the real process.
3. Deciding to increase the adequacy of the model by complicating it, and adding new elements.

Hierarchical models of real objects often require additional relationships that are not embedded in the hierarchy structure. Fig. 4 shows examples of horizontal communication at one level of the hierarchy and diagonal communication between different levels of the hierarchy in different branches, like the well-known "thick tree" topology of telecommunication networks.

Such structures are called mixed. Research by the authors [5] showed that almost any mixed architecture without cyclic links can be transformed into a hierarchical one. At the same time, the primary mixed structure and the

corresponding hierarchical structure will be identical from the point of view of simulation modeling (Fig. 5). But at the same time, the hierarchical structure will be more organized. Therefore, it will be easier to formalize and implement it in a simulation model.

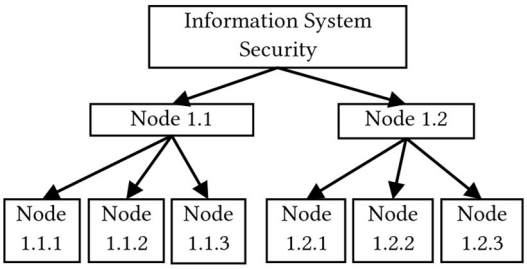

Figure 3: Structural and logical model of information system security

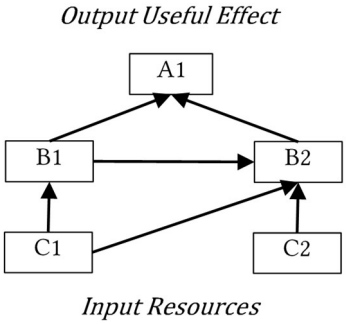

Figure 4: Primary mixed model of the "thick tree" type with diagonal and horizontal ties

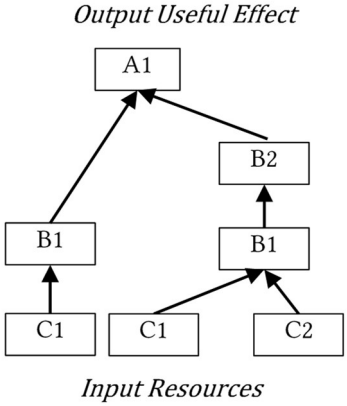

Figure 5: Hierarchical model that was formed after equivalent transformations of the primary mixed model

Mixed models emerge as a result of ongoing efforts to improve model adequacy by adding new elements and new relationships. However, the researcher must remember that for any degree of uncertainty of our knowledge about the process or phenomenon being modeled, there is a certain optimal level of complexity of the model [30]. If the model is too simple, the error is large because the model does not take into account many important factors and regularities (connections between factors). If the model is too complex, errors increase because:

1. It is not possible to provide the model with quality input data.
2. Calculation errors are increasing.
3. Calculation errors regarding secondary factors become commensurate with the errors of the main factors.

The authors' research showed [2, 5] that one of the most adequate models, which can equally successfully take into account purely technical and humanitarian factors, are logistic model.

4. Logistic development models

In the same way as for Moore's law, in the absence of restrictions on development, the dependence of the initial useful effect on input resources has the character of an exponent [2]. If the dependence of development is limited from below and above, then this indicates the presence of corresponding horizontal asymptotes, between which the dependence of development is located (the dependence of the useful effect on the spent resources). Such a dependence has an S-shaped character and is most often specified by the logistic function [2] (Fig. 6).

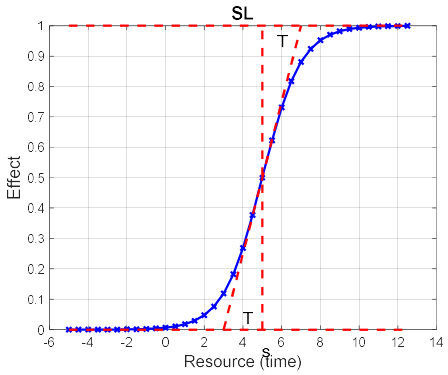

Figure 6: Logistic dependence of the useful effect of business depending on resource costs

The logistic function has the property of central symmetry and in its differential form has the form

$$\frac{dy}{dt} = m\,(y - Y_{min})(Y_{max} - y), \qquad (1)$$

where y is the useful effect, t is time (input resource), Y_{min}, Y_{max} are the lower and upper asymptotes, m is the scaling factor that determines the growth rate and the angle of inclination of the curve at the point of symmetry.

The differential form makes it possible to establish patterns regarding the growth rate at all values of input resources. The growth rate of the useful effect is proportional to the product of the distances of the value of the useful effect from the lower $(y - Y_{min})$ and upper $(Y_{max} - y)$ asymptotes.

With constant coefficients m, Y_{min}, Y_{max}, the given differential equation has analytical solutions

$$y = Y_{min} + \frac{Y_{max} - Y_{min}}{1 + e^{-(m\,(Y_{max} - Y_{min})(\,t - \Delta t))}}. \qquad (2)$$

Here Δt is the shift of the point of symmetry along the abscissa axis.

Let us introduce a special notation for the SL-function [2], which is a characteristic part of the expression and can be considered a normalized logistic dependence increasing from 0 to 1

$$SL_0(t-\Delta t)=\frac{1}{1+e^{-(m\,(Y_{max}-Y_{min})(\,t-\Delta t))}}. \quad (3)$$

To simplify the parametric identification of logistic dependence, we will introduce additional notations: a, d are upper and lower asymptotes, s is abscissa of the point of symmetry, T is constant of logistic dependence. The coefficient T significantly simplifies the identification of the growth rate of the logistic curve at the point of symmetry.

5. Computer model of dynamics of structural transformation

We will use logistic dependencies to build a general dynamic model of the transformation of the information system at the stages of growth of the useful effect of the organization

$$y=d+(a-d)\cdot SL_0(t-s), \quad (4)$$

and at the stages of the decline of the useful effect of the organization

$$y=d-(a-d)\cdot SL_0(t-s). \quad (5)$$

In the second case, the amplitude of the logistic dependence has a negative value $(a-d)$.

The integral form of logistic dependence has the form

$$y=SL(t)=d+\frac{a-d}{1+e^{-\frac{2}{T}(t-s)}}. \quad (6)$$

The resulting useful effect (level of information security) at an arbitrary moment in time is found as the sum of various logistic components with positive and negative signs.

$$SL_\Sigma(t)=SL_+(t)+SL_-(t)+SL_{1-}(t)+SL_2(t), \quad (7)$$

where $SL_+(t)$ is the dependence of the growth of the useful effect for the primary structure of the information system.

$SL_-(t)$ is the dependence of the drop in the useful effect for the primary structure of the information system due to changes in external conditions and the security situation.

$SL_{1-}(t)$ is the dependence of the drop in the useful effect for the primary structure of the information system as a result of the managerial decision to replace it with a more progressive one.

$SL_2(t)$ is the dependence of the growth of the useful effect for the new structure of the information system.

Any input resource or a combination of them can be used as a logistic dependency argument. In our case, the input resource is time. The general picture of changes in the level of information security depending on time contains characteristic stages of growth, decline, re-growth after transformations, etc. Modeling of the life cycle of the level of information security of the information system was performed for the indicator tFall=10 weeks. The value of tFall is equal to the abscissa of the symmetry point of the dependence of the fall of the security level $SL_-(t)$, which occurs as a result of changes in external conditions and the security situation. Simplistically, it can be said that the value of tFall characterizes the time of moral aging of existing protection technologies and the existing structure of the information system.

In conditions where the time indicators of the moral aging of technologies and structures are known (at least approximately), it is important to reasonably choose the time of the beginning of the transformation of the structure and protection technologies tReform (the abscissa of the point of symmetry of the dependence $SL_2(t)$ of the increase in the level of information security for new technologies and new structures of the information system).

Minimization of the information security level can be used as optimality criteria

$$\max_{t_{Reform}} \min_{t} SL_\Sigma(t) \quad (8)$$

or an integral indicator of the level of information security for the period of work $[t_0, t_1]$ in the conditions of transformation

$$\max_{t_{Reform}} \left\{ \int_{t_0}^{t_1} SL_\Sigma(t)\,dt \right\}. \quad (9)$$

In our case, the model was tested for the integral indicator. The mathematical model was implemented in the form of a simulation model in the MatLab algorithmic language. An example of simulation results is shown in Figs. 7–11. The value of tReform varied in the range from 25 to 1.

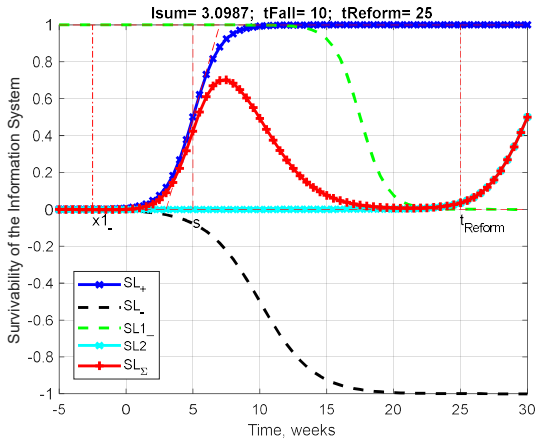

Figure 7: Results of information security level modeling (tFall=10, tReform=25)

Scenario 1 (Fig. 7) with tReform=25 showed that the reforms were significantly delayed. The indicator of the quality criterion is equal to only Isum=3.097. That is, even the integral indicator shows that most of the time the system was practically unprotected. For more than half of the simulation time, the final level of information security is critically low.

Scenario 3 (Fig. 9) with tReform=10 predicts the beginning of transformations in a time commensurate with the time of moral aging of technologies and structures. Therefore, the integral criterion has a rather high level of Isum=17.495. The situation can be assessed as satisfactory.

Scenario 4 (Fig. 10). At tReform=5, the integral criterion also has a high level of Isum=19.3381. There is no noticeable gain in reducing the duration of low-security levels. The script can be characterized as a work on prejudice. But the question arises—whether transformations happen too often. Will such a frequency of transformation leave time for the planned operation of the information system?

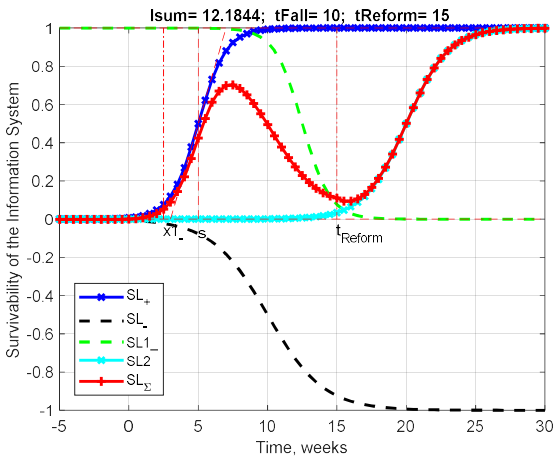

Figure 8: Results of information security level modeling (tFall=10, tReform=15)

Scenario 2 (Fig. 8). tReform=15. The integral quality criterion increased almost 4 times Isum=12.1844. The duration of a critically low level of system protection has also decreased several times. But in general, the level of security should not be considered satisfactory.

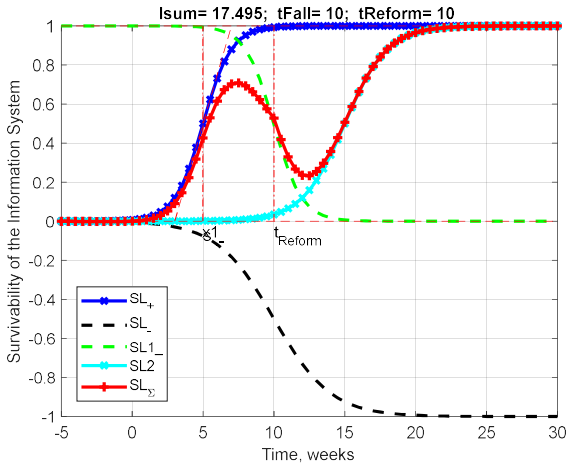

Figure 9: Results of information security level modeling (tFall=10, tReform=10)

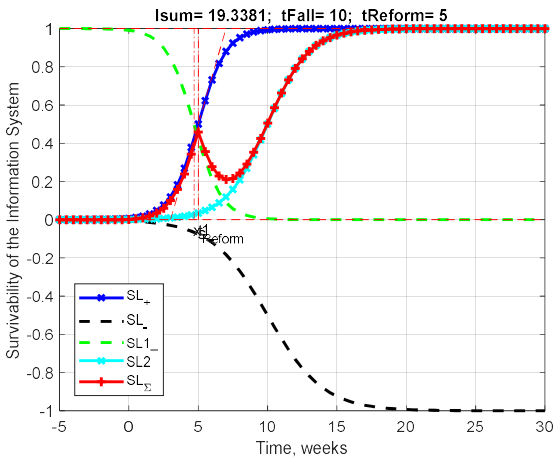

Figure 10: Results of information security level modeling (tFall=10, tReform=5)

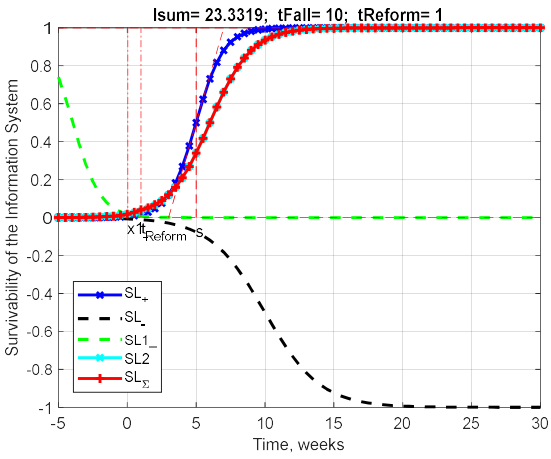

Figure 11: Results of information security level modeling (tFall=10, tReform=1)

Scenario 5 (Fig. 11) (tReform=1, Isum=23.3319) has the best indicators of the integral quality criterion. However, the transformation begins almost simultaneously with the implementation of the previous technology and system structure. Doubts about the too-high frequency of transformations only increase here.

6. Conclusions

The paper proposes a computer model of the transformation of technologies and the information structure of the information system to ensure the survivability of the information system based on ensuring the required level of information security.

The model as part of the management decision support software system allows you to predict the consequences of various management decisions to choose the best one.

The paper uses the criterion of maximizing the lowest level of the organization's useful effect over the entire forecasting period. The integral criterion of the total beneficial effect that the organization will receive in the event of the implementation of a specific transformation scenario is also used.

Directions for further research. To choose the best transformation scenario, it is necessary to add some additional criteria or check the optimality according to the selected integral criterion not at individual points, but at the entire set of permissible values of the tFall and tReform parameters.

References

[1] V. Svanadze, Near Future of Cyber Security and New Trends in Cyberspace, Global Foundation for Cyber Studies and Research (2020).

[2] V. Shevchenko, Optimization Modeling in Strategic Planning, Military and Strategic Research Centre of National Defence University of Ukraine (2011).

[3] V. Shevchenko, et al., Mathematical modeling of processes: Study guide, Taras Shevchenko National University of Kyiv (2020).

[4] A. G. Dodonov, D. V. Lande, Vitality of Information Systems, Nauk. Dumka (2011).

[5] Y. Syvytsky, V. Shevchenko, Computer Simulation Model of the Organization at the Stage of Transformation for the Purpose of Adaptation to New Projects, in: 14th International Scientific and Practical Conference from Programming UkrPROG'2024 (2024).
[6] V. Svanadze, Doctoral Thesis "Cybersecurity Policy and Strategy of Management", Georgian Technical University (2023).
[7] M. Antunes, et al., Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal, J.Cybersecur. Priv. 1 (2021) 219–238. doi: 10.3390/jcp1020012.
[8] E. Y. Handri, P. A. W. Putro, D. I. Sensuse, Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government, in: IEEE Int. Conf. on Cryptography, Informatics, and Cybersecurity (ICoCICs) (2023) 82–87. doi: 10.1109/icocics58778.2023.10277024.
[9] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education:" Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.
[10] A. Storchak, S. Salnyk, A Method of Assessing the Level of Security of the Network Part of a Special Purpose Communication System Against Cyber Threats, Inf. Proces. Syst. 3(158) (2019) 98–109.
[11] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th Int. Conf. on Problems of Infocommun., Sci. and Technol. (2021). doi: 10.1109/picst54195.2021.9772181.
[12] O. Arkhypov, Application of a Risk-based Approach using Reflexive Risk Models in Building Information Security Systems, in: 1st Int. Workshop CITRisk (2020) 130–143.
[13] H. Shevchenko, et al., Information Security Risk Analysis SWOT, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 309–317.
[14] J. Brown, Executive's Cybersecurity Program Handbook: A Comprehensive Guide to Building and Operationalizing a Complete Cybersecurity Program, Packt Publishing (2023).
[15] O. Arkhypov, Y. Arkhypova, J. Krejčí, Adaptation of a Risk-based Approach to the Tasks of Building and Functioning of Information Security Systems, in: 2nd Int. Workshop on Computational & Information Technologies for Risk-Informed Systems, vol. 3101 (2021) 83–92.
[16] S. Shevchenko, Y. Zhdanova, K. Kravchuk, Information Protection Model based on Information Security Risk Assessment for Small and Medium-Sized Business, Cybersecur. Edu., Sci., Technique 2(14) (2021) 158–175. doi: 10.28925/2663-4023.2021.14.158175.
[17] V. L. Shevchenko, et al., Computing methods: Study guide, Taras Shevchenko National University of Kyiv (2019).
[18] V. L. Shevchenko, et al., Predictive Modeling of Computer Virus Epidemics, K.: UkrNC RIT (2019).
[19] V. Shevchenko et al., Management of Defense Resources in the Armed Forces of Ukraine – NSRC DT and MS of Ukraine (2002).
[20] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.
[21] H. Hulak, et al., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, in: 2nd Int. Conf. on Conflict Management in Global Information Networks, vol. 3530 (2023) 102–111.
[22] O. Dovgan, Critical Infrastructure as an Object of Protection Against Cybernetic Attacks, Information Security: Challenges and Threats of Modernity: Materials of a Scientific and Practical Conference (2013) 17–20.
[23] S. Toliupa, I. Parkhomenko, H. Shvedova, Security and Regulatory Aspects of the Critical Infrastructure Objects Functioning and Cyberpower Level 142 Assesment, in: 3rd Int. Conf. Adv. Inf. Commun. Technol. (2019) 463–468.
[24] L. Slipachuk, S. Toliupa, V. Nakonechnyi, The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine, 3rd Int. Conf. Adv. Inf. Commun. Technol. (2019) 451–454.
[25] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 240–245.
[26] V. Shevchenko, et al., Designing of Functionally Stable Information Systems Optimal for a Minimum of Losses, in CADSM 2019, 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM) (2019) 36–40. doi: 10.1109/CADSM.2019.8779299.
[27] V. Shevchenko, D. Rabchun, Setting the Problem of Resource Optimization of a Complex of Software Means of Information Protection in the Conditions of Dynamic Information Confrontation, Weapon Systems and Military Equipment, 3(51) (2017) 89–94.
[28] A Guide to the Project Management Body of Knowledge PMBOK, 6th edition, Project Management Institute, Inc. (2017).
[29] A Guide to the Project Management Body of Knowledge PMBOK, 7th edition, Project Management Institute, Inc. (2021).
[30] Y. P. Zaichenko, Fundamentals of Designing Intelligent Systems: [Learning. Manual], Slovo Publishing House (2004).