Scalarization of the vector criterion of information system survivability based on information security indicators

Oleh Bakaiev[1,†], Ihor Syvachenko[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 considers the formulation of the problem of ensuring the survivability of the information system in the presence of harmful external influences. The main factors affecting survivability are identified, such as the level of information security and the level of cyber security. The possible structure of the vector criterion of survivability, which is based on indicators of the level of information security according to the security profiles of the information system: integrity, availability, and confidentiality, is analyzed. Considered ways of transition from a multi-criteria optimization problem to a single-criteria one: the method of transformation of criteria into constraints and the method of scalarization of a vector criterion. The method of scalarization of the vector criterion using scalar convolutions was chosen as the main method of transition to a single-criteria optimization problem. It was determined that additive convolution was the most widespread in scalarization problems. For the use in one convolution of criteria that may differ in physical nature, approaches were considered for the normalization of information security level values according to security profiles and the normalization of the corresponding weighting factors. An information security level assessment model based on additive convolution was created for the scenario when all component indicators and weighting factors dynamically change according to periodic laws. The simulation result shows the dynamics of changes in the general level of information security, which directly affects the level of survivability of the information system. It is shown that the obtained result is not trivial and the model is practically useful. The simulation model was created using the MatLab algorithmic language.

Keywords

information system, model, scalarization, additive convolution, survivability, cyber security, information security, evaluation, management, decision support

1. Introduction

Digital technologies permeate all spheres of society. A large number of industries can no longer exist without computer support. Digital systems facilitate and speed up many processes of people's activities. But digital accessibility, at the same time, facilitates the implementation of harmful effects on information systems. This reduces the survivability of information systems. Survivability is the ability of an information system to maintain its performance in conditions of harmful effects on the information system. One of the most common types of impacts on the survivability of information systems is impacts on information security, in particular its component—cyber security. Ensuring survivability is relevant for information systems at all levels: personal, corporate, state, and global. Ensuring the viability of information systems that process any state and community information [1], public and private sector enterprises [2], scientific and educational information [3, 4], as well as the personal information of citizens of Ukraine and citizens of Ukraine's partner countries is urgent. This is evidenced by the analysis of the main trends regarding the state of cyber security in the world [5]. This question became especially relevant in the conditions of the full-scale war of the Russian Federation against Ukraine.

Unfortunately, any use of information protection leads to a decrease in performance. That is, the protection systems themselves, in a certain sense, are also a threat to the efficiency, that is, to the survivability of the system. A certain balance is required between the level of protection and the functionality of the information system. For this, it is necessary to optimize information protection according to all information protection profiles: integrity, confidentiality, and availability. That is, it is necessary to solve a multi-criteria problem, according to at least three criteria. Others can be added to these criteria directly related to safety and survivability, for example, minimum time to identify hazards, minimum time to create a security system, minimum costs for security, etc. One of the effective ways to solve multicriteria problems is to reduce them to single

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
oleg.bakaiev@gmail.com (O.Bakaiev);
igor.syvachenko@gmail.com (I. Syvachenko);
gii2014@ukr.net (V. Shevchenko)

0009-0004-5427-1196 (O. Bakaiev);
0009-0005-3248-3371 (I. Syvachenko);
0000-0002-9457-7454 (V. Shevchenko)

criteria using scalar convolutions, among which additive convolutions are the most common.

2. Analysis of existing studies

Usually, the costs of information protection correlate with the costs of information technologies that need protection. The best global practices operate with information protection costs in the range of 10–20% of the company's information technology costs [6]. When making decisions about the specific amount (or share of costs) for information protection, the scale of the information system, the range of tasks it processes, the mode of operation, the quantitative and qualitative indicators of personnel, users, requirements for system performance, etc., must be taken into account. Issues of resource optimization are discussed in [7]. In the conditions of war, special attention should be paid to possible malicious influences. This component is currently poorly developed and does not have adequate models of malicious influences of a military nature, which would help model the situation to find the best protection solution.

General approaches to creating models that allow predicting the consequences of management decisions and finding optimal solutions are considered in [8, 9]. Models based on additive convolutions are presented in [8–10]. Dynamic models of information security based on an epidemiological approach are considered in [11]. However, these approaches do not cover all aspects of survivability, including information security. More complex approaches are presented in [12, 13]. In work [12], the model of cyber protection in the information system of the situational center is considered. In work [13], dynamic models of the state of cyber security based on the assessment of the guarantee capability of automated information systems of critical infrastructure objects are considered. Ensuring the cyber security of critical infrastructure facilities today in the conditions of war in Ukraine is one of the main tasks. In [14], a general analysis of the danger of cybernetic attacks on critical infrastructure is performed. Regulatory aspects of ensuring the information security of critical infrastructure objects are considered in [15]. Approaches to cyber protection of critical infrastructure based on integrated systems at the national level are studied in [16]. The issue of protecting critical infrastructure objects from cyber-attacks by decentralizing telecommunication networks is discussed in [17]. The advantage of works [13–17] is the systematic study of the issue. The disadvantage is the concentration on the features of critical infrastructure objects only. The situation requires universal approaches that could ensure the survivability of information systems within the framework of Ukraine's digital transformation.

General approaches to information security and cyber security management are considered in [18, 19]. More specific methodical approaches of NIST standards for assessing and ensuring cyber security in the creation of electronic government are considered in [20]. Targeted management is possible only if there are metrics and methods for evaluating the state of the process. Approaches to assessing the level of information security in distributed wireless systems are considered in [21]. Methods of assessing the level of security of communication systems against cyber-attacks are studied in [22]. Approaches to the audit of information infrastructure are presented in [23]. Approaches to assessing information security risks are studied in [24, 25]. Methodical approaches to the creation and implementation of complex cybersecurity programs are presented in [26]. Approaches to assessing information security risks and creating information security systems are presented in [27, 28]. Unfortunately, in works [18–28] we did not receive the appropriate development of the model based on additive convolutions, which reduced the possibilities of numerically taking into account all the necessary representative factors, in particular, and not only safety factors.

3. The purpose of the work and optimality criteria

The purpose of the work is the development of models and methods for optimizing information protection according to many criteria by reducing multi-criteria problems to single-criteria ones using scalar additive convolutions.

On the way to the set goal, it is necessary to take into account the fact that on the scale of the organization, costs for information technology and costs for information protection exist within the framework of a single budget. The problem arises of its optimal distribution between functionality and protection on two levels:

1. At the stage of creation of defense systems and information systems in general by establishing the share of defense funding within the general budget.
2. During operation, the computing resource of the information system is between tasks of basic functionality and tasks of information protection. This is done by choosing the mode of operation of the protection system (setting the degree of protection of the information system) by the security scenario of the information system [7].

At the strategic level, certain types of resources can be the governing parameters that determine the level of survivability, in particular, information system protection: $R_{B\,Sys}$ is a resource spent on creating an information system, $R_{B\,Sec}$ is a resource spent on creating an information protection system, $R_{W\,Fun}$ is an information resource spent on the main functions of the system, $R_{W\,Sec}$ is an information resource spent on information protection.

The main quality criteria, according to which information protection optimization should be performed, are as follows: $I_1 = I_{Sec}$ is level of information security, $I_2 = I_{Fun}$—the level of ensuring system functionality, $I_3 = I_{Pr\,B}$ is the level of budget savings in the creation of information technologies, $I_4 = I_{Pr\,W}$ is the level of budget savings when using information technologies.

On the one hand, the given list of criteria can be expanded with other criteria by the situation and clarification of the problem statement. On the other hand, the given criteria can be a collapse of more detailed additional criteria. For example, the information security level criterion may consist of the following subcriteria: $I_{11} = I_{1\,Int}$ is ensuring information security according to the integrity profile (Integrity), $I_{12} = I_{1\,Ava}$ is ensuring information security according to the availability profile

(Availability), $I_{13} = I_{1\,Con}$ is ensuring information security according to the confidentiality profile (Confidentiality).

As you can see, a two-level hierarchy of quality criteria of the optimization process is formed. However, the number of levels of the hierarchy of criteria can be greater. For example, the integrity criterion may contain the following components: $I_{111} = I_{11\,Phy}$ is the level of ensuring data integrity at the physical level (physical destruction of the information carrier), $I_{112} = I_{11\,Prg}$ is the level of ensuring data integrity at the program level (program erasure of information), $I_{113} = I_{11\,FAT}$ is data integrity level at the addressing level (destruction of the FAT file location table).

The number of levels of the hierarchy of quality criteria is determined according to the statement of the problem.

As you can see, many of the criteria are contradictory. Most of the criteria cannot be nested in a complementary hierarchy, such as a situation where improving the integrity criterion can simultaneously improve the performance of the availability criterion. In most cases, the situation is different. For example, the minimum time criterion is contradictory to the minimum cost criterion. Because if you need to speed up the execution of the task, then you need to spend more resources on its implementation (more funding, more equipment, more personnel).

4. Transition to a single-criteria problem by the method of replacing criteria with restrictions

It is precisely because of the inconsistency of the criteria that multi-criteria optimization problems have great difficulties in solving them. To solve the problem, multi-criteria problems are converted to single-criteria problems. The main methods of transition to single-criteria problems are the following: replacing criteria with restrictions and convolution of criteria.

Replacing part of the criteria with restrictions. For example, the minimum time criterion

$$I_t = t_{max} \to min \tag{1}$$

can be replaced by a limitation—to spend no more than a certain time on execution

$$t_{max} \le t_1. \tag{2}$$

Or the minimum cost criterion

$$I_m = m_{max} \to min \tag{3}$$

replace with restrictions—spend no more than a given amount of money on the project

$$m_{max} \le m_1. \tag{4}$$

Usually, all criteria except one, the most uncertain, the most variable, or the most important, are turned into constraints. After that, a solution to the single-criteria optimization problem is found, taking into account the constraints.

For example, the task of minimizing time, finances and simultaneously maximizing the effect

Task 1.

$$I_t = t_{max} \to min,\ \ I_m = m_{max} \to min,\ \ I_e = e_{max} \to max \tag{5}$$

can be transformed into one of the following problems with constraint.

Task 2.1.

$$I_t = t_{max} \to min, m_{max} \le m_1, e_{min} \ge e_1. \tag{6}$$

Task 2.2.

$$t_{max} \le t_1, I_m = m_{max} \to min, e_{min} \ge e_1. \tag{7}$$

Task 2.3.

$$t_{max} \le t_1, m_{max} \le m_1, I_e = e_{max} \to max. \tag{8}$$

Unfortunately, it is not always clear which problem 2.1, 2.2, or 2.3 is the most adequate to the primary formulation of problem 1. Secondly, this transformation of the problem is not always adequate in principle. Such a transformation occurs relatively easily if the importance of one criterion is much higher than the importance of others. If all criteria have approximately the same importance or the importance changes over time, then such a transformation of the problem statement may not be sufficiently justified.

5. Transition to a single-criterion problem by the method of scalar convolution

In such cases, another approach can be used—criteria convolution (or vector criterion scalarization). At the same time, it is worth remembering that for the criteria to be used together in a single calculation procedure, they must be normalized, that is, brought to a single scale of values. In this case, it will be possible to build a general dependency to determine the assessment of the level of information security of the information system as a whole

$$I_1 = f_1(I_{11}, I_{12}, I_{13}). \tag{9}$$

A similar dependency can be used at the next level

$$I_{11} = f_{11}(I_{111}, I_{112}, I_{113}). \tag{10}$$

An additive convolution can be used as a function f [8–10]

$$I_i = \sum_{j=1}^{n} I_{ij}. \tag{11}$$

Here j is the index of constituent elements at the i^{th} level of the hierarchy, n is the number of constituent elements at the i^{th} level of the hierarchy, I_{ij} is the criterion of the lower level of the hierarchy (component of the vector criterion), I_i is the criterion of the upper level of the hierarchy (scalarized criterion).

Additive (or it is also called linear) convolution is the most widespread type of scalar convolution. It is called scalar because it allows us to move from multi-criteria optimization (when we have a multi-dimensional vector of criteria) to single-criteria when the optimization criterion is represented by a scalar value. Additive convolution collapses the set of criteria I_{ij} to one scalar criterion I_i. Next, to simplify the study, we will consider the features of scalar convolutions on the example of a one-level convolution

$$I = \sum_{i=1}^{n} y_i. \tag{12}$$

Here i is the serial number of a separate criterion, n is the total number of criteria, y_i is the component of the collapsing vector criterion, I is a scalar criterion resulting from the convolution.

It is worth noting that the y_i criteria have different importance. Therefore, weight coefficients β_i are usually used, which determine the importance of the relevant criteria

$$I = \sum_{i=1}^{n} \beta_i y_i. \tag{13}$$

Weighting factors are determined expertly based on experience and according to the scenario under consideration. The fact is that different scenarios targeted by the optimization task can have different sets of weighting factors. This should be taken into account when preparing assessments by experts. It would be better to determine the values of the weighting factors based on more objective data. However, this requires a clear mathematical procedure, which is usually simply absent at the initial stages of research. Expert assessment in such a case is a quick decision, which, regardless of its inaccuracy in details, gives a good assessment in general. That is, with the help of expert evaluation, it is possible to determine the value of the weighting coefficients at a level that allows you to adequately find a scalar criterion based on several known constituent criteria. But that's not all.

6. Normalization of scalar convolution

For various components of quality criteria to work together, they must be normalized. For example, so that they all have values in the same range of values. Most often, the range from 0 to 1 is used as such a range. Then, if the non-normalized values of individual criteria were equal to y_i, and the maximum possible value of the corresponding criterion is equal to $y_{max\,i}$, then the normalized value of the criterion will be equal to

$$\bar{y}_i = \frac{y_i}{y_{max\,i}}. \quad (14)$$

The weighting coefficients also need to be normalized. For this, their values are selected in such a way that they add up to unity.

$$\sum_{i=1}^{n} \beta_i = 1. \quad (15)$$

In this case, the result of scalarization will also be in the range from 0 to 1, which significantly simplifies the analysis of the situation for criteria that have a different physical (content) nature. If the sum of the weighting coefficients is not equal to one

$$\sum_{i=1}^{n} \beta_i \neq 1, \quad (16)$$

then they should be normalized. The following calculation procedure can be used to normalize the weighting factors

$$\bar{\beta}_i = \frac{\beta_i}{\sum_{i=1}^{n} \beta_i}. \quad (17)$$

As a result, the additive convolution with normalized component criteria $\bar{y}_i$, which are convoluted with normalized weight coefficients $\bar{\beta}_i$ will take the form

$$I = \sum_{i=1}^{n} \bar{\beta}_i \bar{y}_i. \quad (18)$$

Now all the constituent criteria are in equal conditions and the result of scalarization can be considered as adequate as possible.

7. Modeling of assessment of the level of information security

With the help of the given formalisms regarding the normalization of weighting factors and quality criteria, we will build a model of the level of information security, which includes components according to the profiles of integrity, availability, and confidentiality. Let's introduce the notation for the weighting coefficients.

$\beta_{11} = \beta_{1\,Int}$—the weighting factor for ensuring information security according to the Integrity profile.

$\beta_{12} = \beta_{1\,Ava}$—the weighting factor for ensuring information security according to the availability profile (Availability).

$\beta_{13} = \beta_{1\,Con}$—the weighting factor for ensuring information security according to the confidentiality profile (Confidentiality).

The values of the weighting factors change depending on the scenario of the most likely development of events. For example, weighting factors will differ significantly in peacetime and wartime conditions. Thus, the change in weighting factors may depend on the intensity of the competitive environment and the change in the regulatory framework. At the same time, it should be noted that the weighting factors may change periodically depending on the time of day, day of the week, month of the year, or frequency of events in the business environment. To check the operability of the model of additive convolution of information security levels according to security profiles, we will introduce periodic changes in the weighting coefficients according to the profiles of integrity β_{11} and availability β_{12}. Since the sum of the normalized weighting factors must be equal to one, the weighting factor for the privacy profile β_{13} can be found in the expression

$$\beta_{13} = 1 - \beta_{11} - \beta_{12}. \quad (19)$$

The dynamics of changes over time in the values of the weighting coefficients of the importance of protection according to the profiles of integrity β_{11}, availability β_{12} and confidentiality β_{13} are presented in Fig. 1. The corresponding phase trajectories in two-dimensional space are presented in Fig. 2, Fig. 3, in three-dimensional space in Fig. 4.

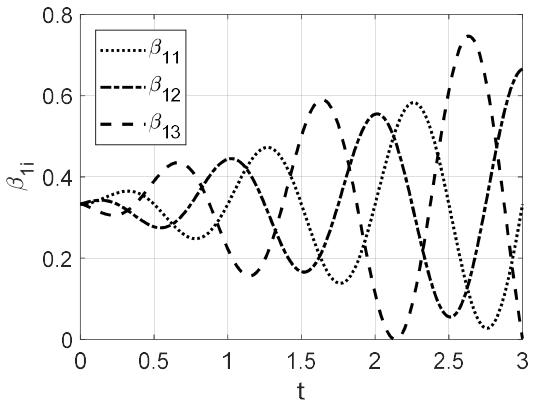

Figure 1: The dynamics of changes over time in the values of the weighting coefficients of the importance of protection according to the profiles of integrity β_{11}, availability β_{12} and confidentiality β_{13}

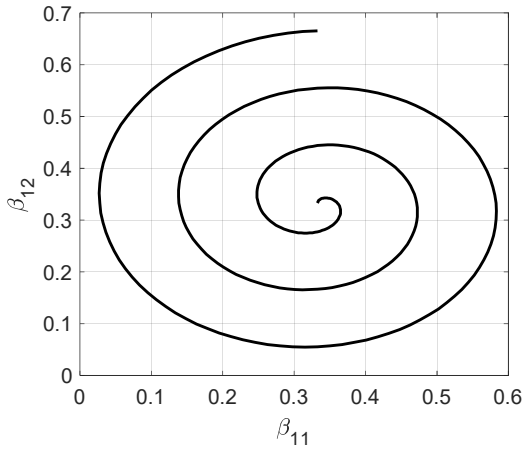

Figure 2: Two-dimensional phase trajectory of the change in the weighting coefficients of the importance of protection according to the profiles of integrity β_{11} and availability β_{12}

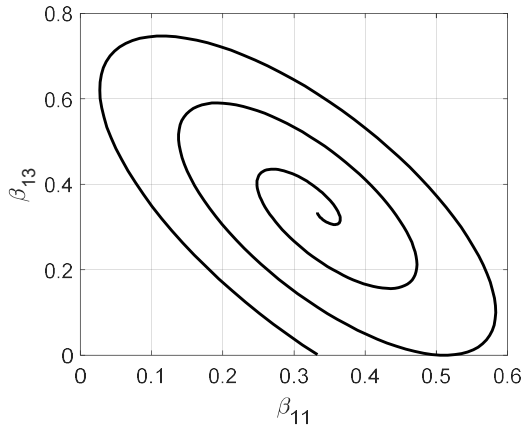

Figure 3: Two-dimensional phase trajectory of the change in weighting coefficients of the importance of protection according to the profiles of integrity β_{11} and confidentiality β_{13}

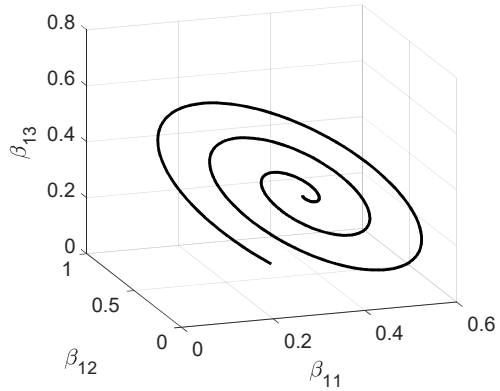

Figure 4: Three-dimensional phase trajectory of the change of weighting coefficients of the importance of protection according to the profiles of integrity β_{11}, availability β_{12} and confidentiality β_{13}

We will present the information security level model as follows

$$I_1 = \sum_{j=1}^{3} \beta_{1j} I_{1j}. \quad (20)$$

Here β_{11}, I_{11}—weight factor and level of ensuring information security according to the integrity profile, β_{12}, I_{12}—weight factor and level of ensuring information security according to the availability profile, β_{13}, I_{13}—the weighting factor and the level of ensuring information security according to the confidentiality profile. At the same time, we take into account that all the specified values change over time and depending on the information risk scenario. That is, the refined model takes the form

$$I_1(t) = \sum_{j=1}^{3} \beta_{1j}(t)\, I_{1j}(t). \quad (21)$$

If the values of the levels of ensuring information security according to the security profiles of integrity, availability, and confidentiality do not change over time and are equal to each other (Fig. 5)

$$I_{11} = I_{12} = I_{13}, \quad (22)$$

then the resulting level of ensuring information security $I_1(t)$ also does not change over time (Fig. 6) without referring to the significant dynamics of changes in weighting factors (Fig. 1).

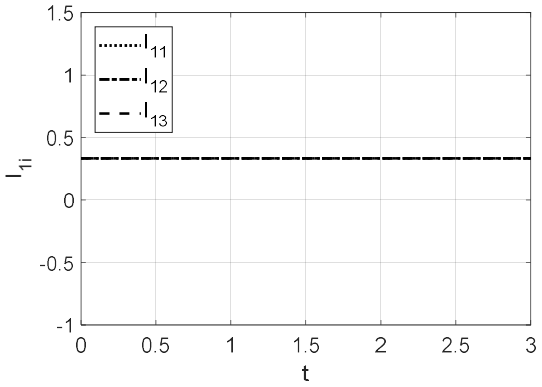

Figure 5: Values of information security levels according to the profiles of integrity I_{11}, availability I_{12} and confidentiality I_{13}, provided that the specified security levels are equal

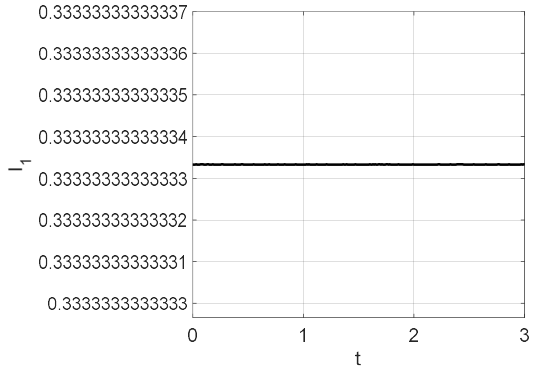

Figure 6: The dynamics of changes in the resulting level of information security ensuring I_1 under the condition of equality of components according to the profiles of integrity I_{11}, availability I_{12} and confidentiality I_{13}

A completely different picture is observed if the values of the levels of ensuring information security according to the profiles of integrity I_{11}, availability I_{12} and confidentiality I_{13} change dynamically over time (Fig. 7). In this case, the resulting level of information security becomes unpredictable, which increases the urgency of developing appropriate forecast models (Fig. 8). The proposed model, without resorting to formal simplicity, adequately takes into account important components of primary information. This makes it possible to obtain a forecast of the dynamics of the level of information security development, predict the consequences of management decisions, and select the optimal options for managing the information security of information systems based on various criteria.

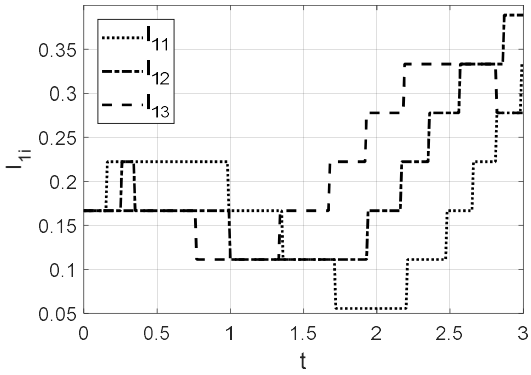

Figure 7: Values of information security levels according to profiles of integrity I_{11}, availability I_{12} and confidentiality I_{13}, subject to dynamic change over time of the specified security levels

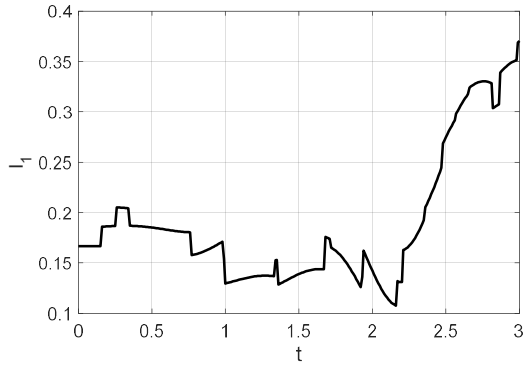

Figure 8: The dynamics of changes in the resulting level of information security ensuring I_1 under the condition of the dynamic change over time of the components according to the profiles of integrity I_{11}, availability I_{12} and confidentiality I_{13}

The problem remains to provide the model with representative input data regarding the values of the criteria. Here you can rely on data from objective observations (direct, indirect, aggregated, etc.) or, just as in the case of weighting coefficients, on data from expert assessments.

8. Conclusions

The creation of an effective information protection system requires determining the correct balance between expenses for protection and the functioning of the system.

Decisions regarding the optimization of protection should be made both for the stage of creating an information system and for the stage of its operation.

Quality criteria for information security should form a certain structure, one of which options is a hierarchical structure.

The study is planned to maximize the level of information protection according to a set of different criteria: integrity, confidentiality, availability, minimum time to detect danger, minimum resources, and minimum time to create an information security system.

Solving a multi-criteria optimization problem is a big problem. To simplify the decision, it was decided to reduce the multi-criteria problem to a single-criteria one.

The scalarization of quality criteria using additive convolution is adopted as the main method of transition to a single-criteria problem.

To simplify the processing of criteria that have different physical nature, individual criteria were normalized and weighting factors were normalized.

The directions of further research are the construction of a complete structure of quality criteria for all security profiles, as well as the approbation of the proposed approach based on simplified data of a real system containing the personal data of users.

References

[1] Y. Dreis, et al., Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection, in: Cyber Security and Data Protection, vol. 3800 (2024) 1–11.

[2] O. Burov, et al., Cybersecurity in Educational Networks, Advances in Intelligent Systems and Computing (2020) 359–364. doi: 10.1007/978-3-030-39512-4_56.

[3] V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master's Program on Cybersecurity, Advances in Computer Science for Engineering and Education II, vol. 938 (2020) 610-624. doi:10.1007/978-3-030-16621-2_57.

[4] V. Buriachok, et al., Implementation of Active Cybersecurity Education in Ukrainian Higher School, Information Technology for Education, Science, and Technics, vol. 178 (2023) 533–551. doi:10.1007/978-3-031-35467-0_32.

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

[6] V. Shevchenko, et al., Designing of Functionally Stable Information Systems Optimal for a Minimum of Losses, in: 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM) (2019) 36–40. doi: 10.1109/CADSM.2019.8779299.

[7] 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.
[8] V. Shevchenko, Optimization Modeling in Strategic Planning, TsVSD NUOU (2011).
[9] V. Shevchenko, et al., Mathematical modeling of processes: Study guide, KNU named after T. Shevchenko (2020).
[10] V. Shevchenko, et al., Management of defense resources in the Armed Forces of Ukraine – NSRC DT and MS of Ukraine (2002).
[11] V. Shevchenko, et al., Predictive modeling of computer virus epidemics, K.: UkrNC RIT (2019).
[12] 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.
[13] 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.
[14] 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.
[15] S. Toliupa, I. Parkhomenko, H. Shvedova, Security and Regulatory Aspects of the Critical Infrastructure Objects Functioning and Cyberpower Level 142 Assesment, 3rd Int. Conf. Adv. Inf. Commun. Technol. (2019) 463–468.
[16] 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.
[17] 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.
[18] V. Svanadze, Doctoral Thesis "Cybersecurity Policy and Strategy of Management", Georgian Technical University (2023).
[19] 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.
[20] 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, IEEE Int. Conf. on Cryptography, Informatics, and Cybersecurity (ICoCICs) (2023) 82–87. doi: 10.1109/icocics58778.2023.10277024.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] H. Shevchenko, et al., Information Security Risk Analysis SWOT, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 309–317.
[26] J. Brown, Executive's Cybersecurity Program Handbook: A Comprehensive Guide to Building and Operationalizing a Complete Cybersecurity Program, Packt Publishing (2023).
[27] 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.
[28] 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.