ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.5:004.75 DOI: 10.32620/reks.2025.1.18

Antonina KASHTALIAN[1], Sergii LYSENKO[1], Anatoliy SACHENKO[2,3], Bohdan SAVENKO[1], Oleg SAVENKO[1], Andrii NICHEPORUK[1]

[1] ***Khmelnitsky National University, Khmelnitsky, Ukraine***
[2] ***Research Institute for Intelligent Computer Systems, West Ukrainian National University, Ternopil, 46009, Ukraine***
[3] ***Department of Informatics and Teleinformatics, Kazimierz Pulaski University of Radom, Radom, 26600, Poland***

EVALUATION CRITERIA OF CENTRALIZATION OPTIONS IN THE ARCHITECTURE OF MULTICOMPUTER SYSTEMS WITH TRAPS AND BAITS

The independent restructuring of the architecture of multicomputer systems during operation is a complex task because such systems are distributed. A task in this restructuring is to change the architecture of system centers. That is, the system can be rebuilt without changes in its center. However, the specific tasks of systems for detecting malicious software and computer attacks require such an organization of systems that it is difficult for attackers to understand their behavior. Therefore, the current task considered in this study is the development of rules to ensure the restructuring of system centers according to different types of architecture. This work aimed to develop criteria for evaluating potential options for centralization in the architecture of multicomputer systems with traps and decoys. To ensure such an assessment, the study analyzed known solutions and established the insufficient mathematical support for organizing the restructuring of system centers during their operation. Taking into account the specifics of the tasks for such systems, no parameters were determined that could be considered for the formation of the restructuring of system centers. The analyzed works establish the main types of centralization used in systems' architecture: centralized, partially centralized, partially decentralized, and decentralized. However, algorithms and methods for transiting systems from one type to another in the process of their functioning are not provided. ***Subject****. The present work defines characteristic properties that can be used when synthesizing systems. They determine the number of potential variants of the system architecture to which they will switch in the next step when deciding about restructuring the architecture. With an increase in the number of characteristic properties, the number of possible variants increases. When approving the variants for the transition, it was necessary to evaluate them by considering the previous experience of the systems' functioning. To evaluate potential centralization variants in systems architecture, evaluation criteria were developed. A feature of the evaluation criteria is that according to them, it is possible to consider the experience of using the centralization variant in the case of repetition and evaluate the prepared variants that are offered for the first time. In other words, the evaluation criteria include previous experience of the functioning of multicomputer systems. This experience made it possible to evaluate the repeated option based on the results of its previous use. This made it possible to diversify the selection of system centers.* ***Methods****. In this study, we developed an objective function to evaluate the next centralization option in the system architecture. The objective function considers four evaluation criteria: operational efficiency, stability, integrity, and security. These criteria are focused on evaluating potential system centers' options. New mathematical models were developed for the criteria for operational efficiency, stability, integrity, and security in relation to the system center, which, unlike the known mathematical models for evaluating system centers for selecting the next options for centralization, are presented in analytical expressions that take into account the features of the types of centralization in the system architecture, indicators of operational efficiency, stability, integrity, and security in relation to the system center, and allow forming on their basis an objective function for evaluating options for centralization in systems, the feature of which is the hiding of components with the system center from detection by attackers.* ***Results****. The study analyzed the results of an experiment conducted with a prototype of the proposed system. The convergence of the experimental and theoretical results was established.* ***Conclusion****. This study introduces mathematical models for evaluating system centers based on operational efficiency, stability, integrity, and security criteria. Unlike existing models, they are presented as analytical expressions that account for various centralization types in system architectures. The models enable the creation of objective functions to evaluate centralization options, thereby emphasizing the concealment of system center components from attackers. The experimental results with a system prototype confirm the validity of the theoretical models, showing minimal deviations in the function graphs. Significant deviations in specific time intervals are addressed to optimize the centralization options.*

Keywords: *centralization; deception systems; deception systems synthesizing; distributed systems; honeynet; trap; baits; malware detection.*

1. Introduction

1.1. Motivation

Many systems for warning, detecting, and countering malicious software and computer attacks are synthesized in such a way that during their operation, the possibility of restructuring their architecture is provided [1, 2]. Such capabilities of systems are especially characteristic [3] for deception systems, systems with traps and decoys, etc. In addition, capabilities for restructuring architectures can be realized in highly specialized systems [4]. For example, in sandboxes.

The capabilities for restructuring the architecture of systems declared by many developers of commercial systems for warning, detecting, and countering malicious software and computer attacks are difficult to study because the time of such restructuring, its depth and breadth, the reasons for its restructuring, etc., are unclear. This is due to the peculiarities of the scope of application of such systems. All such systems are directed against malicious actions and therefore must be synthesized in such a way as to make it impossible for attackers to understand the principles of their functioning. In addition, modern approaches to the synthesis of such systems are those that provide for the restructuring of their architecture in the process of functioning independently, that is, without the involvement of the user [3, 4].

The difficulties associated with implementing the restructuring of the architecture of system increase for distributed systems compared to host systems. The capabilities of host systems in the context of the number of possible options for confusing an attacker [3] are significantly lower than those of distributed systems. The need for new technological solutions for all computer systems is widespread, but corporate networks play a special place among them because they have become part of the business processes of enterprises and therefore play an important role in the economy. The protection of information in such systems by various means, the functioning of which is difficult for attackers to understand, or which are new solutions, remains a pressing problem. Therefore, we consider multi-computer systems [3, 4] for the prevention, detection, and counteraction of malicious software and computer attacks in corporate networks.

When implementing the direct restructuring of the architecture of multicomputer systems, one of the main areas of research is the centers of such systems. Depending on the established options for forming the center of systems, the organization and restructuring of such systems can be more effective. In other words, possible options for the architecture of systems can be determined by developers at the design stage and remain unchanged throughout the entire period of operation of such systems, which significantly simplifies attacker-related research. To significantly increase the number of options in which multicomputer systems can exist, it is necessary to develop approaches that ensure the formation of a large non-deterministic number of options by the systems themselves in the process of their direct operation. The following options for the architecture of such systems, including their centers, should be such that they ensure the stability of the functioning of the systems and the continuation of solving problems by the systems. That is, the following options for systems should not be such that the systems are unbalanced or start performing tasks without considering previous experience in solving them, etc. Therefore, one of the main requirements for restructuring systems is continued stability in their functioning and task performance, and the next architecture can be selected with opposite characteristics to the current architecture.

Thus, the problem of choosing the next option for centralization in the architecture of systems, the functioning of which involves restructuring their architecture without involving system administrators, is relevant in the context of finding the optimal solution without conducting a complete or significant search for options from among the possible ones.

1.2. Previous works

The architecture of multicomputer systems, which includes rules for forming an indefinite number of variants when they are rebuilt without the involvement of administrators, is presented in [3, 4]. The proposed architecture of multicomputer systems is based on the synthesis of characteristic properties, which are given by 10 sets. Each set contains elements with close or opposite properties in the context of the defining characteristic defined by a certain set. Due to such division into sets and their elements, that is, the synthesis of systems through characteristic properties, the ability of multicomputer systems to obtain a large number of architecture variants when they are rebuilt has been achieved. Multicomputer systems with the architecture developed in this way [3, 4] were attributed to class $\mathfrak{S}$ systems. A feature of systems of this class is not only the ability to rebuild the architecture during operation without the involvement of an administrator but also the division of the decision-making center into two parts: the system center; the system controller. The system center prepares options for the next system actions, and the system controller, taking into account the previous experience of the system, in particular

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

with regard to tasks that are repeated over time, selects one option from the options proposed by the system center. Therefore, we will consider class $\mathfrak{S}$ systems, the architecture of which is described in [3, 4].

To confuse attackers about the system centers, a partially centralized system architecture was developed, which is described in [1]. The peculiarity of such architecture is that it provides systems during their active operation with the ability to change the architecture without involving the administrator and provides rules for forming the next option for partial centralization for the next option for partial centralization in the architecture of such systems. The developed and detailed partially centralized architecture is a partial case of the general solution for centralization in the system architecture, which is given in [3, 4], but without considering the division of the decision-making center into two parts. In [1], the effectiveness of the proposed solution was proved; thus, it became the basis for a generalized solution [3, 4].

In [2, 3], a solution was proposed for the application of distributed systems with decentralized architectures to malware detection tasks. A feature of malware detection, which is presented in detail in [2, 3], is the use of a decentralized architecture and its direct involvement in detection tasks by assessing the security levels of its components and making decisions on infecting computer stations based on a comparison of security levels. The decentralized architecture of distributed systems is also a partial solution for the architecture of multicomputer systems, which is presented in [3, 4]. Studies on the effectiveness of a solution with a decentralized system architecture have confirmed [3] the high level of malware detection and its potential use. In [4], the application of class $\mathfrak{S}$ systems was described for the highly specialized task of detecting the metamorphic functionality of malware. Because of the research and synthesis into the architecture of class $\mathfrak{S}$ systems, methods for detecting the metamorphic functionality of malware were implemented. Similarly, for class $\mathfrak{S}$ systems, the same approaches are proposed. Detection methods [5, 6] that are admissible for implementation in the architecture of class $\mathfrak{S}$ systems are combined not by simple combination or addition of the architecture but necessarily become part of the main architecture, which additionally responds to internal and external suspicious and malicious events.

Thus, in previous studies [1-4, 6], the architecture of class $\mathfrak{S}$ systems was presented, its features were considered, the necessary details of elements and components for implementation were carried out, partial cases of different types of architecture were proposed, and a strategy for using such systems with different functionalities, in particular for detecting malicious software and computer attacks, was also proposed. In addition, the possibility of using class $\mathfrak{S}$ systems as a basis for the synthesis of deception systems, systems with bait and traps, etc., was substantiated.

The formation of the next centralization option in the architecture of class $\mathfrak{S}$ systems is not sufficiently detailed in previous studies [3, 4]. The main problem that arises when choosing the next centralization option in such systems is the large number of options. When using a complete or significant partial search for options, the effectiveness of the resulting solution is lost because, over a certain time, changes occur in the system, resulting in loss of relevance of the resulting solution. A random search for the next centralization option in the system architecture is impractical due to its possible imbalance with such an approach. Therefore, the development of a method to determine the next centralization option in the architecture of class $\mathfrak{S}$ systems is necessary to improve their long-term operational efficiency.

In addition, the development of this method should include a mechanism for evaluating potential centralization options in the system architecture, considering previous experience in using centralization options.

In previous studies [1, 2], the mechanism for evaluating the next steps of the systems was different. Thus, in work [1], a partial case of the type of centralization was developed – a partially centralized system architecture. The migration of the center between components, as well as its variants, was detailed. To ensure the movement of the center of the system, mathematical models (trust levels) of the components were developed. In this case, an objective function was not developed, but trust levels for components were used. The selection of components for the transition from the center of the system to these components was based on a comparison of the trust levels of the components. The options for partial centralization in the system are changed not only by moving between components but also by using static and dynamic components. In work [2], a decentralized distributed system for detecting botnets was developed. Its feature is not only the implementation of botnet detection methods, but also the reaction of the system itself to a decrease in the security levels of its components. Security levels were determined for all components because the developed system was completely decentralized. According to these security levels, the system independently determined the computer stations in the network to block their work. Decentralization is presented as a single centralization case. Since the system is decentralized, the center was not moved, and accordingly, a method for such a move was not developed.

In previous studies [3, 4], principles and methods for synthesizing deceptive systems for detecting malicious software and computer attacks were developed. The results of this work provide the basis for the developed direction of the synthesis of deceptive systems. The principles and methods of the synthesis of deceptive systems in previous works [3, 4] require detailing. In the

work [6], in continuation of the development of deceptive systems, a detailed operational criterion was developed. This parameter was defined to evaluate potential centralization options because the operational indicator is important in the context of distributed systems. For this purpose, 19 parameters were developed in the work [6], which characterized the corporate network environment and processes and objects in the developed multicomputer system. The number of parameters requires further study to ensure the completeness of the assessment. This operational criterion can be part of a broader system for evaluating potential centralization options in the architecture of developed deceptive systems. Thus, to ensure the selection of the next centralization option in the architecture of multicomputer systems, it is necessary to develop mathematical models and a system that allow the evaluation of potential centralization options.

1.3. State of the art

The rapid development of Internet technologies requires constant improvement of solutions that ensure the security of computer systems and networks [7], data, and critical infrastructure, for which it is important to obtain information about malicious actions [8]. Some systems for preventing, detecting, and countering malicious software and computer attacks contain rules to ensure their adaptability during operation. [6]. Modern methods use game theory and machine learning methods to provide dynamic deception strategies, which allows users to observe, react, and adapt to the behavior of the attacker in both the short and long term. In decoy technology, dynamic deception methods can have a significant impact on effectiveness. Adaptability and the development of cyber deception models based on the behavior of attackers and artificial intelligence methods make decoys and their networks much more effective in countering malicious attacks. Intelligent decoys that use machine learning methods actively interact with attackers to study their behaviors and adapt. In [9], a decoy that uses reinforcement learning to interact with automated software was developed. Distributed Deception Platforms (DDP) are another modern solution that overcomes the limitations of decoys and can easily deploy cyber deception tools in networks [10].

To attract different types of attackers, a dynamic assessment of individual attackers by a cyber-deception system is used. In [11], the adaptive cyber deception system HoneyBug was proposed, which dynamically creates a personalized deception plan for web applications using false vulnerabilities that meet the expectations of attackers, which are constantly analyzed. Based on the selection, comparison, and combination of Markov and semi-Markov models, a strategy was developed to assess the reliability, availability, and cybersecurity of the cloud environment and the Internet of Things [12]. The dynamic structure of a system requires the dynamic determination of parameters. In [13], a model of parameter estimation in distributed systems with a dynamic structure was proposed, which implements heterogeneous distributed databases. Such a model allows the development of new models of support for the management of a distributed data processing system. Dynamic cyber defense systems with support for artificial intelligence methods must have the property of stability. In [14], possible sources of threats for such systems were analyzed, and methods for ensuring the properties of system stability were considered, which allowed creating stable systems using artificial intelligence by configuring the architecture and training scenarios. In [15], a method of developing and arranging a bait network was proposed, considering the scenario in which the actions of the protection tool affect the attacker, dynamically changing his strategy and tactics, and interacting and is modeled as a partially observable Markov process (POMDP).

One way to ensure the dynamic properties of decoys is virtualization. Algebraic virtual machines (AVM) allow various methods to check the properties of systems and detect behaviors specified in the form of algebraic templates [16]. In [17], a multiphase mechanism for dynamic generation of strategies for deploying virtualize decoys was proposed. This mechanism uses methods for intelligent prediction of attack propagation, combining reinforcement learning methods and the Markov decision-making process. The use of network function virtualization technologies and software-defined networks simultaneously ensures the dynamism and efficient use of resources [18]. The successful operation of decoys depends on their effective deployment.

In [19], the imperfections of traditional decoys is analyzed and substantiated. They are designed to deceive attackers. The main method for their implementation is a method that simulates vulnerable systems. These approaches are less effective in capturing and analyzing advanced threats. The authors propose the use of adaptive decoys, whose functioning is ensured by the use of artificial intelligence methods. This method is primarily focused on performing dynamic changes in the configuration and behavior of the decoy based on real-time threat intelligence. By adapting to real-time attacker tactics, these decoys provide a deeper understanding of the attacker's methods. This direction of decoy research is promising for future development.

In [20], a cyber-deception framework called CONCEAL was proposed, which is a combination of mutations, anonymity, and diversity to maximize the achievement of cyber deception goals, namely, hiding target objects and deterring attackers. Cyber deception

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

systems contain decoy objects of different types, the interaction of which strengthens the protective properties of the system. In [21], a deception mechanism was proposed that combines moving target protection with decoys in software-defined networks. In [22], a method of cyber deception based on a signal game using moving target defense (MTD) was proposed. This method allows for a deep analysis of network attacks and defense scenarios and selection of the optimal strategy based on a probabilistic model. In [23], DodgeTron, a method of autonomous active cyber deception, was proposed, which allows for a comprehensive analysis of the behavior of malicious software and automatically creates deception schemes by changing the deception parameters used by attackers, which allows distorting the attackers' decisions and transmitting falsified information to them. An important part in the development of active defense systems is testing and verifying complex cyber-deception systems under development under conditions close to real ones, as well as predicting and assessing their effectiveness. In [24], a Cybersecurity Deception Experimentation System (CDES) was proposed, which extends the open research emulator, allowing it to be used for the practical implementation of dynamic decoys in complex scenarios. In [25], an algorithm for selecting indicators for predicting the security of computer systems was proposed. This algorithm uses multilevel models in the class of linear and nonlinear models.

Given the constant development of attacks and improvement of attackers' actions, it is difficult to ensure proper protection of target systems using only passive approaches. The use of active protection mechanisms forces attackers to attack the wrong targets and thus lose them [26]. Deception mechanisms should be involved not only to prevent and delay attacks but also to confuse and attract attackers. In [27], an intelligent and adaptive agent was proposed that uses cyber deception to recognize an attacker's intentions, which involves the attacker's involvement at all stages of the attack, forming predictions of the attacker's behavior. Deception is modeled as an interactive, partially observed Markov decision-making process in the context of two agents for a problem with several types of attackers. Adaptive cloaking methods are used to design and configure decoy networks [28]. In [29], an active security control strategy that uses intervals with no attacks to provide control input data in each period was proposed, and this strategy allowed the detection of DoS attacks. In [30], a cyber-deception model was proposed, which involves the defender’s control over the attacker’s perception of the environment, which allows for an improved response to the attacker’s actions. Ensuring the cybersecurity of a cloud environment that uses virtualization is difficult due to the dynamism and complexity. In this case, mechanisms that use static implementation cannot provide sufficient protection. To solve this problem, an automated honeynet deployment system (Automated Honeynet Deployment Strategy AHDS) was proposed for active protection of a container-based cloud environment. This system allows for assessing changes in the target system structure and automatically optimizing the honeynet deployment strategy [31]. In [32], a specific group of Honeypot systems was evaluated. The detection range, emulation accuracy, data quality, reliability, scalability, performance, extensibility, installation options, configuration complexity, and maintenance requirements. The results also provided conclusions on the relative effectiveness of various Honeypot systems in different situations. The authors attributed innovations in Honeypot development to improvements in machine learning, increased automation, integration with other security tools, cloud-based frames, and deception technology using simulated attacks to record information about the attack. In [33], an organizational network in the AWS Cloud environment was developed, which includes an all-in-one decoy, TPOT, and a separate vulnerable web server and a secure web server on which working services are deployed. This allows the system to detect nine types of attacks, such as DoS, brute force attacks. New technologies and tools in the IoT industry have caused attackers to improve existing attacks and develop new attacks, which can make some of these devices vulnerable; thus, the need for cyber protection of IoT devices is increasing [34]. The disadvantages of conventional IoT decoys include scaling and management problems, and their passive nature prevents extensive malware analysis. Intelligent decoys with a high level of interaction can scale up and adapt to the requirements of the target IoT systems [35]. In [36], a proactive HoneyComb cyber-deception technique was proposed for malware forensics using IoT scanning performed in the darknet, thereby positioning this network as a large decoy. In addition, decoy objects in IoT systems have limited ability to evade attacker reconnaissance. In [37], a partially incomplete organizational modeling of IoT-based deception (IoDM) was proposed, which considered dynamic topologies and organizational goals in the IoT domain in real time based on a total-sum game.

In [37], a partially incomplete organizational modeling of IoT-based deception (IoDM) was proposed, which considered dynamic topologies and organizational goals in the IoT domain in real time based on a total-sum game. In [38], a solution for hardware security using specialized cryptographic security modules was presented. In [39], an approach for detecting cyberattacks based on deep learning by compressing network traffic parameters was proposed. In [40], a three-level architecture of building automation system components was considered, as well as ensuring security in them. The security is assessed using fault, attack, availability, and Markov models. Building automation systems are complex systems, and

subsystems are necessary to ensure cyber protection. These subsystems are difficult for attackers to understand. In [41], immune detectors were developed to recognize and classify computer attacks. In [42], an intrusion detection system subsystem was developed to monitor and analyze host network traffic. In particular, a new pattern matching method is presented. In [43], a solution to the viability problem of information systems was presented, as well as solutions related to the architecture of such systems. Artificial intelligence methods are used. Potentially malicious programs are classified, and a methodology for their analysis is presented. The proposed method includes an analysis of the execution of instruction opcodes at the machine level and the use of artificial intelligence methods to circumvent the efforts of malicious program developers. Existing decoy systems provide the system with information about attacker behavior and attack patterns; however, these systems must be improved to ensure adaptive behavior, high levels of interaction with attackers, and optimization of consumed resources.

Thus, the architecture of such systems is closed to research because these systems are protected against attacker actions. Partial information about the features of systems' functioning can be obtained from the information declared by developers. Research in this area is also not presented in detail. A common strategy for ensuring the adaptability of systems in research work is to develop methods based on rules for ensuring the restructuring of systems' architecture. To apply the rules, it is necessary to determine criteria, which will be the basis for forming the rules. Therefore, it is necessary to determine criteria for restructuring the architecture of systems.

1.4. The purpose and tasks of research

From the analysis of literature sources, it follows that the following task needs to be solved: development of criteria for evaluating centralization options in the architecture of multicomputer systems to select the next centralization option when restructuring the system architecture. These criteria for evaluating centralization options provide the basis for determining the next centralization option in the system architecture.

The purpose of this work is to increase the operational efficiency of restructuring system centers during their operations without user involvement by developing criteria for evaluating potential centralization options, which may be the next options in the system. These evaluation criteria provide an opportunity to comprehensively evaluate potential centralization options while considering the operating environment in which the systems will operate.

The structure of the article is as follows.

Section 1 presents previous studies [1-4]. Section 2 presents the section "Related works" - a brief analysis of the latest ideas and methods that are considered to solve the problem of selecting the next centralization option in the architecture of systems in which the adaptability property is synthesized, with its advantages and disadvantages.

Sections 3 and 4 discuss the main idea of the study: the development of criteria for evaluating centralization options in the architecture of multicomputer systems to select the next centralization option when restructuring the system architecture.

Section 5 describes the experimental results.

In addition, the conclusions were drawn from the study results.

2. Materials and Methods

2.1. Features of the formation of centralization options for multi-computer systems

The characteristic properties that can be used when synthesizing systems determine the number of potential options for the system architecture to which it will switch in the next step when making a decision on restructuring the architecture. As the number of characteristic properties increases, the number of possible options increases. When approving options for the transition, it is necessary to evaluate them by considering the previous experience of the systems' functioning. If the selected option is repeated, it will be evaluated in consideration of the effectiveness of its previous use. An important element in this evaluation is the evaluation criteria, which must be developed in such a way that it is possible to take into account the experience of using the centralization option in the case of repetition and evaluate the prepared options that are offered for the first time.

We begin by considering the characteristic properties that can be synthesized in the system architecture, considering their use when developing the evaluation criteria. To develop criteria for evaluating potential options for centralization in the architecture of class $\mathfrak{S}$ systems [3, 4], we use the selected property $(\mathfrak{V}_2)$, which characterizes the types and number of centers in it. The characteristic properties are then given by sets of elements as follows:

$$M_{\mathfrak{V}_2,centr,v_k} == \begin{Bmatrix} m_{\mathfrak{V}_2,centr,v_k,1}, m_{\mathfrak{V}_2,centr,v_k,2}, \\ \dots, m_{\mathfrak{V}_2,centr,v_k,N_{M_{\mathfrak{V}_2,centr,v_k}}} \end{Bmatrix}, \quad (1)$$

where k=1,2,…,10; k is the number of sets $M_{\mathfrak{V}_2,centr,v_k}$; the element $m_{\mathfrak{V}_2,centr,v_k,j}$ reflects the characteristic property of systems of class $\mathfrak{S}$ in the k-th set $M_{\mathfrak{V}_2,centr,v_k}$;

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

j=1,2,…, $N_{M_{\mathfrak{V}_2,centr,v_k}}$); $N_{M_{\mathfrak{V}_2,centr,v_k}}$ – the number of elements in the set $M_{\mathfrak{V}_2,centr,v_k}$.

Sets $M_{\mathfrak{V}_2,centr,v_k}$ (k=1,2,…,10) define such characteristic properties as types of centralization, options for distributing centers in system components, presence of the system center in disconnected parts, types of connections between components when it is distributed, options for the hierarchy of system center components, direction of message transmission between components, options for message transmission, active and inactive state of components, distribution of the center into parts, and combined organization of the center.

The potential number of centralization options is determined by considering the characteristic properties of each set, which are defined by equation (1). Because only one characteristic property can be taken from each set, the number of such characteristic properties is equal to 10 out of 31 possible characteristic properties. Then, 21 characteristic properties are absent in the system. The number of choices of a single characteristic property from the first set is equal to the number of permutations without repetitions of four elements by one element. We determine similarly for the remaining nine sets. The obtained values for each characteristic property from each of the 10 sets are multiplied by the product rule, and we obtain the potentially possible number of centralization options, i.e.

$$K_{centr} = \prod_{i=1}^{10} C_1^{N^{centr}_{M_{\mathfrak{V}_2,centr,i}}},$$

where $N^{centr}_{M_{\mathfrak{V}_2,centr,i}}$ is the number of elements in the set of characteristic properties $M_{\mathfrak{V}_2,centr,i}$; i=1,2,…,10.

The sets of characteristic properties given by Eq. (1) also allow us to establish centralization options to which it is impossible to switch from the previous centralization option. The number of such options is small and is mainly associated with the state of the system when it is divided into two non-empty disconnected parts. Then, upon returning to the full option, attempts are made to choose the next centralization option. In addition, the number of sets can be increased in the case of introducing a characteristic property.

The number of centralization options in the architecture of multicomputer systems, taking into account the features reflected by the elements in Eq. (1), is 220 and higher. The number of features can be increased to a certain number $N_{centr,var}$, increasing the number of elements by detailing the elements from Eq. (1). The number of options is large and cannot be stored directly by the system in the form of a table with all values. Its formation at the beginning of the installation and organization of multicomputer systems will require time. When using a ready-made table, regardless of the software implementation, the system center will spend time searching for an option. Therefore, due to the time consumption, this method is not effective. We use it to present the options for centralization in the architecture of multicomputer systems, taking into account the features of the rule.

The presence of multicomputer systems in one of the centralization options at the current time will be determined by their presence in a certain corresponding state. Thus, transitioning from one centralization option in the process of functioning of multicomputer systems means a transition between states. Being in a certain state of a multicomputer system does not necessarily allow a transition to any of the remaining states. For example, if the system is divided into two parts, then transitioning to the centralization option with a single center is impossible.

After installing the components of multicomputer systems in corporate networks, the question of forming a centralization option arises. Such a centralization option could be set by the system administrator, who installed its components and performed the first launch. However, to avoid possible malicious influence of the administrator on the system, it is necessary to ensure that the system independently determines the centralization option. The start of the system's functioning, which begins daily with the switching on of computer stations with system components, also requires a change in the centralization option compared to the previous day of operation. For example, on the previous day of operation, the system completed work in one of the states, and the next day, continuing work in that state was impossible. To unambiguously determine the centralization options, a flexible organization of the functioning of this subsystem is required, which can be ensured, for example, by specifying a certain set of rules.

Thus, it is necessary to specify a set of rules to determine the centralization option for systems at the stage of the initial start-up of the system, daily start-up of the system, and during long-term operation of the system, which does not include events of periodic daily start-up of the system.

Several centralization options must be prepared by the corresponding subsystem of the system. This is because the system controller must evaluate these options in the context of the actual transition from state to state of the system, taking into account previous experience, and approve one of these options. Therefore, preparing several centralization options for the next state of the system increases the complexity of the subsystem responsible for preparing such options.

The system may not use a certain number of options; however, it must be able to form any of the centralization options. Some options during its operation will not only be selected but also considered. There are many

options for centralization. However, it is not necessary to impose restrictions on certain centralization options. Because this can simplify access to the target system by attackers. Therefore, the number of possible options for centralization should be as large as possible from the permissible options.

The state of the system at the current time is given by the vector $V_{Pr,i}$ ($i = 1,2, \dots, N_{V_{Pr}}$; $N_{V_{Pr}}$ – the number of system states). The values of the elements of the sets using Eq. (1) are given by the elements of the set {0;1}. Then, we introduce a Boolean function to reflect the activity/inactivity of the feature, which is given by the element of the sets from Eq. (1) as follows:

$$F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,m}, i\right) = \begin{cases} 0, \text{if element is absent;} \\ 1, \text{ if element is present,} \end{cases} \quad (3)$$

where l – the number of sets; l=1,2,…10; m – the th element in the set $M_{\mathfrak{B}_2,centr,l}$; i – the system state number.

Thus, the vector $V_{Pr,i}$ ($i = 1,2, \dots, N_{V_{Pr}}$; $N_{V_{Pr}}$ – the number of states of the system) is defined by its coordinates as follows:

$$V_{Pr,i} = \begin{pmatrix} F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_1,1}, i\right), \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,2}, i\right), \dots, \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_{10},3}, i\right) \end{pmatrix}, \quad (4)$$

where $i = 1,2, \dots, N_{V_{Pr}}$; $N_{V_{Pr}}$ – the number of states of the system; i – the number of state of the system.

Then, the matrix $M_{V_{Pr}}$ of the system states in the part of the centralization organization is given as follows:

$$M_{V_{Pr}} = \begin{pmatrix} V_{Pr,1} \\ V_{Pr,2} \\ \dots \\ V_{Pr,N_{V_{Pr}}} \end{pmatrix}, \quad (5)$$

where $N_{V_{Pr}}$ is the number of system states; $V_{Pr,i}$ is the vector that specifies the system state at the current time; i=1,2,…, $N_{V_{Pr}}$.

When detailing the cases and, accordingly, increasing the elements of the sets, the number of system states in the part of the centralization organization, which are reflected in the matrix $M_{V_{Pr}}$, can be increased, or when the elements are reduced - reduced.

The transition from one state to another, which will be determined by the rules from the set of rules M_{Pr}, is given by the function $F^{M_{Pr}}$ as follows:

$$F^{M_{Pr}}: \left(V_{Pr,current}, M_{V_{Pr}}, M_{Pr}, P_{Pr}\right) \rightarrow V_{Pr,next}, \quad (6)$$

where $V_{Pr,current}$ is a vector that specifies the state of the system at the current time and is present in the state matrix $M_{V_{Pr}}$; $M_{V_{Pr}}$ is a matrix of system states in the part of the centralization organization; M_{Pr} is a set of rules; $V_{Pr,next}$ is a vector that specifies the next state of the system at the current time; P_{Pr} is a set of indicators that characterize the current state of the system and the processes in it.

The set P_{Pr} is defined by the following elements:

$$P_{Pr} = \left\{p_{Pr,1}, p_{Pr,2}, \dots, p_{Pr,N_{P_{Pr}}}\right\}, \quad (7)$$

where $p_{Pr,i}$ is the i-th indicator that characterizes the current state of the system and the processes in it; $i = 1,2, \dots, N_{P_{Pr}}$; $N_{P_{Pr}}$ is the number of indicators that characterize the current state of the system and the processes in it and affect the change in the centralization option in the system.

Let $p_{Pr,1}$ be the time for choosing a centralization option in the system and transitioning from one state to another when changing centralization, $p_{Pr,2}$ be the indicator of the available components in the switched-on computer stations, $p_{Pr,3}$ be the indicator of the impossibility of completing the transition to the next state and returning to the previous state; $p_{Pr,4}$ be the indicator of the system being in an emergency state, etc. An emergency state occurs when a certain equipment is turned off, and the system components are divided into several disconnected subsets. Then, a centralization option is selected for each of the formed subsystems. At the same time, each subsystem may have different centralization options. When returning from such a state, the system must also take into account the previous state in which it was before entering the emergency state. In general, for such a class of systems, it is necessary to store information about all selected states, indicators, and rules used when choosing centralization options throughout their operation. For example, it is possible to move from a certain state to another if there is a certain number of system components in the switched-on computer stations; however, with a different number of components, the transition to this state may be impossible, and there will be a transition to another state.

According to Eq. (6), the transition to the next state can occur at different time intervals of the system's operation using different rules from the set of rules M_{Pr} and with different indicators from the set of indicators P_{Pr}, which characterize the current state of the system and the processes in it.

Let us divide the rules from the set of rules M_{Pr} into groups to which rules with certain common features are assigned. We highlight the following common features for dividing rules into groups:

1) transition from a certain state to the next selected state;

2) transition to a certain state because of an emer-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

gency and return to the normal operating mode of the system;

3) The system forms new rules using the rules available in the set and uses them when the system transitions from a certain state to the next selected state.

Let us introduce the matrix M_{Pr}^{1} to store information about the type of rule, i.e., to which group it belongs, the time of application of the rule provided that the transition is performed according to it, and the number of the rule from the set of rules M_{Pr}.

Let us define the matrix M_{Pr}^{1} as follows:

$$M_{Pr}^{1} = \begin{pmatrix} m_{Pr,1}^{1} & m_{Pr,2}^{1} & \dots & m_{Pr,N_{M_{Pr}^{1}}}^{1} \\ t_{Pr,1}^{1} & t_{Pr,2}^{1} & \dots & t_{Pr,N_{M_{Pr}^{1}}}^{1} \\ N_{M_{Pr},1} & N_{M_{Pr},2} & \dots & N_{M_{Pr},N_{M_{Pr}^{1}}} \end{pmatrix}, \quad (8)$$

where $N_{M_{Pr}^{1}}$ is the number of successfully completed transitions between the states of the system; $i = 1,2,\dots, N_{M_{Pr}^{1}}$; $m_{Pr,i}^{1}$ – rule group number for i–th transition; $t_{Pr,i}^{1}$ – current time for completed i–th transition; $N_{M_{Pr},i}$ – element number from the set of rules on i – th transition.

This matrix M_{Pr}^{1} specifies information about the previous states of the system when organizing transitions, as well as about the rules used and the time to complete the transitions. Such information is needed by the system to make decisions about the next centralization option and in the event of an emergency.

Separate rules are required to ensure an exit from non-standard or emergencies. If an emergency or non-standard situation for the system has arisen, the disconnected parts of the system make a decision about the centralization option in parts, and during the subsequent transition to the standard operating mode of the system, the centralization option is also determined by separate rules. For example, there may be a transition to a certain state when the system is unable to complete the corresponding actions, and returning to the previous state is no longer possible as a result of an emergency or non-standard situation, which may be due to a change in the system architecture. Then, returning to the normal operating mode of the system requires rules that ensure the establishment of a centralization option under the existing conditions. Therefore, when the system functions, the set of rules must be divided into groups of rules that can be applied only under certain conditions.

The third group of rules includes rules that are formed by the system itself using simpler rules; that is, they are constructed by it to select the next centralization option. Such a group of rules is added to the set of rules by the system itself. The need to form such a group of rules arises during the operation of the system when the centralization options proposed from the first group of rules are repetitive or their number does not satisfy the requirements of the controller. Then, the system forms new rules by general search. If the controller accepts the new rules, they are included in the set of rules in the third group.

The first group of rules forms not only the rules for transitioning from one state to another in the normal mode of operation, but also establishes another option of centralization in the system. That is, the rules of the first group specify not only a simple combination of possible options of elements of the sets, which are given by Eq. (1). Among the rules of the first group, there must be rules that reject the option of centralization in the system, which is impossible. For example, if the option of centralization in the system involves centralization, then it cannot be combined with the option, which provides for the division into several disconnected subsets of the set of system components. Or, for example, if the system is partially decentralized, then the option with a large number of hierarchy levels in it is impossible. Thus, in the normal mode of operation of the system, the rules form a new option for centralization in the system, not by a simple search of all possible options but by taking into account the impossibility of combining certain properties, which are given by the elements of the sets.

The division of rules into three groups reflects the features of their application at the current moment of the system's functioning, taking into account the events that occur in the system when it performs tasks, including changes in the centralization option.

To form the rules, we describe the features of the four main centralization options. We will specify class $\Subset$ systems by their components as follows;

$$A^{\Subset} = \left\{A_1^{\Subset}, A_2^{\Subset}, \dots, A_{N_{A^{\Subset}}}^{\Subset}\right\}, \quad (9)$$

where $A^{\Subset}$ is the designation of the class $\Subset$ system; $A_i^{\Subset}$ is the i-th component of the $A^{\Subset}$ system of class $\Subset$; i=1,2,…, $N_{A^{\Subset}}$; $N_{A^{\Subset}}$ is the number of components in the $A^{\Subset}$ system.

Considering the need to present centralization options in the system, we divide the components of the $A^{\Subset}$ system into two subsets. The first subset includes the currently active components of the system center. The second subset includes components that are not currently in the system center. We assume that any component of the $A^{\Subset}$ system can be active components of the center if they are in switched-on computer stations. Active components are those that are currently functioning as part of the system. We assume that components of the $A^{\Subset}$ system can be active, but they do not necessarily belong to the system center at the current time. Then, we define the set of components of the $A^{\Subset}$ system as follows:

$$A^{\Subset} = A_1^{\Subset} \cup A_2^{\Subset}, \quad (10)$$

where $A_1^{\Subset}$ is a subset of active components of the system center; $A_2^{\Subset}$ is a set of system components that are not currently components of the system center.

These two subsets are defined by the following elements:

$$A_1^{\Subset} = \left\{A_{1,1}^{\Subset}, A_{1,2}^{\Subset}, \dots, A_{1,N_{1,A^{\Subset}}}^{\Subset}\right\};$$
$$A_2^{\Subset} = \left\{A_{2,1}^{\Subset}, A_{2,2}^{\Subset}, \dots, A_{2,N_{2,A^{\Subset}}}^{\Subset}\right\}, \quad (11)$$

where $A_1^{\Subset}$ is the i-th component of the subset $A_1^{\Subset}$ of the system $A^{\Subset}$ of class $\Subset$; i=1,2,…, $N_{1,A^{\Subset}}$; $N_{1,A^{\Subset}}$ is the number of elements in the subset $A_1^{\Subset}$; $A_{2,j}^{\Subset}$ is the j-th component of the subset $A_2^{\Subset}$ of the system $A^{\Subset}$ of class $\Subset$; j=1,2,…, 2, $N_{2,A^{\Subset}}$; $N_{2,A^{\Subset}}$ is the number of elements in the subset $A_2^{\Subset}$; $A_2^{\Subset}$; $N_{A^{\Subset}} = N_{1,A^{\Subset}} + N_{2,A^{\Subset}}$.

Thus, the features of the formation of centralization options for multi-computer systems have been highlighted, which require their consideration in the criteria for evaluating centralization options.

2.2. Mathematical models and criteria for evaluating centralization options in the architecture of multicomputer systems

The division into four main types of architecture is necessary when forming the next type of architecture because each type of architecture forms its own decision-making option at the center of the $A^{\Subset}$ system. Let us establish criteria for evaluating the four types of centralization considered in the system. The development of a methodology for evaluating centralization options is necessary for the system to choose the next centralization option. The transition of a system to the next centralization option is a complex action. There are many options to which the system can switch; therefore, it is important to determine such an option that is possible for a quick and safe transition. Given the very large number of possible centralization options in the system that can be switched to, the problem of optimal selection of the best option arises; therefore, an objective function for evaluating the next centralization option is needed, the values of which will be based on the criteria and will be used by the controller when approving the centralization option that will be set in the system when switching from the previous option.

The selection of criteria is performed based on the goal of the evaluation objective function for choosing one of the four types of centralization, namely, to minimize its value. In other words, the values of the objective function indicate how effective one of the four types of architecture is depending on the number of components in the system and their activity at the current moment. In this approach to construct the objective function of selection, we consider the number of components in the system, including those active at the current moment. The four types of centralization in the system architecture cannot be evaluated by simple ranking among themselves at four levels. There may be cases when one of the types with a larger number of components is less effective than the type of architecture in which, with the same number of components, operational efficiency is lower, and with a smaller number of components, operational efficiency is better. In other words, for different types of centralization with different numbers of components, there may be intersections in the classes of their types in terms of operational efficiency. To evaluate the types of centralization in architecture depending on the four main types, we introduce the following criteria: operational efficiency; stability; integrity; security. For analytical presentation of the criteria, we use the following indicators: time to perform the restructuring of the architecture in terms of centralization; time to prepare decisions regarding the next option of centralization in the system architecture; total number of components in the system; number of active center components in the system at the current time; number of components with the system center at the current time; number of system center components in the new option to which the transition is planned at the next step; number of segments in the corporate network; presence of system components in the demilitarized zone of the corporate network; presence of system components in server nodes; presence of system center functionality in nodes in the demilitarized zone; presence of system center functionality in server nodes.

The objective function for evaluating the following centralization options for choosing one of the four types of centralization is as follows:

$$F_{kr}^{centr}\left(\begin{array}{c} f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right), f_{2,kr}^{centr}\left(p_{2,kr}^{centr}\right), \dots, \\ f_{N_{F_{kr}^{centr},kr}}^{centr}\left(p_{N_{F_{kr}^{centr},kr}}^{centr}\right), \\ F_{var}^{centr}(u), F_{var}^{centr}(v) \end{array}\right) \rightarrow \min, \quad (12)$$

where $f_{i,kr}^{centr}\left(p_{i,kr}^{centr}\right)$ is the i -th function that specifies the calculation of the value of the i-th criterion; $p_{i,kr}^{centr}$ is the vector whose coordinates are the parameters of the i -th criterion and the centralization option; $N_{F_{kr}^{centr}}, kr$ is the number of arguments of the F_{kr}^{centr} function and the number of vectors $p_{i,kr}^{centr}$;

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

$$p_{i,kr}^{centr} = \begin{pmatrix} p_{1,i,kr}^{centr}, p_{2,i,kr}^{centr}, \dots, p_{N_{p_{i,kr}^{centr}},i,kr}^{centr}, \\ V_{Pr,u}, V_{Pr,v}, \\ A_{1,u}^{\Subset}, A_{1,v}^{\Subset}, A_{2,u}^{\Subset}, A_{2,v}^{\Subset} \end{pmatrix},$$

where $p_{m,i,kr}^{centr}$ is the value of the m-th parameter for i–th criterion with respect to v – that centralization variant in the system; $N_{p_{i,kr}^{centr}}$ is the number of parameters i–th criterion; u and v are the numbers of the centralization variants; u is the number of the current centralization variant in the system; v is the number of the studied centralization variant in the system after u – that number of the centralization variant; $V_{Pr,u}$, $V_{Pr,v}$ – vectors given by coordinates according to formula (4); $F_{var}^{centr}(v)$ – function, the value of which is the number of one of the types of centralization in the system at the current time or the number of the studied type; $A_{1,u}^{\Subset}$ – subset of active components of the system center at u – that current number of the centralization variant; $A_{2,u}^{\Subset}$ – set of system components that at the current time are not components of the system center at u – that current number of the centralization variant; $A_{1,v}^{\Subset}$ – subset of active components of the system center for v – the number of the studied centralization variant in the system, which can be after u – that number of the centralization variant; $A_{2,v}^{\Subset}$ is the set of system components that are not currently components of the system center for v – the number of the centralization variant under study in the system, which may be after u – the number of the centralization variant.

The sets of system components $A_{1,u}^{\Subset}, A_{1,v}^{\Subset}, A_{2,u}^{\Subset}, A_{2,v}^{\Subset}$ will reflect the type of components in the context of centralization and information about them is necessary to apply the criteria for operational efficiency, stability, integrity and security. These sets denote the components at the current time for a certain centralization option and for the studied centralization option to assess its admissibility in the next centralization option.

For the studied value of the function F_{kr}^{centr}, which is given by Eq. (12), the value $N_{F_{kr}^{centr}} = 4$, since four criteria are defined. The number of criteria can be increased, but their addition must consider the requirements for their independence and the need to avoid compensation of the resulting values.

Let us define the function $F_{var}^{centr}(v)$ as follows:

$$F_{var}^{centr}(v) \to \{1,2,3,4\}, \quad (13)$$

where the value {1} corresponds to a centralized architecture, i.e. $F_{var}^{centr}(v)=1$; the value {2} corresponds to a partially centralized architecture, i.e. $F_{var}^{centr}(v)=2$; the value {3} corresponds to a partially decentralized architecture $F_{var}^{centr}(v)$; the value {4} corresponds to a decentralized architecture $F_{var}^{centr}(v)=4$.

Considering Eq. (4), the vector $p_{i,kr}^{centr}$ is given in the expanded form as follows:

$$p_{i,kr}^{centr} = \begin{pmatrix} p_{1,i,kr}^{centr}, p_{2,i,kr}^{centr}, \dots, p_{N_{p_{i,kr}^{centr}},i,kr}^{centr}, \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_1,1}, u), F_{Pr}(m_{\mathfrak{B}_2,centr,v_l,2}, u), \dots, \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_{10},3}, u), \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_1,1}, v), F_{Pr}(m_{\mathfrak{B}_2,centr,v_l,2}, v), \dots, \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_{10},3}, v), \\ A_{1,u}^{\Subset}, A_{1,v}^{\Subset}, A_{2,u}^{\Subset}, A_{2,v}^{\Subset} \end{pmatrix}. \quad (14)$$

Let us consider the definition of each of the four selected criteria. First, we define the criteria in the general case as follows:

$$f_{i,kr}^{centr} \begin{pmatrix} p_{1,i,kr}^{centr}, p_{2,i,kr}^{centr}, \dots, \\ p_{N_{p_{i,kr}^{centr}},i,kr}^{centr}, \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_1,1}, u), \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_l,2}, u), \dots, \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_{10},3}, u), \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_1,1}, v), \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_l,2}, v), \dots, \\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_{10},3}, v), \\ A_{1,u}^{\Subset}, A_{1,v}^{\Subset}, A_{2,u}^{\Subset}, A_{2,v}^{\Subset} \end{pmatrix} \to [0,1], \quad (15)$$

where i=1,2,3,4.

The numerical values calculated for each of these criteria belong to the numerical interval [0,1]. For each considered centralization option in the system, which may be the next in the system architecture, the objective function of evaluating the next centralization option for choosing one of the options from the four types of centralization is minimized due to the parameters available in the criteria.

The criterion for operational efficiency is defined by the function $f_{1,kr}^{centr}(p_{1,kr}^{centr})$, which specifies the calculation of the numerical value considering the parameters of the vector $p_{1,kr}^{centr}$, the coordinates of which are determined by eq. (15). Since operational efficiency is characterized by the speed of information transmission and the timeliness of its receipt, to determine the corresponding criterion, we consider time, and also, taking into account the distribution of the system, we consider the number of components that will be involved in the process of transmitting and receiving information.

Let us discuss the definition of the criterion $f_{1,kr}^{centr}(p_{1,kr}^{centr})$ regarding operational efficiency in detail, considering the relationships between certain parameters that are specified in the vector $p_{i,kr}^{centr}$ according to eq. (15). Let the indicator $p_{1,1,kr}^{centr} = t_1^{p_{1,kr}^{centr}}$ be the time for the

center of the system to make a decision regarding a certain next type of centralization. For different types of centralization, this time will be different because different types of centralization involve the involvement of a different number of components to form the centralization center. The process of directly changing the type of centralization in the system requires a certain amount of time to perform its various stages, and at the same time, it may be the case that some of these stages will be performed in parallel, which will reduce the time required to implement the entire process. Therefore, we introduce presentation indicators that reflect the stages of changing the type of centralization [6]:

1) $p_{2,1,kr}^{centr} = t_2^{p_{1,kr}^{centr}}$ – time to define new components with the center functionality and components without such functionality;

2) $p_{3,1,kr}^{centr} = t_3^{p_{1,kr}^{centr}}$ – time to notify components of the next state of centralization and their assignment to the new system architecture;

3) $p_{4,1,kr}^{centr} = t_4^{p_{1,kr}^{centr}}$ – time to notify all system components of the completion of the current type of centralization in the system architecture;

4) $p_{5,1,kr}^{centr} = t_5^{p_{1,kr}^{centr}}$ – time of receiving confirmation from all system components about their processing of the message about the completion of the current type of centralization and transition to a new type of centralization in the system architecture;

5) $p_{6,1,kr}^{centr} = t_6^{p_{1,kr}^{centr}}$ – time of sending a command to all system components to start work with the new system center and receive confirmation from them regarding the successful transition;

6) $p_{7,1,kr}^{centr} = t_7^{p_{1,kr}^{centr}}$ – time of sending messages between the system center components to coordinate work;

7) $p_{8,1,kr}^{centr} = k_8^{p_{1,kr}^{centr}}$ – total number of components in the system;

8) $p_{9,1,kr}^{centr} = k_9^{p_{1,kr}^{centr}}$ – the number of active system components at the current time;

9) $p_{10,1,kr}^{centr} = k_{10}^{p_{1,kr}^{centr}}$ – the number of components in the system with the system center functionality at the current time;

10) $p_{11,1,kr}^{centr} = u_{11}^{p_{1,kr}^{centr}}$ – a vector whose coordinates are information about the system components at the current time in the nodes of the corporate network for subsets $A_{1,u}^{\Subset}, A_{2,u}^{\Subset}$;

11) $p_{12,1,kr}^{centr} = v_{12}^{p_{1,kr}^{centr}}$ – vector whose coordinates are information about system components at the current time in corporate network nodes for subsets $A_{1,v}^{\Subset}, A_{2,v}^{\Subset}$;

12) $p_{13,1,kr}^{centr} = u_{13}^{p_{1,kr}^{centr}}$ – vector whose coordinates are information about system center components at the current time in corporate network nodes for subset $A_{1,u}^{\Subset}$, which reflect active center components and inactive ones, but which were defined as being part of the system center;

13) $p_{14,1,kr}^{centr} = k_{14}^{p_{1,kr}^{centr}}$ – number of inactive components with system center functionality at the current time;

14) $p_{15,1,kr}^{centr} = k_{15}^{p_{1,kr}^{centr}}$ – the number of inactive components without the system center functionality at the current time;

15) $p_{16,1,kr}^{centr} = k_{16}^{p_{1,kr}^{centr}}$ – the number of segments in the corporate network in which the system components are installed;

16) $p_{17,1,kr}^{centr} = k_{17}^{p_{1,kr}^{centr}}$ – the number of system components in demilitarized zone of corporate network;

17) $p_{18,1,kr}^{centr} = k_{18}^{p_{1,kr}^{centr}}$ – the number of system components in the server nodes;

18) $p_{19,1,kr}^{centr} = k_{19}^{p_{1,kr}^{centr}}$ – the number of components with the functionality of the system center in the nodes in the demilitarized zone;

19) $p_{20,1,kr}^{centr} = k_{20}^{p_{1,kr}^{centr}}$ – the number of components with the functionality of the system center in the server nodes;

20) $p_{21,1,kr}^{centr} = t_{21}^{p_{1,kr}^{centr}}$ – additional time spent on establishing the state of components that did not respond to confirm the processing of the message about the completion of the current type of centralization and the transition to a new type of centralization in the system architecture.

In a decentralized architecture, the time indicators $t_7^{p_{1,kr}^{centr}}$ will be larger than in other architecture types. For a centralized architecture without a distributed system center, $t_7^{p_{1,kr}^{centr}} = 0$. If the type of centralization in the system architecture is different from the decentralized type, then the time indicator $t_7^{p_{1,kr}^{centr}}$ will be affected by the number of components with the system center. As their numbers increase, the time for coordinating work between them will also increase.

For a decentralized architecture, the indicator $t_2^{p_{1,kr}^{centr}} = 0$, since decisions about the time for defining new components with the center functionality and components without such functionality do not need to be made because all these components will be components of the center. However, in this architecture, the time $t_7^{p_{1,kr}^{centr}}$ for sending messages between the components of the system center for coordinating work is the largest compared to other types of architecture.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Let us define $f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right)$ for the operational efficiency criterion as follows [6]:

$$f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right)=1-\frac{1}{10}\cdot\left(\frac{\sum_{i=1}^{7}t_i^{p_{1,kr}^{centr}}}{\sum_{i=1}^{7}t_{i,max}^{p_{1,kr}^{centr}}}+\frac{k_8^{p_{1,kr}^{centr}}}{k_9^{p_{1,kr}^{centr}}}+\right.$$
$$+\frac{k_{10}^{p_{1,kr}^{centr}}}{k_{10}^{p_{1,kr}^{centr}}+k_{14}^{p_{1,kr}^{centr}}}+\frac{k_8^{p_{1,kr}^{centr}}-\left(k_{15}^{p_{1,kr}^{centr}}+k_{16}^{p_{1,kr}^{centr}}\right)}{k_8^{p_{1,kr}^{centr}}}+$$
$$+\frac{k_{16}^{p_{1,kr}^{centr}}-1}{k_{16}^{p_{1,kr}^{centr}}}+\frac{k_8^{p_{1,kr}^{centr}}-k_{17}^{p_{1,kr}^{centr}}}{k_8^{p_{1,kr}^{centr}}}+\frac{k_{17}^{p_{1,kr}^{centr}}-k_{19}^{p_{1,kr}^{centr}}}{k_{17}^{p_{1,kr}^{centr}}}+$$
$$\left.+\frac{k_8^{p_{1,kr}^{centr}}-k_{18}^{p_{1,kr}^{centr}}}{k_8^{p_{1,kr}^{centr}}}+\frac{k_{18}^{p_{1,kr}^{centr}}-k_{20}^{p_{1,kr}^{centr}}}{k_{18}^{p_{1,kr}^{centr}}}+\frac{t_{21}^{p_{1,kr}^{centr}}}{t_5^{p_{1,kr}^{centr}}}\right),\qquad(16)$$

where $t_{i,max}^{p_{1,kr}^{centr}}$ is the largest time value for the i-th characteristic, which was obtained during the system operation, starting from the first independent solution by the system; i=1,…,7.

Thus, the criterion for operational efficiency can be determined by Eq. (16), and the values calculated from its definition can be used in the objective function (Eq.(12)) to evaluate the next centralization options to select one of the four types of centralization. Eq. (16) considers the experience of the system's operation in terms of independent decision-making regarding the next centralization option and saving the obtained indicators for use in subsequent steps of their largest values.

The system stability when determining the criterion $f_{2,kr}^{centr}\left(p_{2,kr}^{centr}\right)$ will be considered only with respect to its center. The stability of the system center, regardless of the type of centralization in the system architecture, will be considered in terms of its ability to provide functionality in the operating environment when changing internal and external parameters, including in the case of minimal loss of functionality. External influences may occur when the system is restructuring the centralization option. In addition, when a malicious attack occurs and it affects components with the functionality of the center, it is carried out on computer network nodes in which components with the center of the system are located. Other external events may also affect the operation of the center. For example, failure of equipment that connects parts of the network nodes, and accordingly, the system can fall apart into parts. The internal influences on the operation of the center of the system may be due to incomplete message exchanges. Because the system is distributed, there may be emergencies with the equipment. In such cases, the exchange of messages may be interrupted, and some messages may be lost. In addition, operations to form a new center may be interrupted for some system components. To determine the stability criterion of the center of the system, we form two sets of possible events that affect the functionality of the center of the system, which are caused by external and internal influences, as well as their combination. The set of events that are caused at the center of the system by external influences and affect its stability is defined as follows:

$$A_{2,kr}^{z}=\left\{\begin{matrix}a_{2,kr,1}^{z},a_{2,kr,2}^{z},\\ \cdots,\\ a_{2,kr,N_{A_{2,kr}^{z}}}^{z}\end{matrix}\right\},\qquad(17)$$

where $a_{2,kr,i}^{z}$ is the i-th element corresponding to an event caused by external influences; $N_{A_{2,kr}^{z}}$ is the number of elements in the set $A_{2,kr}^{z}$; i=1,2,…, $N_{A_{2,kr}^{z}}$.

The set of events that are caused at the center of the system by internal influences and affect its stability is defined as follows:

$$A_{2,kr}^{v}=\left\{\begin{matrix}a_{2,kr,1}^{v},a_{2,kr,2}^{v},\\ \cdots,\\ a_{2,kr,N_{A_{2,kr}^{v}}}^{v}\end{matrix}\right\},\qquad(18)$$

where $a_{2,kr,i}^{v}$ is the i-th element corresponding to an event caused by internal influences; $N_{A_{2,kr}^{v}}$ is the number of elements in the set $A_{2,kr}^{v}$; i=1,2,…, $N_{A_{2,kr}^{v}}$.

We define the set of events that occur at the center of the system by a combination of internal and external influences that affect its stability as follows:

$$A_{2,kr}^{vz}=\left\{\begin{matrix}a_{2,kr,1}^{vz},a_{2,kr,2}^{vz},\cdots,\\ a_{2,kr,N_{A_{2,kr}^{vz}}}^{vz}\end{matrix}\right\},\qquad(19)$$

where $a_{2,kr,i}^{vz}$ is the i-th element corresponding to an event caused by external influences; $N_{A_{2,kr}^{vz}}$ is the number of elements in the set $A_{2,kr}^{vz}$; i=1,2,…, $N_{A_{2,kr}^{vz}}$.

The part of events that affect the operation of the center of the system and its stability and is given by the set $A_{2,kr}^{vz}$ can be generated only by a combination of both external and internal influences. If the event is generated separately by external or internal influence but is combined, such events are attributed to the sets $A_{2,kr}^{z}$ and $A_{2,kr}^{v}$.

Each event that affects the stability of the center of the system will violate the stability of the center of the system with a certain probability. Therefore, we define the stability of the center of the system by the value $P_{st}^{centr}(t)$, the value of which will belong to the interval [0,1] and depends on time. That is, at different values of time, different values of stability are possible, or in the

process of the system functioning, the stability of the center of the system for a certain time may change. The center of the system will be more stable at a larger value of the value $P_{st}^{centr}(t)$, that is, the closer the value of $P_{st}^{centr}(t)$ to one, the better the stability of the center of the system.

In the general representation, we define the criterion for the stability of the center of the system by considering Eq. (15) as follows:

$$P_{st}^{centr}(t) = 1 - f_{2,kr}^{centr}\left(\begin{array}{c} p_{1,2,kr}^{centr}, p_{2,2,kr}^{centr}, \dots, p_{N_{p_{i,kr}^{centr}},2,kr}^{centr}, \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_1,1}, u\right), F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,2}, u\right), \\ \dots, \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_{10},3}, u\right), \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_1,1}, v\right), F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,2}, v\right), \\ \dots, \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_{10},3}, v\right), \\ A_{1,u}^{\circledS}, A_{1,v}^{\circledS}, A_{2,u}^{\circledS}, A_{2,v}^{\circledS} \end{array}\right) \quad (20)$$

Unlike the definition of the operational efficiency criterion, for the criterion of the stability of the center of the system, the stability value is determined by the function $P_{st}^{centr}(t)$ through the function $f_{2,kr}^{centr}$, which is better when the value is close to unity, and the functions for the criteria should be close to zero, because the objective function F_{kr}^{centr} (formula (12)) of evaluating the following centralization options for choosing one of the options from the four types of centralization should be minimized.

Let us detail the values of the arguments of the function $f_{2,kr}^{centr}$, i.e. the criterion for the stability of the center of the system, as follows:

1) $p_{1,1,kr}^{centr} = t$ – the current time at which the value $P_{st}^{centr}(t)$ was determined;

2) $p_{2,1,kr}^{centr} = k_1^{p_{2,kr}^{centr}}$ – the total number of components in the system at the current time t (if the system has been operating for a long time, the total number of system components can be changed);

3) $p_{3,1,kr}^{centr} = k_2^{p_{2,kr}^{centr}}$ – the number of active system components at the current time;

4) $p_{4,1,kr}^{centr} = k_3^{p_{2,kr}^{centr}}$ – the number of components in the system with the functional of the center of the system at the current time;

5) $p_{5,1,kr}^{centr} = k_4^{p_{2,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were determined as active to participate in the work of the system center, but they did not confirm their activity as components of the system center and continue to function as part of the system;

6) $p_{6,1,kr}^{centr} = k_5^{p_{2,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were determined as active to participate in the work of the system center, but they were turned off correctly together with the computer stations in which they were installed;

7) $p_{7,1,kr}^{centr} = k_6^{p_{2,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were defined as active to participate in the work of the system center, but they were turned off in an emergency together with the computer stations in which they were installed;

8) $p_{8,1,kr}^{centr} = k_7^{p_{2,kr}^{centr}}$ – the number of active components of the system center at the current time;

9) $p_{9,1,kr}^{centr} = k_8^{p_{2,kr}^{centr}}$ – a vector whose coordinates are information about events from the set of events $A_{2,kr}^{z}$ to the current time defined by the indicator $p_{1,2,kr}^{centr} = t$, which are caused in the system center by external influences, and affect its stability;

10) $p_{10,1,kr}^{centr} = k_9^{p_{2,kr}^{centr}}$ – vector whose coordinates are information about events from the set of events $A_{2,kr}^{v}$ to the current time determined by the indicator $p_{1,2,kr}^{centr} = t$, which are caused in the center of the system by internal influences, and affect its stability;

11) $p_{11,1,kr}^{centr} = k_{10}^{p_{2,kr}^{centr}}$ – vector whose coordinates are information about events from the set of events $A_{2,kr}^{vz}$ to the current time determined by the indicator $p_{1,2,kr}^{centr} = t$, which are caused in the center of the system by external and internal influences, which are caused in the center of the system by a combination of external and internal influences and affect its stability;

12) $p_{12,1,kr}^{centr} = k_{11}^{p_{2,kr}^{centr}}$ – the number of inactive components with the functionality of the system center at the current time;

13) $p_{13,1,kr}^{centr} = k_{12}^{p_{2,kr}^{centr}}$ – the number of inactive components without the functionality of the system center at the current time;

14) $p_{14,1,kr}^{centr} = k_{13}^{p_{2,kr}^{centr}}$ – the number of segments in the corporate network in which the system components are installed;

15) $p_{15,1,kr}^{centr} = k_{14}^{p_{2,kr}^{centr}}$ – the number of system components in the demilitarized zone of the corporate network;

16) $p_{16,1,kr}^{centr} = k_{15}^{p_{2,kr}^{centr}}$ – the number of system components in server nodes;

17) $p_{17,1,kr}^{centr} = k_{16}^{p_{2,kr}^{centr}}$ – the number of components with the functionality of the system center in nodes in the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

demilitarized zone;

18) $p^{centr}_{18,1,kr} = k^{p^{centr}_{2,kr}}_{17}$ – the number of components with the functionality of the system center in server nodes;

19) $p^{centr}_{19,1,kr} = k^{p^{centr}_{2,kr}}_{18}$ – the number of system parts, each of which has components with the functionality of the system center, in the case of temporary system division;

20) $p^{centr}_{20,1,kr} = k^{p^{centr}_{2,kr}}_{19}$ – the number of parts of the system in which there are no active components with the function of the system center, with a temporary division of the system;

21) $p^{centr}_{21,1,kr} = k^{p^{centr}_{2,kr}}_{20}$ – the number of parts of the system in which there are active components with the function of the system center, with a temporary division of the system;

22) $p^{centr}_{22,1,kr} = k^{p^{centr}_{2,kr}}_{21}$ – the time during which the system functioned without the system center until the current time, which was determined by the indicator $p^{centr}_{1,2,kr} = t$;

23) $p^{centr}_{23,1,kr} = k^{p^{centr}_{2,kr}}_{22}$ – the number of events from the set of events $A^{z}_{2,kr}$ to the current time determined by the indicator $p^{centr}_{1,2,kr} = t$, which are caused at the center of the system by external influences, and affect its stability;

24) $p^{centr}_{24,1,kr} = k^{p^{centr}_{2,kr}}_{25}$ – the number of events from the set of events $A^{v}_{2,kr}$ to the current time determined by the indicator $p^{centr}_{1,2,kr} = t$, which are caused at the center of the system by internal influences, and affect its stability;

25) $p^{centr}_{25,1,kr} = k^{p^{centr}_{2,kr}}_{24}$ – the number of events from the set of events $A^{vz}_{2,kr}$ up to the current time defined by the indicator $p^{centr}_{1,2,kr} = t$, which are caused in the center of the system by external and internal influences, which are caused in the center of the system by a combination of external and internal influences and affect its stability;

26) $p^{centr}_{26,1,kr} = k^{p^{centr}_{2,kr}}_{25}$ – the number of $N_{A^{z}_{2,kr}}$ elements in the set $A^{z}_{2,kr}$, i.e. the number of coordinates in the vectors $u^{p^{centr}_{2,kr}}_{8}$;

27) $p^{centr}_{27,1,kr} = k^{p^{centr}_{2,kr}}_{26}$ – the number of $N_{A^{v}_{2,kr}}$ elements in the set $A^{z}_{2,kr}$, i.e. the number of coordinates in the vectors $u^{p^{centr}_{2,kr}}_{9}$;

28) $p^{centr}_{28,1,kr} = k^{p^{centr}_{2,kr}}_{27}$ – the number of $N_{A^{vz}_{2,kr}}$ elements in the set $A^{vz}_{2,kr}$, i.e. the number of coordinates in the vectors $u^{p^{centr}_{2,kr}}_{10}$.

For each of the vectors $u^{p^{centr}_{2,kr}}_{8}$, $u^{p^{centr}_{2,kr}}_{9}$, $u^{p^{centr}_{2,kr}}_{10}$ it is necessary to establish the probability of impact on the stability of the center of the system by its coordinates. The zero coordinates of the vectors indicate the absence of events. The non-zero values of the coordinates of the vectors indicate the number of events at the center of the system. If the coordinate value is greater than one, then the event corresponding to a certain coordinate occurred a certain number of times, which will cause a greater impact.

Each event has an impact on the center of the system. Some events affecting the center of the system can stop the system's operation. Then, such events that are reflected by the coordinates in the vectors have a 100% probability of stopping the functioning of the center of the system. There will also be events that will partially affect its functioning, and under certain circumstances, it will be possible to continue operations. Then, such events have a probability of less than 100%. However, there may be a significant decrease in the possibility of the system center functioning when certain events are combined, which in fact will not be equal to 100% but will be close to 100%.

The probability of an event affecting the stability of the system center functioning, the manifestation of which is given by the vector coordinate, will be within the interval [0,1]. If, during a certain time of the center functioning, there were manifestations of several events, then their probabilities will be added; however, in the case of an event occurring and the system overcoming its consequences, then after a certain time, information about such an event will remain only in the event archive and not in the vector. The vector displays only current events.

After processing, the vector coordinate values are updated. We define the functions that establish the probability of an event for the coordinates of vectors as follows:

$$F^{i}_{u^{p^{centr}_{2,kr}}_{7+i}}\left(u^{p^{centr}_{2,kr}}_{7+i,J}, t\right) = \begin{cases} 0, \text{if } u^{p^{centr}_{2,kr}}_{7+i,J} = 0; \\ P, \text{ if the system center continues its functioning}; 0 < P < 1; \\ 1, \text{if } u^{p^{centr}_{2,kr}}_{7+i,J} > 2 \text{ or the system center stopped its functioning} \end{cases} \quad (21)$$

where $i = 1,2,3$; J is the vector coordinate number; $J = 1,2,\dots, N_{A^{q}_{2,kr}}$; $N_{A^{q}_{2,kr}}$ is the number of elements in the set $A^{q}_{2,kr}$; q corresponds to z if i=1; q corresponds to v, if i=2; q corresponds to vz, if i=3.

The value of P does not depend on the number of

active components of the system center, the number of all system components, or the problematic components of the system. This value characterizes only the event and its impact on system stability. Taking into account the number of system components and the center of the system with different options at the current moment of operation is possible when determining the value of $P_{st}^{centr}(t)$ directly according to Eq. (20). To determine the value of P, it is possible to sort all possible events that affect the stability of the system depending on one of the four types of its possible architecture and from the smallest impact to the largest impact and assign them a value as follows:

$$P = 1 - \frac{1}{k}, \tag{22}$$

where k is the number of sorted vector coordinates; $k = 1,2,\dots,N_{A_{2,kr}^{q}}$; $N_{A_{2,kr}^{q}}$ is the number of elements in the set $A_{2,kr}^{q}$; q corresponds to z, if i=1; q corresponds to v, if i=2; q corresponds to vz if i=3.

The value of P can also be determined by other analytical expressions. This is influenced by the features of the analyzed events in relation to each other regarding their impact on system stability. In the context of the events considered regarding the center of the system, they can be, for example, as follows: during the operation of the center of the system, the connection with one component of the center of the system was lost; the connection with a component that does not belong to the center of the system was lost; the center of the system was divided into two parts due to the loss of the connection; the center of the system did not complete the transition to the next new architecture defined by it, etc. According to such events, it is necessary to form event bases for each of the three sets $A_{2,kr}^{z}$, $A_{2,kr}^{v}$, $A_{2,kr}^{vz}$ and set the coordinate parameters of the vectors $u_{8}^{p_{2,kr}^{centr}}$, $u_{9}^{p_{2,kr}^{centr}}$, $u_{10}^{p_{2,kr}^{centr}}$ with the values of the probability of impact on the stability of the center of the system. Each vector coordinate value depends on the four types of centralization in the system architecture. For example, the loss of a component with the center of the system for a centralized architecture with the center located in one component will lead to the failure of the entire center of the system, and then, the value $F^{i}_{u_{7+i}^{p_{2,kr}^{centr}}}\left(u_{7+i,J}^{p_{2,kr}^{centr}}, t\right) = 1$ (formula (21)). However, for a decentralized type of architecture, such an event will have a negligible impact, and this impact will only be on the time spent on establishing the fact of reducing the system and the center of the system by one component.

After determining the values of the vector coordinates using eq. (22), we obtain the value of $P_{st}^{centr}(t)$ as follows:

$$P_{st}^{centr}(t) = 1 - \frac{k_{2}^{p_{2,kr}^{centr}}}{k_{1}^{p_{2,kr}^{centr}}} \cdot \frac{k_{7}^{p_{2,kr}^{centr}}}{e + k_{3}^{p_{2,kr}^{centr}} - k_{5}^{p_{2,kr}^{centr}}} \cdot \frac{k_{3}^{p_{2,kr}^{centr}} - k_{4}^{p_{2,kr}^{centr}} - k_{6}^{p_{2,kr}^{centr}} + e}{e + k_{3}^{p_{2,kr}^{centr}}} \cdot \frac{k_{1}^{p_{2,kr}^{centr}} - k_{1}^{p_{2,kr}^{centr}} + e}{e + k_{1}^{p_{2,kr}^{centr}}} \cdot \frac{t - t_{21}^{p_{2,kr}^{centr}} + e}{e + t} \cdot \frac{1}{3} \cdot \left(\sum_{J=1}^{N_{A_{2,kr}^{z}}} F^{1}_{u_{8}^{p_{2,kr}^{centr}}}\left(u_{8,J}^{p_{2,kr}^{centr}}, t\right) + \sum_{J=1}^{N_{A_{2,kr}^{v}}} F^{2}_{u_{9}^{p_{2,kr}^{centr}}}\left(u_{9,J}^{p_{2,kr}^{centr}}, t\right) + \sum_{J=1}^{N_{A_{2,kr}^{vz}}} F^{3}_{u_{10}^{p_{2,kr}^{centr}}}\left(u_{10,J}^{p_{2,kr}^{centr}}, t\right) \right) \cdot \frac{k_{1}^{p_{2,kr}^{centr}} - k_{1}^{p_{2,kr}^{centr}} + e}{e + k_{1}^{p_{2,kr}^{centr}}} \cdot \frac{k_{1}^{p_{2,kr}^{centr}} - k_{1}^{p_{2,kr}^{centr}} + e}{e + k_{1}^{p_{2,kr}^{centr}}} \cdot \frac{k_{1}^{p_{2,kr}^{centr}} - k_{1}^{p_{2,kr}^{centr}}}{k_{1}^{p_{2,kr}^{centr}}} \cdot \frac{k_{1}^{p_{2,kr}^{centr}} - k_{1}^{p_{2,kr}^{centr}}}{k_{1}^{p_{2,kr}^{centr}}} \cdot \frac{k_{1}^{p_{2,kr}^{centr}} - k_{1}^{p_{2,kr}^{centr}} + e}{e + k_{1}^{p_{2,kr}^{centr}}} \cdot \frac{1}{k_{1}^{p_{2,kr}^{centr}}};$$

$$f_{2,kr}^{centr}\left(p_{2,kr}^{centr}\right) = 1 - P_{st}^{centr}(t), \tag{23}$$

where e=0.00001; $J = 1,2,\dots,N_{A_{2,kr}^{v}}$; $N_{A_{2,kr}^{v}}$ – number of elements in the set $A_{2,kr}^{v}$; $J = 1,2,\dots,N_{A_{2,kr}^{z}}$; $N_{A_{2,kr}^{z}}$ – number of elements in the set $A_{2,kr}^{vz}$; $J = 1,2,\dots,N_{A_{2,kr}^{vz}}$; $N_{A_{2,kr}^{vz}}$ – number of elements in the set $A_{2,kr}^{vz}$; $N_{A_{2,kr}^{vz}}$ – number of elements in the set $A_{2,kr}^{vz}$; $k_{i}^{p_{2,kr}^{centr}}$ – indicators for the stability criterion; $i = 1,2,\dots,24$; t – current time.

Thus, the criterion $f_{2,kr}^{centr}\left(p_{2,kr}^{centr}\right)$ regarding the stability of the center of the system can be determined by Eq. (23) and the values calculated from its definition can be used in the objective function (Eq. (12)) to evaluate the following centralization options to select one of the options from the four types of centralization.

The criterion for the integrity of the system center is defined by the function $f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right)$, which specifies the calculation of a numerical value taking into account the parameters of the vector $p_{3,kr}^{centr}$, the coordinates of which are determined by formula (16). Under the integrity of the system center, we consider the internal unity of the interconnected components of the system center and the parts from which the system center is formed. For the centralized architecture of the system center with its placement in one component, we consider only the unity of the parts from which the system center is formed. The integrity of the system center reflects the unity of its parts and the connections between them compared to the system components external to it and external components in relation to the system. Thus, in a corporate network in the context of the integrity of the system center, four types of connections can be distinguished: between the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

components of the system center; between the system components outside the center; between the components of the system center and components outside the center; and between components that do not belong to the system. Then, it is possible to determine the priority of the processes at the center of the system compared to the other types of connections in the system and outside it. Connections between components of the center of the system should be prioritized over those that support system integrity. In addition, connections between components outside the center of the system and between them and the components of the center of the system have different priorities; however, in the context of the integrity of the center of the system, they have the same priority because they are responsible for preserving and maintaining the integrity of the entire system.

The integrity of the center of the system was positioned separately from its stability, since integrity is considered concerning connections to assess the unity of the center of the system, and the stability of the center of the system was considered as its ability to continue to perform the tasks set in conditions of failure of some components and elements under internal and external influences. Therefore, we introduce the indicators for the function $f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right)$ regarding the unity of the center of the system due to the peculiarities of the connections between the components and its elements as follows:

1) $p_{25,3,kr}^{centr} = t$ – the current time at which the value $f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right)$ was determined;

2) $p_{2,3,kr}^{centr} = k_1^{p_{3,kr}^{centr}}$ – the total number of components in the system at the current time t (if the system has been operating for a long time, the total number of system components can be changed);

3) $p_{3,3,kr}^{centr} = k_2^{p_{3,kr}^{centr}}$ – the number of active system components at the current time;

4) $p_{4,3,kr}^{centr} = k_3^{p_{3,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time;

5) $p_{5,3,kr}^{centr} = k_4^{p_{3,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were determined as active to participate in the work of the system center, but they did not confirm their activity as components of the system center and continue to function as part of the system;

6) $p_{6,3,kr}^{centr} = k_5^{p_{3,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were determined as active to participate in the work of the system center, but they were turned off correctly together with the computer stations in which they were installed;

7) $p_{7,3,kr}^{centr} = k_6^{p_{3,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were defined as active to participate in the work of the system center, but they were turned off in an emergency together with the computer stations in which they were installed;

8) $p_{8,3,kr}^{centr} = k_7^{p_{3,kr}^{centr}}$ – the number of active components of the system center at the current time;

9) $p_{9,3,kr}^{centr} = k_8^{p_{3,kr}^{centr}}$ – the total calculated number of connections between all components of the system center at the current time, i.e. the number of edges in the complete graph, in which the vertices are the components of the system center;

10) $p_{11,3,kr}^{centr} = k_9^{p_{3,kr}^{centr}}$ – the available number of connections between all components of the system center at the current time, i.e., the number of edges in the graph in which the vertices are the components of the system center;

11) $p_{11,3,kr}^{centr} = k_{10}^{p_{3,kr}^{centr}}$ – the full calculated number of connections between all components of the system at the current time, i.e. the number of edges in the complete graph in which the vertices are the components of the system;

12) $p_{12,3,kr}^{centr} = k_{11}^{p_{3,kr}^{centr}}$ – the available number of connections between all components of the system at the current time, i.e. the number of edges in the graph in which the vertices are the components of the system;

13) $p_{13,3,kr}^{centr} = k_{12}^{p_{3,kr}^{centr}}$ – the number of segments in the corporate network in which the system components are installed;

14) $p_{14,3,kr}^{centr} = k_{13}^{p_{3,kr}^{centr}}$ – the number of system components in the demilitarized zone of the corporate network;

15) $p_{15,3,kr}^{centr} = k_{14}^{p_{3,kr}^{centr}}$ – the number of system components in the server nodes;

16) $p_{16,3,kr}^{centr} = k_{17}^{p_{3,kr}^{centr}}$ – the number of components with the functionality of the system center in nodes in the demilitarized zone;

17) $p_{17,3,kr}^{centr} = k_{16}^{p_{3,kr}^{centr}}$ – the number of components with the functionality of the system center in server nodes;

18) $p_{18,3,kr}^{centr} = k_{17}^{p_{3,kr}^{centr}}$ – the number of system parts, each of which has components with the functionality of the system center, with a temporary division of the system;

19) $p_{19,3,kr}^{centr} = k_{20}^{p_{3,kr}^{centr}}$ – the number of system parts in which there are no active components with the functionality of the system center, with a temporary division of the system;

20) $p^{centr}_{20,3,kr} = k^{p^{centr}_{3,kr}}_{19}$ – the number of parts of the system in which there are active components with the functionality of the system center, with a temporary division of the system;

21) $p^{centr}_{21,3,kr} = k^{p^{centr}_{3,kr}}_{20}$ – the time during which the system functioned without the system center until the current time, which is determined by the indicator $p^{centr}_{1,3,kr} = t$;

22) $p^{centr}_{22,3,kr} = k^{p^{centr}_{3,kr}}_{21}$ – the total number of elements (parts) of the system center, which can be placed in different components and maintain communication with each other to perform tasks;

23) $p^{centr}_{23,3,kr} = k^{p^{centr}_{3,kr}}_{22}$ – the current number of components in which the elements (parts) of the central part of the system are placed;

24) $p^{centr}_{24,3,kr} = k^{p^{centr}_{3,kr}}_{23}$ – the total number of connections between the system components during time t;

25) $p^{centr}_{25,3,kr} = k^{p^{centr}_{3,kr}}_{24}$ – the total number of connections between the components of the center of the system during time t.

The indicator $k^{p^{centr}_{3,kr}}_{24}$ will reflect the priority of connections when detailing the integrity criterion. Similarly to the previous two criteria, which are defined by the corresponding functions $f^{centr}_{3,kr}\left(p^{centr}_{3,kr}\right)$, the better value of the two obtained values is the one that is smaller, i.e. closer to zero. According to the entered indicators, we detail the function as follows:

$$f^{centr}_{3,kr}\left(p^{centr}_{3,kr}\right) = 1 - \frac{k^{p^{centr}_{3,kr}}_{2}}{k^{p^{centr}_{3,kr}}_{1}} \cdot \frac{k^{p^{centr}_{3,kr}}_{7} + k^{p^{centr}_{3,kr}}_{5}}{k^{p^{centr}_{3,kr}}_{3}} \cdot \frac{k^{p^{centr}_{3,kr}}_{7} - k^{p^{centr}_{3,kr}}_{6} + e}{k^{p^{centr}_{3,kr}}_{7} + e} \cdot \frac{k^{p^{centr}_{3,kr}}_{7} - k^{p^{centr}_{3,kr}}_{4} + e}{k^{p^{centr}_{3,kr}}_{7} + e} \cdot \frac{k^{p^{centr}_{3,kr}}_{7}}{k^{p^{centr}_{3,kr}}_{8}} \cdot \frac{k^{p^{centr}_{3,kr}}_{11}}{k^{p^{centr}_{3,kr}}_{10}} \cdot \frac{k^{p^{centr}_{3,kr}}_{12} - k^{p^{centr}_{3,kr}}_{15} - k^{p^{centr}_{3,kr}}_{16}}{k^{p^{centr}_{3,kr}}_{12}} \cdot \frac{k^{p^{centr}_{3,kr}}_{17} - k^{p^{centr}_{3,kr}}_{18}}{k^{p^{centr}_{3,kr}}_{17}} \cdot \frac{k^{p^{centr}_{3,kr}}_{19} - k^{p^{centr}_{3,kr}}_{18}}{k^{p^{centr}_{3,kr}}_{19}} \cdot \frac{t - t^{p^{centr}_{3,kr}}_{20}}{t} \cdot \frac{k^{p^{centr}_{3,kr}}_{21} - k^{p^{centr}_{3,kr}}_{22} + e}{k^{p^{centr}_{3,kr}}_{21} - 1 + e} \cdot \frac{k^{p^{centr}_{3,kr}}_{22} + e}{k^{p^{centr}_{3,kr}}_{23} + e}, \quad (24)$$

where e=0.00001; t is the current time.

Thus, the criterion for the integrity of the center of the system can be determined by Eq. (24) and the values calculated from its definition can be used in the objective function (Eq. (12)) to evaluate the following centralization options to select one of the four types of centralization. The peculiarity of determining the integrity criterion is to take into account the priority of connections in the system between components, connection options in the context of components with the center of the system, and possible division of the center of the system into elements with their placement in different components. Such a definition of the criterion when taking it into account in the objective function, provided that its value is minimized, will be the basis for preparing the next centralization option in the system because, in addition to evaluating the current centralization option, it will provide data on the optimal options and the optimal number of connections between the components of the center of the system.

The security criterion of the system center is defined by the function $f^{centr}_{4,kr}\left(p^{centr}_{4,kr}\right)$, which specifies the calculation of a numerical value considering the parameters of the vector $p^{centr}_{4,kr}$. We consider the security of the system center according to two main characteristics: the correct and full implementation of the requirements for it by the system center; the state of security to ensure the confidentiality, availability, and integrity of information. For each characteristic, we will introduce indicators of security levels as follows: $P^{centr}_{bezp,1}(t)$ – functional security level; $P^{centr}_{bezp,2}(t)$ – cybersecurity level. The overall security level of the system center is set considering the values for the characteristics as follows:

$$P^{centr}_{bezp}(t) = \alpha_1 \cdot P^{centr}_{bezp,1}(t) + \alpha_2 \cdot P^{centr}_{bezp,2}(t), \quad (25)$$

where α_1 is the weighting factor for the first level $P^{centr}_{bezp}(t)$; α_2 is the weighting factor for the second level $P^{centr}_{bezp,2}(t)$; $\alpha_1+\alpha_2=1$; t is the current time; $0 \le P^{centr}_{bezp,1}(t) \le 1$; $0 \le P^{centr}_{bezp,2}(t) \le 1$.

Then, let us define the security criterion for the center of the system as follows:

$$f^{centr}_{4,kr}\left(p^{centr}_{4,kr}\right) = 1 - (\alpha_1 \cdot P^{centr}_{bezp,1}(t) + \alpha_2 \cdot P^{centr}_{bezp,2}(t)). \quad (26)$$

To determine the value of the overall security level $P^{centr}_{bezp}(t)$, various methods can be used. The selection of a specific method for determining the values of the levels must be made, considering the requirement that the value belong to the interval [0,1]. To determine the levels, you can use the formula (11, [44]), according to which you can determine the values of the levels in each individual component of the system. Then, for the components at the center of the system, the arithmetic mean value is calculated. In [44], a comprehensive system for assessing the environment of a corporate network and computer stations in terms of functional and cybersecurity was presented. This system can also be modified for the developed target evaluation function.

According to the security criterion given by Eq. (26), we assume that the better of the two values obtained by the criterion will be the smaller of the two values. For

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

the security level $P_{bezp}^{centr}(t)$ (formula (25)), the better of the two values will be the larger of the two values.

Some indicators presented in [44] apply to other elements of the proposed multicomputer system. Therefore, to avoid duplication and, accordingly, to correlate the results, we introduce indicators for one of the options for a more detailed definition of the criterion for the security of the center of the system $f_{4,kr}^{centr}(p_{4,kr}^{centr})$ as follows:

1) $p_{1,4,kr}^{centr} = t$ – the current time at which the value $P_{bezp}^{centr}(t)$ was determined;

2) $p_{2,4,kr}^{centr} = k_1^{p_{4,kr}^{centr}}$ – the total number of tasks performed by the system center during the system operation time t;

3) $p_{3,4,kr}^{centr} = k_2^{p_{4,kr}^{centr}}$ – the total number of tasks performed by the system center during the operation time in its current version of centralization;

4) $p_{4,4,kr}^{centr} = k_3^{p_{4,kr}^{centr}}$ – the number of tasks that the system center completed in full during the system operation time t;

5) $p_{5,4,kr}^{centr} = k_4^{p_{4,kr}^{centr}}$ – the number of tasks that the system center completed in full during its operation in its current centralization variant;

6) $p_{6,4,kr}^{centr} = k_5^{p_{4,kr}^{centr}}$ – the number of tasks that the system center was unable to complete during the operation of system t;

7) $p_{7,4,kr}^{centr} = k_6^{p_{4,kr}^{centr}}$ – the number of tasks that the system center was unable to complete during its operation in its current centralized variant;

8) $p_{8,4,kr}^{centr} = k_7^{p_{4,kr}^{centr}}$ – the number of tasks that the system center continues to perform at the current time t, including the start of execution under previous centralization variants;

9) $p_{9,4,kr}^{centr} = k_8^{p_{4,kr}^{centr}}$ – the number of tasks that the system center continues to perform in its current version of centralization;

10) $p_{10,4,kr}^{centr} = k_9^{p_{4,kr}^{centr}}$ – the number of transitions of the system center to the new centralization architecture during time t;

11) $p_{11,4,kr}^{centr} = k_{10}^{p_{4,kr}^{centr}}$ – the number of unsuccessful transitions of the system center to the new centralization architecture during time t, i.e. those that did not occur, but were started;

12) $p_{12,4,kr}^{centr} = k_{11}^{p_{4,kr}^{centr}}$ – the number of active components in the system with the functionality of the system center at the current time;

13) $p_{13,4,kr}^{centr} = k_{12}^{p_{4,kr}^{centr}}$ – the total number of components in the system with the functionality of the system center determined during the last transition to the new centralization architecture;

14) $p_{14,4,kr}^{centr} = k_{13}^{p_{4,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were determined as active to participate in the work of the system center, but they did not confirm their activity as components of the system center and continue to function as part of the system;

15) $p_{15,4,kr}^{centr} = k_{14}^{p_{4,kr}^{centr}}$ – the number of components in the system with the functionality of the system center at the current time, which were defined as active to participate in the work of the system center in the last version of centralization, but they were turned off in an emergency together with the computer stations in which they were installed;

16) $p_{16,4,kr}^{centr} = k_{15}^{p_{4,kr}^{centr}}$ – the number of components in the system with the functionality of the system center during the entire time of its operation from the start of operation to time t, which were defined as active to participate in the work of the system center, but they were turned off in an emergency together with the computer stations in which they were installed;

17) $p_{17,4,kr}^{centr} = k_{16}^{p_{4,kr}^{centr}}$ – the number of components in the system with the system center functionality for the current centralization option, which were defined as active to participate in the system center operation, but they were disabled correctly together with the computer stations in which they were installed;

18) $p_{18,4,kr}^{centr} = k_{17}^{p_{4,kr}^{centr}}$ – the number of components in the system with the system center functionality for all centralization options during the entire time of system operation up to time t, which were defined as active to participate in the system center operation, but they were disabled correctly together with the computer stations in which they were installed;

19) $p_{19,4,kr}^{centr} = k_{18}^{p_{4,kr}^{centr}}$ – the number of segments in the corporate network in which the system center components are installed;

20) $p_{20,4,kr}^{centr} = k_{19}^{p_{4,kr}^{centr}}$ – the total number of segments in the corporate network;

21) $p_{21,4,kr}^{centr} = k_{20}^{p_{4,kr}^{centr}}$ – the number of demilitarized zones of the corporate network;

22) $p_{22,4,kr}^{centr} = k_{21}^{p_{4,kr}^{centr}}$ – the number of demilitarized zones of the corporate network with system center components;

23) $p_{23,4,kr}^{centr} = k_{22}^{p_{4,kr}^{centr}}$ – the number of segments in the corporate network with server nodes;

24) $p_{24,4,kr}^{centr} = k_{23}^{p_{4,kr}^{centr}}$ – the number of segments in the corporate network with server nodes, in which the

components of the system center are located;

25) $p_{25,4,kr}^{centr} = k_{24}^{p_{4,kr}^{centr}}$ – the number of divisions of the system center into parts during the system operation time;

26) $p_{26,4,kr}^{centr} = k_{25}^{p_{4,kr}^{centr}}$ – the number of divisions of the system center into parts during the current version of the system centralization;

27) $p_{27,4,kr}^{centr} = k_{26}^{p_{4,kr}^{centr}}$ – the number of system parts, each of which has components with the functionality of the system center, during temporary system division;

28) $p_{28,4,kr}^{centr} = k_{27}^{p_{4,kr}^{centr}}$ – the number of parts of the system in which there are no active components with the function of the system center, with a temporary division of the system;

29) $p_{29,4,kr}^{centr} = k_{28}^{p_{4,kr}^{centr}}$ – the number of parts of the system in which there are active components with the function of the system center, with a temporary division of the system;

30) $p_{30,4,kr}^{centr} = k_{29}^{p_{4,kr}^{centr}}$ – the time during which the system functioned without the system center until the current time, which was determined by the indicator $p_{1,4,kr}^{centr} = t$;

31) $p_{31,4,kr}^{centr} = k_{30}^{p_{4,kr}^{centr}}$ – arithmetic mean value of the cybersecurity level of a computer station with a system center component;

32) $p_{32,4,kr}^{centr} = k_{31}^{p_{4,kr}^{centr}}$ – number of system center components removed from the system due to a high level of malware infection or as a result of a computer attack on a computer station with the corresponding component;

33) $p_{33,4,kr}^{centr} = k_{32}^{p_{4,kr}^{centr}}$ – number of components without a system center that were removed from the system due to a high level of malware infection or as a result of a computer attack on a computer station with the corresponding component.

34) $p_{34,4,kr}^{centr} = k_{33}^{p_{4,kr}^{centr}}$ – the number of components of the center of the system in the current version of centralization;

35) $p_{35,4,kr}^{centr} = k_{34}^{p_{4,kr}^{centr}}$ – the total number of components of the system.

The introduced parameters, unlike the well-known set of parameters in [44], are focused on the results of the functioning of a multi-computer system. For example, the number of components of the system center in the current version of centralization, the total number of system components, the total number of segments in the corporate network, etc. These parameters can be obtained at any time during system operation. Some parameters introduced in work [1] require the involvement of a system administrator or expert to evaluate them and enter values into the system. Parameters 1-35 relate to time, number of components, network topology in terms of division into segments, and number of tasks performed by the system. Together, these parameters comprehensively characterize the state of functional security and cybersecurity of the entire developed system, and they can be used as criteria to evaluate the security of the system center.

According to the introduced indicators $p_{1,4,kr}^{centr} - p_{35,4,kr}^{centr}$, we detail the function $f_{4,kr}^{centr}\left(p_{4,kr}^{centr}\right)$ for the criterion for the security of the center of the system as follows:

$$f_{4,kr}^{centr}\left(p_{4,kr}^{centr}\right) = 1 - \left(\alpha_1 \cdot \frac{k_3^{p_{4,kr}^{centr}} + e}{k_1^{p_{4,kr}^{centr}} + e} \cdot \frac{k_4^{p_{4,kr}^{centr}} + e}{k_2^{p_{4,kr}^{centr}} + e} \cdot \frac{k_6^{p_{4,kr}^{centr}} + e}{k_5^{p_{4,kr}^{centr}} + e} \cdot \frac{k_8^{p_{4,kr}^{centr}} + e}{k_7^{p_{4,kr}^{centr}} + e} \cdot \frac{k_9^{p_{4,kr}^{centr}} - k_{10}^{p_{4,kr}^{centr}} + e}{k_9^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{11}^{p_{4,kr}^{centr}} + e}{k_{12}^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{11}^{p_{4,kr}^{centr}} + k_{13}^{p_{4,kr}^{centr}} + k_{14}^{p_{4,kr}^{centr}} + k_{16}^{p_{4,kr}^{centr}} + e}{k_{12}^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{21}^{p_{4,kr}^{centr}}}{k_{20}^{p_{4,kr}^{centr}}} \cdot \frac{k_{18}^{p_{4,kr}^{centr}}}{k_{19}^{p_{4,kr}^{centr}}} \cdot \frac{k_{23}^{p_{4,kr}^{centr}} + e}{k_{22}^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{25}^{p_{4,kr}^{centr}} + e}{k_{24}^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{28}^{p_{4,kr}^{centr}} + e}{k_{26}^{p_{4,kr}^{centr}} + k_{27}^{p_{4,kr}^{centr}} + e} \cdot \frac{t - t_3^{p_{4,kr}^{centr}}}{t} + \frac{\alpha_2}{3} \cdot \left(p_{30}^{p_{4,kr}^{centr}} + \frac{k_{33}^{p_{4,kr}^{centr}} - k_{31}^{p_{4,kr}^{centr}} + e}{k_{33}^{p_{4,kr}^{centr}} + e} + \frac{k_{34}^{p_{4,kr}^{centr}} - k_{31}^{p_{4,kr}^{centr}} - k_{32}^{p_{4,kr}^{centr}} + e}{k_{34}^{p_{4,kr}^{centr}} + e} \right) \right), \quad (27)$$

where e=0.00001; t is the current time; α_1 is the weighting factor for the first level $P_{bezp,1}^{centr}(t)$; α_2 is the weighting factor for the second level $P_{bezp,2}^{centr}(t)$; $\alpha_1 + \alpha_2 = 1$.

Thus, the criterion for the security of the system center can be determined by Eq. (26) with the option of detailing according to Eq. (27) and the values calculated from its definition can be used in the objective function (Eq. (12)) to evaluate the following centralization options to select one of the four types of centralization. A feature of determining the security criterion is to consider the levels of functional security and cybersecurity for the computer stations in which the components of the system center are located. This allows us to assess the current state of centralization, consider assessments from previous centralization options, and use these results to determine the next centralization option in the system. The arguments in the function for the security criterion of the system center, which are taken into account and affect the evaluation result, are the number of components removed by the system in connection with attacks carried out on

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

the computer stations in which they are located. Considering these indicators is important in the context of the purpose of class $\Subset$ systems.

Thus, as a result, new mathematical models have been developed for the criteria of operational efficiency, stability, integrity, and security relative to the system center, which, unlike the known mathematical models for evaluating system centers for choosing the following centralization options, are presented in analytical expressions that take into account the features of the types of centralization in the architecture of systems, indicators of operational efficiency, stability, integrity, and security relative to the system center and make it possible to form an objective function for evaluating centralization options in systems, the feature of which is the concealment of components with the system center from detection by attackers.

The developed mathematical models for evaluating system centers for selecting the next centralization options are based on parameters that reflect the features of the corporate network environment, objects, and interaction processes in multi-computer systems. An important element of these mathematical models is the consideration of the distribution of centralization options according to their types: centralized; partially centralized; partially decentralized; and decentralized. Since the transition from the current centralization option to the next option in the system architecture within one type of centralization can be performed more easily than between different types of centralization, such a characteristic affects the overall assessment of the next centralization option. In addition to the criteria of efficiency, stability, integrity, and security in relation to the system center, an important element of the evaluation system is information about the previous states of the system when organizing transitions, as well as about the rules used and the time of complete completion of transitions. That is, the mathematical models for evaluating the next options for centralization incorporate the previous experience of the systems' functioning, which is given by numerical values. Therefore, the peculiarity of the solution for the developed mathematical models for evaluating the next options for centralization is to obtain, with their application, a numerical value for determining the next option for centralization, taking into account the previous experience of using options for centralization in the system and criteria, the number of which may be different, including their parameters. Assessments based on such models can be used in the development of deceptive systems, including traps and decoys. These models are also designed in such a way that they can be modified as required. The included parameters can be changed, expanded, or reduced, which does not affect the overall construction of the analytical expressions. A possible parameter option is the option in which the parameters of the models can be changed by the system in the process of its functioning by considering internal and external influences.

3. Experiments

The purpose of the experiment was to study the criteria of operational efficiency, stability, integrity, and security relative to the system center to establish the correspondence of their values to real states during the functioning of the system at the moments of changing the centralization options in the system architecture and the adequacy of the parameters selected for them.

Experimental setup. The experiment was conducted for 90 days in the context of the criteria of operational efficiency, stability, integrity, and security relative to the system center defined for the system characteristics. The first series of experiments consisted of studying the system in the case of its regular functioning without the occurrence of critical events for it and its operating environment. The remaining series of experiments were aimed at studying the system according to the criteria of operational efficiency, stability, integrity, and security relative to the system center in the event of critical events for it and its operating environment. To achieve completeness in terms of the experimental results, the series were conducted separately for cases of critical change in the indicators of one of the criteria and for indicators that are characteristic exclusively for a single criterion. In addition, the experimental series was conducted in cases of impact on several criteria simultaneously through indicators common to them.

The first experimental series. During the operation of the system, the center was changed 100 times according to the different options. To determine the next option of centralization in the system architecture, the values of the operational efficiency, stability, integrity and security criteria were calculated using analytical expressions, which were determined by formulas (16), (23), (24) and (27). The results of the first experimental series are presented in a fragment in Table. 1. All obtained values belong to the interval [0;0.65]. This meets the requirements for the developed analytical expressions for the four criteria, which are given by the general formula (15). At the same time, a restriction on the belonging of the obtained values to each criterion of the interval [0;1] is observed.

The first series of experiments was conducted during the normal operation of the proposed system. Four graphs of discrete functions are shown in Fig. 1, which display 100 points for each of the four criteria. No problematic events occurred during system operation.

The depicted graphs display values in the range of 0 to 0.065, which corresponds to the limitations specified in the analytical expressions for the specified criteria regarding operational efficiency, stability, integrity, and security. All points on the graphs correspond to the values

Table 1

Results of the first series of experiments

Reconfiguration number	Time. sec	Function value				
		Operational efficiency $f_{1.kr}^{centr}$	Stability $f_{2.kr}^{centr}$	Integrity $f_{3.kr}^{centr}$	Security $f_{4.kr}^{centr}$	Objective function F_{kr}^{centr}
1	0	0.060488135	0.061778165	0.058117959	0.064065555	0.061112454
2	$7.94 \cdot 10^3$	0.062151894	0.05770008	0.061963435	0.062740473	0.06113897
3	$1.59 \cdot 10^4$	0.061027634	0.06235194	0.058777518	0.058331452	0.060122136
4	$2.38 \cdot 10^4$	0.060448832	0.064621885	0.056796037	0.055811014	0.059419442
…	…	…	…	…	…	…
99	$7.78 \cdot 10^6$	0.0632894	0.055580292	0.064729195	0.055163285	0.059690543
100	$7.96 \cdot 10^6$	0.055046955	0.059344166	0.064608347	0.056852323	0.058962948

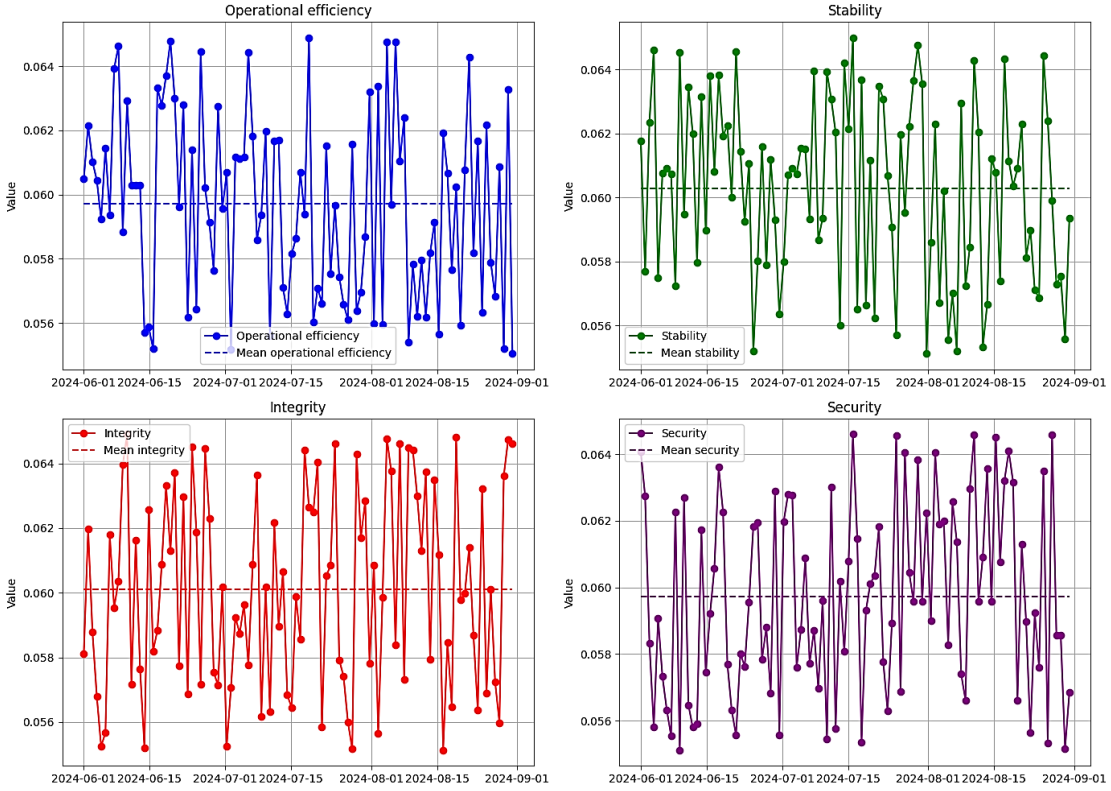

Fig. 1. Function graphs for four criteria

of the functions obtained during the preparation of the next option for centralization in the system. The specified criteria mainly do not have common indicators; therefore, the values obtained according to their analytical expressions are not correlated.

Let us construct a graph for the objective function according to the obtained values for the criteria according to Eq. (12). Let us calculate its value as the arithmetic mean of all four criteria. If necessary, the value can be determined as a weighted average value if a greater influence of a certain criterion is established or indicated. The graph of the objective function for the first series of the experiment, which is shown in Fig. 2, shows the permissible values for transitions to the next option for centralization in the system architecture during the experiment. In addition, based on the values of the objective function, a graph of a theoretical curve was constructed, which reflects and determines possible further values of the objective function when determining the next options for centralization. The deviations between the theoretical curve and the values obtained experimentally according to the least squares method are within permissible limits.

In particular, the difference between the maximum (minimum) value from the experiment and the value of the corresponding point of the theoretical curve was approximately 0.03, i.e., 3%. This is a consequence of the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

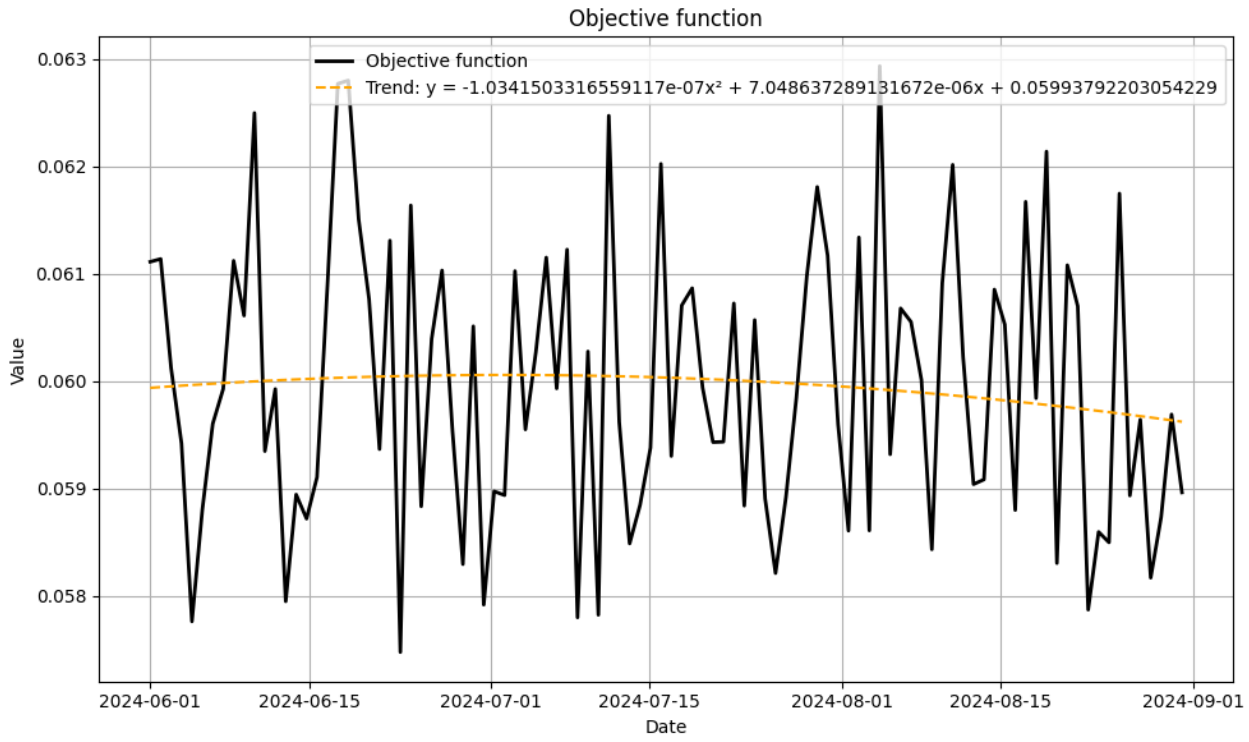

Fig. 2. Graph of the objective function

selection of successful options for centralization. The resulting theoretical curve, for which an analytical expression is defined, is given by a semi-parabola with a gradual downward trend. This reflects the consideration of previous experience in terms of each new option. The system has been operating for a long time; thus, this is an indicator of successful self-learning and, accordingly, the definition of the objective function for the standard case of system operation.

The following series of experiments were conducted to study the system for the application of the criteria for cases of separate influences on the indicators of the criteria, and each criterion was studied separately.

The second series of experiments was carried out considering the changes in the indicators that affected the value of the operational efficiency criterion. Significant deviations in the obtained values over the three time periods were observed during system operation. The graphs of all four functions are shown in Fig. 3.

The obtained values considering significant deviations of some values for the operational efficiency criterion are acceptable for the continued operation of the system. In other words, the system stability was not violated because of events that affected the value of the operational efficiency criterion. The objective function, which is depicted by the graph in Fig. 4, was obtained empirically, also confirms the ability of the system to continue functioning and determine the next option for centralization. In this case, the evaluated centralization options according to the definition of the objective function will have larger values, and among them, fewer of these values will be prioritized for approval.

The objective function, which is determined theoretically, confirms the ability of a system to determine the next option for its centralization.

Similarly, for the stability criteria (the graphs in Fig. 5 and Fig. 6), integrity (graphs in Fig. 7 and Fig. 8) and security (the graphs in Fig. 9 and Fig. 10), we confirm the admissibility of performing the task of determining the next option of centralization in the system architecture.

The trend of the theoretical curve of the objective function for the criterion of impact on stability (see Fig. 6) is upward, and for the theoretical curves of the objective function for the criteria of efficiency, safety, and integrity are downward. At the same time, all values of the objective functions when changing all criteria separately are less than 7%, which is acceptable for the functioning of the work. In the graphs for these cases, the further steps of the system for rebuilding the center were stable. Thus, the four criteria specified by the functions adequately reflect the behavior of the system.

In the next three series, the number of time intervals should be changed from 4 to 5 for larger deviations. The adequacy of the description of the analytical expressions of the criteria is confirmed by the insignificant deviations of their function graphs. In cases of significant deviations at certain time intervals during the operation of the system, the results of determining the options for centralization are obtained. The analytical expressions for the objective function in all cases, which are obtained from the

theoretical method, also confirm the possibility of obtaining an acceptable result. The trend of the theoretical curve of the objective function for the criterion of impact on stability (Fig. 6) is upward, and for the theoretical curves of the objective function for the criteria of efficiency, safety, and integrity are downward. At the same time, all values of the objective functions when changing

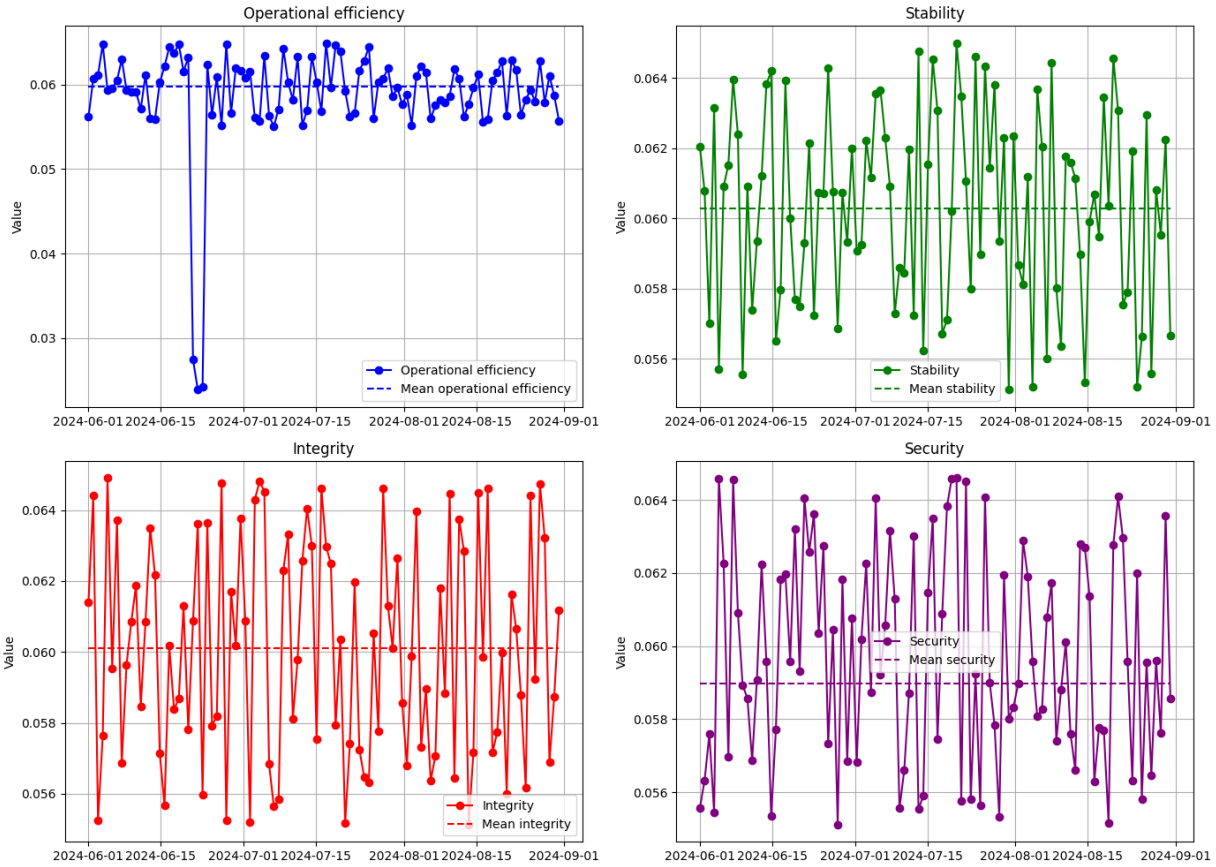

Fig. 3. Graphs of functions of the second series of experiments for four criteria

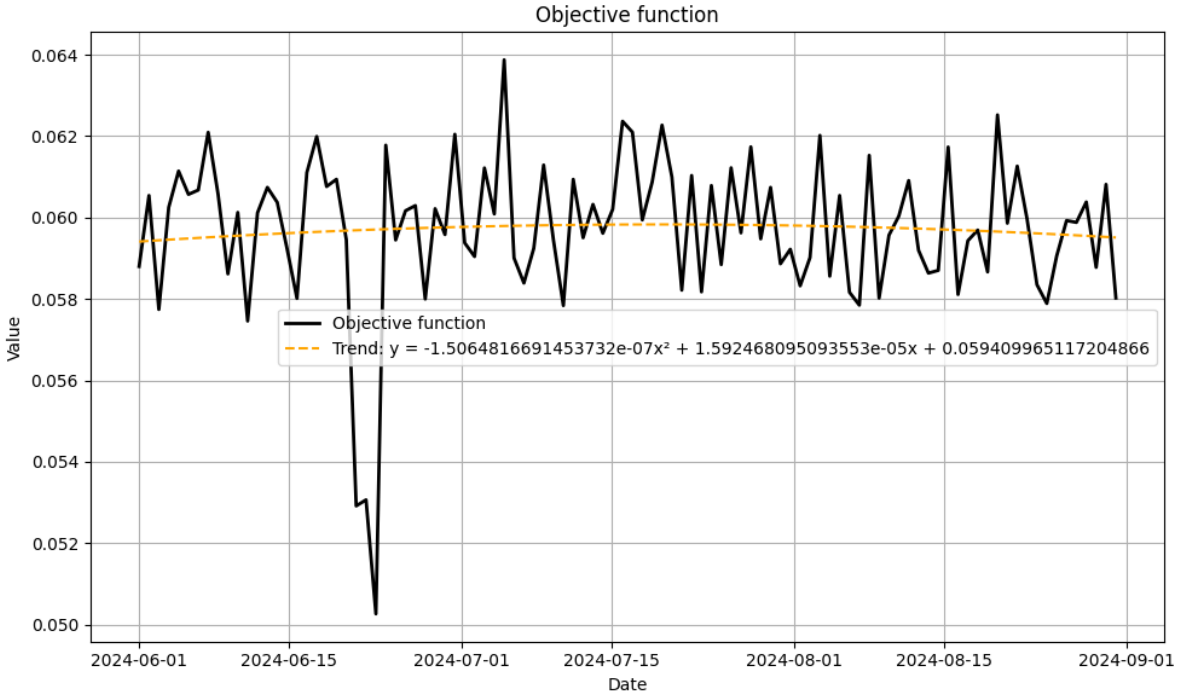

Fig. 4. The graph of the objective function of the second series of the experiment

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

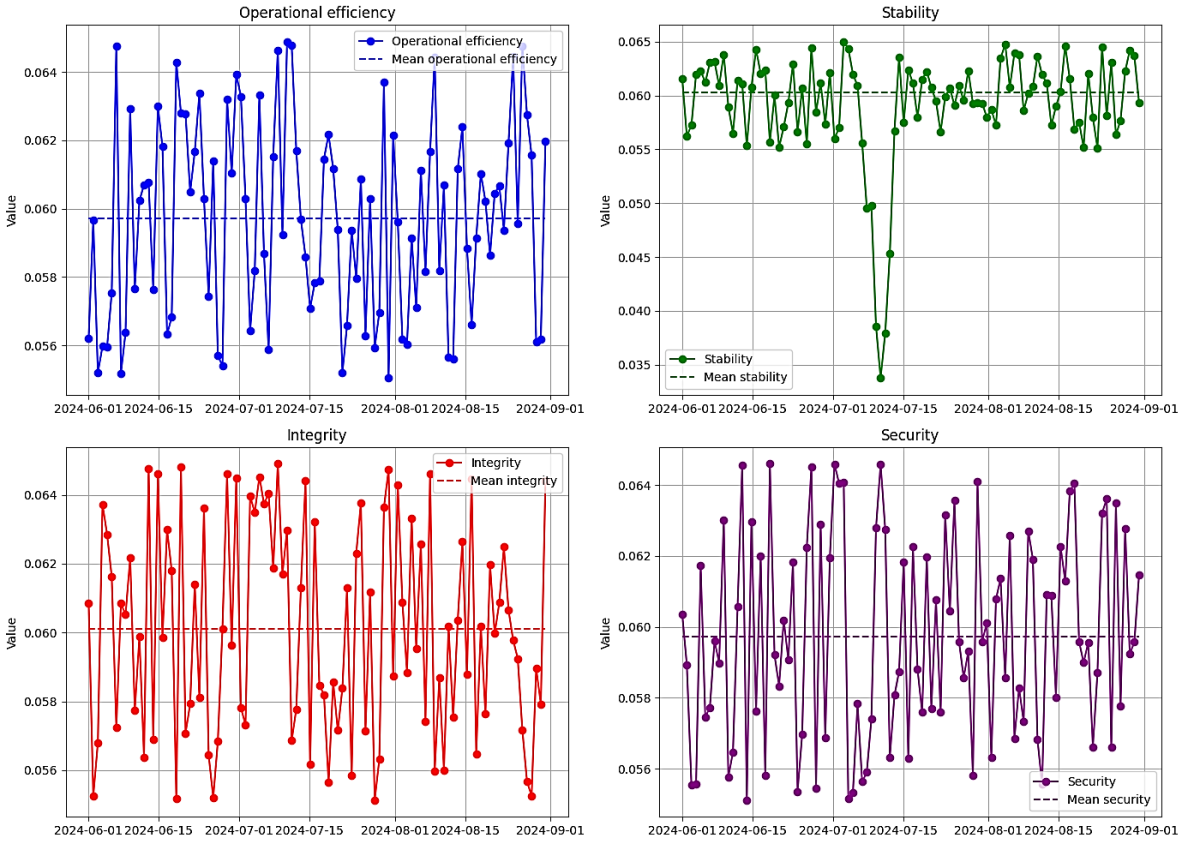

Fig. 5. Graphs of functions of the third series of the experiment for four criteria

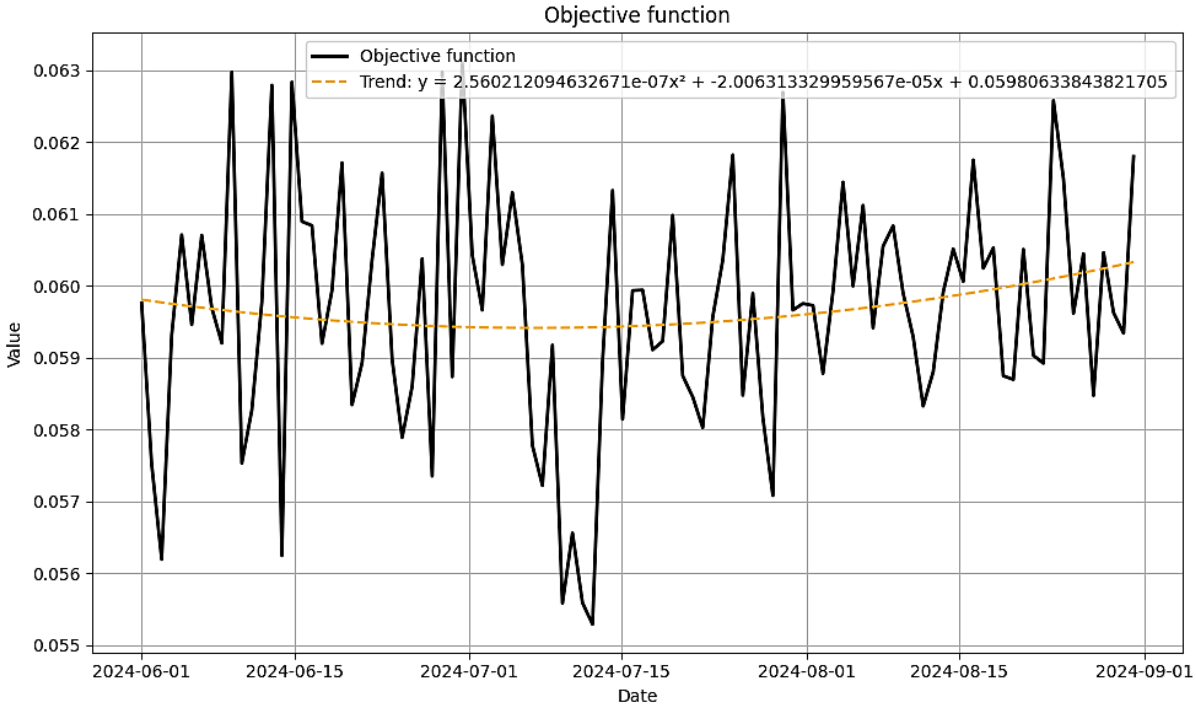

Fig. 6. Graph of the objective function of the third series of the experiment

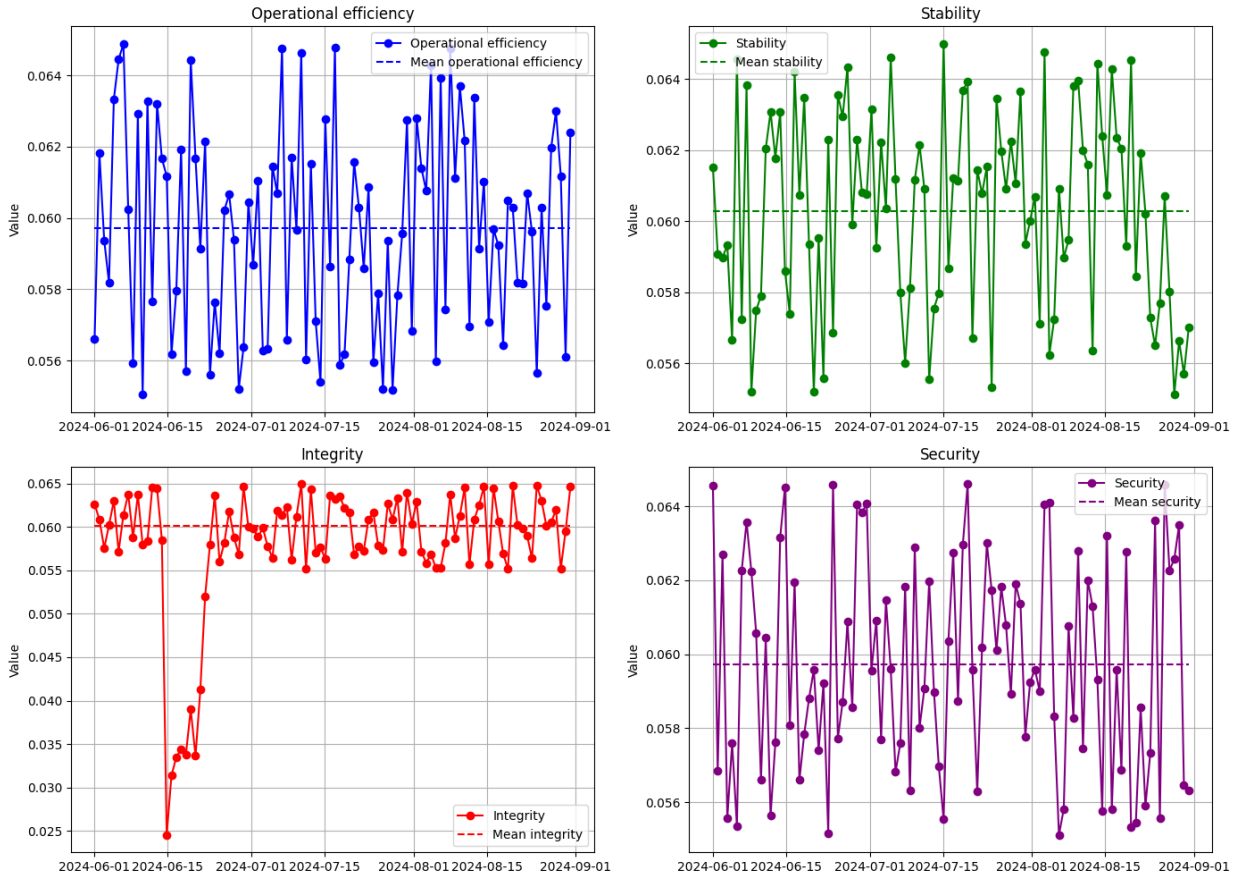

Fig. 7. Graphs of functions of the fourth series of the experiment for four criteria

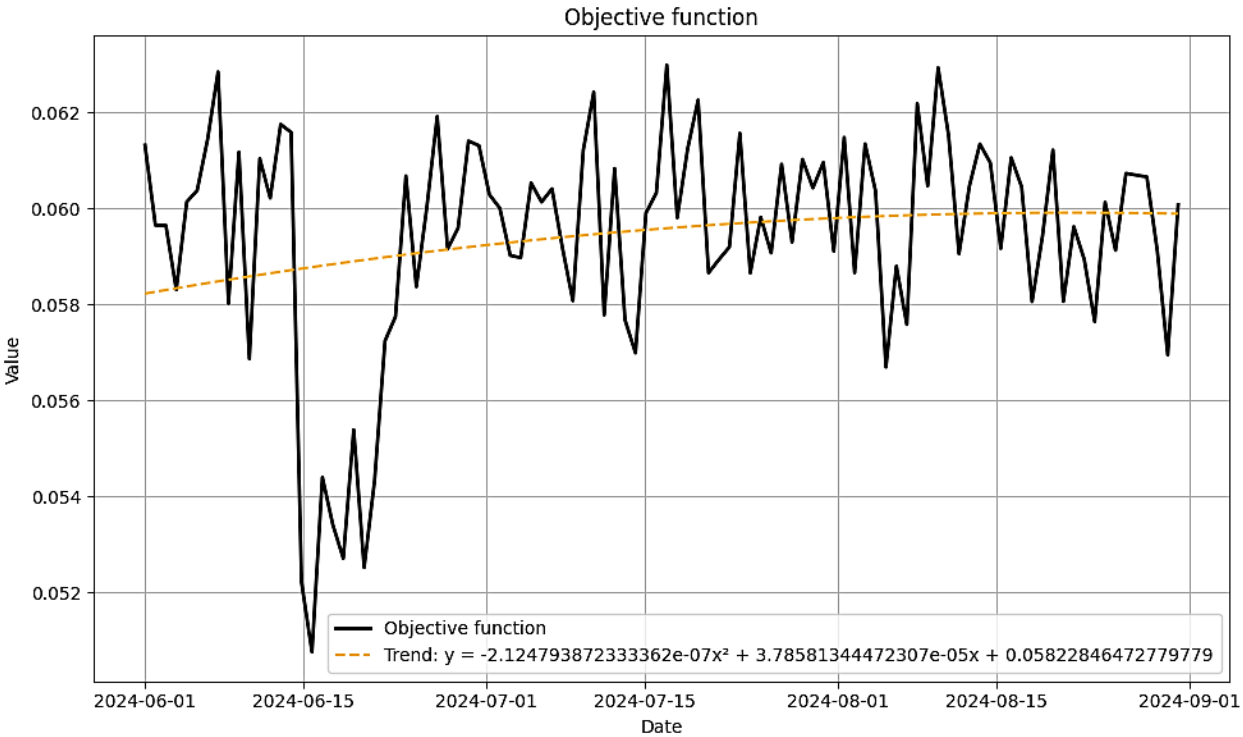

Fig. 8. Graph of the objective function of the fourth series of the experiment

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

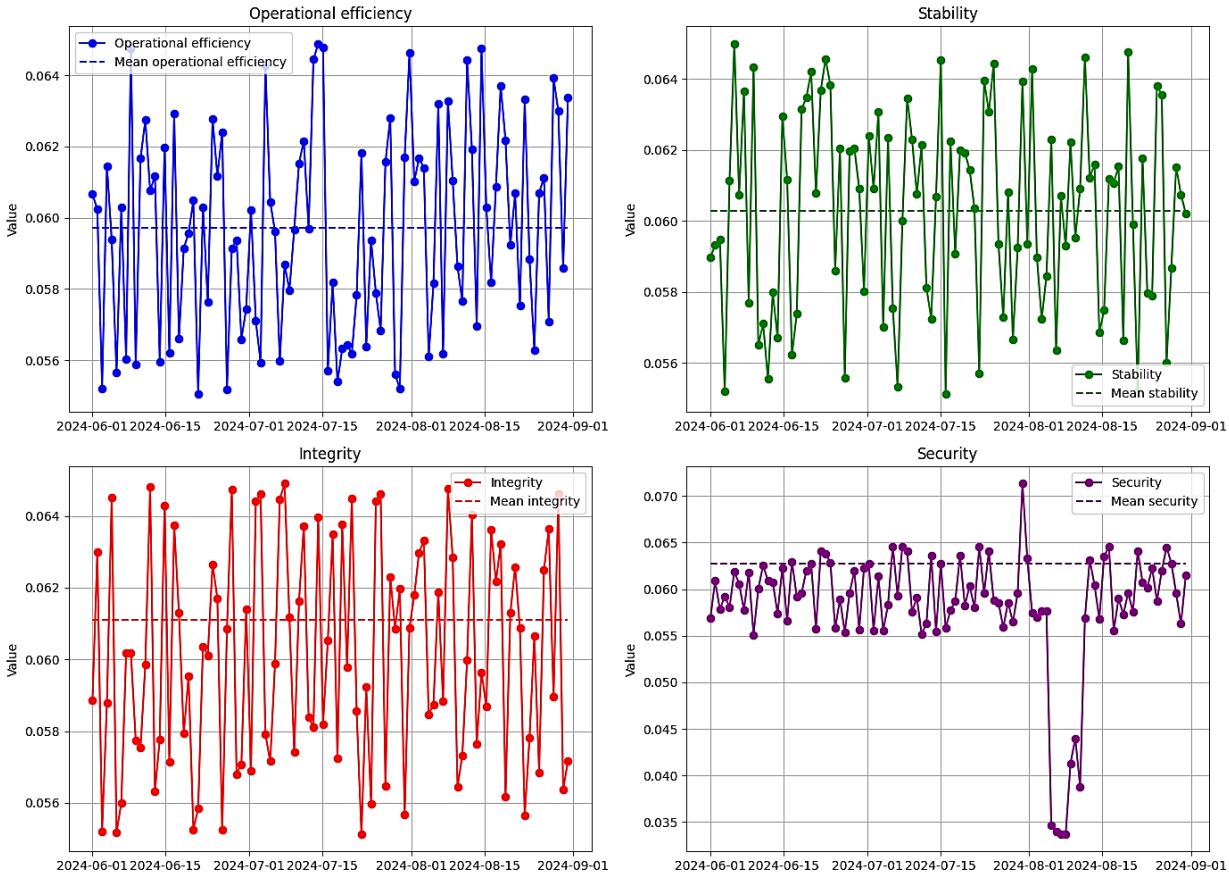

Fig. 9. Function graphs of the fifth series of the experiment for four criteria

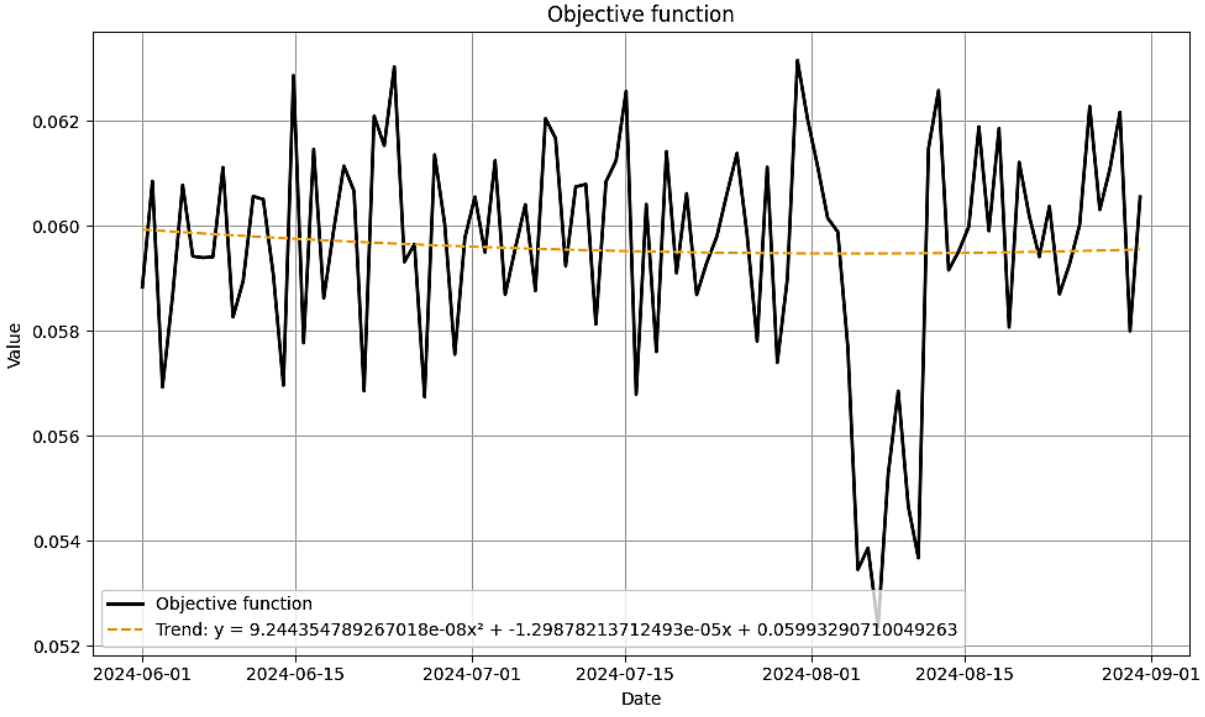

Fig. 10. Graph of the objective function of the fifth series of the experiment

Table 2

Summary

Reconfig-uration number	Time. sec	Function value				
		Operational efficiency $f_{1.kr}^{centr}$	Stability $f_{2.kr}^{centr}$	Integrity $f_{3.kr}^{centr}$	Security $f_{4.kr}^{centr}$	Objective function F_{kr}^{centr}
…	…	…	…	…	…	…
17	$1.27 \cdot 10^6$	0.061176355	0.058599781	**0.024556127**	0.064518745	0.052212752
18	$1.35 \cdot 10^6$	0.056187277	0.057378928	**0.031408288**	0.058068101	0.050760649
19	$1.43 \cdot 10^6$	0.057961402	0.064194826	**0.033481409**	0.061956254	0.054398473
20	$1.51 \cdot 10^6$	0.061924721	0.060722519	**0.034404319**	0.056594145	0.053411426
21	$1.59 \cdot 10^6$	0.055710361	0.063480082	**0.033818294**	0.057835188	0.052710981
…	…	…	…	…	…	…
23	$1.75 \cdot 10^6$	**0.063209932**	0.057487531	0.057817301	0.059304024	0.059454697
24	$1.83 \cdot 10^6$	**0.027444256**	0.059287687	0.060883171	0.06403984	0.052913738
25	$1.91 \cdot 10^6$	**0.023918779**	0.062142413	0.063621915	0.062567786	0.053062723
26	$1.99 \cdot 10^6$	**0.024218483**	0.057239247	0.055978445	0.063605512	0.050260422
27	$2.06 \cdot 10^6$	**0.062392636**	0.060722519	0.063638556	0.060361775	0.061778871
…	…	…	…	…	…	…
42	$3.18 \cdot 10^6$	0.061531083	**0.049575421**	0.061874883	0.05589603	0.057219354
43	$3.26 \cdot 10^6$	0.064636628	**0.049754205**	0.064903389	0.057400203	0.059173606
44	$3.34 \cdot 10^6$	0.059236548	**0.038600776**	0.061699165	0.062786954	0.055580861
45	$3.41 \cdot 10^6$	0.064883738	**0.033778165**	0.062980468	0.064589827	0.05655805
46	$3.49 \cdot 10^6$	0.064786183	**0.037965466**	0.056856359	0.062740473	0.055587121
…	…	…	…	…	…	…
73	$5.64 \cdot 10^6$	0.058154284	0.06230122	0.0587417	**0.034605388**	0.053450648
74	$5.72 \cdot 10^6$	0.063209932	0.056354741	0.061874883	**0.033997959**	0.053859379
75	$5.80 \cdot 10^6$	0.056182744	0.060699649	0.058834639	**0.033720478**	0.052359378
76	$5.88 \cdot 10^6$	0.0632894	0.059287687	0.064774951	**0.033720478**	0.055268129
77	$5.96 \cdot 10^6$	0.061048455	0.062220556	0.062851529	**0.041288984**	0.056852381
…	…	…	…	…	…	…

all criteria separately are less than 7%, which is acceptable for the functioning of the work. In the graphs for these cases, the further steps of the system for rebuilding the center were stable. Thus, the four criteria specified by the functions adequately reflect the behavior of the system.

The test environment, including network topology parameters, number of nodes, and testing options, was the same in all experiments. For the experiment, system components were installed in 60 computer stations. The corporate network is divided into 8 segments. The demilitarized zone consists of three computer stations in one segment of the corporate network.

We did not investigate testing for specific types of computer attacks. The effects were carried out on individual parameters affecting the values of the criteria and were carried out in separate series of experiments.

The influence of previous experience on using a certain centralization option can be analyzed by points on the graphs of the objective evaluation functions, where the trend of the curve line changes. In addition, the successful selection of the next centralization option in the architecture and the transition to it are reflected by a small deviation of the curve points from the trend curve.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

4. Discussion

Two experiments confirmed that the system could perform tasks when changing its parameters for different criteria. The deviations for each criterion did not create critical problems for its functioning. Thus, the system demonstrated the stability of its work. The analytical expressions obtained for the evaluation criteria sufficiently consider the parameters, which ensured the completeness of the description of the processes occurring in it.

When applying equation (16), 20 parameters were used, and in the equation from work [6], 19 parameters were used. The last term in Eq. (6) can be equal to zero, so the formula is presented as in Eq. [6]. The additional time spent on establishing the state of components that did not respond to confirm processing of the message about the completion of the current type of centralization and transition to a new type of central identification in the system architecture can be equal to zero. This term is introduced for the case of a long response or no response from certain components. It is an important parameter in the context of the efficiency criterion. Similarly, the remaining parameters of the four criteria were investigated. All parameters of the four criteria were considered in their extreme values during the study. At maximum extreme values, the results of calculating the functions for the criteria are values equal to one in the parameters of the objective function. However, all parameters and all four criteria cannot have maximum extreme numerical values at the same time because the system will evaluate such an option as an option with a low level of security and reject it. If the parameter values are equal to zero or are such that the values of the functions for the criteria are close to zero in the objective function, then such centralization options will be considered by the system as options for the next transition to them.

5. Conclusions and Future Work

Mathematical models have been developed for the criteria of operational efficiency, stability, integrity, and security relative to the system center, which, unlike the known mathematical models for evaluating system centers for selecting the following centralization options, are presented in analytical expressions that take into account the features of the types of centralization in the architecture of systems, indicators of operational efficiency, stability, integrity, and security relative to the system center and allow forming on their basis an objective function for evaluating centralization options in systems, the feature of which is the hiding of components with the system center from its detection by attackers.

The paper analyzes the results of the experiment with the prototype of the proposed system. The convergence of the experimental and theoretical results was established. The adequacy of the description of the criteria by analytical expressions is confirmed by the insignificant deviations of their function graphs. In cases of significant deviations at certain time intervals during system operation, the result for determining centralization options is obtained.

The developed objective function for evaluating centralization options can be used in systems that involve restructuring their architecture independently without the involvement of an administrator. Such systems are actively being developed in the cybersecurity field. The approach based on the objective evaluation function can be adapted to evaluate the next steps of the system. The transition to the next centralization option is only one of the possible steps of the system that can be performed without the involvement of an administrator. The generalized representation of the evaluation objective function can be integrated into existing security mechanisms of corporate networks, in particular, deceptive systems, including bait and trap systems. Most modern commercial deceptive systems are presented [1,2] as a rule describing the declared capabilities. In addition, most research (non-commercial) adaptive systems presented in scientific works do not detail the mechanisms and rules for ensuring adaptability. At the same time, they present a detailed architecture of the systems. The synthesis of the adaptability properties for systems of this purpose is not detailed; therefore, this approach details the part for ensuring adaptability. The decisive factor here is that if the objective function and its evaluation criteria are open, it is impossible to predict the numerical value of the next centralization option. This condition is necessary for building deceptive systems that are resistant to malicious influences.

The directions of further research are the development of rules and methods for organizing structural parts of systems and systems as a whole to ensure their ability to independently restructure the architecture, taking into account previous operating experience.

Contributions of authors: analysis of known approaches to changing the architecture of systems during their operation, development of mathematical models of criteria for evaluating centralization options in the architecture of multi-computer systems for detecting malicious software and computer attacks, setting up and conducting an experiment - **Antonina Kashtalian;** formulation of the task regarding the ability of systems to independently restructure in terms of centralizing their architecture - **Sergii Lysenko;** formulation of the problem regarding evaluating centralization options in the architecture of multi-computer systems for detecting malicious software and computer attacks for restructuring the archi-

tecture of systems - **Anatoliy Sachenko;** analysis of systems with partially centralized architecture to take into account their parameters in the evaluation criteria, conducting the experiment and processing its results - **Bohdan Savenko;** checked the analytical dependencies and set up the experiment - **Oleg Savenko and Andriy Nicheporuk.**

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, author ship or otherwise, that could affect the research and its results presented in this paper.

Financing

This research was supported by the Ministry of Education and Science of Ukraine. The state registration number of the project "A system for detecting malicious software and computer attacks in corporate networks using false attack objects and traps" is 0124U000980 (2024-2025).

Data Availability

The manuscript has no associated data.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

Project information

The study was carried out as part of the implementation of the 0124U000980 project. The project aims to solve the current scientific and applied problem of increasing the level of security, fault tolerance, survivability and information protection of computer systems of corporate networks by developing a system for detecting malicious software and computer attacks in corporate networks using false attack objects and traps.

To achieve the goal of the project, the following tasks are solved: development of the architecture of partially centralized distributed systems for detecting malicious software in computer networks and an abstract model of the effects of malicious software on computer system objects; formalization of the characteristic properties of cyberattacks; development of methods for detecting cyberattacks on computer systems; development of a method and means of verifying the inclusion of subject area information; implementation of a system for detecting malicious software and computer attacks in corporate networks using false attack objects and traps, conducting experimental research, developing and applying a methodology for determining the effectiveness of increasing the level of security, fault tolerance, survivability and information protection of computer systems in corporate networks.

All the authors have read and agreed to the published version of this manuscript.

References

1. Savenko, B., Kashtalian, A., Lysenko S., & Savenko O. Malware Detection By Distributed Systems with Partial Centralization, *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023, pp. 265-270, DOI: 10.1109/IDAACS58523.2023.10348773.

2. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., & Vasylkiv, N. Botnet detection approach based on the distributed systems, *International Journal of Computing*, 2020, vol. 19, iss. 2, pp. 190-198. DOI: 10.47839/ijc.19.2.1761.

3. Kashtalian, A., Lysenko, S., Savenko, B., Sochor, T., & Kysil, T. Principle and method of deception systems synthesizing for malware and computer attacks detection, *Radioelectronic and Computer Systems*, 2023, vol. 4, pp.112-151. DOI: 10.32620/reks.2023.4.10.

4. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. Multicomputer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 2024, vol. 1, pp. 152-175. DOI: 10.32620/reks.2024.1.13.

5. Lysenko, S., Bobrovnikova, K., Shchuka, R., & Savenko, O. A Cyberattacks Detection Technique Based on Evolutionary Algorithms, *11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2020, vol. 1, pp. 127-132.

6. Kashtalian, A. The criterion of promptness in centralization in the architecture of multicomputary systems of combined antivirus baits and traps to detect malicious software and computer attack [The criterion of promptness in centralization in the architecture of multicomputary systems of combined antivirus baits and traps to detect malicious software and computer attacks]. *Visnyk Khmel'nyts'koho natsional'noho universytetu. Tekhnichni nauky – Herald of Khmelnytskyi National University. Technical sciences*, 2024, vol. 345, vol. 2, no. 6, pp. 172–178. Available at: https://elar.khmnu.edu.ua/handle/123456789/17828. (accessed 11.11.2024) (In Ukrainian).

7. Svanadze, V., & Gnatyuk, S. Challenges and solutions for cybersecurity and information security management in organizations, *CEUR-WS*, 2024, vol. 3654, pp. 497–504. Available at: https://ceur-ws.org/Vol-3654/short20.pdf. (accessed 11.11.2024)

8. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S., Milov, O., Pro-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

kopenko, O., Sievierinov, O., & Chopenko, D. Development of a concept for building a critical infrastructure facilities security system, *Eastern-European Journal of Enterprise Technologies*, 2021, vol. 3, no. 9(111), pp. 63–83. DOI: 10.15587/1729-4061.2021.233533.

9. Dowling, S., Schukat, M., & Barrett, E. New framework for adaptive and agile honeypots. *ETRI Journal*, 2020, no. 42, pp. 965-975. DOIL 10.4218/etrij.2019-0155.

10. Viola, V. *From honeypots to distributed deception platforms: Theory and testing of emerging technologies for IT security*. Master Degree Thesis. Politecnico di Torino. 2019. 78 p. Available at: https://webthesis.biblio.polito.it/13096/1/tesi.pdf (accessed December 10, 2024).

11. Niakanlahiji, A., Jafarian, J., Chu, B.-T., & Al-Shaer, E. HoneyBug: Personalized cyber deception for web applications, *Proceedings of the Hawaii International Conference on System Sciences* (HICSS), 2020, article no. 233. DOI: 10.24251/HICSS.2020.233.

12. Kharchenko, V., Ponochovnyi, Y., Ivanchenko, O., Fesenko, H., & Illiashenko, O. Combining Markov and semi-Markov modelling for assessing availability and cybersecurity of cloud and IoT systems, *Cryptography*, 2022, vol. 6, no. 44. DOI: 10.3390/cryptography6030044.

13. Mukhin, V., Kornaga, Y., Bondarenko, V., Zavgorodnii, V., Herasymenko, O., & Sholokhov, O. Mathematical model for heterogeneous databases parameters estimation in distributed systems with dynamic structure, *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory* (ATIT), Kyiv, Ukraine, 2020, pp. 158–161. DOI: 10.1109/ATIT50783.2020.9349331 .

14. Moskalenko, V., Kharchenko, V., Moskalenko, A., & Kuzikov, B. Resilience and resilient systems of artificial intelligence: Taxonomy, models and methods, *Algorithms*, 2023, vol. 16, article no. 165. DOI: 10.3390/a16030165.

15. Amin, M. A. R. A., Shetty, S., Njilla, L., Tosh, D. K., & Kamhoua, C. Online cyber deception system using partially observable Monte-Carlo planning framework. In: Chen, S., Choo, KK., Fu, X., Lou, W., & Mohaisen, A. (eds), *Security and Privacy in Communication Networks*. SecureComm 2019, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 305. Springer, Cham. DOI: 10.1007/978-3-030-37231-6_11.

16. Letychevskyi, O., & Peschanenko, V. Applying algebraic virtual machine to cybersecurity tasks, *Proceedings of the IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), IEEE*, Hammamet, Tunisia, 2022, pp. 161–169. DOI: 10.1109/SETIT54465.2022.9875895.

17. Gao, Y., Zhang, G., & Xing, C. A multiphase dynamic deployment mechanism of virtualized honeypots based on intelligent attack path prediction. *Security and Communication Networks*, 2021, vol. 2021, article no. 6378218. 15 p. DOI: 10.1155/2021/6378218.

18. Thang, N., Park, M., & Joo, Y. EVHS - Elastic Virtual Honeypot System for SDNFV-Based Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 2022, vol. 12, iss. 3. DOI: 10.17762/ijcnis.v12i3.4701.

19. Kareem, S. A., Sachan, R. C., & Malviya, R. K, AI-Driven Adaptive Honeypots for Dynamic Cyber Threats. *SSRN*, 2024, pp. 1-9. DOI: 10.2139/ssrn.4966935.

20. Islam, M. M., & Al-Shaer, E. Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception. *2020 IEEE Secure Development (SecDev)*, Atlanta, GA, USA, 2020, pp. 41-48. DOI: 10.1109/SecDev45635.2020.00023.

21. Belalis, I., Kavallieratos, G., Gkioulos, V., & Spathoulas, G. *Enabling defensive deception by leveraging software defined networks. International Academy*, Research and Industry Association (IARIA), 2020. Available at: https://hdl.handle.net/11250/2685618 (accessed December 10, 2024).

22. Gao, C., Wang, Y., & Xiong, X. A cyber deception defense method based on signal game to deal with network intrusion. *Security and Communication Networks*, 2022, vol. 2022, iss. 1, article no. 3949292. DOI: 10.1155/2022/3949292.

23. Sajid, M. S. I., Wei, J., Alam, M. R., Aghaei, E., & Al-Shaer, E. DodgeTron: Towards autonomous cyber deception using dynamic hybrid analysis of malware. *2020 IEEE Conference on Communications and Network Security (CNS)*, Avignon, France, 2020, pp. 1-9. DOI: 10.1109/CNS48642.2020.9162202.

24. Acosta, J. C., Basak, A., Kiekintveld, C., Leslie, N., & Kamhoua, C. Cybersecurity deception experimentation system. *2020 IEEE Secure Development (SecDev)*, Atlanta, GA, USA, 2020, pp. 34–40. DOI: 10.1109/SecDev45635.2020.00022.

25. Khoroshko, V., Khokhlachova, Y., & Vyshnevska, N. Choice of indicators for forecasting cyber protection of computer systems. *Ukrainian Scientific Journal of Information Security*, 2023, vol. 29, no. 1, pp. 41–47.

26. Yi, H., Li, F., Wang, R., Hu, N., & Tian, Z. A survey of deception defense: Approaches used to counter malicious behavior. *2023 IEEE 12th International Conference on Cloud Networking (CloudNet)*, Hoboken, NJ, USA, 2023, pp. 418–422. DOI: 10.1109/CloudNet59005.2023.10490043.

27. Shinde, A., Doshi, P., & Setayeshfar, O. Cyber attack intent recognition and active deception using fac-

tored interactive POMDPs. *Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems, International Foundation for Autonomous Agents and Multiagent Systems*, 2021, pp. 1200-1208.

28. Putrevu, V. S. C., Mukhopadhyay, S., Manna, S., Rani, N., Vaid, A., Chunduri, H., Putrevu, M. A., & Shukla, S. ADAPT: Adaptive camouflage-based deception orchestration for trapping advanced persistent threats. *Digital Threats: Research and Practice*, 2024, vol. 5, no. 3, article 21. 35 p. DOI: 10.1145/3651991.

29. Li, T., Chen, B., Yu, L., & Zhang, W.-A. Active security control approach against DoS attacks in cyber-physical systems, *IEEE Transactions on* Automatic *Control*, 2021, vol. 66, no. 9, pp. 4303–4310. DOI: 10.1109/TAC.2020.3032598.

30. Ferguson-Walter, K., Fugate, S., Mauger, J., & Major, M. Game theory for adaptive defensive cyber deception. *HotSoS '19: Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, 2019, article no. 4. 8 p. DOI:10.1145/3314058.3314063.

31. Kong, T., Wang, L., Ma, D., Xu, Z., Yang, Q., Lu, Z., & Lu, Y. Automated honeynet deployment strategy for active defense in container-based cloud, *2020* IEEE *22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2020, pp. 483–490.

32. Moric, Z., Mršić, L., Kunić, Z., Đambić, G. Honeypots in Cybersecurity: Their Analysis, Evaluation and Importance. *Preprints*, 2024. https://doi.org/10.20944/preprints202408.0946.v1

33. Subhash, P., Qayyum, M., Varsha, C.L., Mehernadh, K., Sruthi, J., & Nithin, A. A security framework for the detection of targeted attacks using honeypot. In: Devi, B.R., Kumar, K., Raju, M., Raju, K.S., & Sellathurai, M. (eds), *Proceedings of Fifth International Conference on Computer and Communication Technologies (IC3T 2023)*. Lecture Notes in Networks and Systems, vol. 897, Springer, Singapore, 2024. DOI: 10.1007/978-981-99-9704-6_16.

34. Lobanchykovaa, N. M., Pilkevychb, I. A., & Korchenko, O. Analysis of attacks on components of IoT systems and cybersecurity technologies. *QuaInT+ doors*, 2021, pp. 83–96. Available at: https://ceur-ws.org/Vol-2850/paper6.pdf. (accessed 11.11.2024).

35. Surber, J., & Zantua, M. Intelligent interaction honeypots for threat hunting within the Internet of Things. *Journal of The Colloquium for Information Systems Security Education*, 2022, vol. 9, pp. 1–5. DOI: 10.53735/cisse.v9i1.147.

36. Pour, M. S., Khoury, J., & Bou-Harb, E. HoneyComb: A darknet-centric proactive deception technique for curating IoT malware forensic artifacts. *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, Budapest, Hungary, 2022, pp. 1–9. DOI: 10.1109/NOMS54207.2022.9789827.

37. Seo, S., & Kim, D. IoDM: A study on an IoT-based organizational deception modeling with adaptive general-sum game competition. *Electronics*, 2022, vol. 11, article no. 1623. DOI:10.3390/electronics11101623.

38. Kehret, O., Walz, A., & Sikora, A. Integration of Hardware Security Modules into a Deeply Embedded TLS Stack. *International Journal of Computing*, 2016, vol. 15, iss. 1, pp. 22-30. DOI:10.47839/ijc.15.1.827.

39. Komar, M., Sachenko, A., Golovko, V., & Dorosh, V. Compression of Network Traffic Parameters for Detecting Cyber Attacks Based on Deep Learning, *Proceedings of the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2018),* Kyiv, Ukraine, 2018, pp. 44-48.

40. Kharchenko, V., Ponochovnyi, Y., Abdulmunem, A.-S. M. Q., & Boyarchuk, A. Security and Availability Models for Smart Building Automation Systems, *International Journal of Computing*, 2017, vol. 16(4), pp. 194-202. DOI: 10.47839/ijc.16.4.907.

41. Komar, M., Golovko, V., Sachenko, A., & Bezobrazov, S. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification, *Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (IDAACS), Berlin, Germany, 2013, pp. 665-668.

42. Obeidat, I., & AlZubi, M. Developing a Faster Pattern Matching Algorithms for Intrusion Detection System, *International Journal of Computing*, 2019, vol. 18, iss. 3, pp. 278-284. DOI: 10.47839/ijc.18.3.1520.

43. Doukas, N., Stavroulakis, P., & Bardis, N. Review of artificial intelligence cyber threat assessment techniques for increased system survivability. In *Malware Analysis Using Artificial Intelligence and Deep Learning*, Springer International Publishing, 2021, pp. 207-222. DOI: 10.1007/978-3-030-62582-5_7.

44. Lysenko, S., & Savenko, B. Distributed Discrete Malware Detection Systems Based on Partial Centralization and Self-Organization. *International Journal of Computing*. 2023. vol. 22, pp. 117-139. DOI: 10.47839/ijc.22.2.3082.

Received 27.01.2025, Accepted 17.02.2025

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

КРИТЕРІЇ ОЦІНЮВАННЯ ВАРІАНТІВ ЦЕНТРАЛІЗАЦІЇ В АРХІТЕКТУРІ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ З ПАСТКАМИ ТА ПРИМАНКАМИ

А. С. Каштальян, С. М. Лисенко, А. О. Саченко, Б. О. Савенко, О. С. Савенко, А. О. Нічепорук

Самостійна перебудова архітектури мультикомп'ютерних систем виявлення комп'ютерних атак та зловмисного програмного забезпечення в процесі їх функціонування є складним завдань, оскільки такі системи розподілені. Одним із завдань при цій перебудові є зміна архітектури центрів систем. Тобто система може перебудовуватись без змін в її центрі. Але специфіка завдань систем щодо виявлення зловмисного програмного забезпечення та комп'ютерних атак потребує такої організації систем, щоб зловмисниками було складно зрозуміти їх поведінку. Тому, актуальним завданням, яке розглядається в роботі, є розроблення правил для забезпечення перебудови центрів систем за різними типами архітектури. **Метою** роботи є розроблення критеріїв оцінювання потенційних варіантів централізації в архітектурі мультикомп'ютерних систем з пасктами та приманками. Для забезпечення такого оцінювання в роботі проведено аналіз відомих рішень і встановлено недостатність математичного забезпечення щодо організації перебудови центрів систем в процесі їх функціонування. Враховуючи специфіку завдань для таких систем не було визначено параметрів, які б могли бути враховані для формування перебудови центрів систем. В аналізованих роботах встановлено основні типи централізації, які використовуються в архітектурі систем: централізовані, частково централізовані, частково децентралізовані, децентралізовані. Але не деталізовані та представлені алгоритми та способи переходу систем від одного типу до іншого в процесі їх функціонування. **Предмет дослідження.** В роботі визначено характеристичні властивості, які можна використати при синтезуванні систем. Вони визначають кількість потенційних варіантів архітектури систем, в які вона перейти на наступному кроці при прийнятті рішення щодо перебудови архітектури. Із збільшенням кількості характерних властивостей буде зростати кількість можливих варіантів. При затвердженні варіантів для переходу потрібно було здійснити оцінювання їх з врахуванням попереднього досвіду функціонування систем. Для здійснення оцінювання потенційних варіантів централізації в архітектурі систем було розроблено критерії оцінювання. Особливістю критеріїв оцінювання є те, що згідно них можна враховувати досвід використання варіанту централізації у випадку повтору та оцінити підготовлені варіанти, які пропонуються вперше. Тобто, в критерії оцінювання закладено попередній досвід функціонування мультикомп'ютерних систем. Цей досвід дав змогу оцінити варіант, що повторився, за результатами його використання раніше. Це дало змогу урізноманітнити вибір центрів систем. **Методи.** В роботі розроблено цільову функцію оцінювання наступного варіанту централізації в архітектурі систем. Цільова функція враховує чотири критерії оцінювання щодо оперативності, стійкості, цілісності та безпеки. Всі ці критерії орієнтовані на оцінювання саме потенційних варіантів центрів систем. Розроблено нові математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які на відміну від відомих математичних моделей оцінювання центрів систем для вибору наступних варіантів централізації, подані аналітичними виразами, в яких враховані особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи і дають змогу сформувати на їх основі цільову функцію для оцінювання варіантів централізації в системах, особливістю яких є приховування компонент з центром системи від його виявлення зловмисниками. **Результати.** В роботі проаналізовано результати проведеного експерименту з прототипом системи. Встановлено збіжність результатів експерименту та результатів, які отримано теоретичним способом. **Висновки.** Розроблено математичні моделі для оцінювання центрів систем на основі критеріїв ефективності, стабільності, цілісності та безпеки. На відміну від існуючих моделей, вони представлені як аналітичні вирази, які враховують різні типи централізації в системних архітектурах. Моделі дозволяють створювати цільові функції для оцінки варіантів централізації, наголошуючи на приховуванні компонентів системного центру від зловмисників. Результати експерименту з прототипом системи підтверджують справедливість теоретичних моделей, демонструючи мінімальні відхилення на графіках функцій. Значні відхилення в певних інтервалах часу враховуються для досягнення оптимальних варіантів централізації.

Ключові слова: централізація; системи обману; синтез систем обману; розподілені системи; honeynet; приманки-пастки; виявлення зловмисного програмного забезпечення.

Каштальян Антоніна Сергіївна – канд. техн. наук, доц. каф. фізики та електротехніки, докторантка, Хмельницький національний університет, Хмельницький, Україна.

Лисенко Сергій Миколайович – д-р техн. наук, проф., проф. каф. комп'ютерної інженерії та інформаційний систем, Хмельницький національний університет, Хмельницький, Україна.

Саченко Анатолій Олексійович – д-р техн. наук, проф., директор Науково-дослідного інституту інтелектуальних комп'ютерних систем, Західноукраїнський національний університет, Тернопіль, Україна; Радомський університет імені Казімежа Пуласького, Радом, Польща.

Савенко Богдан Олегович –д-р філос., старш. викл. каф. комп'ютерної інженерії та інформаційний систем, Хмельницький національний університет, Хмельницький, Україна.

Савенко Олег Станіславович - д-р техн. наук, проф., проф. каф. комп'ютерної інженерії та інформаційний систем, Хмельницький національний університет, Хмельницький, Україна.

Нічепорук Андрій Олександрович – канд. техн. наук, доц., доц. каф. комп'ютерної інженерії та інформаційний систем, Хмельницький національний університет, Хмельницький, Україна.

Antonina Kashtalian – PhD, Associate Professor at the Department of Physics and Electrical Engineering, Doctoral Student, Khmelnytskyi National University, Khmelnytskyi, Ukraine,
e-mail: yantonina@ukr.net, ORCID: 0000-0002-4925-9713.

Sergii Lysenko – DrS, Full Professor, Professor at the Computer Engineering & Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine,
e-mail: sirogyk@ukr.net , ORCID: 0000-0001-7243-8747.

Anatoliy Sachenko – Doctor of Technical Sciences, Professor, Director of the Research Institute for Intelligent Computer Systems, West Ukrainian National University, Ternopil, Ukraine; Kazimierz Pulaski University of Radom, Radom, Poland,
e-mail: as@wunu.edu.ua, ORCID: 0000-0002-0907-3682, Scopus Author ID: 35518445600

Bohdan Savenko – PhD, Associate Professor at the Computer Engineering & Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine,
e-mail: savenko_bohdan@ukr.net , ORCID: 0000-0001-5647-9979.

Oleg Savenko – DrS, Full Professor, Professor at the Computer Engineering & Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine**,**
e-mail: savenko_oleg_st@ukr.net , ORCID: 0000-0002-4104-745X

Andrii Nicheporuk – PhD, Associate Professor at the Department of Computer Engineering & Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine,
e-mail: kysil_ nicheporuka@khmnu.edu.ua , ORCID: 0000-0002-7230-9475.