Design Methodology of Cybersecurity Situational Center

Ihor Subach[1,2], Dmytro Mogylevych[1,2], Artem Mykytiuk[1], Volodymyr Kubrak[1],
and Stanislav Korotayev[1]

[1] *National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky," 4 Verkhnoklyuchova str., Kyiv, 03056, Ukraine*
[2] *Kruty Heroes Military Institute of Telecommunications and Informatization, 45/1 Moscow str., Kyiv, 01011, Ukraine*

Abstract

The process of designing a cybersecurity situational center as a complex organizational and technical system is considered. It is proposed to consider the problem of designing the cybersecurity situational center from a formal point of view, as a problem of a class of multi-criteria multi-parameter problems, and as an approach to solving it we chose the decomposition of the design process into separate stages using the methods of successive approximations. The main stages are highlighted and described, the principles of implementing a systematic approach to the design of cybersecurity situational center are formulated and disclosed. The formal statement of the problem of task distribution between the operational personnel of situation center is presented. Criteria for choosing the type of organizational structure of the cybersecurity situational center are formulated and described, and on their basis the choice of the matrix hierarchical structure for its implementation is substantiated. The performance indicators for assessing the functioning of the cybersecurity situational center and its organizational and technical structure are considered.

Keywords

Cybersecurity, Situational Center, Design, Organizational Structure, Criteria for Evaluation, Cybersecurity Situational Centers, Cybersecurity Operations Center, Computer Security Incident Response Team, Computer Emergency Response Team, Security Operations Center, Network Operations Center.

1. Introduction

According to researchers, cyberspace is an environment that is fundamentally different from the ordinary physical world. Nevertheless, cyberspace is an extremely physical environment: it is created by physical networks and systems that are interconnected and subject to certain rules that are manifested through software and communication protocols. Moreover, the very basis of cyberspace is purely physical laws of electromagnetism and light. They create its main feature – the possibility of global communications and transmission of large amounts of data, carried out almost instantly and transmitted over long distances, neglecting geographic boundaries. Speed and independence from physical obstacles provide a major advantage and at the same time creates a problem, since the capabilities of cyberspace can be used by anyone and for any purpose [1].

Ensuring the confidentiality, integrity and accessibility of institutions or organizations in the era of modern information technology (IT) is a solid piece of work. It includes many information security functions, ranging from robust systems engineering and configuration management to effective cybersecurity policy or ensuring information security and comprehensive training of personnel. It should also include operations in cyberspace, where a group of individuals is tasked with monitoring and protecting an institution or organization from potential cyber threats [2].

Cyber threats are growing and becoming more complex. One of the most effective ways to counter these threats is to create a global ecosystem of computer security incident response teams (CERT, CSIRT) and security operations centers (SOC), the so-called cybersecurity situational centers (CSC), that can effectively

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine

EMAIL: igor_subach@ukr.net (I. Subach); mogilev11@ukr.net (D. Mogylevych); mukuta8888@gmail.com (A. Mykytiuk); volodymir.kubrak@ukr.net (V. Kubrak); meduha1998@gmail.com (S. Korotayev)
ORCID: 0000-0002-9344-713X (I. Subach); 0000-0002-4323-0709 (D. Mogylevych); 0000-0002-8307-9978 (A. Mykytiuk); 0000-0001-8877-5289 (V. Kubrak); 0000-0003-3823-8375 (S. Korotayev)

interact and exchange information on cyber threats in order to respond to them effectively. This can be provided by appropriate common mechanisms, increasing the number of CERTs, CSIRTs and SOCs around the world and improving existing ones [2–4].

There are many terms used to define the group of individuals (experts) tasked with ensuring cybersecurity [5, 8]:

- Computer Security Incident Response Team (CSIRT)
- Computer Incident Response Team (CIRT)
- Computer Incident Response Center (or Capability) (CIRC)
- Computer Security Incident Response Center (or Capability) (CSIRC)
- Security Operations Center (SOC)
- Network Operations Center (NOC)
- Cybersecurity Operations Center (CSOC)
- Computer Emergency Response Team (CERT), etc.

The most common terms used to describe incident response teams are CSIRT, CERT and SOC.

To accomplish the assigned tasks, they are empowered with the following functions:

- Proactive monitoring of IT systems and constant analysis of the current state of threats
- Identification of vulnerabilities in IT security and their elimination
- Centralized management of various security devices in the system
- “Signaling” in case of detection of attacks and threats;
- Direct measures of protection and/or minimizing damage during cyberattacks
- Assessment of the state of IT security systems
- Technical support on all IT security issues
- Reporting on the operation of all IT security-related systems

Typically, a CSIRT is a team tasked with handling computer security incidents. This often includes additional responsibilities, from detection to analysis and even correction, as well as activities related to multi-situational awareness, knowledge transfer and vulnerability management.

The SOC or CSC provides incident detection services by observing technical events in networks and systems and may also be responsible for incident response and handling. In large enterprises, SOCs sometimes focus only on monitoring and detection services and then outsource incident handling to a separate CSIRT. In smaller organizations, CSIRTs and SOCs are often considered synonymous.

Over the years, the role of the CSC has evolved from providing monitoring and incident handling services to coordinating and communicating with different interested parties, countries and specific sectors. Currently, the activities of the CSC are organized according to the main functions [6], which are further divided into subfunctions (Fig. 1).

However, it should be noted that CSC is the core of the cybersecurity system of an organization. As a centralized location for detecting cyber threats, reducing risks and responding to cyber incidents, the CSC is the single most important factor in overall cybersecurity capabilities.

A recent Gartner study has identified five different models for deploying and maintaining a SOC (CSC) [7]:

- SOC-as-a-Service (SOCaaS) solutions are decentralized cloud portals that connect your company's infrastructure to the event monitoring and response team. The virtual cloud-based approach is becoming more common as enterprises support remote operations and staff.
- Multifunctional SOC/NOC. Using this approach, a single team of security and network specialists can share resources and infrastructure. It is an on-site operations center that handles IT operations, compliance and risk management alongside cybersecurity operations.
- Co-operated SOC. This model uses on-site monitoring solutions in addition to external personnel. Such approach can also be called a hybrid approach because it contains both on-site and off-site elements. These elements can vary greatly between different organizations, making co-operation a universal option.

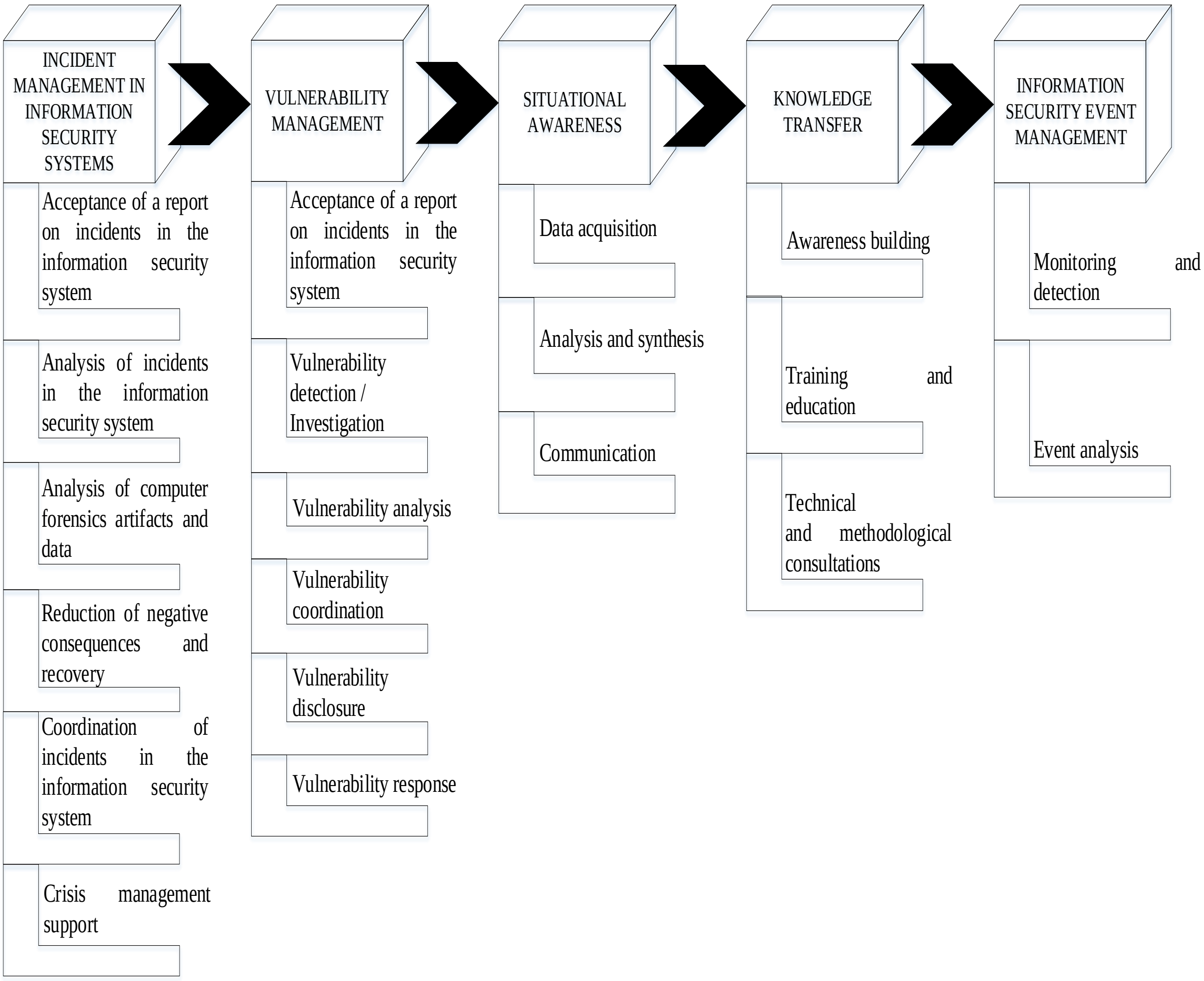
INCIDENT MANAGEMENT IN INFORMATION SECURITY SYSTEMS
Acceptance of a report on incidents in the information security system
Analysis of incidents in the information security system
Analysis of computer forensics artifacts and data
Reduction of negative consequences and recovery
Coordination of incidents in the information security system
Crisis management support
VULNERABILITY MANAGEMENT
Acceptance of a report on incidents in the information security system
Vulnerability detection / Investigation
Vulnerability analysis
Vulnerability coordination
Vulnerability disclosure
Vulnerability response
SITUATIONAL AWARENESS
Data acquisition
Analysis and synthesis
Communication
KNOWLEDGE TRANSFER
Awareness building
Training and education
Technical and methodological consultations
INFORMATION SECURITY EVENT MANAGEMENT
Monitoring and detection
Event analysis

Figure 1: The main functions of CSC

- Dedicated SOC is a centralized solution that has its own infrastructure, its own team, and a set of processes dedicated exclusively to cybersecurity.
- SOC team. The SOC team model describes a SOC network distributed over several territories. Most commonly, it is a connected, global cybersecurity operations center that consists of several specialized SOCs working in tandem with each other. The SOC team may have special functions dedicated to specific tasks, such as forensics, cybersecurity research or cyber threat intelligence.

Each of these models has unique characteristics – some are better suited for large enterprises, while others are ideal for small and medium-sized organizations [9, 10].

But no organization has the same basic infrastructure, regulatory requirements or budget, that is why different CSCs are needed. Thus, today there is an urgent scientific task to develop approaches to the deployment and optimization of CSC.

2. Problem Statement

The process of designing a CSC as a complex organizational and technical system should include the following stages [11, 13, 17, 18]:

- Defining the goals of functioning
- Formalization of tasks
- Grouping the tasks in accordance with the set goals
- Selection of the type of CSC management structure
- Determination of the number and composition of CSC units at each level of SOC management
- Determination of the number of employees of each unit

- Selection of hardware and software
- Design of communication systems to ensure effective decision making
- Calculation of costs for the maintenance of the organizational and technical structure of the CSC

Since the design of CSC requires consideration of a large number of factors: system-wide, organizational, technical, economic, etc., with the need to take into account both the criteria of CSC functioning and the cost of its maintenance, this task belongs to the class of ill-structured tasks. On the other hand, from a formal mathematical point of view, it can be reduced to the class of multi-criteria multi-parameter problems, which are usually solved by decomposition into separate stages, and then methods of successive approximations are applied to refine the results obtained by their implementation. [13, 14]. Correspondingly, during such decomposition there are stages of system (defining the CSC goals, formulation and grouping of tasks), organizational (selection of CSC management structure, composition and number of units), technical (selection of hardware and software, provision of means of communication between units and officials) and ergonomic design (determination of the number of personnel, synthesis of algorithms for the performance of official duties).

3. Basic Principles of a Systematic Approach to Designing a Cybersecurity Situational Center

Since CSCs are complex ergatic organizational and technical systems [19], its synthesis consists in the design of the collective activities of operational personnel in conjunction with technical and software tools that ensure their activities. According to [11], the principles of implementation of a systematic approach to the design of CSC should be: compliance with the organizational and technical structure of the tasks, purposefulness, relativity, adaptability, connectivity, modelability, reflectivity and operativeness.

Correspondence of the organizational and technical structure to the CSC tasks consists in a clear organization of the interaction of operational personnel in solving complex problems.

Purposefulness implies that in order to achieve the goals, a system should be formed, which is a combination of effectively organized hardware, software and operational personnel.

Relativity lies in the fact that a combination of elements of a system can be considered both as its independent unit and as part of another system into which it is included.

Adaptability implies the ability of the CSC structure to change in accordance with the goals and conditions of its functioning.

The coherence lies in the fact that each element (combination of elements) of the structure is considered from the position of two levels of grouped elements associated with it: higher and lower. From the side of the higher level, the parameters of the cylinder block enter the input of the element, and to the lower level it transfers the selected parameters and controls their implementation. At the higher level, the input of the element receives the targeting parameters, and at the lower level, it transmits the selected parameters and monitors their implementation.

To implement the principle of adaptability of CSC structure, it is necessary to have a mechanism for predicting the nature of changes in its structure in different conditions, which can be achieved by modeling.

The essence of the principle of reflectivity is that the antagonistic structure (hacker group, criminals, etc.) is imposed on certain data about its structure, which motivates it to take certain actions. According to this principle, the organizational and technical structure of the SOC should be capable of learning and gaining experience.

4. Stages of Designing a Cybersecurity Situational Center

The analysis of the literature [11–13, 17–19, 21] shows that the process of synthesis of the organizational and technical structure can be represented in the form of the following stages of systemic, organizational, ergonomic and technical design (Fig. 2).

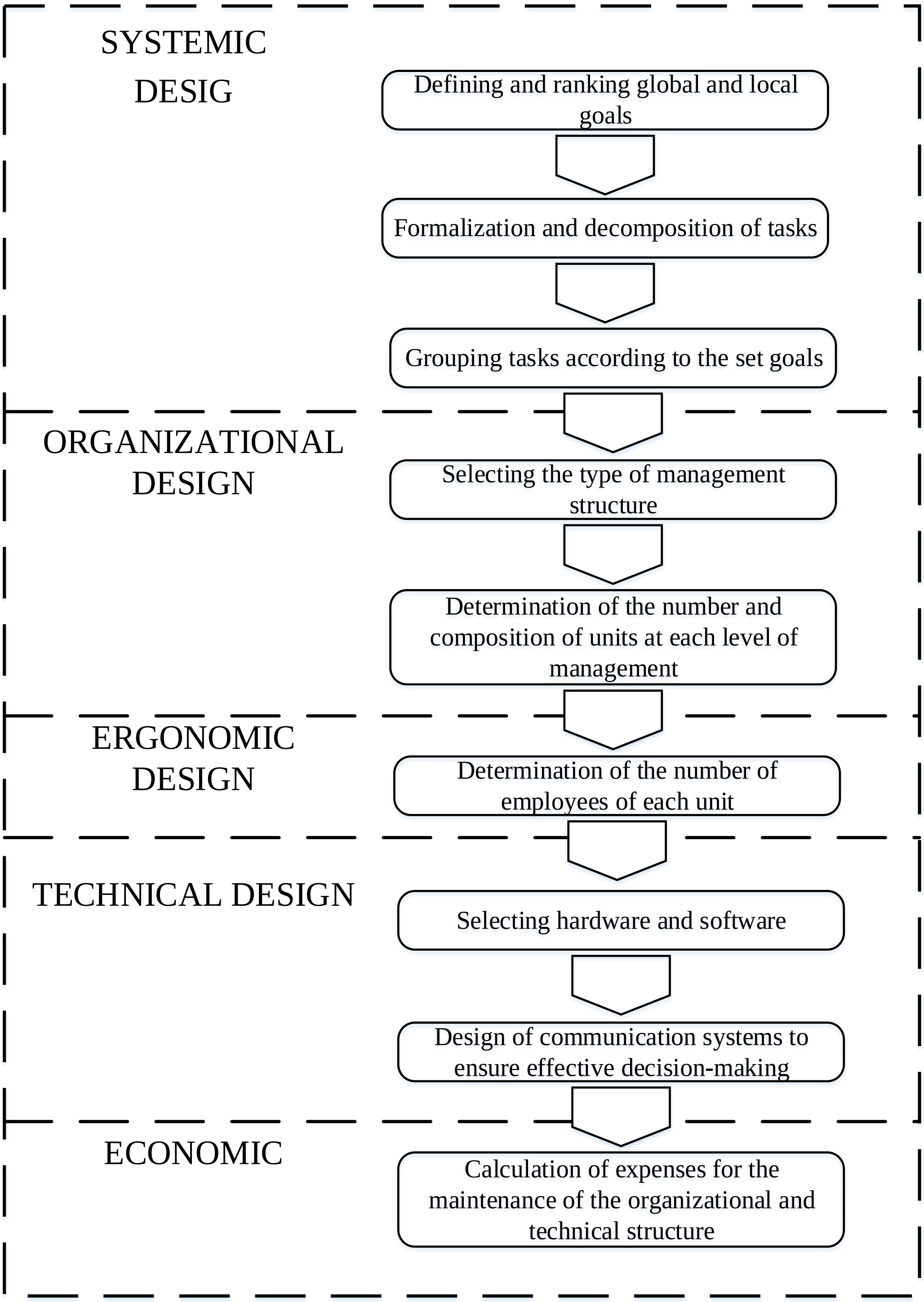
SYSTEMIC DESIG
Defining and ranking global and local goals
Formalization and decomposition of tasks
Grouping tasks according to the set goals
ORGANIZATIONAL DESIGN
Selecting the type of management structure
Determination of the number and composition of units at each level of management
ERGONOMIC DESIGN
Determination of the number of employees of each unit
TECHNICAL DESIGN
Selecting hardware and software
Design of communication systems to ensure effective decision-making
ECONOMIC
Calculation of expenses for the maintenance of the organizational and technical structure

Figure 2: The main stages of designing a cybersecurity situational center

At the initial stage of systemic design, the global goals facing the CSC are formulated. They should also be ranked in order of importance. After that, they are divided into subsets of local goals, the achievement of which is ensured by solving certain sets of problems. At the same time, these sets are divided into tasks that are solved automatically, automated and non-automated.

Thus, the central point of this stage is the definition and formulation of tasks and their distribution among the CSC operational personnel.

The formal statement of this problem can be formulated as follows [20].

Suppose that the input of the CSC (system Ψ) receives n inputs $X = \{x_1, x_2, \cdots, x_i, \cdots, x_n\}$, which are the control actions from the operational personnel and m outputs $Y = \{y_1, y_2, \cdots, y_j, \cdots, y_m\}$ – indicators of the efficiency of CSC functioning. The system Ψ sets the display $\Psi : X \rightarrow Y$. The operation of the CSC is provided by operational personnel $O = \{o_1, o_2, \cdots, o_k\}$, and the set O is divided into groups that unite officials $O = O_1 \bigcup O_2 \bigcup \cdots \bigcup O_s \bigcup \cdots \bigcup O_l$ performing the same functions.

In the case of the current CSC, the assessment of the degree of influence of CSC operational team $O_s X = \{x_1, x_2, \cdots, x_i, \cdots, x_n\}$ on the performance indicators of its functioning $Y = \{y_1, y_2, \cdots, y_j, \cdots, y_m\}$ can be determined by the probabilistic method through the correlation coefficient:

$$C(x_i, y_j) = M\left\{\left(x_i - m_{x_i}\right)\left(y_j - m_{y_j}\right)\right\} / \sigma_{x_i}\sigma_{y_j}, \tag{1}$$

where m_{x_i}, m_{y_j}jh – mathematical expectation of the values x_i and y_j, and the values σ_{x_i} and $\sigma_{y_j}$are their standard deviation.

The result of solving this problem is the influence matrix of the i-task on the j-indicator. At the same time, at a strong influence the correlation coefficient approaches to 1 and vice versa, at weak one – to 0.

However, when designing a CSC, an expert method is used to assess the influence of tasks [20–24], the essence of which is an expert survey of specialists (experts) to assess the importance of tasks or when it is difficult to distinguish the properties of tasks, the method of paired comparison is used (each pair of tasks) [25–26].

To determine the scope of tasks solved by CSC operational personnel, the concept of intensity or frequency of their occurrence, or the number of tasks that occur per unit of time, is used.

In turn, restrictions on the time for solving the problem are introduced through the scheduled or maximum permissible time.

At the stage of the CSC organizational design, the following tasks are solved:

- Selection of structure type
- Determination of the number of structure levels
- Determination of the required number of functional groups and each level
- Preliminary estimation of the number of people in each functional group
- Determination of the nature of interaction between operational personnel and their groups

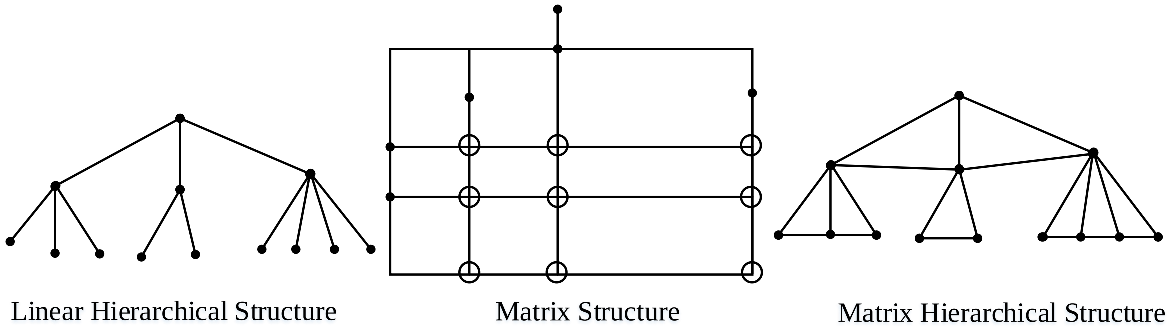

Figure 3: Types of organizational structures

Herewith, there are various options for choosing an organizational structure: chain, star, circle, network, linear and matrix hierarchical structures, etc. According to the CSC structure, the nature of the tasks it solves, the relationship between operational personnel, the most promising is a mixed matrix hierarchical structure (Fig. 3), characterized by number of levels, number and functional purpose of subsystems at each level, as well as the types of relationships between levels of the structure. It allows you to use CSC resources more efficiently, act more quickly in conditions of rapid change and uncertainty, coordinate the work of different links more clearly and overcome conflicts.

At the stage of ergonomic design, based on the limiting capabilities for information processing and decision-making (throughput, span of control, ultimate load, etc.) of each person of SOC operational personnel, the number of persons in groups of operational personnel is determined [12, 13, 19]. To do this, the structures of problem solving are analyzed by the CSC operational personnel and presented in a formalized form – problem-solving algorithm.

At the stage of technical design, the most perspective hardware and software tools, which satisfy technical requirements for CSC, are selected out of the many possible options [15].

5. Assessment Criteria

To select a variant of the organizational and technical structure of the CSC from possible alternatives, the following efficiency criteria are used: efficiency, cost, speed, adaptability, survivability, reliability, etc.

In the general, the effectiveness of CSC depends on the probability of timely solution of tasks arising in the course of the functioning of operational personnel (blocking cyber-attacks, investigating cyber incidents, etc.) [16] and can be represented as follows [14]:

$$E = P(p_1,\ p_2, \cdots, p_j, \cdots, p_m), \qquad (2)$$

where $p_j, j = \overline{1,m}$; – the probability of a timely solution of the task j.

After combining the tasks of the same type into groups, expression (2) can be represented as follows:

$$E = E_0 + \sum_{j=1}^{m} w_j n_j p_j, \qquad (3)$$

where E_0– efficiency of solving tasks by CSC in automatic mode (without the participation of operational staff);

w_j – the value characterizing the degree of influence of the j group of tasks on the efficiency of CSC, which in practice is usually determined by the expert method under the condition: $\sum_{j=1}^{m} w_j = 1$;

n_j – the number of tasks of the j group of tasks, solved by CSC operational personnel, which is usually represented as the relative frequency of occurrence of the task$j$– $\overline{\xi}_j = \xi_j / \sum_{j=1}^{m} \xi_j$.

p_j – the probability of a timely solution of the j group of tasks by CSC operational personnel.

Accordingly, the normalized generalized criterion takes the form:

$$\overline{E} = \sum_{j=1}^{m} w_j \overline{\xi}_j p_j. \qquad (4)$$

To assess the effectiveness, in the case where each task solved by a certain person of the CSC operational staff is highlighted, the criterion (5) can be applied:

$$\overline{E}_1 = \sum_{i=1}^{n} \sum_{j=1}^{m_i} w_j \xi_{ij} p_{ij}\ , \qquad (5)$$

where $\overline{\xi}_{ij}$ – the relative frequency of solution of the task$j$ by the person i of CSC operational personnel;

p_{ij} – the probability of a timely solution of the task j by the person i of CSC operational personnel;

m_i – the number of tasks solved by the person i of the CSC operational personnel;

n – the number of persons of CSC operational personnel;

It should be noted that the probability of a timely solution of the problem by a person of the CSC operational personnel depends on the standard and scheduled time for problem solving [24]:

$$p_{ij} = p(t_n, T_p), j = \overline{1,m}; i = \overline{1,n}, \qquad (6)$$

where t_n – the standard time for problem solving, which is determined by analyzing the complex algorithm for solving the problem by the person of CSC operational personnel;

T_p – the directive time for problem solving, which is set for each task at the stage of systemic design. In its turn, to assess the organizational and technical structure of the CSC, we should use indicators such as the number of levels of the hierarchy, the number of elements at each level, the coefficient of centralization of management, the coefficient of coherence of the structure, etc.

The coefficient of centralization of management characterizes the degree of connection of the head of CSC department with other employees. It can be represented as follows:

$$CCM_k = NS_k / \sum_{i=1}^{n} NE_{ki}, \qquad (7)$$

where NS_f – the number of functional connections of the head of the department with other employees;

NE_{ki} – the number of functional connections of the employee i of the departrent k of CSC.

The coefficient of coherence of the structure characterizes the relative proportion of tasks during the solution of which the employees of the department interact with each other:

$$RNT_k = TC_k/(\mathrm{TC}_k + TI_k), \tag{8}$$

where TC_k – the number of tasks solved by the department k of CSC and the solution of which requires the interaction of its employees;

TI_k – the number of tasks to be done in the department k individually;

In addition, you can apply such characteristics of structure elements as: the number of functional relations with other elements, the relative rank of the element, which characterizes the relative proportion of its relations, etc.

To synthesize the organizational and technical structure of the CSC, it is necessary to create models for the formation of structure parameters according to such criteria for assessing their quality as: minimizing the interaction of SOC units in the process of its functioning, maximizing the homogeneity of its elements (technical means, operational personnel, etc.). However, the methods of their construction, which are currently available, have a significant drawback associated with the a priori task of the structures of subsystems, which in its turn should be considered as the subject of definition.

The elimination of this drawback can be done by developing and including in the composition of the synthesis methods special optimization models that establish relationships between the indicators of the functioning of organizational and technical structures and the set of their parameters. At the same time, when selecting a model in each specific case, it is necessary to take into account its target orientation, accuracy and detail. Therefore, if the initial data required for calculations are inaccurate or uncertain, then there is no need to build a detailed model and to optimize the solution accurately.

Thus, the problem of selecting a rational option for the organizational and technical structure of the SOC can be solved on the basis of a systematic approach, within which it is quite expedient to use the methods of multicriteria optimization and the vector performance indicator, including a set of partial indicators, each of which is represented by a functional and satisfies one of following requirements [14]:

- Timely acquisition of the results of solving problems
- Validity of the results of solving problems
- Completeness of information for decision making
- Cost-effectiveness

6. Conclusions

Since the cybersecurity situational center is a complex organizational and technical system, the task of its design, from a formal point of view, should be classified as a multi-criteria multi-parameter problem.

To solve this problem, it is advisable to apply a systematic approach, within which the decomposition of the design process into separate stages using the methods of successive approximations is carried out.

The main stages of designing a cybersecurity situational center should be the stages of systemic, organizational, technical and ergonomic design, and the main principles of its implementation are: compliance of the organizational and technical structure with the tasks, civilization, relativity, adaptability, connectivity, modelability, reflectivity and efficiency.

The central point of the synthesis of the organizational and technical structure of the cyber security situation center is the definition and formulation of tasks and their distribution among the operational personnel of the situation center.

Criteria such as efficiency, cost, speed, adaptability, survivability and reliability can be used to select the type of organizational structure of a cybersecurity situational center. In addition, to assess the organizational and technical structure of the cybersecurity situation center, it is advisable to use such indicators: the number of hierarchy levels in it, the number of elements at each level, the coefficient of centralization of management and the coefficient of coherence of the structure.

To synthesize the organizational and technical structure of the CSC, it is necessary to create models for the formation of structure parameters according to such criteria for assessing their quality as: minimizing the interaction of SOC units in the process of its functioning, maximizing the homogeneity of its elements.

As an indicator of efficiency for solving the problem of choosing a rational variant of the organizational and technical structure of the CSC, it is advisable to use a vector indicator, which includes the following partial indicators: timely acquisition of the results of solving problems, validity of the results of solving problems, completeness of information for decision making, cost-effectiveness.

References

[1] European Union Agency for Cybersecurity, Methodology for a Sectoral Cybersecurity Assessment, September 13, 2021. URL: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.

[2] A. Zhylin, M. Khudyncev, M. Litvinov, Functional model of cybersecurity situation center, Information Technology and Security. July-December 2018. Vol. 6. Iss. 2 (11), DOI: 10.20535/2411-1031.2018.6.2.153490.

[3] J. Voo, I. Hemani, S. Jones, W. DeSombre, D. Cassidy, National Cyber Power Index 2020 (Methodology and Analytical Considerations), 2020. URL: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.

[4] European Union Agency for Cybersecurity, 2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries, January 26, 2021. URL: https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation.

[5] C. Onwubiko, Rethinking Security Operations Centre Onboarding, Proc. of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).

[6] European Union Agency for Cybersecurity, How to set up CSIRT and SOC, December 10, 2020. URL: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc.

[7] Gartner, Selecting the Right SOC Model for Your Organization, 24 February 2021. URL: https://www.gartner.com/en/documents/3997342-midmarket-context-selecting-the-right-soc-model-for-your.

[8] C. Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE, 2014. URL: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

[9] R. Samson Jr, Five Security Operations Center Models Compared: Find The Right SOC Model, 2021. URL: https://www.clearnetwork.com/types-of-security-operations-centers-soc.

[10] D. Znakharev, The concept of creating the next generation SOC, 2020. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Next-Generation-SOC-Concept.

[11] V. Morozov, Ya. Dymarsky, Elements of the theory of control of flexible automated production: software, Mechanical Engineering, Leningrad, 1994.

[12] B. Gerasimov, B. Egorov, Group activity of operators in automated control systems, KVIRTU PVO, Kiev, 1980.

[13] A. Cricket, Fundamentals of the synthesis of the structure of complex systems, Nauka, Moscow, 1982.

[14] I. Subach, and B. Gerasimov, Quality indicators of information support and their impact on the effectiveness of decision support systems, Bulletin of Taras Shevchenko National University of Kiev, volume 20 (2008), pp. 27–29.

[15] I. Subach, V. Kubrak, and A. Mykytiuk, Methodology of rational choice of security incident management system for building operational security center, CEUR Workshop Proceedings, 2019, 2577, pp. 11–20.

[16] I. Subach,, V. Kubrak, A. Mykytiuk, and S. Korotayev, Rule-oriented method of cyber incidents detection by SIEM based on fuzzy logical inference, CEUR Workshop Proceedings, 2021, 2859, pp. 210–219.

[17] V. Burkov, N. Korgin, D. Novikov, Introduction to the theory of management of organizational systems, Nauka, Moscow, 2009.

[18] N. Karabutov, Structural Identification of Systems: Analysis of Information Structures, Nauka, Moscow, 2009.

[19] B. Gerasimov, V. Kamyshyn, Organizational ergonomics: methods and algorithms of research and design, Infosystems, Kyiv, 2009.

[20] E. Shugaliy, O. Musienko, M. Kachanov, Methods of obtaining characteristics of tasks in public administration, Standardization, certification, quality, 3 (115), 2019, P. 29-34.

[21] V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, Cybersecurity Providing in Information and Telecommunication Systems (CPITS), pp. 23–32, Jul. 2020.

[22] E. Shugaliy, Methodology of generation of variants of functional structures of public administration bodies, Standardization, certification, quality, 1 (113), 2019, P. 49-53.

[23] Carlsson, A., et al. Sustainability Research of the Secure Wireless Communication System with Channel Reservation. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020. https://doi.org/10.1109/tcset49122.2020.235583

[24] E. Shugaly, V. Penkivsky, Methods of processing expert information on the characteristics of tasks in public administration, Standardization, certification, quality, 1 (119), 2020, P. 63-69.

[25] T. Saati, Decision Making. Method of analysis of hierarchies, Radio and communication, Moscow, 1993.

[26] I. Subach, O. Saenko, Messages analysis plan formation by the information network operator**,** Modern Problems of Radio Engineering, Telecommunications and Computer Science - Proceedings of the 10th International Conference, TCSET'2010, 2010, p. 246, 5446079.