Dynamic model of guarantee capacity and cyber security management in the critical automated systems

Hennadii Hulak [1], Pavlo Skladannyi [1], Volodymyr Sokolov [1], Yevhen Hulak [2] and Viktor Korniiets [2]

[1] *Borys Grinchenko Kyiv University, Bulvarno-Kudriavska str. 18/2, Kyiv, 04053, Ukraine*
[2] *Institute of Mathematical Machines and Systems Problems National Academy of Science of Ukraine, Academician Glushkov ave. 42, Kyiv, 03187, Ukraine*

Abstract

The paper examines the methods of increasing the effectiveness of guarantee capacity management and cyber security of automated systems in critical infrastructure. The use of Anthony's business management model is proposed to build a management system. A binary relation of partial order on a set of functional security profiles of computer systems is proposed to arrange the levels of security. The dynamic model of the provision of capacity and cyber security and critical performance indicators proposed in the paper can be used to model the behavior of critical infrastructure objects and form balanced management decisions in the relevant industries.

Keywords

Dynamic management model, Anthony triangle, guarantee capacity, cybersecurity, cybersecurity culture, critical infrastructure

1. Introduction

Scientific and practical interest in constructing protected, guarantee-capable automated systems (AS) is constantly growing. This is due to high requirements for information services to critical infrastructure objects. The task of rational management of such systems is greatly facilitated by the use of effective platforms such as SIEM [2], Threat Intelligence [3], the MITRE ATT&CK knowledge base [4], cyber attack attribution technology [5], and many other tools. Let us note that the system's guarantee capacity is an integral characteristic of its ability to provide services, defined in its use regulations and conditions [1].

At the same time, comprehensive support of dynamic rational management of guarantee capacity and cyber security (G&C) in AS is a relatively expensive and complex process, for which proposing a practical methodology is a non-trivial task. Many scientific publications are devoted to solving such problems, but searching for new solutions continues. The main difficulty of the task lies in the fact that protection functions in computer systems are primarily discrete by definition, which entirely or partially makes it impossible to apply known mathematical methods of management optimization.

2. Related Works

In particular, in [6], the issue of applying situational management methods based on signature models was considered to make the best decision regarding the management of information protection

CMiGIN 2022: 2nd International Conference on Conflict Management in Global Information Networks, November 30, 2022, Kyiv, Ukraine
EMAIL: h.hulak@kubg.edu.ua (H. Hulak); p.skladannyi@kubg.edu.ua (P. Skladannyi); v.sokolov@kubg.edu.ua (V. Sokolov); geg180579@gmail.com (Y. Hulak); viktor.korniets@gmail.com (V. Korniiets)
ORCID: 0000-0001-9131-9233 (H. Hulak); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-9349-7946 (V. Sokolov); 0000-0003-4984-686X (Y. Hulak); 0000-0002-4967-8395 (V. Korniiets)
© 2022 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3530/paper11.pdf

objects. At the same time, it was noted that the features of these systems influence the possibility of applying traditional methods of optimal management.

It is necessary to clarify the essence of these differences a little, agreeing in principle with this thesis. Namely, it concerns the implementation of system management (in our case, the management of G&C) in conditions of uncertainty and negative influence on it both from the side of cyberspace and as a result of intentional or accidental actions of its legal users; management goals and objectives can be formulated both qualitatively and quantitatively; the description of the object is very difficult to formalize.

In [7,8], the methodology of formalization of the states of the controlled system underwent further development, but, in our opinion, a particular shortcoming of these works, as well as of the previous study [6] by these authors, is the lack of criteria for achieving a defined goal, which would determine the state of information security. As a result, in [6], the conclusion announces only the possibility of applying an algorithmic approach to determining the complete set of situations, creating a knowledge base, the use of which will contribute to increasing the validity of management decisions in the case of applying the proposed method of using the signature model of the management of objects of the information protection system.

In [9], it is proposed how to build a mathematical model of comprehensive security of computer systems (CS) based on expert judgments. The research uses indicators of the level of security according to some undefined criteria. It is shown that the application of the modified method of loose ranking allows determining the Fishburn weights for one level of the hierarchy. In [10], the author continued the study of the comprehensive security of CS by assessing the probabilities of the realization of some threats without reference to specific security criteria.

In [11], the conceptual provisions of several research initiatives related to innovative technologies for cloud computing in environmental security, quality assurance, service composition, and system management are considered. Also, intrusion detection technologies, customer security issues, experimental evaluation of routing for grid and cloud, and improving the simulator for validating an approach to environmental cloud computing are presented without formalization. In general, the problems of the top management of an enterprise are considered.

In [12], the critical organizational tasks of a cyber security center are defined in terms of security management, including the implementation of the components of the organizational and technical model of cyber protection; monitoring of the global state of cyber security of nuclear energy facilities; combating cyber threats by increasing general situational awareness of incidents and vulnerabilities of information systems and systems for protecting critical infrastructure objects; reduction of vulnerabilities, prevention of threats and their effective localization; conducting training and increasing the level of awareness in terms of cyber security among managers of critical infrastructure [13].

Scientific and practical interest in security management is the generally unsolved problem of dynamically linking the states of an automated system to the established criteria of its security. This work is dedicated to the steps to its solution.

3. Problem Statement

To begin with, according to the canons of philosophical science, the protection of information, in general, should be characterized by the same categories as other types of productive human activity [14]. This provides logical grounds for the use of the best scientific and practical developments in the field of effective management of entrepreneurial (business) activity for the formation of general approaches to the rational management of the system of G&C provision, which should be supplemented with methods and models specific to the field under investigation.

In the classic work of Robert Anthony [15], to describe the structure of effective management of a company (organization), an organizational model called the Anthony triangle (Fig. 1) was proposed, which was later used to define the tasks of information systems [16].

In [15], it is proposed to distinguish the following categories (levels) of management:

- *Strategic planning* is a decision-making process regarding the goals of the enterprise (organization), changes in these goals, resources used to achieve these goals, and the policy that

should guide the acquisition, use, and disposal of these resources. This category corresponds to the strategic level of management.

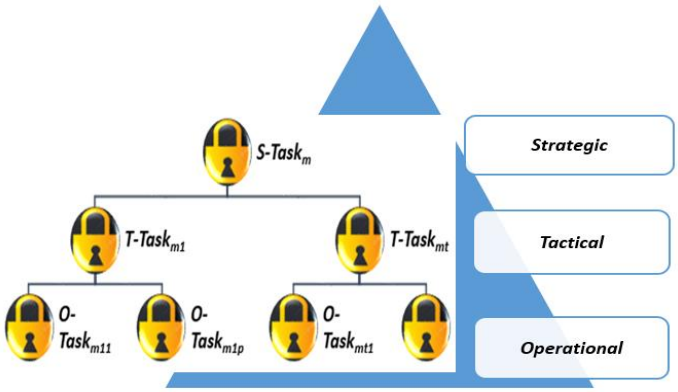

Figure 1: Anthony triangle

- *Management control* is a process by which managers ensure that resources are used efficiently and effectively to achieve the organization's goals. This category corresponds to the so-called tactical level of management.
- *Operational control* is the process of ensuring the effective and efficient performance of specific tasks. This process is implemented at the operational level of management.

For a better understanding of the term "operational control" (English), please note that this concept in German corresponds to the term "Betriebskontrolle" (production control). Therefore, in the Ukrainian translation of the English term, we prefer the term "operations control" (the adjective is related to the subject of control operations) instead of "operational" control (the adjective is associated with the time of control execution).

The main difference between management control and operational control is due [15] to the difference between the set of activities called management and the actions related to the performance of defined tasks.

In particular, operational control is concerned with technology and procedures, while managerial control is primarily concerned with personnel. In addition, operational control only requires the adoption of a small number of decisions since the tasks, goals, and resources required for the effective functioning of the organization must be defined in detail during strategic planning and management control.

The Anthony triangle model shown in Fig. 1 differs from its widespread depictions by the presence of an essential, in our opinion, addition. Each task at the strategic management level $STask_m, m = \underline{1, N_s}$ generates a set of tasks at the tactical and operational levels associated with it

$$\{TTask_{m1}, \dots, TTask_{mp}\} \text{ and } \{OTask_{m11}, \dots, OTask_{mtq}\}. \quad (1)$$

Taking into account the multi-year comprehensive approbation of the Anthony triangle model, it is proposed to consider the mechanism of its application in the case of managing measures to ensure the safety and security of G&C of information systems of critical infrastructure.

Namely, by analogy with the Anthony triangle to increase the efficiency of management activities, it seems appropriate to divide measures to support, develop, improve or restore the level of G&C of information systems into several levels (Table 1) based on characteristics of the tasks to be solved, categories and competencies of personnel, which is directly responsible for and takes care of solving the problems of G&C as well as the amount of financial, material and time costs for their implementation.

4. Ranking of Systems by Management Levels

The primary tasks of different levels of management in Table 1 are defined based on NATO approaches to cyber defense [17] and developments in [13].

In the general case, without focusing on a specific area of the organization's work, to assess the effectiveness of management actions according to [18], key performance indicators (KPI) should be

formed, the use of which allows for the analysis and measurement of the success of selected measures on the way to achieving the expected result. Having reliable KPIs is critical for companies implementing performance management systems. It is proposed to choose ordered functional security profiles as KPIs that will be dynamically changing.

Table 1
Primary tasks of different levels of security management

Management level / role	Basic tasks	Costs	Term
Strategic IC owner	1. Approval of security policy, determination of its goals and objectives, and financial, material, and human resources. 2. Normative regulation of aspects of cyber security. 3. Allocation of additional resources to eliminate the consequences of cyber incidents. 4. Making decisions regarding the work order in an emergency. 5. Organization of training and education of personnel and their motivation. 6. Ensuring physical security.	Significant (purchase of fixed assets + training and maintenance of personnel + work of external contractors)	Long
Tactical Security administrator	1. Monitoring and assessment of the current state of threats to the system. 2. Organization of system security assessment and audit. 3. Determination of authority and management of the access control system. 4. Monitoring the level of training and education of security operators and system users. 5. Planning work in emergency conditions. 6. Management of restoration measures.	Average (maintenance)	Medium
Operational Security operator	1. Management of hardware and software protection, including installation, adjustment, and maintenance. 2. Carrying out recovery works after incidents.	Average (maintenance + supplies)	Short

From the beginning, to formalize some procedures, we will introduce the relation operator on the set of security criteria of CS against unauthorized access $\{K_1, \dots, K_M\}$ [19].

Note that we further consider that if some criterion K_j is not applied to describe the security of a particular CS, its current value is equal to ∅ an "empty" element, and this is the lowest level of security compared to any other value of this criterion.

The two values $K_j(1)$ and $K_j(2)$ of the quantitative or qualitative criterion $K_j\ for\ \forall\ j = \underline{1, M}$ will be called those connected by the "majority" ratio: $K_j(1) \prec K_j(2)$ if the second value of the criterion corresponds to the highest level of security. For instance, in the case of the examples of security profiles given in [20]:

$$K_1(1) = \{\text{KA} = 1\}, K_1(2) = \{\text{KA} = 3\} \text{ and } K_1(3) = \{\emptyset\}, \quad (2)$$

we have

$$K_1(3) \prec K_1(1), K_1(3) \prec K_1(2), K_1(1) \prec K_1(2). \quad (3)$$

Next, we consider that the available security profile of the CS is a tuple $\mathcal{K}(t) = \langle K_1(t_1), \dots, K_M(t_M)\rangle$, which includes all criteria of CS security against unauthorized access from their set $\{K_1, \dots, K_M\}$ [21].

We will assume that two security profiles are connected by the ratio $\mathcal{K}(1) \prec \mathcal{K}(2)$ if the inequality holds:

$$\left|\left\{(\mu_1, \dots, \mu_p)\colon K_{\mu j}(2) \prec K_{\mu j}(1)\ \forall j = \underline{1, p}\right\}\right| < \left|\left\{(\nu_1, \dots, \nu_q)\colon K_{\nu j}(1) \prec K_{\nu j}(2)\ \forall j = \underline{1, q}\right\}\right|. \quad (4)$$

We will call two profiles practically indistinguishable $\mathcal{K}(1) \cong \mathcal{K}(2)$ if it has:

$$\left|\left\{(\mu_1, \dots, \mu_p)\colon K_{\mu j}(2) \prec K_{\mu j}(1)\ \forall j = \underline{1, p}\right\}\right| = \left|\left\{(\nu_1, \dots, \nu_q)\colon K_{\nu j}(1) \prec K_{\nu j}(2)\ \forall j = \underline{1, q}\right\}\right|. \quad (5)$$

The binary relation constructed in this way is not an equivalence relation [22]. It is reflexive and symmetrical but not transitive. Regarding non-fulfillment of the transitivity property, it is enough to consider the following example: let $\mathcal{K}(1) = \langle 1,2,1,2\rangle$, $\mathcal{K}(2) = \langle 2,1,2,1\rangle, \mathcal{K}(3) = \langle 1,3,2,1\rangle$. According to (5), we have $\mathcal{K}(1) = \mathcal{K}(2)$, $\mathcal{K}(2) = \mathcal{K}(3)$, while according to (1), we have $\mathcal{K}(1) \prec \mathcal{K}(3)$. Intuitively, in the proposed trio, the last hypothetical profile is, in a certain sense, correct.

Let us pay attention to that from (4) and (5) follows that $p = q$ and

$$p + q = 2 \cdot p = M - s, \quad (6)$$

where s is the number of criteria not used simultaneously in the security profiles $\mathcal{K}(1)$ and $\mathcal{K}(2)$.

5. Method of Decision-Making

To build security management, conducting an analysis of the output data for implementing the cyber protection system project and decision-making regarding current actions in various conditions is considered appropriate. First, let's consider that according to the definition of regulatory documents of the technical information protection system [23], a computer system is a set of hardware and software that is a target of evaluation. A security profile characterizes this object of evaluation after testing.

At the same time, information services necessary for organizations (enterprises) are provided by various automated systems—AS (information, telecommunications, etc.), which all include the personnel for these systems. The execution of the primary tasks of G&C at all levels of management (Table 1) requires the person to possess specific knowledge, abilities, skills, and qualities [24].

In [25], the corresponding set of characteristics is defined as the Cyber Security Culture (CSC) of the organization, which refers to the knowledge, beliefs, ideas, attitudes, assumptions, norms, and values of people regarding cyber security and how they manifest in people while handling information technologies. Note that the high level of CS security specified by the protection profile only guarantees the security of the accurate AS if the CSC level is low [26].

Thus, within the framework of an integrated approach to ensuring the G&C of the AS, the implementation of effective management requires consideration at the strategic and tactical levels of the current state and dynamics of changes in the CSC level.

It is generally challenging to formulate an integral characteristic of CSC, so a heuristic approach to assess the achievement of the required level of CSC based on the Turing test [27] has been proposed, which is theoretically applicable for distinguishing artificial intelligence from natural intelligence.

The test mentioned above can be interpreted as follows: the expert interacts with a computer and a person. Using the answers to the questions, the expert must establish with whom or what he is in contact. The task of artificial intelligence is to give the expert the impression of communication with natural intelligence.

In the situation under study, we have the opposite case: a person's activity (security operator, user) in typical situations must fully meet the requirements of the approved instructions. The risk of erroneous

actions must be minimal. Based on this, the critical task of the operational and tactical levels of management is to increase and maintain CSC in the organization at a level that is adequate to the degree of reliability of the applied information technologies and to exclude the possibility of such a negative phenomenon as the "human factor" [28] in the AC.

6. Cyber Security Culture Level Sufficiency Model

Raising the level of CSC should be facilitated by conducting exercises, training, and ongoing monitoring of acquired skills at the tactical level [29, 30]. At the same time, the European Credit Transfer System (ECTS) scale [30] should be an effective tool for rating the control of knowledge and skills of a student.

Let us take into account that this evaluation scale includes five positive levels of the quality of training of a future specialist, namely, the highest—**A** (negligible number of errors), medium levels **B**, **C**, satisfactory level **D**, and the lowest—**E** (satisfies the minimum criteria) as well as negative evaluations of **F** and **Fx**.

On the example of the model of the required level of CSC in the organization (Table 2), it is possible to find out how the security of the organization's personnel can be managed using the definition of the criticality category of the critical infrastructure object (CIO) [27]—the indicator that characterizes the probability of the implementation of cyber attacks and the average assessment of the level of cyber security culture in the organization.

Table 2
Model of CSC level sufficiency for different categories of the criticality of critical infrastructure objects

Categories of criticality of CIO	M_{ects} the average score of the CSC level for the state of aggressiveness of the external environment S_{ex}			
	$S_{ex} = 0/T_{ex}$	$S_{ex} = 1/T_{ex}$	$S_{ex} = 2/T_{ex}$	$S_{ex} = 3/T_{ex}$
IV necessary objects	E/D	D/C	C/B	B
III important objects	D/C	C/B	B/A	A
II vitally important objects	C/B	B/A	A	A
I especially important objects	B/A	A	A	A

In Table 2, the following designations are used: S_{ex} is an indicator that characterizes the probability of implementing cyber attacks against the object of information activity, which should be called the state of aggressiveness of the external environment. In [11], as part of analyzing the motives, goals, and tasks of invasions from different positions, it was noted that knowledge of these factors improves the situation by preventing possible consequences.

In our case, from the point of view of implementing preventive measures, the emphasis of the managerial response is somewhat different. Namely, the question arises of how the current situation in cyberspace differs from the typical situation and how to use human potential to increase the resistance of the AS.

Clearly, the relevant states' definition requires a global analysis [15] of the political, military, economic, and other goals and aspirations of individual states and their alliances or criminal groups. This issue is of separate scientific interest and requires individual processing. Within the framework of this study, we highlight the following situations:

- $S_{ex} = 0$ normal state of the external environment.
- $S_{ex} = 1$ increased level of danger.
- $S_{ex} = 2$ high level of danger.
- $S_{ex} = 3$ a very high level of danger.

Note that the S_{ex} characteristic related to the value ex is the T_{ex} trend of the number of cyberattacks observed in cyberspace over a certain period: if the number of cyberattacks increases, then we have $T_{ex} > 0$, in the case of no increase in the number of cyberattacks $T_{ex} \leq 0$. At the same time $|T_{ex}|$ is the

absolute value of the trend is the difference in the number of cyber attacks in the external environment for two consecutive periods (week, decade, or month).

Significant growth of this trend $(T_{ex}\uparrow)$ over a certain period may indicate the need to recognize the environment's new state of aggressiveness. Conversely, a significant drop in the number of observed cyberattacks may be a reason to return to the previous state of determining the CSC characteristics S_{ex}.

Adopting a decision at the strategic level of management to establish a higher state of aggressiveness of the environment S_{ex} should immediately activate the mechanisms for increasing the level of system security with the help of organizational measures and additional software and technical means (Table 1).

In particular, organizational measures can provide for the work of reinforced regular shifts, the early change of keys and passwords, the limitation of the powers of users in the access control system, and most importantly—targeted work with personnel that affects the level of the system's GIS, to increase its professionalism and discipline (indicators: M_{ects} is the average current rating, T_{hr} is the trend of the CSC indicator, which reflects changes in the level of professional training and compliance with the norms (discipline) of cyber security).

It should be noted that even under normal conditions, M_{ects} and T_{hr} indicators can considerably deteriorate as a result [14] of significant changes in the organizational structure of the enterprise, ineffective management motivation policy, miscalculations in personnel work, staff turnover, and the influence of external factors. Therefore, an essential task of the tactical level of management (Table 1) is to monitor the level of training and education of personnel.

In the proposed model, the characterization of the criticality of a specific object of information activity, if it does not fall under the legally established classification [27], should be determined a priori taking into account the importance of the sphere of public production, possible damage in the event of a decrease or loss of the guarantee capacity of the system (inaccessibility of its services), destruction of information resources and software systems, lost profits and costs of restoration work.

7. Functional Security Profile of Computer Systems

Based on what has been stated regarding the connection of CSC indicators with the level of G&C of an AS, it seems appropriate to supplement the functional profile of the security of the CS, which was checked during its evaluation and presented in the form of the tuple $\mathcal{K}(t) = \langle K_1(t), \dots, K_M(t)\rangle$, by another mandatory criterion $K_{M+1}(t)$ expressing the level of cyber security culture of CSC personnel, which takes values from the set $\{E.D, C, B, A\}$ based on the model of the given Table 2 and explanations to it.

Thus, the additional criterion can acquire the following meanings:

$$K_{M+1}(1) = \{CSC = E\}, \tag{7}$$
$$K_{M+1}(2) = \{CSC = D\}, \dots, K_{M+1}(5) = \{CSC = A\},$$

at that

$$K_{M+1}(1) \prec K_{M+1}(2) \prec K_{M+1}(3) \prec K_{M+1}(4) \prec K_{M+1}(5). \tag{8}$$

A critical condition in the security profile for the AS is this criterion can never be "empty:"

$$K_{M+1} \neq \{\emptyset\}. \tag{9}$$

This means that the formation of the organization's AC security profile should begin with an answer to the question: What level of CSC should security personnel and system users meet?

Next, using the partial ordering given by conditions (4) and (5) on a set of different operational security profiles and the lexicographic order, we renumber all possible security profiles in the direction of increasing protection requirements from 0 (for an empty profile) to N_{max}, which corresponds to the highest level of security with the maximum level of guarantees [20].

Before the organization or modernization of the computer security system, the parameters of the criticality category (CC) of the object, the trend T_{ex}, the state of aggressiveness of the environment S_{ex}, the required level of CSC in the organization, and, based on the available financial and material resources, the initial security profile must be determined (in Table 3 the profile is defined conditionally).

Based on the defined parameters, measures are taken in the management process to adjust the protection profile and increase the level of CSC.

Table 3
The dynamic model of AS security management

	Dynamics of events over time							
	less T_0	$T_0..T_1$	$T_1..T_2$	$T_2..T_3$	$T_3..T_4$	$T_4..T_5$	$T_5..T_6$	$T_6..T_\infty$
strategic		Tasks + provision			Recovery	Tasks + provision		
tactical		Management + training			of state	Management + training		
operational		Asset management				Asset management		
T_{ex}	=	↑	↑	↑	↑	=	=	=
S_{ex}	0	0	0	1	1	1	1	0
CC	IV	IV	IV	IV	III	IV	IV	IV
M_{ects}	*E*	*E*	*E*	*D*	*D*	*D*	*D*	*D*
$K_1(T)$	1	1	1	3	3	3	3	3
$K_2(T)$	2	2	2	2	2	2	2	2
$K_3(T)$	1	2	2	2	2	2	2	2
$K_4(T)$	∅	1	1	1	1	1	2	2
$K_5(T)$	∅	∅	∅	∅	∅	∅	1	1

Measures are taken to strengthen security, including instructions and staff training. In the time interval (T_0, T_3), based on the constant increase in the number of cyberattacks (T_{ex}), the parameters S_{ex}, M_{ects} and the security profile are adjusted on the system. This calculates the current costs of strengthening the security system, including training and motivating security personnel.

The time interval (T_3, T_4) in Table 3 and on the diagram Fig. 2 corresponds to the restoration of the system after a cyber attack. This point is characterized by determining the damage caused, comparing it with previous costs for improving security, and deciding to strengthen security measures further. Considering that during this period, the system is most vulnerable to new damage, it is advisable to temporarily increase the organization's criticality category by one level based on the decision of the strategic management level.

The adopted decision regarding further strengthening security measures is implemented in the time interval (T_4, T_6). Please note that at the tactical management level, security management tries to maintain the CSS level within the reached value of the M_{ects} parameter.

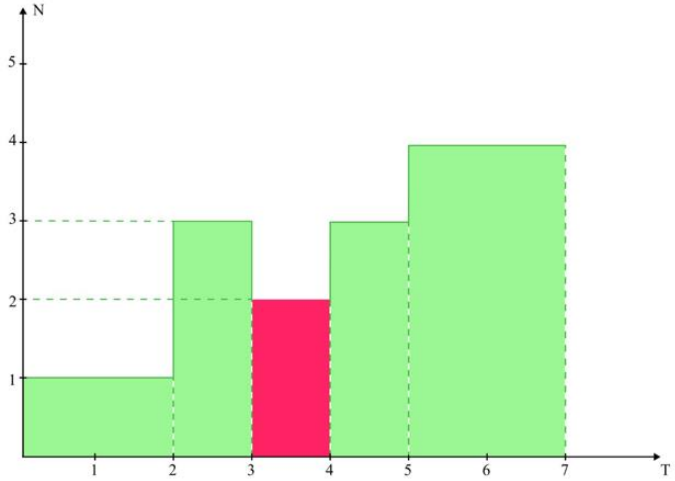

Figure 2: Diagram of security system state changes over time

The ratio of damages resulting from attacks and the total cost of improving security indicates the effectiveness of the selected management decisions. Based on this ratio, based on statistics for a specific branch of social activity (industry, energy, environmental protection, etc.), the first KPI_1 should be

determined—a vital indicator of the effectiveness of the organization's management activities in the field of providing G&C.

As the second key indicator of KPI_2, it is advisable to choose T_{hr} is the trend of changes in the CSC level of the organization as a result of the training, education, and motivation of personnel implemented at the operational and tactical levels.

8. Conclusion and Future Work

The dynamic model of the provision of G&C and critical performance indicators proposed in the paper can be used to model the behavior of critical infrastructure objects and form balanced management decisions in the relevant industries.

The issue of defining and normalizing the parameter is the state of aggressiveness of the environment, as well as sufficient levels of CSC for different categories of the criticality of critical infrastructure objects, which require further research.

In the following studies, it is planned to consider the application of dynamic model of guarantee capacity and cyber security management in distributed commercial systems.

9. References

[1] V. Grechaninov, H. Hulak, V. Sokolov, P. Skladannyi, N. Korshun, Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Proceedings of the Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, 2022, pp. 107–117.

[2] M. Vielberth, Security Information and Event Management (SIEM), in: S. Jajodia, P. Samarati, M. Yung (Eds.), Encyclopedia of Cryptography, Security and Privacy, Springer, Berlin, Heidelberg, 2021. doi:10.1007/978-3-642-27739-9_1681-1.

[3] A. Zhilin, B. Nikolayenko, O. Bakalinsky, Increasing the Security of State Information Resources Through the Use of the Threat Intelligence platform, Information Protection 23(3) (2021) 136–146. [in Ukrainian]

[4] Mitre ATT&CK, 2021. URL: https://attack.mitre.org/.

[5] T. Rid, B. Buchanan, Attributing Cyber Attacks, Journal of Strategic Studies 38(1–2) (2015) 4–37. [in Russian]

[6] S. Borzenkova, et al., Management of Information Security System based on Signature Models, Technical Sciences 2(2) (2010) 200–205. [in Russian]

[7] S. Borzenkova, O. Chechuga, The Concept of using Discrete Situational Models in Information Security Management Systems, News of TulGU, Technical Sciences 6(2) (2011) 328–336. [in Russian]

[8] S. Borzenkova, O. Chechuga, Decision-Making Model for Managing the Information Security System, News of TulGU. Technical Sciences 3 (2013) 471–478. [in Russian]

[9] I. Azhmukhamedov, Mathematical Model of Complex Security of Computer Systems and Networks based on Expert Judgments, Infocommunication Technologies 7(4) (2009) 103–107. [in Russian]

[10] I. Azhmukhamedov, Dynamic Fuzzy Cognitive Model for Assessing the Level of Security of University Information Assets, Management, Computer Engineering and Informatics 2 (2012) 137–141. [in Russian]

[11] C. B. Westphall, et al., Management and Security for Grid, Cloud and Cognitive Networks, Revista de Sistemas de Informação da FSMAn. 8 (2011) 8–21. URL: http://www.fsma.edu.br/si/sistemas.html.

[12] H. Hulak, I. Skiter, Y. Hulak, Methodological Principles of the Creation and Functioning of the Cyber Security Center of the Information Infrastructure of Nuclear Energy Facilities, Cybersecurity: Education, Science, Technology 4(12) (2021) 172–186. doi:10.28925/2663-4023.2021.12.184186. [in Ukrainian]

[13] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Proceedings of the 8th International Conference on Mathematics. Information Technologies. Education, 2019, pp. 222–233.
[14] O. Dovgan, et al., Information Protection Methodology, 2012. [in Ukrainian]
[15] R. Anthony, Planning and Control Systems: A Framework for Analysis. Division of Research, Graduate School of Business Administration, Harvard University, Boston, 1965.
[16] G. A. Gorry, M. S. S. Morton, A Framework for Management Information Systems, Sloan Management Review: Journal 13 (1971) 21–36.
[17] Cybersecurity. A Generic Reference Curriculum, NATO Headquarters Supreme Allied Commander Transformation, 5000/TTS TTX 0310/TT-161157/Ser. NU0766(INV) (2016). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf.
[18] D. Parmenter, Key Performance Indicators – Developing, Implementing, and Using Winning KPIs, 4th ed., John Wiley & Sons, 2019.
[19] Criteria for Evaluating the Security of Information in Computer Systems against Unauthorized Access, RD TIP 2.5-004-99. [in Ukrainian]
[20] H. Hulak, Mechanisms for Ensuring the Security of Software Information Protection Tools, in: Problems of Cyber Security of Information and Telecommunication Systems (2017) 66–72. [in Ukrainian]
[21] Classification of Automated Systems and Standard Functional Profiles of Protection of Processed Information from Unauthorized Access, RD TIP 2.5-005-99. [in Ukrainian]
[22] A. G. Akritas, Elements of Computer Algebra With Applications, 1st ed., Wiley-Interscience, 1989.
[23] Terminology in the Field of Information Protection in Computer Systems against Unauthorized Access, RD TIP 1.1-003-99 (in Ukrainian).
[24] I. Skiter, Model for Assessing the Level of Cyber Security Culture in the Information System, Cybersecurity: Education, Science, Technology 1(13) (2021) 158–169. doi:10.28925/2663-4023.2021.13.158169. [in Ukrainian]
[25] Cyber Security Culture in Organizations, European Union Agency for Network and Information Security (ENISA), 2017. URL: https://www.enisa.europa.eu/.
[26] L. Leenen, J.C. Jansen van Vuuren, Framework for the Cultivation of a Military Cybersecurity Culture, in: 14th International Conference on Cyber Warfare and Security (ICCWS), 2019, pp. 212–220.
[27] A. Turing, Computing Machinery and Intelligence, Mind LIX (236) (1950) 433–460.
[28] Handbook of Human Factors and Ergonomics, 5th ed., G. Salvendy, W. Karwowski (Eds.), 2021.
[29] P. Patrascu, Promoting Cybersecurity Culture Through Education, in: 15th International Scientific Conference on eLearning and Software for Education (eLSE) New Technologies and Redesigning Learning Spaces, New Technologies and Redesigning Learning Spaces II, 2019, pp. 273–279.
[30] B. Stackpole, How to Build a Culture of Cybersecurity, 2022. URL: https://mitsloan.mit.edu/ideas-made-to-matter/how-to-build-a-culture-cybersecurity.