UDC 621.396.075 **doi:** https://doi.org/10.20998/2522-9052.2024.2.07

Bayram Ibrahimov[1], Arif Hasanov[2], Elshan Hashimov[1,2]

[1] Azerbaijan Technical University, Baku, Azerbaijan
[2] Military Defense University, Baku, Azerbaijan

RESEARCH AND ANALYSIS OF EFFICIENCY INDICATORS OF CRITICAL INFRASTRUCTURES IN THE COMMUNICATION SYSTEM

Abstract. The efficiency indicators of the functioning critical information infrastructures in the communication system are analyzed based on the architectural concept of future networks. **The object of the study is** hardware and software complexes critical information infrastructures for special purposes. Critical information infrastructure represents information and telecommunication communication systems, the maintenance, reliability and security which are necessary for the safe operation special-purpose enterprises. In order to avoid the occurrence of various security and reliability incidents, the studied critical infrastructures communication systems require constant analysis and updating operating rules. **The subject of the research is** a method for calculating quality indicators of the functioning of critical information infrastructures in communication systems. In this work, using the example of a communication system based on modern technologies, the sequence of actions for analyzing threats to the security of a critical information infrastructure facility is considered. **The purpose of the study is** to develop a new approach for creating methods for calculating indicators of efficiency, reliability and information security systems. Based on the analysis of the work, a method for calculating efficiency indicators critical information infrastructures of communication systems is proposed and important analytical expressions for further research are obtained. As a result of the study, **the main conclusions of the study** were obtained, which can be implemented and used in critical infrastructures of communication systems to calculate the quality of functioning public computer and telecommunication systems.

Keywords: critical information infrastructures; threat probability; effectiveness assessment; risk; information security system; vulnerability probability.

Introduction

The rapid development of the infrastructure of the digital economy and the formation strategic plans “Digitalization Road Map” require new principles and global approaches to the study of critical information infrastructures in the communication system based on the architectural concept of future FN networks (FN, Future Networks) with increased efficiency, security and reliability [1, 2].

In this regard, ITU-T adopted the first recommendations of the Y.3000 series on the fourth concept of digitalization of communication networks - Future FN networks.

The beginning of the fourth concept of digitalization communication networks coincided with the beginning of the Fourth Industrial Revolution [1, 3] and the sixth technological structure, which improve the quality of functioning of telecommunication processes as an element of the efficiency of domestic critical information infrastructures for special purposes operating in the field of telecommunications [4, 5].

It should be noted that the basis future FN networks as an object of critical information infrastructures in the communication system [6, 7] and NGN networks (Next Generation Network) are important objects both complex information systems and information security systems. In this case, the principles of “efficiency, reliability and comprehensive security in one communication network” are based, using advanced digital technologies, protocols and control systems for service channels and design and technological solutions.

These include primarily information and telecommunication technologies such as:

SDN (Software Defined Networking) [8],

NFV (Network Functions Virtualization) [9],

IMS (Internet Protocol Multimedia Subsystem),

artificial intelligence (AI),

WDM&DWDM (Wavelength Division Multiplexing & Dense WDM),

cloud computing, mobile technologies LTE (Long Term Evolution) & 5G/IMT-2020,

IoT (Internet of Think),

quantum technologies [10, 11].

It is known that critical information infrastructure is information and communication systems, the maintenance, reliability and security of which are necessary for the effective functioning of special-purpose enterprises, and in some cases, for the security of the country as a whole.

Therefore, the tasks of research and analysis performance indicators critical infrastructures in the communication system based on the architectural concept of future networks to ensure the protection government and commercial special-purpose facilities using advanced methods, algorithms and technologies are the most relevant [12, 13].

This paper examines the solution to the problem formulated above - the study and assessment of performance indicators and information protection systems critical infrastructures in the communication system based on the architectural concept of future FN networks.

General statement of the research problem

The analysis showed [3, 9] that a modern strategy for ensuring network security and stability of critical information infrastructures in the communication system based on the architectural concept of future FN networks based on SDN, NFV and multimedia IMS technologies should take into account a number of such factors:

- ensuring the efficient functioning of critical information infrastructures for special purposes [14];
- increasing the reliability hardware and software systems of critical information infrastructures [15];
- effective management of the security of service and information communication channels [16];
- a system of protection against constantly evolving threats and new types of cyber attacks [17].

It is worth noting that some sources provide a clear distinction between critical information infrastructure and information infrastructure in a telecommunications system [18, 19].

Information infrastructures are technical, social and political structures encompassing people, technologies, algorithms, tools and services used to facilitate the distributed sharing content over time and distance [20].

However, critical information infrastructure represents information and telecommunication systems, the maintenance, reliability and security which are necessary for the quality of functioning of enterprises.

Based on the study [7, 8], it was established that the key content definitions of the critical information infrastructure in the communication system are characterized by many important characteristics to ensure its efficiency, reliability and security.

Taking into account the constituent technical components of the quality vector for the functioning of critical information infrastructures in the communication system $Q[K(\lambda_i)]$, it is functionally described by the following relationship:

$$Q\left[K\left(\lambda_i,t\right)\right]= \\ =W\left[E_{EF}\left(\lambda_i,t\right),R_{HF}\left(\Lambda_i\right),I_{IS}\left(\lambda_i,t\right)\right],\ i=\overline{1,k}, \tag{1}$$

where is $I_{IS}(\lambda_i,t)-$ a function that takes into account information security criteria, taking into account the intensity of service and useful traffic λ_i at a point in time t, which are an indicator of the information security system in the critical information infrastructure during the implementation of telecommunication processes;

$E_{EF}(\lambda_i,t)-$ a function that takes into account the efficiency criteria of critical information infrastructures in the communication system, taking into account the intensity of service and useful traffic λ_i at a time t, which are the network characteristics of the system's hardware and software systems when providing various telecommunications services and applications;

$R_{HF}(\Lambda_i)-$ function that takes into account criteria for the reliability of the functioning of critical information infrastructures, taking into account the failure Λ_i rate of hardware and software systems of communication systems at a time t.

Expressions (1) define the essence of the new approach under consideration for analyzing complex indicators of the quality of functioning critical information infrastructures in communication systems in the provision of telecommunications services and applications.

Development of methods for calculating the efficiency of important critical objects

With in order to assess the complex characteristics of the important object under study, it is necessary to maximize the quality indicators functioning critical information infrastructures in communication systems with a limit on the total cost of the system's hardware and software complexes, terminal, switching and channel equipment basic innovative technologies [1, 7].

To solve the problem under consideration, a calculation method is proposed, based on simplifications in the description of the important object under study, where complex indicators of the quality of functioning critical information infrastructures and the cost of the communication system are selected as the objective function.

The mathematical formulation of the problem of the proposed calculation method for assessing complex indicators of efficiency, reliability and information security of hardware-software systems and communication system equipment is described by the following objective functions:

$$E\left[\Pi(\lambda,t)\right]= \\ =W\left\{\operatorname{Arg}\max_i Q\left[K\left(\lambda_i,t\right)\right]\right\},\ i=\overline{1,k}, \tag{2}$$

under the following restrictions

$$K_{ek}\left(\Lambda_i,t\right)\geq K_{ek.all.}\left(\Lambda_i,t\right); \\ A_{apk}\left(\lambda_i\right)\leq A_{apk.all.}\left(\lambda_i\right),\quad i=\overline{1,k}; \tag{3}$$

$$\chi_{kb}\left(\lambda_i,r,t\right)\geq \chi_{kb.all.}\left(\lambda_i,r,t\right); \\ S_{cia}\left(A_n\right)\leq S_{cia.all.}\left(A_n\right),\quad i=\overline{1,k}, \tag{4}$$

where $S_{cia}(A_n)-$ the degree of sustainability critical information infrastructures in communication systems, taking into account activity and security threats A_n, which characterizes the criteria of confidentiality, integrity and availability of each asset;

$A_{apk}(\lambda_i)-$ economic efficiency and cost of hardware and software integrated communication systems λ_i, taking into account when servicing $i-$ the flow of traffic packets in the provision of multimedia services and applications $i=\overline{1,k}$;

$\chi_{kb}(\lambda_i,r,t)-$ the information security coefficient of the functioning of hardware and software systems of the communication system, taking into account the intensity λ_i when servicing $i-$ the flow of traffic packets, $i=\overline{1,k}$ and taking into account the risks of information security of important objects of critical infrastructure r at a time t;

$K_{ek}(\Lambda_i,t)-$ accordingly, single and complex indicators of the reliability of hardware and software complexes of communication systems when performing $i-$ multimedia services with a failure Λ_i rate at time t, $i=\overline{1,n}$;

$S_{cia.all.}(A_n)$, $K_{ek.all.}(\Lambda_i,t)$, $A_{apk.all.}(\lambda_i)$ and $\chi_{kb.all}(\lambda_i,r,t)-$ accordingly, the permissible values of the resistance of a telecommunication system to threats to information security , single and complex reliability indicators, economic efficiency and cost, the information security coefficient of the functioning of hardware and software systems of the communication system, taking into account the intensity λ_i when servicing $i-$ the flow of traffic packets at time t, $i=\overline{1,k}$.

Expressions (2), (3) and (4) define the essence of the new approach under consideration when studying the intensity flows of useful and service traffic packets, on the basis of which a method is proposed for calculating quality indicators of the functioning critical information infrastructures in communication systems when providing telecommunication services and applications.

In addition, the latest proposed expressions describe the features of the calculation method and are one of the important criteria for the quality of functioning critical information infrastructures in communication systems based on SDN, NFV and IMS technologies when providing multimedia services and when establishing connections, which allow more accurately taking into account the telecommunication processes occurring in those analyzed in public network nodes.

Research information security system with information risks

This subsection discusses the assessment of information risks taking into account threat factors, which are an important criterion for the information security of the functioning software and hardware systems of communication systems in critical information infrastructures.

One of the key elements of the strategy for the development modern critical information infrastructure is the solution to the problem transforming the information security risk management system in the communications system.

Since, today, more and more often, modern important critical infrastructures are moving away from a model based on maturity in favor of a new approach based on risk assessment [10].

To ensure the successful operation of highly loaded critical infrastructures communication systems and the effective use of big data in them, it is necessary to manage emerging risks and assess their extent. In this case, it is necessary to know with what probability a violation of the information quality properties can occur.

Therefore, it is necessary to investigate the risks of information quality in such communication systems where information security is important in important critical infrastructures with information risks, as well as in the information security system.

The task arises - to develop a model for their assessment, taking into account the security indicators of the business process oriented telecommunications company, which will be based on mathematical methods for assessing the effectiveness of the information protection system critical infrastructures of the communication system with risks [23, 24].

Risk management in critical infrastructures is a set actions to identify risks of communication systems, analyze them and make decisions to minimize the negative consequences risk events and increase their positive consequences.

Any risk has the following characteristics: cause, condition, probability occurrence, potential damage and consequences.

To assess risk, the proposed calculation method is used [7], which is based on the use of the following algorithms and criteria, which as a functional dependence are described as follows:

$$\chi_{kb}(\lambda_i,r,t)= \\ =W\left[P_{pt}(\lambda_i,r),S_{cl}(r,t),P_{pv}(t,r)\right],i=\overline{1,k}, \quad (5)$$

where $P_{pt}(\lambda_i,r,t)-$ is the probability of a threat in important objects of critical infrastructures of communication systems, taking into account the intensity λ_i when servicing $i-$ the flow of traffic packets and the risks of information security r at the moment of time t, $i=\overline{1,k}$;

$S_{cl}(r,t)-$ the cost of loss in important objects critical infrastructures of communication systems, taking into account the risks of information security r at the time t, $i=\overline{1,k}$;

$P_{pv}(t,r)-$ the probability of vulnerability in important objects critical infrastructures of communication systems, taking into account the risks information security r at the time t, $i=\overline{1,k}$.

Expressions (5) describe a method for calculating the effectiveness of an information security system with information risks based on the proposed new approach and algorithms for quantitative assessment security indicators oriented to the business process of a telecommunications company [25, 26].

Thus, in the general case $\chi_{kb}(\lambda_i,r,t)$ it can be calculated by summing the products of the possible values of damage $S_{cl}(r,t)$ as a result of the impact of threat factors $P_{pt}(\lambda_i,r,t)$ on the probabilities of the implementation of these factors for each hazard:

$$\chi_{kb}(\lambda_i,r,t)= \\ =\sum_{i=1}^{K}S_{i.cl}(r,t)\cdot P_{i.pt}(\lambda_i,r,t),\ i=\overline{1,K}, \quad (6)$$

where $K-$ is the total number of hazards potentially leading to damage in important facilities of critical infrastructures of communication systems.

Formula (6) is the mathematical expectation of the information security value functioning of software and hardware systems in important objects critical infrastructures communication systems.

It should be noted that quantitative risk assessment carried out using formula (6) is difficult in real

conditions. In this case [12], if statistical data are limited in volume and time samples of probability and damage values, or forecast indicators, statistical risk assessment can be used

$$\chi_{kb}^{S}(\lambda_i, r, t),$$

which is based on an assessment of the value of damage $S_{cl}^{S}(r,t)$ and the frequency of occurrence of threats

$$P_{pt}^{S}(\lambda_i, r, t).$$

Taking into account (6) the analyzed value is found as follows:

$$\chi_{kb}^{S}(\lambda_i, r, t) = \\ = K \cdot S_{cl}^{S}(r,t) \cdot P_{pt}^{S}(\lambda_i, r, t), \ i = \overline{1,K}. \quad (7)$$

Expression (7) defines a statistical assessment of risks and characterizes the information security coefficient in important objects of critical infrastructures of communication systems.

In this case, from the last expressions (6) and (7) it follows that the risk

$$\chi_{kb}(\lambda_i, r, t)$$

can be calculated as the product of the probability of threat

$$P_{pt}(\lambda_i, r, t),$$

probability of vulnerability

$$P_{pv}(t, r)$$

and cost of loss

$$S_{cl}(r,t),$$

which is described by the expression:

$$\chi_{kb}(\lambda, r, t) = \\ = P_{pt}(\lambda, r, t) \cdot S_{cl}(r,t) \cdot P_{pv}(t, r). \quad (8)$$

Based on the calculation method, the resulting formula (8) is a formulation of the general problem in important objects of critical infrastructures of communication systems in the case of using qualitative scales.

In addition, in important objects of critical infrastructures of communication systems, risk can be expressed not only as a product, but also as a combination of probability values and damage forecast [7, 26].

One of the main examples of a risk assessment method can be the matrix method, with the help of which damage forecast indicators and threat recurrence rates are ranked in the form of a matrix.

Results numerical calculations and modeling

In this work, the installation system manager, who acts together with a representative of the relevant service, is also considered as a potential violator.

Therefore, it can be assumed that the dynamics threat activity depends on the important object involved in the technological telecommunications process.

Let's consider the case when the characteristic time of change in activity is much less than the time τ_a, and the activity of the threat changes abruptly from 0 to ΔT_a and continues for some characteristic time greater than τ_a. Then (8) has the following analytical solution:

$$\chi_{kb}(\tau_a, r, t) = \\ = \tau_a \cdot \Delta T_a \left\{1 - \exp\left[-(t - t_0)/\tau_a\right]\right\}, \quad (9)$$

where $\tau_a -$ time of relaxation of a threat in the absence of its activity; $t_0 -$ random start time of the threat; $\Delta T_a -$ compensated threat activity by taking counteraction measures in control systems.

Expressions (9) take into account the activity of the threat (a single threat to the security of confidentiality, integrity and availability) and the risk measure for the asset component (A_n) of communication network management systems in critical facilities, where specific assets can be servers, hardware and software systems and local networks connected to telecommunication systems $A_n, n = 1, 2, 3, ..., N$.

We will assume that in a communication network management system, the risks of confidentiality, integrity and availability are not independent, and we will take into account the risk for each asset A_n, which consists of three components, $n = 1, 2, 3$.

In the latter expression for $\Delta T \to \Delta T_{\max}$, then formula (9) will take the following form:

$$\chi_{kb}(\tau_a, r, t) = 1 - \exp\left[-(t - t_0)/\tau_a\right]; \\ \max\left[\chi_{kb}(\tau_a, r, t)\right] = 1. \quad (10)$$

According to the results of the study (10), the value

$$1 - \chi_{kb}(\tau_a, r, t) = exp[-(t\text{-}t_0)/\tau_a],$$

will be considered as the degree resistance to threats.

From the latter it follows that as the degree of threat realization increases, the degree stability decreases.

Next, by analogy with (10) and using (8), we consider $S_{cia}(A_n)$ the degree of sustainability to threats of each asset A_n, $n = 1, 2, 3, ..., N$ and is found as follows:

$$S_{cia}(A_n) = 1 - \chi_{kb}(\tau_a, r, t) \quad (11)$$

From (11) it follows that the failure of one asset communication network management systems leads to a loss of stability of critical information infrastructures.

In order to assess the stability of important critical information infrastructures to information security threats, a communication network management system is considered as an object study, which has an input x and output system y, and also has feedback subsystems to improve their degree stability. Therefore, the impact on telecommunication systems for managing information processes critical elements in important objects is being studied.

In accordance with (9), (10) and (11), the output of the subsystem $S_{cia}(y)$ is related to its input $S_{cia}(x)$ by an equation, which is expressed as follows:

$$S_{cia}(y) = \frac{S_{cia}(x)}{1 - k_f\left[1 - S_{cia}(x)\right]}, \qquad (12)$$

where k_f – feedback coefficient and $k_f \le 1$.

Expressions (12) characterize the degree of resistance of critical information infrastructures to threats to information security using an elementary subsystem with feedback (feedback) and determine the quality of the communication network. In addition, from (12) it follows that feedback increases the stability of the critical information infrastructure subsystem.

Using the Communications Toolbox package - an extension of the standard environment Matlab R 2019b (9.7; 64 bit), the importance of system stability criteria was calculated.

Based on the numerical values in Fig. 1, a graphical dependence of the response $S_{cia}(P_y)$ of this subsystem to the input influence $S_{cia}(P_x)$ is constructed for different feedback coefficients k_f.

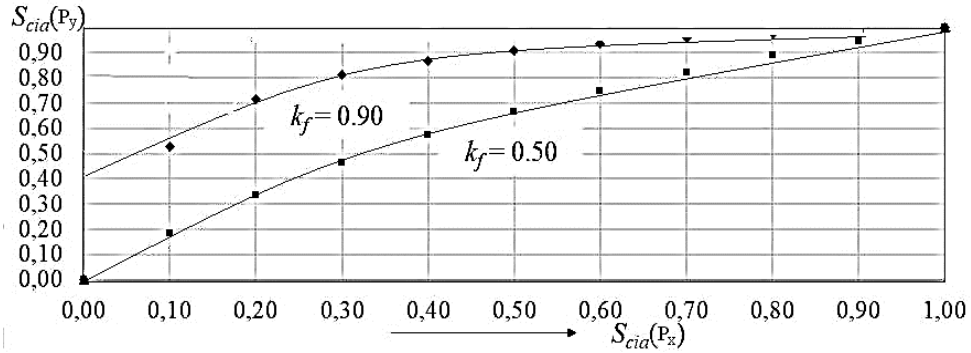

Fig. 1. Graphical dependence of the response feedback subsystem on the input influence for given different feedback coefficients

Analysis of the graphical dependence shows that in the event of a risk to the threat of technical impact of the communication network, with an increase in the response of the feedback subsystem from the input impact $S_{cia}(P_x)$, meeting the requirements for the stability of critical information infrastructures with the effective use of the feedback subsystem for a given indicator k_f, the magnitude of the response increases $S_{cia}(P_y)$.

Its noticeable change begins with values

$$S_{cia}(P_x) \ge 0,25$$

at a given

$$k_f = 0.90.$$

The dependency graphs shown in fig. 1 clearly demonstrate the improvement in the degree sustainability to information security threats in critical objects as the coefficient increases

$$k_f \ge 0.50.$$

The results of the study show that with an increase in the response of the feedback subsystem, the degree of resistance to threats to aggregates and to threats to information security increases.

This one is focused on critical objects in telecommunication systems.

Taking into account the above, we will determine the degree of sustainability of the resource A_n. For each resource $A_n, n = 1, 2, 3$ you can determine the degree of its system sustainability (Sustainability) $S_{cia}(A_n)$ by assessing the criteria $S(A_1)$, $S(A_3)$ and $S(A_3)$ and can be defined as follows:

$$S_{cia}(A_n) = \left[S(A_1) + S(A_2) + S(A_3)\right] \le \le S_{cia.all.}(A_n); \quad n = \overline{1,3}, \qquad (13)$$

here $S_{cia.all.}(A_n)$ – permissible value degree of resistance to threats to units and to threats to information security of important critical objects of the communication system, taking into account assets or resources A_n, $n = 1, 2, 3, ..., N$.

Using the Communications Toolbox package on the Matlab 9.7, R 2019b environment, the importance of system stability criteria was calculated and the results are shown in Table 1.

Table 1 – **Importance of system stability criteria**

Designation	Meaning
$S(A_1)$	0.442
$S(A_2)$	0.271
$S(A_3)$	0.243

From table 1 it is clear that

$$S_{cia.}(A_n) = 0.44 + 0.27 + 0.24 = 0.956 < 1.$$

It is worth noting that the degree of system stability must be at least 0,950, that is, deviation from the full stability of the system is allowed no more than 5% [26].

This means that

$$S_{cia.all.}(A_n) \ge 0.950,$$

that is

$$0.950 \le S_{cia.all.}(A_n) \le 1.000 .$$

Conclusions

As a result of the study, a method was proposed for calculating indicators effectiveness of critical information infrastructures communication systems, taking into account the criteria reliability, information security and business processes important objects.

Based on the calculation method, analytical expressions are obtained for assessing various categories risks that affect the provision of the required quality of information, which are based on the use of the following important quantities: the probability of a threat, the probability of vulnerability and the cost of losing the system.

In further research, the authors propose to test the proposed calculation method algorithms on specific important objects communication systems.

REFERENCES

1. Zhurakovskyi, B., Toliupa, S., Druzhynin, V., Bondarchuk, A. and Stepanov, M. (2022), "Calculation of Quality Indicators of the Future Multiservice Network", *Lecture Notes in Electrical Engineering*, vol 831, pp. 197–209, Springer, Cham, doi: https://doi.org/10.1007/978-3-030-92435-5_11
2. Kaczmarek, S. and Sac, M. (2022), "Performance Evaluation of a Multidomain IMS/NGN Network Including Service and Transport Stratum", *Applied Sciences,* vol. 12, is. 22, 11643, doi: https://doi.org/10.3390/app122211643
3. Babko M. N., Gaidachuk A. V. and Kondratyev A. V. (2017), "Safety category as an element of the efficiency of domestic civil aircraft", *Collection of scientific papers - Issues in the design and production of aircraft structures*, vol. 1 (89), January – March, pp. 7–15, doi: https://doi.org/10.32620/aktt.2017.3.04
4. Ibrahimov B. G., Hashimov E. G., Talibov A. M. and Hasanov, A. H. (2022), "Research and analysis indicators fiber-optic communication lines using spectral technologies", *Advanced Information Systems*, vol. 6, no. 1, pp. 61–64, doi: https://doi.org/10.20998/2522-9052.2022.1.10.
5. Ibrahimov B. G. and Hashimov E. G. (2023), "Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies", *Problems of Informatization,* Proceedings of 11-th International Scientific and Technical Conference, November 16–17, vol. 1, pp. 29–30, doi: https://doi.org/10.32620/PI.23.t1
6. Goldobina, A. S., Isaeva, Yu. A., Selifanov, V. V., Klimova, A. M. and Zenkin, P.S. (2018), "Construction of an adaptive three-level model of processes for managing the information security system of critical information infrastructure objects", *TUSUR Reports*, vol. 21, no. 4, pp. 51–58, doi: https://doi.org/10.1109/APEIE.2018.8545579
7. Ibrahimov, B. G., Hasanov, A. H., Alieva, A. A. and Isaev, A. M. (2019), "Research quality of indicators functioning of multiservice telecommunication networks based on the architectural concept future networks", *Reliability and quality of complex systems*, no. 1 (25), pp. 88–95, doi: https://doi.org/10.21685/2307-4205-2019-1-10
8. Li, Jin, Guoan, Zhang, Hao, Zhu and Wei, Duan (2020), "SDN-Based Survivability Analysis for V2I Communications", *Sensors,* vol. 20, 4678, doi: https://doi.org/10.3390/s20174678
9. Dokuchaev, V. A., Gorban, E. V. and Maklachkova, V. V. (2019), "The System of Indicators for Risk Assessment in High-Loaded Infocommunication Systems", *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*, doi: https://doi.org/10.1109/SOSG.2019.8706726
10. Gorban E. V., Dokuchaev V. A. and Maklachkova V. V. (2018), "Architectura of the Regional Transport Navigation and Information Systems", *Systems of signals generating and processing in the field of on board communications*, March 14–15, pp. 136–141, doi: https://doi.org/10.1109/SOSG.2018.8350588
11. Shishkin, Yu. E. and Skatkov, A. V. (2019), "Quality metrics for assessing and predicting critical conditions", *Quality and life*, no. 1(21), pp. 61–66, doi: https://www.ql-journal.ru/ru/content/kachestvo-i-zhizn-no-121-2019
12. Ibrahimov, B. G. and Alieva, A. A. (2021), "Research and Analysis Indicators of the Quality of Service Multimedia Traffic Using Fuzzy Logic", *Advances in Intelligent Systems and Computing*, vol. 1306, Springer, Cham, pp. 773–780, doi: https://doi.org/10.1007/978-3-030-64058-3_97
13. Hasanov A. H., Iskandarov, K. I. and Sadiyev S.S. (2019), "The evolution of NATO's cyber security policy and future prospects", Journal of Defense Resources Management, vol 10(1), pp. 94–106, available at: http://www.jodrm.eu/issues/Volume10_issue1/07%20-%20hasanov_iskandarov_sadiyev.pdf
14. *Kovalenko, A. and Kuchuk, H. (2022), "Methods to Manage Data in Self-healing Systems",* Studies in Systems, Decision and Control, *Vol. 425, pp. 113–171, doi: https://doi.org/10.1007/978-3-030-96546-4_3*
15. Kovalenko, A., Kuchuk, H., Kuchuk, N. and Kostolny, J. (2021), "Horizontal scaling method for a hyperconverged network", *2021 International Conference on Information and Digital Technologies* (IDT), Zilina, Slovakia, doi: https://doi.org/10.1109/IDT52577.2021.9497534
16. Petrovska, I. and Kuchuk, H. (2023), "Adaptive resource allocation method for data processing and security in cloud environment", *Advanced Information Systems*, Vol. 7(3), pp. 67–73, doi: https://doi.org/10.20998/2522-9052.2023.3.10
17. Illiashenko, O., Kharchenko, V. and Kovalenko, A. (2013), "Cyber security lifecycle and assessment technique for FPGA-based I&C systems", Proceedings of IEEE East-West Design and Test Symposium, EWDTS 2013, doi: https://doi.org/10.1109/EWDTS.2013.6673155
18. Hasanov, A. H., Hashimov, E. G. and Zulfugarov, B. S. (2023), "Comparative analysis of the efficiency of various energy storages", *Advanced Information Systems*, 2023, vol. 7, no. 3, pp.74–80, doi: https://doi.org/10.20998/2522-9052.2023.3.11
19. Bayramov, A. A. and Hashimov, E. G. (2016), "Seismic Location Station for Detection of Unobserved Moving Military Machineries", *Journal of Management and Information Science*, vol. 4, is. 2, pp. 61–66, doi: https://doi.org/10.17858/jmisci.82365.
20. Hashimov, E. G. and Huseynov B. S. (2021), "Some aspects of the combat capabilities and application of modern UAVs", National Security and military knowledges, no. 3. pp. 14–24, available at:

http://mmu.edu.az/assets/files/magazine/6c76692129d7fc24.pdf
21. Dotsenko, N., Chumachenko, I., Galkin, A., Kuchuk, H. and Chumachenko, D. (2023), "Modeling the Transformation of Configuration Management Processes in a Multi-Project Environment", *Sustainability (Switzerland)*, Vol. 15(19), 14308, doi: https://doi.org/10.3390/su151914308
22. Adejimi, Al. O., Sodiya, A. S., Ojesanmi, O. A. and Adeniran, O. J. (2024), "A structured model for identification and classification of critical information infrastructure", *International Journal of Critical Infrastructures*, vol. 20, is. 2, pp.139 – 162, doi: https://doi.org/10.1504/IJCIS.2024.137407
23. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mykhailo, M. and Lohvynenko, M. (2017), "Multiservice network security metric", *2nd International Conference on Advanced Information and Communication Technologies*, AICT 2017 – Proceedings, pp. 133–136, doi: https://doi.org/10.1109/AIACT.2017.8020083
24. Stelkens-Kobsch, T. H., Boumann, H. Piekert, F., Schaper, M. and Carstengerdes, N. (2023), "A Concept-Based Validation Approach to Validate Security Systems for Protection of Interconnected Critical Infrastructures", *ACM International Conference Proceeding Series,* 29 August 2023, no. 110, pp. 1–10, doi: https://doi.org/10.1145/3600160.3605025
25. Trujillo, R. E. M., Henríquez, S. D. M. and Lengua, M. A. C. (2023), "Business Intelligence to Optimize Decision-Making in a Telecommunication Company", *International Journal of Engineering Trends and Technology*, vol. 71, is. 8, pp. 85–101, doi: https://doi.org/10.14445/22315381/IJETT-V71I8P208
26. Erokhin S. D., Petukhov, A. N. and Pilyugin P. L. (2019), "Event-oriented security policy and a formal model of the mechanism for protecting critical information infrastructures", Proceedings of educational institutions of communication, vol. 5., no. 4., pp. 99–105, doi: https://doi.org/10.31854/1813-324X-2019-5-4-99-105

Received (Надійшла) 11.01.2024
Accepted for publication (Прийнята до друку) 27.03.2024

ABOUT THE AUTHORS / ВІДОМОСТІ ПРО АВТОРІВ

Ібрагімов Байрат Ганімат – доктор технічних наук, професор, завідувач кафедри радіоелектроніки та аерокосмічних систем, Азербайджанський технічний університет, Баку, Азербайджан;
Bayram Ibrahimov – Doctor of technical sciences, professor, Head of the Department of Radioelectronics and Aerospace Systems, Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: i.bayram@gmail.com; ORCID ID: https://orcid.org/0000-0002-5364-1181;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=37028384100.

Гасанов Аріф Гасан – доктор філософії з національної безпеки та військових наук, доцент, ректор Військового науково-дослідного інституту Національного Університету Оборони, Баку, Азербайджан;
Arif Hasanov– doctor of philosophy in national security and military sciences, associate professor, rector of Military Scientific Research Institute of the National Defense University, Baku, Azerbaijan;
e-mail: arif.h.hasanov@gmail.com; ORCID ID: http://orcid.org/0000-0002-8814-1590;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=58318799700.

Гашимов Ельшан Гіяс – доктор національної безпеки та військових наук, професор, професор (науковий секретар), Національний університет оборони, професор Азербайджанського технічного університету, Баку, Азербайджан;
Elshan Hashimov – Doctor in national security and military sciences, professor, Academic secretary of National Defense University, professor of Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: hasimovel@gmail.com; ORCID ID: http://orcid.org/0000-0001-8783-1277;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57195631270.

Дослідження та аналіз показників ефективності критичних інфраструктур у системі зв'язку

Б. Г. Ібрагімов, А. Г. Гасанов, Е. Г. Гашимов

Анотація. На основі архітектурної концепції майбутніх мереж проаналізовано показники ефективності функціонування критичних інформаційних інфраструктур у системі зв'язку. **Об'єктом дослідження** є апаратно-програмні комплекси критичних інформаційних інфраструктур спеціального призначення. Критична інформаційна інфраструктура являє собою інформаційно-телекомунікаційні системи зв'язку, технічне обслуговування, надійність і безпека яких необхідні для безпечної роботи підприємств спеціального призначення. Щоб уникнути виникнення різноманітних інцидентів безпеки та надійності, системи зв'язку досліджуваних критичних інфраструктур вимагають постійного аналізу та оновлення правил роботи. **Предметом дослідження** є метод розрахунку показників якості функціонування критичних інформаційних інфраструктур систем зв'язку. У даній роботі на прикладі системи зв'язку на основі сучасних технологій розглянуто послідовність дій для аналізу загроз безпеці об'єкта критичної інформаційної інфраструктури. **Метою дослідження** є розробка нового підходу до створення методів розрахунку показників ефективності, надійності та інформаційної безпеки систем. **Результати.** На основі аналізу роботи запропоновано метод розрахунку показників ефективності критичних інформаційних інфраструктур систем зв'язку та отримано важливі аналітичні вирази для подальших досліджень. В результаті проведеного дослідження отримано основні висновки дослідження, які можуть бути реалізовані та використані в критичних інфраструктурах систем зв'язку для розрахунку якості функціонування загальнодоступних комп'ютерних та телекомунікаційних систем.

Ключові слова: критичні інформаційні інфраструктури; ймовірність загрози; оцінка ефективності; ризик; система захисту інформації; ймовірність уразливості.