RESEARCH METHODS FOR INCREASING THE SECURITY OF COMMUNICATION SYSTEMS IMPORTANT OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

DOI: 10.36724/2072-8735-2024-18-6-61-66

Manuscript received 14 May 2024;
Accepted 12 June 2024

Bayram G. Ibrahimov,
Azerbaijan Technical University, Baku, Azerbaijan;
Military Defense University of the Republic of Azerbaijan, Baku, Azerbaijan, ***i.bayram@mail.ru***

Tural H.Mammadov,
Military Defense University of the Republic of Azerbaijan, Baku, Azerbaijan

Keywords: *critical information infrastructures, threat probability, effectiveness assessment, risk, information security system, vulnerability probability, performance evaluation.*

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 of security management systems for communication systems critical information infrastructures for special purposes. Critical information infrastructure represents information and telecommunication communication systems, the maintenance, reliability and security of which are necessary for the safe operation important facilities when performing various business processes. 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. In this work, using the example of a communication system based on modern technologies, the sequence 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 efficiency indicators communication systems of important objects critical information infrastructure when performing business processes. 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.

Information about authors:

Bayram G. Ibrahimov, *Doctor of Technical Sciences, professor, Head of the Department of Radioelectronics and Aerospace Systems; Azerbaijan Technical University; Military Defense University of the Republic of Azerbaijan*

Tural H. Mammadov, *Adjunct of the National Defense University, Baku, Azerbaijan*

Для цитирования:
Ибрагимов Б.Г., Мамедов Т.Г. Исследование методов повышение защищенности систем связи важных объектов критической информационной инфраструктуры // T-Comm: Телекоммуникации и транспорт. 2024. Том 18. №6. С. 61-66.

For citation:
Ibrahimov B.G., Mammadov T.H. (2024). Research methods for increasing the security of communication systems important objects of critical information infrastructure. *T-Comm*, vol. 18, no.6, pp. 61-66.

Introduction

Intensive development of the infrastructure digital economy based on promising end-to-end technologies requires new approaches to the study of critical information infrastructures in the communication system based on the architectural concept of future networks (FN, Future Networks) with increased efficiency, security and reliability [1-3].

These include primarily promising technologies such as SDN (Software Defined Networking), NFV (Network Functions Virtualization) IMS (Internet Protocol Multimedia Subsystem), mobile technologies LTE (Long Term Evolution) & 5G/IMT-2020, Internet of Think [4-7].

It is known that critical information infrastructure is information and communication systems, the maintenance, reliability and security which are necessary for the effective functioning of special-purpose enterprises, and in some cases, for the security of the country as a whole [1, 4, 8].

In [1, 2, 5], security management systems are considered, the category security is defined as an element of their effectiveness, and models processes for managing the information security system critical information infrastructure objects are studied.

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 [9-12].

This paper examines the solution to the problem formulated above – the study methods for increasing the security communication systems important objects of critical information infrastructure when performing various business processes.

General statement of the research problem

The analysis showed [2, 4, 6, 13] 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;

– increasing the reliability hardware and software systems of critical information infrastructures;

– effective management of the security of service and information communication channels;

– a system of protection against constantly evolving threats and new types of cyber attacks.

It is worth noting that some sources provide a clear distinction between critical information infrastructure and information infrastructure in a telecommunications system. 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 [2, 14, 15].

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 [1, 6, 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 $B[K(\lambda_i)]$, it is functionally described by the following relationship:

$$B[K(\lambda_i,t)] = \mathrm{W}[\mathrm{K}_{\mathrm{ek}}(\Lambda_{\mathrm{i}},\mathrm{t}),\mathrm{S}_{\mathrm{cia}}(A_n)], \quad i=\overline{1,k}\ , \qquad (1)$$

where $S_{cia}(A_n)-$ is the degree sustainability critical information infrastructures in communication systems, taking into account activity and security threats A_n, which characterizes the criteria confidentiality, integrity and availability each asset; $K_{ek}(\Lambda_i,t)-$ accordingly, single and complex indicators of the reliability hardware and software complexes communication systems when performing $i-$ multimedia services with a failure Λ_i rate at time t, $i=\overline{1,k}$.

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

Development methods for calculating the efficiency of important critical objects

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 [1, 2, 4, 7, 8]. The mathematical formulation of the problem of the proposed calculation method for assessing complex indicators of efficiency, reliability and information security hardware-software systems and communication system equipment is described by the following objective functions:

$$Q(\lambda,t) = \mathrm{W}\{Arg\max_i B[K(\lambda_i,t)]\}, \qquad i=\overline{1,k}, \qquad (2)$$

under the following restrictions

$$\chi_{kb}(\lambda_{\mathrm{i}},r,t) \geq \chi_{\mathrm{kb.all.}}(\lambda_i,r,t)\ ,\ A_{apk}(\lambda_i) \leq A_{apk.all.}(\lambda_i)\ ,$$
$$i=\overline{1,k}\ , \qquad (3)$$

where $A_{apk}(\lambda_i)$ – 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;

$A_{apk.all.}(\lambda_i)$, $\chi_{kb.all}(\lambda_i, r, t)$ – accordingly, the permissible values economic efficiency and cost, the information security coefficient of the functioning hardware and software systems 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 (1), (2) and (3) 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.

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 communication systems in critical information infrastructures. 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 communication system with risks [3, 8, 15].

To assess risk, the proposed calculation method is used [8, 9, 11], which is based on the use of the following algorithms and criteria, which as a functional dependence are described as follows:

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

where $\mathrm{P}_{\mathrm{pt}}(\lambda_i, r, t)$ – 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 [1, 3, 14].

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 $\mathrm{P}_{\mathrm{pt}}(\lambda_i, r, t)$ on the probabilities of the implementation of these factors for each hazard:

$$\chi_{kb}(\lambda_i, r, t) = \sum_{i=1}^{K} S_{i.cl}(r,t) \cdot P_{i.pt}(\lambda_i, r, t),\ i = 1,2,3,...,K, \quad (6)$$

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

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

In this case [7, 8, 9, 11], if statistical data are limited in volume and time samples of probability and damage values, or forecast indicators, statistical risk assessment can be used $\chi^{S}_{kb}(\lambda_i, r, t)$, which is based on an assessment of the value of damage $S^{S}_{cl}(r,t)$ and the frequency occurrence of threats $\mathrm{P}^{\mathrm{S}}_{\mathrm{pt}}(\lambda_i, r, t)$.

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

$$\chi^{S}_{kb}(\lambda_i, r, t) = K \cdot S^{S}_{cl}(r,t) \cdot P^{S}_{pt}(\lambda_i, r, t),\ i = 1,2,3,...,K. \quad (7)$$

Expression (7) defines a statistical assessment risks and characterizes the information security coefficient in important objects 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 $\mathrm{P}_{\mathrm{pt}}(\lambda_i, r, t)$, 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 communication systems in the case using qualitative scales.

Analysis of simulation results

Let's consider the case when the characteristic time 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:

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

Where τ_a – время релаксации угрозы в отсутствии ее активности; t_0 – random start time of the threat; ΔT_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:

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

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

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

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 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 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:

$$S_{cia}(P_y) = S_{cia}(P_x)/\{1 - k_f[1 - S_{cia}(P_x)]\}, \quad (12)$$

where k_f – feedback coefficient and $k_f < 1$.

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

Using an application package in the standard Python environment, the importance of system stability criteria was calculated.

***Python* program:**

```
import matplotlib.pyplot as plt
import numpy as np
plt.figure(figsize=(10, 10))
S_cia_x = np.arange(0.1, 1, 0.1)
k_f = 0.50
S_cia_y = (S_cia_x)/(1 - k_f * (1 - S_cia_x))
plt.plot(S_cia_x, S_cia_y, color="b", marker="o",
label="k_f=0.50")
for x, y in zip(S_cia_x, S_cia_y):
plt.annotate(str(round(y, 3)), xy=(x - 0.05, y + 0.02))
plt.legend(loc=2)
plt.grid(True, which='major', axis='both',
      color='#d3d3d3', linewidth=0.8,
      linestyle='-.')
plt.xlim([0, 1.0])
plt.ylim([0, 1.2])
plt.title('Function: S_cia_y =(S_cia_x)/(1 - k_f*(1-S_cia_x))')
plt.xlabel('x-axis')
plt.ylabel('y-axis')
plt.show().
```

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

Analysis of the graphical dependence shows that in the event of a risk to the threat of a technical impact of a communication network, with an increase in the feedback coefficient from the input impact, meeting the requirements for the stability critical information infrastructures with the effective use of the feedback subsystem for a given indicator k_f , the magnitude of the response increases. Its noticeable change begins $S_{cia}(x) \geq 0{,}40$ with values at a given $k_f \geq 0.90$. In this case, the relative error is $\delta[S(x)] = 4.250\%$.

The dependency graphs shown in Figure 1 clearly demonstrate the improvement in the degree of resistance to information security threats in critical objects as the coefficient increases $k_f = 0.55$

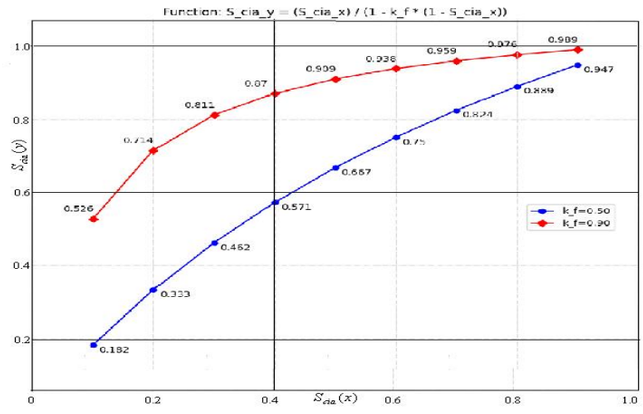

Fig. 1. Graphical dependence of the response feedback subsystem on the input influence at given feedback coefficients

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 vulnerability and the cost losing the system.

Using the proposed calculation method, numerical calculations were carried out with the help of which a graphical dependence of the response of a given subsystem to the input influence was constructed for different feedback coefficients and the importance system stability criteria was calculated.

The results of the study can be applicable when developing or troubleshooting information security systems of public communication networks critical information infrastructure facilities.

References

1. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Security management of critical information infrastructures. Moscow: Hotline – Telecom, 2021. 240 p.

2. Mamedov T.H. Study of the effectiveness of special-purpose service communication networks. *Materials of the XXVII-International Scientific and Technical Conference on "Modern Communications"*, BGAS, Minsk. 2023, pp. 202-204.

3. Babko M.N., Gaidachuk A.V., Kondratyev A.V. 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*. No.1 (89) January – March 2017, pp. 7-15.

4. Kosichkina T.P., Kosichkin G.R. Mobile communication system as an object of critical information infrastructure. *REDS:Telecommunication devices and systems.* No.1, 2022, pp. 26-31.

5. Goldobina A.S., Isaeva Yu.A., Selifanov V.V., Klimova A.M., Zenkin P.S. Construction of an adaptive three-level model of processes for managing the information security system of critical information infrastructure objects. *TUSUR Reports*, 2018. Vol. 21, no. 4, pp. 51-58.

6. Humbatov R.T., Ibrahimov B.G., Alieva A.A., Ibrahimov R.F. Approaches to analyzing the performance indicators of multiservice telecommunication networks based on SDN technology. *Information Technologies*. Vol. 27, No. 8, Moscow, 2021, pp. 419-424.

7. Dokuchaev V.A., Maklachkova V.V., Gorban E.V., Statyev V.Yu. Assessing the quality of processing large volumes of data in highly loaded infocommunication systems. *Proceedings of the international scientific and technical conference Telecommunication and Computing Systems*. 2018. Moscow: Hotline – Telecom, 2018, pp. 25-28.

8. Ibrahimov B.G., Orujov A.O., Hasanov A.H., Tahirova K.M. (2021) Research and analysis efficiency fiber optical communication lines using quantum technology. *T-Comm*. Vol. 15, no.10, pp. 50-54. (*in Russian*). DOI: 10.36724/2072-8735-2021-15-10-50-54.

9. Gorban E.V., Dokuchaev V.A., Maklachkova V.V. Architectura of the Regional Transport Navigation and Information Systems. *2018 Systems of signals generating and processing in the field of on board communications*. Moscow, MTUSI, (March 14-15), 2018, pp. 136-141.

10. Shishkin Yu.E., Skatkov A.V. Quality metrics for assessing and predicting critical conditions. *Quality and life*. 2019. No. 1(21), pp. 61-66.

11. Hasanov A.H., Iskandarov K.I., Sadiyev S.S. The evolution of nato's cyber security policy and future prospects. *Journal of Defense Resources Management*. No. 10(1), 2019, pp. 94-106.

12. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Event-oriented security policy and a formal model of the mechanism for protecting critical information infrastructures. *Proceedings of educational institutions of communication*. 2019. Vol. 5. No. 4, pp. 99-105.

13. Hasanov A.H., Hashimov E.Q., Zulfugarov B. Comparative analysis of the efficiency of various energy storages. *Advanced Information Systems*. No. 7 (3), pp. 74-80. 2023.

14. Andrey E. Krasnov, Alexander S. Mosolov, Nataliya A. Feoktistova. Assessing the resilience of critical information infrastructures to information security threats. *IT Security.* Vol. 28. No. 1, 2021, pp. 106-120. DOI: http://dx.doi.org/10.26583/bit.2021.1.09.

15. Lipatnikov V.A., Shevchenko A.A., Melekhov K.V., Tkachev D.F. Methodology for improving the security of the data transmission network of critical information infrastructure objects under multi-stage attacks. *Information and Control Systems*, 2024. No. 1, pp. 44-55.

ИССЛЕДОВАНИЕ МЕТОДОВ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ СИСТЕМ СВЯЗИ ВАЖНЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Ибрагимов Байрам Ганимат оглы, *Азербайджанский Технический Университет, Баку, Азербайджан;*
Университет Национальной Обороны, Баку, Азербайджан, ***i. bayram@mail.ru***
Мамедов Турал Гусейн оглы, *Университет Национальной Обороны, Баку, Азербайджан*

Аннотация

Проанализированы показатели эффективности функционирования критических информационных инфраструктур в системе связи на базе архитектурной концепции будущих сетей. Объектом исследования является аппаратно-программных комплексов систем связи критических информационных инфраструктур. Критическая информационная инфраструктура представляет собой информационные и телекоммуникационные системы связи, техническое обслуживание, надежность и безопасность которых необходимы для безопасного функционирования важных объектов при выполнении различных бизнес-процессов. Исследуемые важных критических инфраструктур систем связи во избежание реализации различных инцидентов безопасности и надежности нуждаются в постоянном анализе и обновлении правил работы. В данной работе на примере системы связи на базе современных технологий рассмотрена последовательность действий по анализу угроз безопасности объекта критической информационной инфраструктуры. Цель исследования – разработка нового подхода для создания методов расчета показатели эффективности систем связи важных объектов критической информационной инфраструктуры при выполнении бизнес-процессов. На основе анализе работы предложен метод расчета показателей эффективности критических информационных инфраструктур систем связи и получены важных аналитических выражение для дальнейших исследование. В результате исследования получены новые выводы, которые может быть реализованы и использованы в критических инфраструктурах систем связи для анализа качества функционирования компьютерных и беспроводных сетей общего пользования.

Ключевые слова: *критическая информационная инфраструктура, вероятность угроза, риск, система защиты информации, вероятность уязвимости, оценка эффективности.*

Литература

1. *Ерохин С.Д., Петухов А.Н., Пилюгин П.Л.* Управление безопасностью критических информационных инфраструктур. М.: Горячая линия – Телеком, 2021. 240 с.
2. *Мамедов Т.Г.* Исследование эффективности служебных сетей связи специального назначения // Материалы XXVII-Международная научно-техническая конференция по "Современные средства связи", БГАС, Минск. 2023. С. 202-204.
3. *Бабко М.Н., Гайдачук А.В., Кондратьев А.В.* Категория безопасности как элемент эффективности отечественных гражданских самолетов // Сборник научных трудов - Вопросы проектирования и производства конструкций летательных аппаратов. 1 (89) январь - март 2017. С. 7-15.
4. *Косичкина Т.П., Косичкин Г.Р.* Система мобильной связи как объект критической информационной инфраструктуры // REDS:Телекоммуникационные устройства и системы, №1, 2022. С. 26-31.
5. *Голдобина А.С., Исаева Ю.А., Селифанов В.В., Климова А.М., Зенкин П.С.* Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры // Доклады ТУСУР, 2018, том 21, № 4. С. 51-58.
6. *Гумбатов Р.Т., Ибрагимов Б.Г., Алиева А.А., Ибрагимов Р.Ф.* Подходы к анализу показателей производительности мультисервисных телекоммуникационных сетей на базе технологии SDN // Информационные технологии, Том 27, №8, 2021. С. 419-424.
7. *Докучаев В.А., Маклачкова В.В., Горбань Е.В., Статьев В.Ю.* Оценка качества обработки больших объемов данных в высоконагруженных инфокоммуникационных системах // Труды международной НТК Телекоммуникационные и вычислительные системы. М.: Горячая линия – Телеком, 2018. С. 25-28.
8. *Ibrahimov B.G., Orujov A.O., Hasanov A.H., Tahirova K.M.* Research and analysis efficiency fiber optical communication lines using quantum technology. T-Comm, 2021, vol. 15, no.10, pp. 50-54. DOI: 10.36724/2072-8735-2021-15-10-50-54
9. *Горбань Е.В., Докучаев В.А., Маклачкова В.В.* Архитектура региональных транспортных навигационных и информационных систем // 2018 Системы формирования и обработки сигналов в области бортовой связи. М., МТУСИ, (14-15 марта), 2018, pp. 136-141.
10. *Шишкин Ю.Е., Скатков А.В.* Метрики качества для оценки и прогнозирования критических состояний // Качество и жизнь. 2019. №1(21). С. 61-66.
11. *Hasanov A.H., Hashimov E.Q., Zulfugarov B.* Comparative analysis of the efficiency of various energy storages // Advanced Information Systems. no. 7(3), pp. 74-80. 2023.
12. *Erokhin S.D., Petukhov A.N., Pilyugin P.L.* Event-oriented security policy and a formal model of the mechanism for protecting critical information infrastructures // Proceedings of educational institutions of communication. 2019. Vol. 5. No. 4. pp. 99-105.
13. *Hasanov A.H., Hashimov E.Q., Zulfugarov B.* Comparative analysis of the efficiency of various energy storages // Advanced Information Systems, no. 7(3), pp. 74-80. 2023.
14. *Краснов А.У., Мосолов А.С., Феоктистова Н.А.* Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий. Том. 28, №1, 2021. С. 106-120. doi: http://dx.doi.org/10.26583/bit.2021.1.09.
15. *Липатников В.А., Шевченко А.А., Мелехов К. В., Ткачев Д.Ф.* Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках // Информационно-управляющие системы, 2024, №1. С. 44-55. doi:10.31799/1684-8853-2024-1-44-55.

Информация об авторах:
Ибрагимов Байрам Ганимат оглы, *д.т.н., профессор, зав. кафедрой "Радиоэлектроники и аэрокосмических систем" Азербайджанского Технического Университета, Национального Университета Обороны, Баку, Азербайджан*
Мамедов Турал Гусейн оглы, *адъюнкт Национального Университета Обороны, Баку, Азербайджан*