Methods of information systems protection

UDC 004.056 **doi:** https://doi.org/10.20998/2522-9052.2026.2.10

Vagif Gasimov[1], Jabir Mammadov[1], Islam Islamov[1], Elshan Hashimov[2,3]

[1] Baku Engineering University, Baku, Azerbaijan
[2] Azerbaijan Technical University, Baku, Azerbaijan
[3] National Defense University, Baku, Azerbaijan

EVALUATION OF ALTERNATIVE SOLUTIONS FOR THE EFFECTIVE STRUCTURE OF THE CYBER SECURITY SYSTEM IN CRITICAL INFORMATION INFRASTRUCTURES BY THE HIERARCHICAL ANALYSIS METHOD

Abstract. The **subject matter** of this article is the evaluation of alternative solutions for ensuring cyber security of critical information infrastructures and the selection of a more effective solution. The **goal** of the study is to create a cybersecurity system with an effective structure for critical information infrastructures. The **tasks** to be solved include determining the methods, tools, and measures to be included in the system. For this purpose, the hierarchical analysis method was used, and first of all, the decomposition of the problem was given and the corresponding hierarchical structure was compiled. On the basis of expert evaluations for each level of the hierarchical structure, pairwise comparison matrices of alternatives and priorities were constructed and their priority vectors were calculated sequentially. Taking into account the main priorities vector (Confidentiality, Integrity, Availability, Manageability), the degrees of importance of information protection measures (methods and means) were calculated and sorted according to the pairwise preference relations of alternative solutions obtained from the synthesis of the intermediate priorities vector (Physical Security, Network Security, Data Security, Application Security, Access Security). As a **result** of such a ranking, it is possible to determine which security measures should be given more importance to ensure the cyber security of critical information infrastructures. **Conclusion**. Thus, based on the hierarchical analysis method, it is possible to quantitatively evaluate alternative solutions for ensuring cyber security of critical information infrastructures, which allows for easy ranking of these solutions by degree of importance. As a result, an effective decision can be made about which methods are more important to include in the cyber security system, and which are relatively less important. The corresponding calculations and analyses were performed on the example of special purpose organizations based on a generalized hierarchical scheme of the cyber security system of critical infrastructures. Thus, the information infrastructure of one of the organizations producing special equipment was taken as the object of the study. According to the obtained results, it was determined that among the methods, means and measures of security, cryptographic and steganographic methods of data protection for this type of organization have higher degrees of importance than others.

Keywords: cyber security; critical infrastructure; hierarchical analysis method; decomposition; pairwise comparison matrix; confidentiality; integrity; availability; manageability.

1. Introduction

1.1. Motivation. In modern times, the evaluation and providing the state of cyber security in critical infrastructures is in the center of experts' attention as a particularly important issue. As it is known, critical infrastructure (CI) means a vitally important structure, i.e., the most important, exceptionally important, strategically assigned structures that ensure the viability of the state. In international practice, critical infrastructures include the most important areas of the country, such as public administration, national security, defense industry, energy supply, transport, ecology, food (water supply and food safety), healthcare, finance, banking, taxation and telecommunications, and in modern times their normal activity is directly related to information security and cyber security. In the “Patriot Act” (2001) adopted in the United States after the events of September 11, the meaning of "critical infrastructure" is defined as " as a set of physical and virtual systems and tools that can lead to serious consequences in the fields extremely important for the state, the breakdown or destruction of which is national defense and security, economy, health care, etc.” In order to support and ensure the normal operation of the CI, as a rule, information systems and technologies, computer networks, etc. are used. Such systems and technologies are called critical information infrastructures. In other words, critical information infrastructures (CII) are a set of information systems that ensure the operation of public administration, defense, healthcare, financial markets, energy, transport and other important areas, automated control systems and information-communication networks. Since the disruption of the functionality of the CII can cause important damage to the interests of the state, society and citizens, they are more exposed to the continuously increasing cyber threats. For this reason, ensuring the security of the CII, has become a priority issue for every state and organization.

All this makes it necessary to approach sensitively to decision-making for the study and provision of cyber security of the CII, as well as the use of appropriate expert evaluations in these matters.

It should be noted that certain standards, intrusion detection and prevention systems, threat modeling, penetration testing, risk analysis, and a number of other methods and means are widely used for the study of the cyber security of the CII. However, these methods and means, in most cases, do not fully cover the solution of the problem and do not allow to take into account all

specific features. It is obvious that there is no universal and common methodology that can be acceptable to all organization for the study, evaluation and analysis of the cyber security of the CII. It is clear that in the process of evaluating and analyzing cyber security, the characteristics of the enterprise and organization have a serious effect and their consideration is of great importance. One of the most successful approaches is not the usage and application of separate methods and means, but the creation of a software-technical complex cyber security system (CSS) that includes all the necessary methods and means for more reliable and efficient provision of cyber security of the CII [1]. Due to the features of the CII and the requirements, in order to construct such a system, the necessary protection methods (means and technologies) should be determined and included in the CSS.

1.2. State of the art. Hierarchical analysis method (HAM) suggested by the American mathematician T. Saaty in 1972 has recently been widely used for the study of structurally complex, multi-criteria systems that include various subsystems, and for solving numerous problems of various nature.

HAM is based on solving the problem by dividing the studied problem into more simple components, comparing criteria and alternatives pairwise among them, and continuing the expert' judgment sequence. HAM serves to justification of decision-making in conditions of uncertainty and multicriteria [2]. Using ITM, the issues of making decisions on choosing a place to store pharmaceutical products [3], the area of a household waste landfill [4], the corresponding programming method [5], and determining the relative value of the power system units' performance [6] were solved. In [7], based on the hierarchies analysis method, the issue of project ranking was solved from the point of view of efficiency, and it was noted that the obtained results will be used to determine investment priorities at the next stage. Some research works are dedicated to the solution of cyber security issues using HAM [8–13]. In [8], the HAM multi-criteria analysis methodology used to evaluate the level of real threats from cyberspace and affecting cyber security is presented. In that research work, the authors analyzed awareness of the threats of cyberspace and how employees react to incidents that happen in systems, according to the results of surveys conducted among selected employees of the government agency. Taking into account the results of the research, an appropriate mechanism was suggested to provide the necessary level of cyber security. In another research study [9], the issue of antivirus software selection has been investigated and a multi-criteria decision-making solution using HAM has been presented. Cyber security risk assessment issues are also among the areas where HAM has been successfully applied [10–12]. In [10], HAM was used to obtain the weights of risk factors for the purpose of cyber security risk assessment. According to the authors, risk management can be ensured by developing appropriate cyber security measures in the enterprise according to the calculated weights of risk factors. In [11], research works devoted to the HAM model, neural networks, fuzzy logic, group decision-making, software-computing and hybrid models of cyber security risk analysis were examined. According to the results obtained, the HAM model is preferred in most studies and its use in combination with other models may be more efficient. In [12], the HAM methodology was presented to obtain a quantitative measure for the purpose of cybersecurity risk assessment. This methodology helps to prioritize the components of the system for its successful operation and improves subjective judgments by ensuring consistency in the cybersecurity risk assessment process. The usefulness of the HAM process in IT security of organizations and prioritization of defense-in-depth measures was examined in [13]. According to the results of the study, the integration of the HAM process into decision-making in the field of defense-in-depth creates conditions for improving the overall level of IT security.

As it can be seen, the application of HAM allows to analyze the data in a structured manner, considering the opinion of experts when solving multi-criteria issues, to make balanced and efficient decisions by consistently evaluating the importance of each criterion.

1.3. Objective and approach. In this presented research work, using the hierarchical analysis method, in order to ensure the cyber security of the CII, the issue of determining the ones with a higher degree of importance according to the given criteria among the possible methods, means and measures, and based on them, evaluating alternative solutions for the efficient structure of the CSS was considered.

Using the hierarchical analysis method to select the most efficient of the numerous alternative options available towards solving the considered problem seems attractive as an interesting direction and can make a great contribution. Thus, the hierarchy and complexity of the structure, multi-criteria, extensive usage of experts' opinions in decision-making processes are characteristic features of many infrastructures, including the security system of the CII [1]. Having these characteristics makes exactly the application of HAM attractive for the evaluation of the security of the CII.

Taking into account the above, the article proposes the application of the HAM approach to create a CSS with a more effective architecture for CII. As a practical solution, possible criteria and alternatives for a special purpose institution (SPI) are identified, and the issue of selecting an alternative that meets the relevant requirements based on expert assessments is resolved.

The remainder of this paper is organized as follow. The next section examines the hierarchical analysis method and its application for designing the effective structure of a cybersecurity system in critical information infrastructures.

Section 3 considered the issue of creating a cybersecurity system for KII. For this, the decomposition of the issue was first given and the corresponding hierarchical structure was drawn up.

In Section 4, the study of cybersecurity by the method of hierarchy analysis on the example of a special purpose enterprise is given. For this purpose, on the basis of expert assessments for each level of the hierarchical structure, matrices for comparing alternatives and criteria

in pairs were sequentially built and their vectors of priorities were calculated. Taking into account the vector of main priorities, the degrees of importance of information protection measures based on the preference relations in pairs of possible alternative solutions derived from the synthesis of the vector of intermediate priorities were calculated and their ranking according to the degrees of importance was carried out.

Finally, at the end of the article, a brief generalization of the results obtained was carried out and further directions of the study were indicated.

2. Materials and methods of research

HAM is based on the decomposition of the solved problem and its description in the form of a hierarchical structure. Such a structure is used to describe the influence of higher-level priorities ("degree of influence") on lower-level priorities. For this reason, special square matrices are compiled by pairwise comparison of alternatives and criteria. The goal (criterion) is written in the upper left corner of the matrix, the compared elements in the rows and columns, and the relative importance values of those elements according to the goal or criterion are written in the cells located at the intersection of the lines and columns. Those compiled matrices allow for pairwise comparisons of the criteria of the second level in relation to the general goal located in the first level, the alternatives of the third level in relation to the criteria located in the second level, and so on. A pairwise comparison matrix is generally written as follows:

$$A = \begin{pmatrix} a_{11} & a_{121} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad (1)$$

where a_{ij} is the value of relative importance (advantage) of the criterion in the *i*-th row compared to the criterion in the *j*-th column.

The elements of the matrix get values $a_{ii}=1$, $a_{ij}=k$ and $a_{ji}=1/a_{ij}$, $i,j=1,2,....,n$; $k=1,2,...,9$. Where k is the degree of importance, the values of which are taken from Table 1. As can be seen, this matrix is an reverse symmetric matrix, because its diagonal elements are equal to unit, and the elements below the diagonal are equal to the reverse of the elements above.

Table 1 – **The scale of relative importance [2]**

Degree of importance (*k*)	Meaning	Explanation
1	Same importance	The contribution of the criteria to the goal is the same
3	A slight preference of one over the other	Experience and judgments give a slight preference of one alternative over the other
5	An important or serious preference	Experience and judgments give a strong preference of one criterion over the other
7	A significant preference	One of the criteria is so preferred that it becomes practically important
9	A very strong preference	The clear preference of one criterion over the other is more strongly confirmed
2, 4, 6, 8	Interval solutions between two neighboring judgments	It is applied in cases of compromise
Reverse values of the above given numbers	If one of the above given numbers is obtained when comparing one criterion with the other, then, the opposite of that number is obtained, when comparing the second criterion with the first	

After the hierarchical description of the studied system is given, the priorities of the criteria are determined, the alternatives for each criterion are compared in pairs, and pairwise comparison matrices are compiled based on the obtained values. The comparison of criteria is carried out by experts and this time, as a rule, which criteria are more important or which criterion is more likely to influence is considered. The result of the comparison is conducted according to the scale of relative importance (Table 1) and the results are written in the comparison matrix in pairs.

In the next stage, the priority vector $\Lambda = (\lambda_1, \dots, \lambda_n)$ of the matrix is determined. For this purpose, first the eigenvector of the matrix is calculated, and the priorities vector is calculated based on it.

As one of the existing methods for calculating the eigenvectors of the matrix, the method of finding the geometric mean of lines is used:

$$\lambda_i = \sqrt[n]{a_{i1} \cdot a_{i2} \cdot \ldots \cdot a_{in}} = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}, \quad i \in \overline{1,n}, \quad (2)$$

where, λ_i is the *i*-th eigenvector and $a_{i1} \cdot a_{i2} \cdots a_{in}$ is the *i*-th line elements of the matrix.

The calculation of the priorities vector $M = (\mu_1, \mu_2, \dots, \mu_n)$ based on the eigenvectors is performed by the following expression:

$$\mu_i = \frac{\lambda_i}{\lambda_1 + \lambda_2 + \cdots + \lambda_n} = \lambda_i \Big/ \sum_{j=1}^{n} \lambda_j. \quad (3)$$

After that, based on the following expression the maximum eigenvalue of the matrix is calculated:

$$\lambda_{\max} = \mu_1 \cdot \sum_{i=1}^{n} a_{i1} + \mu_2 \cdot \sum_{i=1}^{n} a_{i2} + \cdots. \quad (4)$$

By determining the values that define the relationship between the criteria in the pairwise comparison matrix, theoretically, one can calculate the rest of the elements based on them. It should be noted that in practice, in most cases, it is not possible to achieve such matching, because it is impossible to express human

feelings with any exact formula. As a rule, the evaluation is matched according to the formula $a_{ij} = 1/a_{ji}$. When a successful matching is carried out, the maximum eigenvalue λ_{max} is equal to the size (n) of the matrix, i.e., $\lambda_{max} = n$. For a reverse symmetric square matrix, the formula $\lambda_{max} \geq n$ must be met.

The degree of incompatibility is evaluated by the compatibility index of the elements of the matrix [2]:

$$U_i = \lambda_{\max} / (n-1). \quad (5)$$

By dividing the U_i indicator by the corresponding random matching (T_u) indicator, the matching ratio is calculated:

$$U_n = U_i / T_u . \quad (5)$$

The parameter T_u depends on the size (n) of the matrix, and its numerical value is determined according to the table of the dependence of the random matching indicator on the size of the matrix (Table 2).

It was determined that the acceptable matching ratio (U_n) should not be more than 10%, otherwise the matrix is considered incompatible and the elements of the matrix are re-evaluated by experts.

It was determined that the acceptable matching ratio (U_n) should not be more than 10%, otherwise the matrix is considered incompatible and the elements of the matrix are re-evaluated by experts.

Table 2 – **Table of the dependence of the random matching indicator on the matrix size [2]**

The matrix size (n)	1	2	3	4	5	6	7	8	9	10	11
The random matching indicator (Tu)	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51

After an acceptable matching is obtained, the level 2 pairwise comparison matrices and other appropriate quantities are calculated in an analogical way. The number of level 2 pairwise comparison matrices matches the number of level 1 criteria, and their size matches the number of level 2 criteria. According to the results of the appropriate calculations, in relation to the 1st level criteria the degrees of importance of the 2nd level criteria are determined.

To determine the influence of the level 2 criteria on the common goal, it is necessary to compile a matrix from the vector of priorities of the level 2 pairwise comparison matrices and multiply this matrix by the vector of priorities of the level 1 matrix. In general, regardless of the type of problems to which it is applied, the HAM algorithm is carried out in the following order:

1. Decomposition of the problem to be solved and the image with a hierarchical scheme.
2. Building a pairwise comparison matrix of lower-level elements with respect to the upper-level element (elements) of the hierarchical scheme.
3. Calculation of the eigenvector of the matrix.
4. Calculation of the priorities vector of the matrix according to the eigenvector.
5. Calculation of the maximum eigenvalue of the matrix.
6. Performing appropriate calculation and matching operations to obtain the matching ratio.
7. Building pairwise comparison matrices of the elements of the next level with respect to the elements of the second level (the level after the upper level) and performing paragraphs 3-6 of the algorithm on these matrices.
8. Multiplying the matrix consisting of the priorities vector of the pairwise comparison matrices of the second level of the hierarchical structure by the priorities vector of the matrix compiled for the upper level.
9. Performing similar operations shown in paragraphs 7-8 of the algorithm for other levels of the hierarchical scheme.

The last vector calculated by implementing these operations is the vector of global priorities obtained from the synthesis of the vector of interval priorities, and provides the sought solution of the problem, that is, the best solution for achieving the goal.

3. Results (Application of HAM for development of CSS for CII)

The features of the CSS for the CII and the opportunities of the HAM according to these characteristics are given in Table 3.

Table 3 – **Features of the CII security system and appropriate capabilities of the HAM**

	Features of the CII security system	Appropriate capabilities of the HAM
1	CII, in most cases, consists of complex systems that combines subsystems and components interacting with one another	ICM is an appropriate means for analyzing complex systems, so that it allows solving complex problems by dividing them into more simple problems and manageable components
2	In the CII, as a rule, a large number of different components and parameters influence cyber security	HAM allows systematizing the hierarchy of criteria, taking into account their priority over one another
3	Most of the time, to evaluate the importance of different criteria and alternatives in cyber security, the expert judgment is required	HAM provides a structured approach to get and process expert opinions
4	In many cases, to ensure cyber security we need to compare different security strategies and measures	HAM allows you to identify the best options by performing a comparative analysis of alternatives, considering many criteria
5	In some cases, some aspects of cyber security are required to give more preference in the CII	The HAM allows you to consider the priorities and weights of different criteria and sub-criteria

In order to evaluate the cyber security situation of a CII using the HAM and create an appropriate CSS, first a hierarchical structure must be determined according to the Saaty approach. “Cyber security of the CII” is accepted as the main goal for the problem studied here and this is called level 0.

The followings are suggested as criteria that influence the coal of the hierarchical structure or are of special importance for this purpose: confidentiality; integrity; availability; manageability [14].

Confidentiality (C) reflects in itself the protection of confidential information from unauthorized access, usage, and explanation. Ensuring the confidentiality of information is very important for the CII. Thus, sensible information interception by a malicious person can cause serious problems**.**

Integrity (I) contains ensuring the integrity and completeness of information and systems, that is, preventing their unauthorized modification, distortion, damage or elimination. Integrity is an important factor in preventing changes in the CII that could obtain incorrect results or security breaches.

Availability (A) refers to ensuring the continuous and uninterrupted operation of CII, so that information and services remain accessible at any time and under any conditions. In this context, availability is closely linked to resilient power supply, and the selection and efficiency of energy storage solutions can serve as a supporting factor [15]. A lack of availability may result in substantial economic losses and increased security risks [16].

Manageability (M) reflects the processes for effectively managing and controlling the cyber security of the CII [18]. Manageability includes risk management and the realization of appropriate policies, procedures, and technical means to manage risks and ensure matching with security standards.

In the suggested hierarchical structure, the level that includes the criteria of confidentiality, integrity, availability, and manageability is accepted as level 1 and is called “General Criteria”. General criteria provide security at the physical and network, data and software, as well as information system access levels to protect information as a whole.

Physical security (PS) means the protection of physical resources - buildings, equipment, server rooms, personnel, and facilities of other infrastructure.

Network security (NS) means the protection of network infrastructure, information, and communications from unauthorized access and attacks.

Data security (DS) – carries out the protection of the confidentiality, integrity, and availability of data stored and transmitted in the CII.

Application security (AS*)* means the protection of programs used in CII from malicious attacks and weaknesses.

Access control (AC) provides control and management of user logins to CII resources.

Each of the above components plays an important role in providing the cyber security of the CII and their detailed review and realization is of great importance for preventing possible threats and attacks and protecting from them. In the hierarchical structure that includes the above-mentioned directions, they are accepted as elements of the 2nd level and are called the “Sub-criteria” level.

To achieve the main goal, the realization of a large number of security methods, means and measures that will provide the sub-criteria is necessary. Each of the sub-criteria is considered separately below.

The following measures should be taken to provide the physical protection of the CII cyber security [1, 18]:

- analyzing and evaluating weaknesses and risks;
- creation of a security strategy and policy for the physical protection of CII facilities;
- providing access control using locks, card readers, biometric devices, etc.;
- deploy video surveillance systems, which may be complemented by automated drone detection using neural network-based classifiers [19, 20];
- construction of fences, turnstiles, barriers and other physical obstacles to protect the perimeter of facilities;
- preparation of evacuation and emergency response plans to reply quickly to emergencies and physical security threats;
- providing the protection of server rooms, information centers and other facilities where critical information is stored and processed;
- using physical security measures like fire protection systems and cooling devices;
- training staff on security policies and procedures, and also access control, emergency reply, and suspicious activity detection procedures.

These measures help to create the first protective barrier between threat sources and the protected objects of the CII, to provide their reliable physical protection and to prevent different security threats and incidents.

It is recommended to realize the following measures, to reliably provide network security in the information systems of the CI:

- carrying out regular analysis of network infrastructure weaknesses and risks;
- construction of firewalls to filter traffic and protect the network perimeter from foreign attacks;
- using intrusion detection systems (IDS) and intrusion prevention systems (IPS);
- using encryption methods to protect the information;
- using authentication methods to provide the identification of users and devices;
- placement of access control systems;
- preventing unauthorized access to wireless networks using encryption methods such as WPA2 or WPA3;
- regular updating of software, operating systems and network infrastructure devices;
- controlling network traffic using special means to identify suspicious activity and anomalous network packages;
- determination of security incidents, and registration of log analysis and incident to give them a reply;
- conducting training on network security practices, and also detecting fishing emails, preventing buffer overflow attacks, and other attack defense methods.

The following measures, which are essential for providing data security, help ensure reliable protection of confidential information in the CII and prevent unauthorized access:

- data encryption - this measure should be realized for both data storage and exchange condition;
- realization of access control;
- creating and regularly updating reserve copies;
- monitoring to detect data leakage and analyzing suspicious activity and using incident registration and monitoring systems;
- conducting training for personnel on data security protection rules and procedures;
- providing physical security of server rooms and data storage areas, constructing of video surveillance systems, access control and intrusion sensors;
- carrying out audits and inspections to check the matching of data security with legislation, standards and policies.

Providing application security plays an important role in preventing different threats and attacks in the cyber security of CII. The main measures required to provide application security are as follows:

- updating of software from time to time, and also deleting of out-of-date programs;
- safe programming (this mainly means the use of safe programming methods, safe APIs and libraries);
- using safe authentication and authorization methods to protect access to programs;
- using antivirus and other appropriate programs to protect from viruses and other malicious codes;
- activity monitoring and analysis - this mainly means monitoring program activity to determine suspicious activity and anomalous behavior, determining security incidents, event log analysis and carrying out registration measures to reply them;
- carrying out penetration testing and security audits to determine software weaknesses.

Providing access security in information systems of critical infrastructures covers a number of measures to provide protection against unauthorized access and the confidentiality, integrity and availability of information. These measures can mainly include the followings:

- identification and authentication measures;
- access restriction - this means measures such as determining access rights for users and applying the principle of least privilege so that each user only has access to the resources necessary to perform only their own tasks;
- regularly updating user privileges, controlling the movements of users with higher privileges;
- using encryption methods to protect sensitive information transmitted over the network and stored in devices;
- construction of user activity monitoring and analysis systems to determine suspicious activities and potential security threats;
- involving users in training and enlightenment activities on access security rules and recommendations for preventing security threats;
- realization of access lifecycle management processes - here measures for creating, modifying and deactivating accounts according to changes in user status is also intended;
- providing security for physical access to devices and resources, and also measures for restricting access to server rooms and other critical areas.

These shown measures help to provide access security in the information systems of the CII and prevent different threats and attacks related to unauthorized access. From the above mentioned, it is clear that the 3rd level elements of the hierarchical structure will exactly consist of these methods, means and measures.

It should be noted that in the hierarchical structure, a number of measures can at the same time take part in providing several of the "Sub-criteria" at level 2. Encryption, authentication, physical protection, etc. can be shown as an example to such measures. Taking these into account and making some generalizations, the following measures have been included in the list of elements of level 3 (called "Measures level"): Cryptography & Steganography, Backup Copy, Malware protection, Network Analyzer, Firewall, Physical protection, Authorization & Authentication, Risk Management, HR Management. Thus, for the purpose of studying the cyber security of the CII with the HAM, a hierarchical structure of the CSS consisting of 4 levels is suggested as follows (Fig. 1).

Level 0 - "Cyber Security of the CII", the main purpose and the highest level of the Hierarchy.

Level 1 - "Criteria" level, consists of 4 elements: confidentiality; integrity; availability; manageability.

Level 2 - "Sub-criteria" level, consists of 5 elements: physical security; network security; data security; application security; access security.

Level 3 - "Methods and Means" level, consists of 9 elements: cryptography & steganography; backup copy; malware protection; network analyzer; firewall; physical protection; authorization & authentication; risk management; HR management.

In the hierarchy structure, the number of pairwise comparison matrices that are going to be compiled at each level is determined by the number of elements in the previous level and their sizes are determined by the number of elements in the current level. Thus, for the 1st level of the hierarchy, 1 matrix should be constructed reflecting the importance degree of the criteria in relation to the main goal, which is the only component determined at level 0. Since 4 criteria are intended at level 1, the sizes of these matrices will be 4x4. According to the hierarchical scheme, 4 matrices (dimensions 5x5) should be compiled for level 2, and 5 matrices (dimensions 9x9) should be compiled for level 3. However, it should be taken into account that as the number of compared elements increases, the number of pairwise comparison operations increases approximately in an exponential way, and this makes the work of experts and the processing of results complicated. In this regard, it is recommended that the number of compared elements should not exceed nine [21].

4. Discussion

Now, the construction of pairwise comparison matrices for evaluating the factors influencing the cyber security of a SPI is considered. Conditionally, the information infrastructure of one of the institutions that produces special equipment was taken as the object of study. As mentioned above, the possible negative effects on the overall security of information in such systems are reflected in violations of the criteria of confidentiality (C), integrity (I), availability (A) and manageability (M).

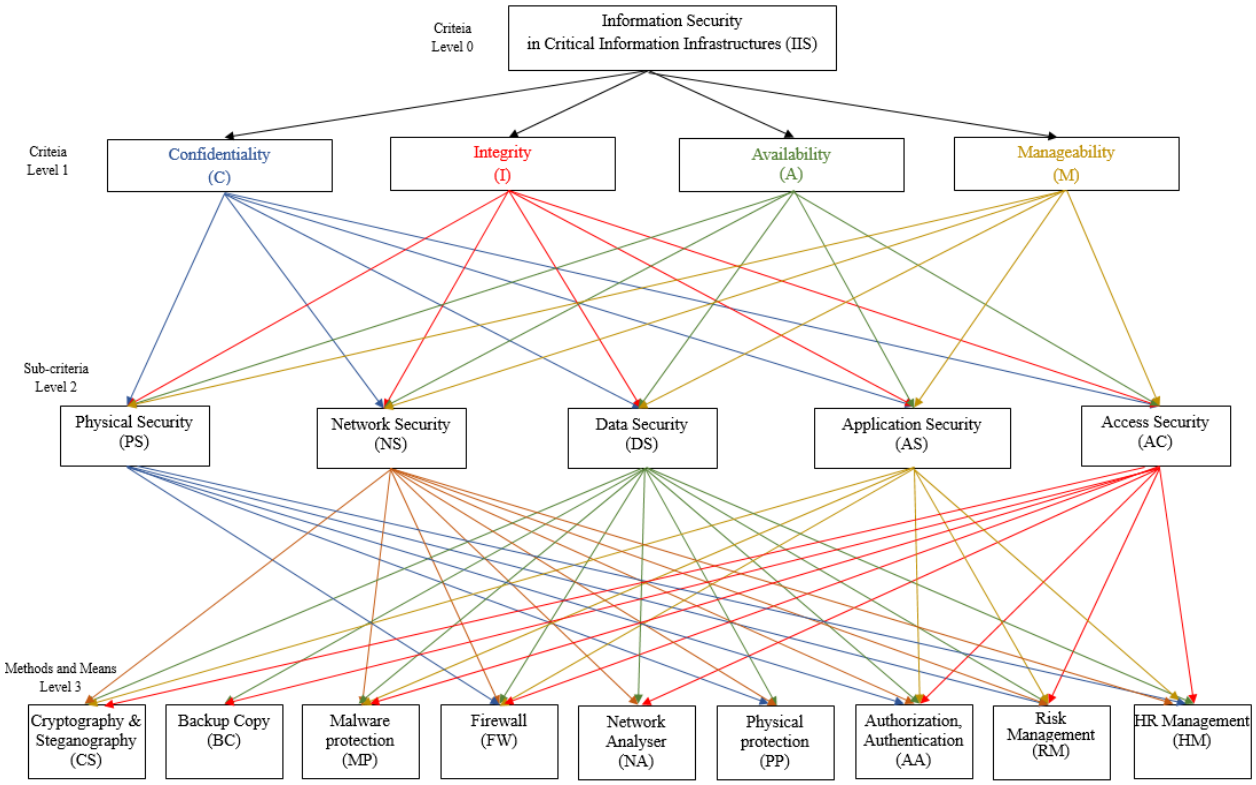

Fig. 1. Hierarchical scheme of Cyber Security of CII

Taking into account the above mentioned, a pairwise comparison matrix was constructed based on statement (1) and the experts' relative importance degrees according to Table 2, and its elements are given in columns 2-5 of Table 4. As can be seen, the confidentiality (C) criterion was evaluated with 9, 9, and 8 degrees of priority, respectively, compared to the general purpose, completeness (I), availability (A), and manageability (M). This shows that, according to the experts' opinion, confidentiality has a significant advantage over other criteria according to general security reasons. According to (1), since $a_{ji} = 1/a_{ij}$, the relative importance degree of the completeness (I), availability (A), and manageability (M) criteria compared to the confidentiality (C) criterion will respectively be 0,11, 0,11 and 0,13. As shown above, the pairwise comparison matrix is a reverse symmetric matrix, its diagonal elements are equal to unit and its elements below the diagonal are equal to the reverse of the elements above. This principle has been taken into account while calculating the appropriate elements of the matrix (columns 2-5 of the Table). After the pairwise comparison matrix is constructed, according to expressions (2)-(4), the eigenvector, priority vector, and maximum eigenvalue are calculated. Since the size of the matrix is 4, the number of the eigenvectors and priorities elements will be equal to 4. According to the results of the calculation, the elements of the eigenvector become equal to $\lambda_1 = 5{,}0454$, $\lambda_2 = 0{,}4387$, $\lambda_3 = 0{,}4082$, $\lambda_4 = 1{,}1067$; elements of the priority vector become equal to μ_1=0,7209, μ_2=0,0627, μ_3=0,0583, μ_4=0,1581 and the maximum eigenvalue becomes equal to λ_{max}= 4,2389. As it is seen, the formula $\lambda_{max} \geq n$, which is necessary for a reverse symmetric square matrix, is satisfying (n = 4).

After that, according to expression (5), the relevance index of the matrix elements is being calculated:

$$U_i = \frac{4{,}2389-4}{3} = 0{,}796.$$

We calculate the matching ratio by dividing the received number by the random matching (T_u=0,9) indicator taken from Table 2:

$$U_n = \frac{0{,}796}{0{,}9} = 0{,}0885.$$

Since the value of the matching ratio is not more than 10% (U_n=8,9%), there is no need to re-evaluate the matrix elements by experts, and the appropriate calculations can be continued for the next stages of the hierarchical scheme.

As mentioned, the 2nd level of the hierarchical scheme consists of 4 elements, and that's why 4 pairwise comparison matrices should be compiled for the next level. The matrices constructed based on expert evaluations and their eigenvectors and priority vectors, maximum eigenvalues, and also the appropriate values of the matching index and matching ratios are given in Tables 5-8.

As can be seen from Tables 5-8, the order of ranking according to degrees of importance of the sub-criteria under the criteria is different. Thus, the data security (0,6601) for the confidentiality criterion, the physical security (0,4429) for the integrity criterion, the physical security (0,5567) for the availability criterion, and in relation to the manageability criterion, the access security sub-criteria (0,6233) have the greatest importance degrees. There is also a difference in the order of ranking the lowest importance for the criteria. Thus, accordingly, physical security (0,0388), application security (0,0343), data security (0,0343), and data security (0,0312) sub-

criteria have the smallest degrees of importance on the confidentiality, integrity, availability, and manageability criteria.

Now, let's look at the evaluation of the importance degree of the sub-criteria in relation to common security. For this purpose, as shown in the algorithm given above, a matrix should be constructed from the priority vectors of the second-stage matrices and it should be multiplied by the priority vector of the pairwise comparison matrix of the previous stage.

Table 4 – **Pairwise comparison matrix of effects on SPI cyber security by common criteria and its appropriate parameters**

IT	C	I	A	M	Eigen-vector (λ)	Priority vector (μ)	Maximum eigenvalue (λ_{max})	Relevance index (U_i)	Matching ratio (U_n)
C	1,00	9,00	9,00	8,00	5,0454	0,7209	4,2389	0,796	0,0885
I	0,11	1,00	1,00	0,33	0,4387	0,0627			
A	0,11	1,00	1,00	0,25	0,4082	0,0583			
M	0,13	3,00	4,00	1,00	1,1067	0,1581			

Table 5 – **Pairwise comparison matrix of effects on the confidentiality criterion and its appropriate parameters**

C	PS	NS	DS	AS	AC	Eigen-vector (λ)	Priority vector (μ)	Maximum eigenvalue (λ_{max})	Relevance index (U_i)	Matching ratio (U_n)
PS	1,00	0,33	0,11	0,33	0,33	0,3333	0,0388	5,4170	0,1043	0,0931
NS	3,00	1,00	0,13	5,00	2,00	1,3026	0,1518			
DS	9,00	8,00	1,00	9,00	9,00	5,6645	0,6601			
AS	3,00	0,20	0,11	1,00	1,00	0,5818	0,0678			
AC	3,00	0,50	0,11	1,00	1,00	0,6988	0,0814			

Table 6 – **Pairwise comparison matrix of effects on the integrity criterion and its appropriate parameters**

I	PS	NS	DS	AS	AC	Eigen-vector(λ)	Priority vector (μ)	Maximum eigenvalue (λ_{max})	Rele-vance index (U_i)	Matching ratio (U_n)
PS	1,00	5,00	2,00	7,00	7,00	3,4517	0,4429	5,3747	0,0937	0,0836
NS	0,20	1,00	0,14	5,00	2,00	0,7784	0,0999			
DS	0,50	7,00	1,00	7,00	7,00	2,7980	0,3590			
AS	0,14	0,20	0,14	1,00	0,33	0,2671	0,0343			
AC	0,14	0,50	0,14	3,00	1,00	0,4979	0,0639			

Table 7 – **Pairwise comparison matrix of effects on the availability criterion and its appropriate parameters**

A	PS	NS	DS	AS	AC	Eigen-vector (λ)	Priority vector(μ)	Maximum eigenvalue (λ_{max})	Rele-vance index (U_i)	Matching ratio (U_n)
PS	1,00	5,00	8,00	7,00	5,00	4,2582	0,5567	5,4312	0,1078	0,0963
NS	0,20	1,00	5,00	3,00	0,33	1,0000	0,1307			
DS	0,13	0,20	1,00	0,25	0,20	0,2627	0,0343			
AS	0,14	0,33	4,00	1,00	0,33	0,5762	0,0753			
AC	0,20	3,00	5,00	3,00	1,00	1,5518	0,2029			

Table 8 – **Pairwise comparison matrix of effects on the manageability criterion and its appropriate parameters**

M	PS	NS	DS	AS	AC	Eigen-vector (λ)	Priority vector (μ)	Maximum eigenvalue (λ_{max})	Rele-vance index (U_i)	Matching ratio (U_n)
PS	1,00	0,50	5,00	0,33	0,13	0,6361	0,0774	5,4263	0,1066	0,0952
NS	2,00	1,00	5,00	2,00	0,14	1,2336	0,1501			
DS	0,20	0,20	1,00	0,25	0,11	0,2565	0,0312			
AS	3,00	0,50	4,00	1,00	0,14	0,9696	0,1180			
AC	8,00	7,00	9,00	7,00	1,00	5,1228	0,6233			

According to the values of the elements of the final vector (Tables 9), it can be noted that, the ranking of the sub-criteria on general safety in descending order of importance is as follows:

1. Data security (DS) – 0,5053.
2. Access security (AS) – 0,1731.
3. Network security (NS) – 0,1470.
4. Physical security (PS) – 0,1005.
5. Application security (AS) – 0,0741.

This leads to that conclusion when providing the cyber security of the studied SPI, greater attention should be given to the data security criterion. At the same time, access security, network security, physical security which are close to each other, and also application security with a lower indicator has close and considerable weight, and they should not be ignored when planning and realizing common security measures.

In the next stage, the importance degrees of the protection measures, which are the 3rd level of the hierarchical scheme, are determined. For this purpose, first, pairwise comparison matrices of the 3rd level elements according to the 2nd level elements are constructed and the appropriate priority vectors are calculated for them. The elements of the pairwise comparison matrix constructed with respect to the physical security sub-criterion according to expert evaluations, calculated vectors and other parameters, are given in Tables 10 and 11.

Table 9 – **Calculation of the final vector of the second level**

IT	C	I	A	M	Final vector of the 2nd level
PS	0,0388	0,4429	0,5567	0,0774	0,1005
NS	0,1518	0,0999	0,1307	0,1501	0,1470
DS	0,6601	0,3590	0,0343	0,0312	0,5053
AS	0,0678	0,0343	0,0753	0,1180	0,0741
AC	0,0814	0,0639	0,2029	0,6233	0,1731
Final vector of the 1st level	0,7209	0,0627	0,0583	0,1581	

Table 10 – **Pairwise comparison matrix of level 3 elements (measures) based on the physical security sub-criterion**

PS	CS	BC	MP	FW	NA	PP	AA	RM	HM
CS	1,00	1,00	1,00	0,14	1,00	0,11	0,33	0,33	0,33
BC	1,00	1,00	1,00	0,14	1,00	0,11	0,33	0,33	0,33
MP	1,00	1,00	1,00	0,14	1,00	0,11	0,33	0,33	0,33
FW	7,00	7,00	7,00	1,00	7,00	0,20	5,00	3,00	3,00
NA	1,00	1,00	1,00	0,14	1,00	0,11	0,33	0,33	0,33
PP	9,00	9,00	9,00	5,00	9,00	1,00	5,00	5,00	5,00
AA	3,00	3,00	3,00	0,20	3,00	0,20	1,00	0,33	0,33
RM	3,00	3,00	3,00	0,33	3,00	0,20	3,00	1,00	3,00
HM	3,00	3,00	3,00	0,33	3,00	0,20	3,00	0,33	1,00

Table 11 – **Eigenvalues, priority vectors and appropriate parameters of the pairwise comparison matrix for physical security**

PS	Eigenvector (λ)	Priority vector (μ)	Maximum eigenvalue (λ_{max})	Relevance index (U_i)	Matching ratio (U_n)
CS	0,4376	0,0316	9,7675	0,0959	0,0662
BC	0,4376	0,0316			
MP	0,4376	0,0316			
FW	3,0313	0,2189			
NA	0,4376	0,0316			
PP	5,4295	0,3920			
AA	0,8927	0,0645			
RM	1,5396	0,1112			
HM	1,2061	0,0871			

The results of calculations carried out using this method are reflected in Table 9. In columns 2-5 of the table a 5x4-sized matrix consisting of the priority vector of the 2nd stage, in the last row the priority vector of the

pairwise comparison matrix of the 1st stage, and in the 6th column the sum (the output) - the final vector has been given.

As can be seen from the table, the final vector of the second level λ^{II} is as follows (the vector is given in transposed form to reduce the size of the text):

$$\lambda^{II} = (0{,}1005;\ 0{,}1470;\ 0{,}5053;\ 0{,}0741;\ 0{,}1731)^T.$$

The maximum eigenvalue of the pairwise comparison matrix of level 3 elements (measures) on physical security was $\lambda_{max}^{PS} = 9{,}7675$, and the matching ratio was 6,6%.

According to the results of the appropriate calculations, the eigenvectors and priorities of the matrix are as follows:

$$\lambda^{PS} = (0{,}44; 0{,}44; 0{,}44; 3{,}03; 0{,}44; 5{,}43; 0{,}89; 1{,}54; 1{,}21)^T,$$

$$\mu^{PS} = (0{,}03; 0{,}03; 0{,}03; 0{,}22; 0{,}03; 0{,}39; 0{,}07; 0{,}11; 0{,}87)^T.$$

Appropriate calculations have also been carried out according to pairwise comparison matrices based on the sub-criteria of network security, data security, application security, and access security, and the results have been given below.

On network security:

- maximum eigenvalue, $\lambda_{max}^{NS} = 9{,}7792$;
- matching ratio, $U_n = 6{,}7\%$;
- eigenvector.

$$\lambda^{NS} = (0{,}55; 1{,}05;\ 0{,}98; 0{,}71; 3{,}29; 0{,}43; 1{,}68; 0{,}43;\ 0{,}37)^T;$$

- vector of priorities.

$$\mu^{NS} = (0{,}04; 0{,}08; 0{,}07; 0{,}35; 0{,}24; 0{,}03; 0{,}13; 0{,}03; 0{,}03)^T.$$

On data security:

- maximum eigenvalue, $\lambda_{max}^{NS} = 9{,}74$;
- matching ratio, $U_n = 6{,}7\%$;
- eigenvector.

$$\lambda^{DS} = (0{,}55; 1{,}05; 0{,}98; 7{,}71; 3{,}29; 0{,}43; 1{,}68; 0{,}43; 0{,}37)^T;$$

- vector of priorities.

$$\mu^{DS} = (0{,}04; 0{,}08; 0{,}07; 0{,}35; 0{,}24; 0{,}03; 0{,}13; 0{,}03; 0{,}08)^T.$$

On application security:

- maximum eigenvalue, $\lambda_{max}^{AS} = 9{,}5972$;
- matching ratio, $U_n = 5{,}1\%$;
- eigenvector.

$$\lambda^{AS} = (1{,}35; 2{,}03; 3{,}32; 0{,}46; 0{,}75; 0{,}40; 1{,}84; 0.57; 0{,}76)^T;$$

- vector of priorities.

$$\mu^{AS} = (0{,}12; 0{,}18; 0{,}29; 0{,}04; 0{,}07; 0{,}04; 0{,}16; 0{,}05; 0{,}07)^T.$$

On access (entry) security:

- maximum eigenvalue, $\lambda_{max}^{AC} = 9{,}7930$;
- matching ratio, $U_n = 6{,}8\%$;
- eigenvector.

$$\lambda^{AC} = (0{,}59; 0{,}33; 0{,}57; 4{,}77; 1{,}67; 1{,}61; 3{,}32; 0{,}51; 0{,}41)^T;$$

- vector of priorities.

$$\mu^{AC} = (0{,}04; 0{,}02; 0{,}04; 0{,}35; 0{,}12; 0{,}12; 0{,}24; 0{,}04; 0.03)^T.$$

To evaluate the effect of measures on common security, let's compile a new matrix from the priority vector of the 3rd level pairwise comparison matrices and multiply it by the final vector of the 2nd level (λ^{II}).

As a result of the appropriate matrix and calculation, the final matrix of the obtained 3rd level is reflected in Table 12.

Thus, the final vector reflecting the effect of level 3 elements, that is, measures, on common security will be as follows in transposed form:

$$\lambda^{III} = (0{,}29; 0{,}09; 0{,}09; 0{,}16; 0{,}10; 0{,}10; 0{,}12; 0{,}04; 0{,}04)^T.$$

As can be seen, the elements of the final vector (λ^{III}) at level 3 ranking in descending order of importance in common security is as follows:

- cryptographic and steganographic protection (CS) - 0,268 (26,8%);
- firewall protection (FW) – 0,162 (16,2%);
- protection with authorization and authentication AA) – 0,119 (11,9%);
- protection with network analyzer (NA) – 0,103 (10,26%);
- physical protection (PP) – 0,095 (9,5%);
- antivirus protection (MP) – 0,090 (9,0%);
- protection with reserve copies (BC) – 0,087 (8,7%);
- risk management (RM) – 0,041 (4,1%);
- human resources management (HM) – 0,036 (3,6%).

Table 12 – **Final matrix of level 3**

Final matrix of level 3						**The final vector of the third level**
IT	**PS**	**NS**	**DS**	**AS**	**AC**	
CS	0,032	0,041	0,480	0,118	0,043	0,268
BC	0,032	0,078	0,110	0,177	0,024	0,087
MP	0,032	0,073	0,094	0,289	0,041	0,090
FW	0,219	0,349	0,051	0,040	0,346	0,162
NA	0,032	0,244	0,075	0,065	0,121	0,103
PP	0,392	0,032	0,055	0,035	0,117	0,095
AA	0,064	0,125	0,081	0,160	0,241	0,119
RM	0,111	0,032	0,030	0,050	0,037	0,041
HM	0,087	0,027	0,026	0,066	0,030	0,036
The final vector of the second level	0,101	0,147	0,505	0,074	0,173	

The obtained result gives reason to say that among all the measures shown for protecting the cyber security of the considered institution, cryptographic and steganographic protection measures have a higher priority.

This can be explained by the fact that the confidentiality and integrity of information are of special importance in the area under study. However, the fact that the degree of importance of protection measures that use cryptographic and steganographic methods is 1,6 times higher than that of firewall protection measures, which becomes second in the ranking given above, makes necessary a more careful approaching to these measures in providing common security. Here, together with standard methods, depending on the assignment of the CII objects, specially designed methods and means can also give positive results. For example, in [21, 22], a DNA-based image encryption algorithm was proposed, which showed promising results in this area. In addition, an encryption algorithm using DNA pseudo-symbols and chaotic maps was developed to further enhance security [23]. Another approach involves a flow encryption method based on the chaotic Brownian motion model of molecules, as demonstrated by the authors in [24]. In [25], a labyrinth-based image encryption method was applied, which was constructed by generating random numbers. A method for protecting information by steganographic means based on fractals was proposed in [26].

The use of inter-network screens is widely used in the construction of the common cybersecurity strategy of institutions. As the main task, protecting the network, and also information and other resources from external threats, falls on Firewalls. That is why, among the necessary measures providing the cyber security of the studied object, the use of network screens - Firewalls is reflected as the second most important and heaviest measure.

The third measure according to most important degree is authorization and authentication, and they have a weight of 0,119 (11,9%). Authentication not only prevents unauthorized access to the system by malicious people, but also allows users to record their actions, and this is especially important to detect and investigate security breaching incidents. The authorization process provides the user with certain rights and powers to access resources after successful authentication. The combined use of authentication and authorization, which are inseparable components of the CSS, are processes that provide reliable protection of information and resources from threats. All this makes authentication and authorization measures have a relatively high degree of importance in providing the common security of the system.

So, in the CSS that is going to be created for SPI, cryptographic and steganographic protection methods, inter-network protection screens, protection with authorization and authentication should occupy the main place.

In addition to these, other methods, means and measures (network analyzer protection, physical protection, antivirus protection, protection with reserve copies, risk management, human resources management) should not be out of sight.

Although the importance levels obtained for them as a result of calculations are not very high, they must be taken into account in the CSS, since they are values that need to be taken into account.

Conclusions

An evaluation of alternative solutions for providing cyber security of the CII has been carried out according to the hierarchical analysis method. It has been determined that, the creation of a single cyber security system, which includes the most important methods and means for reliable providing of cyber security of CII objects, is of great importance. However, the inclusion of all possible methods and means in the composition of the CSS may complicate its activity, reduce its ability to react, and ignore the main requirements. In this regard, according to the requirements imposed on the protected objects of the CII, the degree of importance of these or those methods and means of protection can be identified and sorted.

As a result, it is possible to make a decision on which included in the composition of the CSS methods should be more important, and which ones are comparatively less important.

According to the results obtained based on expert evaluations during the studies carried out, it has been determined that cryptographic and steganographic protection measures have a greater weight compared to other measures to provide the necessary level of cyber security in the studied CII. And this is 1,6 times higher than the indicator of the firewall protection measure, whose indicator is in the second place according to degrees of importance. At the same time, the results of the study carried out show that other protection measures should also be taken into account to provide common security. Thus, according to the general ranking, authorization and authentication, using a network analyzer, physical protection, antivirus protection, protection by making reserve copies, risk management, and human resource management measures also have close importance indicators and play an important role in providing common security.

As a future direction of the research, it is planned to carry out relevant work on integrating the proposed system with artificial intelligence (AI) and machine learning (ML).

As a result, the automation of expert evaluations and the development of dynamic, self-learning cybersecurity assessment systems can be ensured.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

REFERENCES

1. Gasimov V.A. and Mammadov J.I. (2023), "Model and method for determining the optimal structure of a security system for critical information infrastructure", Reports of BSUIR, vol. 21, no. 2, pp. 95–103, doi: https://doi.org/10.35596/1729-7648-2023-21-2-95-103
2. Saaty, T.(2008), "Decision making with the analytic hierarchy process", *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, doi: https://doi.org/10.1504/IJSSCI.2008.017590
3. Arslan, M. (2020), "Application of AHP method for the selection of pharmaceutical warehouse location", *J. Fac. Pharm.*, vol. 44, no. 2, pp. 253–264, doi: https://doi.org/10.33483/jfpau.709528
4. Abdelouhed, F., Ahmed, A., Abdellah, A., Yassine, B., and Mohammed, I. (2022), "GIS and remote sensing coupled with analytical hierarchy process (AHP) for the selection of appropriate sites for landfills: a case study in the province of Ouarzazate", Journal of Engineering and Applied Science, vol. 69, no. 19, pp. 1–23, doi: https://doi.org/10.1186/s44147-021-00063-3
5. Helingo, M., Purwandari, B., Satria, R., and Solichah, I. (2017), "The Use of Analytic Hierarchy Process for Software Development Method Selection: A Perspective of e-Government in Indonesia", Procedia Computer Science, vol. 124, pp. 405–414, doi: https://doi.org/10.1016/j.procs.2017.12.171
6. Aydın, Z. (2025), "Detecting Cybersecurity Threats in Digital Energy Systems Using Deep Learning for Imbalanced Datasets", *International Journal of Energy Economics and Policy*, vol. 15, no. 3, pp. 614–628, doi: https://doi.org/10.32479/ijeep.19649
7. Kouskoura, A., Kalliontzi, E., Skalkos, D. and Bakouros, I. (2025), "Analysis of Results of Experts' Perspectives of Sustainable Regional Competitiveness Using the Analytic Hierarchy Process Multi-Criteria Method", *Sustainability*, vol. 17, 2681, doi: https://doi.org/10.3390/su17062681
8. Zaburko, J. and Szulżyk-Cieplak, J. (2019), "Information security risk assessment using the AHP method", *IOP Conference Series Mater. Sci. Eng*., vol. 710, no. 1, art. numb. 12036, doi: https://doi.org/10.1088/1757-899X/710/1/012036.2019
9. Nurhayati, A., Gautama, A. and Naseer, M.(2018), "Decision making model design for antivirus software selection using Factor Analysis and Analytical Hierarchy Process", *MATEC Web of Conferences*, vol. 154, pp. 1–6, doi: https://doi.org/10.1051/matecconf/201815403006
10. Meng, M. and Enping, L. (2015), "The Application Research of Information Security Risk Assessment Model Based on AHP Method", Journal of Advances in Information Technology, vol. 6, no. 4, pp. 201–206, doi: https://doi.org/10.12720/jait.6.4.201-206
11. Ming-Chang, L. (2014), "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method", *International Journal of Computer Science & Information Technology*, vol 6, no. 1, pp. 29–45, doi: https://doi.org/10.5121/ijcsit.2014.6103
12. Haque, G.M.M., Akula, D.K., Mohammed, Y.S., Syed, A. and Arafat, Y. (2025), "Cybersecurity Risk Management in the Age of Digital Transformation: A Systematic Literature Review", *The American Journal of Engineering and Technology*, vol. 7, no. 8, pp. 126–150, doi: https://doi.org/10.37547/tajet/Volume07Issue08-14
13. Rodney, A. (2017), "Using the Analytical Hierarchy Process Model in the Prioritization of Information Assurance Defense In-Depth Measures? - A Quantitative Study", *Journal of Information Security*, vol. 8, no. 3, pp. 166–173, doi: https://doi.org/10.4236/jis.2017.83011
14. Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Yu., Yevstrat, D.,Chyrva, Y., Kuchuk, H. (2022), "Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples", *Eastern-European Journal of Enterprise Technologies*, vol. 6(4-120), pp. 40–49, doi: https://doi.org/10.15587/1729-4061.2022.269128
15. Hasanov, A.H., Hashimov, E.G. and Zulfugarov, B.S. (2023), "Comparative analysis of the efficiency of various energy storages", *Advanced Information Systems*, vol. 7, no. 3, pp.74–80, doi: https://doi.org/10.20998/2522-9052.2023.3.11
16. Bayramov, A.A. and Hashimov, E.G. (2018), "Assessment of invisible areas and military objects in mountainous terrain", *Defence Science Journal*, vol. 68(4), pp. 343–346, doi: https://doi.org/10.14429/dsj.68.11623
17. Kuchuk, H., Kalinin, Y., Dotsenko, N., Chumachenko, I. and Pakhomov, Y. (2024), "Decomposition of integrated high-density IoT data flow", *Advanced Information Systems*, vol. 8, no. 3, pp. 77–84, doi: https://doi.org/10.20998/2522-9052.2024.3.09
18. Kharchenko, V., Kovalenko, A., Andrashov, A. and Siora, A. (2012), "Cyber security of FPGA-based NPP I&C systems:challenges and solutions", *8th International Conference Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies*, San Diego, California, Westin San Diego, available at: https://www.researchgate.net/publication/319292444_CYBER_SECURITY_OF_FPGA-BASED_NPP_IC_SYSTEMS_CHALLENGES_AND_SOLUTIONS
19. Hashimov E.G. and Khaligov G. (2024), "The issue of training of the neural network for drone detection", *Advanced İnformation Systems*, vol. 8, no. 3, pp. 53–58, doi: https://doi.org/10.20998/2522-9052.2024.3.06
20. Dergachov, K., Hurtovyi, O. and Hashimov, E. (20250, "Adaptive algorithm for visual positioning of UAVs in the local environment", *CEUR Workshop Proceedings*, vol. 3981, pp. 103–114, available at: https://ceur-ws.org/Vol-3981/paper09.pdf
21. Song, C. and Qiao, Y. (2015), "A Novel Image Encryption Algorithm :Based on DNA Encoding and Spatiotemporal Chaos", *Entropy*, vol. 17, pp. 6954–6968, doi: https://doi.org/10.3390/e17106954
22. Hashimov, E., Pashayev, A. and Khaligov, G. (2025), "Camera control algorithm and image quality assessment method to obtain a quality image", *Advanced Information Systems*, vol. 9, no. 3, pp. 50–56, doi: https://doi.org/10.20998/2522-9052.2025.3.06
23. Li, P. and Zhang, X.(2024), "Image encryption algorithm based on a novel cascade chaotic system and DNA mutation", *Physica Scripta*, vol. 99, no.10, doi: https://doi.org/10.1088/1402-4896/ad6f48
24. Gasimov V.A., Mammadov J.I. and Mammadzada N.F. (2022), "Stream encryption method based on the chaotic Brownian motion model of molecules", International Conference on Innovative Data Communication Technologies and Application, *Procedia Computer Science*, vol. 215, pp. 577–588, doi: https://doi.org/10.1016/j.procs.2022.12.060

25. Gasimov V.A., Mammadzada N.F., Mammadov J.I., and Mustafayeva E.A. (2024), “Maze based image encryption method constructed by random number generation”, *Eurasian Journal of Mathematical and Computer Applications*, vol. 12, no. 3, pp. 35–50, doi: https://doi.org/10.32523/2306-6172-2024-12-3-35-50
26. Alia, M. and Suwais, K. (2020), “Improved Steganography Scheme based on Fractal Set”, *The International Arab Journal of Information Technology* (IAJIT), vol. 17(1), pp. 128–136, doi: https://doi.org/10.34028/iajit/17/1/15

Received (Надійшла) 30.11.2025
Accepted for publication (Прийнята до друку) 11.03.2026

ABOUT THE AUTHORS / ВІДОМОСТІ ПРО АВТОРІВ

Гасимов Вагіф Аліджавад – доктор технічних наук, професор, декан факультету інформаційних та комп’ютерних технологій, Бакинський інженерний університет, Баку, Азербайджан
Vagif Gasimov – Doctor of Technical Sciences, Professor, Dean of Information and Computer Technologies Faculty, Baku Engineering University, Baku, Azerbaijan;
e-mail: vaqasimov@beu.edu.az ; ORCID Author ID: http://orcid.org/0000-0003-3192-4225;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=7801667181.

Мамедов Джабір Ісмаїл – доктор філософії з інженерії, доцент, завідувач кафедри кібербезпеки та комп’ютерної інженерії, Бакинський інженерний університет, Баку, Азербайджан;
Jabir Mammadov – Doctor of Philosophy in Engineering, Associate Professor, Head of the Department of Cybersecurity and Computer Engineering, Baku Engineering University, Baku, Azerbaijan
e-mail: camammadov@beu.edu.az; ORCID Author ID: http://orcid.org/0000-0003-3939-4708;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57214997321.

Ісламов Ислам Джамал – доктор технічних наук, професор кафедри автоматизації, телекомунікацій та енергетики, Бакинський інженерний університет, Баку, Азербайджан;
Islam Islamov – Doctor of Technical Sciences, Professor of the Department of Automation, Telecommunications and Energy, Baku Engineering University, Baku, Azerbaijan
e-mail: isislamov@beu.edu.az; ORCID Author ID: http://orcid.org/0000-0001-8645-0640;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56941786100.

Гашимов Ельшан Гіяс – доктор національної безпеки та військових наук, професор, професор Азербайджанського технічного університету; професор Національного університету оборони, Баку, Азербайджан;
Elshan Hashimov – Doctor in National Security and Military Sciences, Professor of Azerbaijan Technical University, Professor of National Defense University, Baku, Azerbaijan;
e-mail: hasimovel@gmail.com; ORCID Author ID: http://orcid.org/0000-0001-8783-1277;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57195631270.

Оцінка альтернативних рішень для ефективної структури системи кібербезпеки в критичних інформаційних інфраструктурах методом ієрархічного аналізу

В. А. Гасимов, Д. І. Мамедов, І. Д. Ісламов, Е. Г. Гашимов

Анотація. Предметом цієї статті є оцінка альтернативних рішень для забезпечення кібербезпеки критичних інформаційних інфраструктур та вибір більш ефективного рішення. **Метою** дослідження є створення системи кібербезпеки з ефективною структурою критичних інформаційних інфраструктур. **Завдання**, що вирішуються, включають визначення методів, інструментів та заходів, які мають бути включені до системи. Для цього було використано метод ієрархічного аналізу, і перш за все було проведено декомпозицію проблеми та складено відповідну ієрархічну структуру. На основі експертних оцінок для кожного рівня ієрархічної структури було побудовано матриці попарного порівняння альтернатив та пріоритетів та послідовно обчислено їх вектори пріоритетів. З урахуванням вектора основних пріоритетів (Конфіденційність, Цілісність, Доступність, Керованість) були розраховані ступені важливості заходів захисту інформації (методів та засобів) та відсортовані відповідно до попарних співвідношень переваги альтернативних рішень, отриманих в результаті синтезу вектора проміжних пріоритетів (Фізична безпека, Мережева безпека, Безпека даних, Безпека додатків, Безпека доступу). В **результаті** такого ранжування можна визначити, яким заходам безпеки слід надати більше значення для забезпечення кібербезпеки критичних інформаційних інфраструктур. **Висновки.** Таким чином, на основі методу ієрархічного аналізу можна кількісно оцінити альтернативні рішення щодо забезпечення кібербезпеки критичних інформаційних інфраструктур, що дозволяє легко ранжувати ці рішення за ступенем важливості. В результаті можна прийняти ефективне рішення про те, які методи є більш важливими для включення до системи кібербезпеки, а які є відносно менш важливими. Відповідні розрахунки та аналізи були виконані на прикладі організацій спеціального призначення на основі узагальненої ієрархічної схеми системи кібербезпеки критичних інфраструктур. Таким чином, за об'єкт дослідження була взята інформаційна інфраструктура однієї з організацій, що виробляє спеціальне обладнання. Згідно з отриманими результатами, було визначено, що серед методів, засобів та заходів безпеки, криптографічні та стеганографічні методи захисту даних для цього типу організацій мають вищу ступінь важливості, ніж інші.

Ключові слова: кібербезпека; критична інфраструктура; метод ієрархічного аналізу; декомпозиція; матриця попарних порівнянь; конфіденційність; цілісність; доступність; керованість.