Experimental study of the method for prioritizing it incidents at critical information infrastructure facilities of the state*

Sergiy Gnatyuk[1,†], Viktoria Sydorenko[1,†], Artem Polozhentsev [1,*,†], and Nazerke Baisholan[2,†]

[1] National Aviation University, 1 Liubomyra Huzara ave., Kyiv, 03058, Ukraine
[2] Al Farabi Kazakh National University, 71 al-Farabi ave., Almaty, 050040, Kazakhstan[1]

Abstract

This paper presents an experimental study of a method for prioritizing IT incidents at critical information infrastructure facilities of the state. The method builds on established frameworks such as ITIL, COBIT, ISO/IEC 20000, and the NIST Cybersecurity Framework, integrating them with the Analytic Hierarchy Process (AHP) to assess and rank IT threats based on their impact. The proposed method involves a multi-stage approach, including threat identification, local and global prioritization, and synthesis of results for effective IT security management. The method takes into account the impact of incidents on key stakeholders, including citizens, society, the state, and law and order. Experimental validation was conducted using real-world data, demonstrating that hardware incidents hold the highest priority for state protection, while software and security incidents are most critical for citizens. The results highlight the importance of maintaining robust physical infrastructure and developing reliable IT security software. This method provides a practical tool for optimizing resource allocation and enhancing the security and resilience of critical information infrastructure.

Keywords

Critical infrastructure, critical information infrastructure, critical information infrastructure facilities, IT incidents, ITIL, IT incident prioritization

1. Introduction

Ensuring the security of national critical infrastructure (CI) is one of the most important areas of modern management. In a world where information technology permeates all areas of activity, the reliability and sustainability of IT systems are becoming the foundation of national security. Critical information infrastructure facilities (CIIF) of the state require special attention, as their vulnerability can lead to large-scale negative consequences for the economy, public security and stability of the state (Fig 1).

The urgency of studying IT incident priorities is due to the growing number and complexity of threats in the world that require effective management and response methods. IT incidents that occur in critical information infrastructure facilities can have a variety of causes and consequences, so their correct classification and prioritization is a prerequisite for ensuring an appropriate level of security and sustainability.

This article presents a method for prioritizing IT incidents at critical government information infrastructure facilities, based on the integration of international best practices in the field of IT service management and security. The developed method allows a systematic approach to threat

AdvAIT-2024: 1st International Workshop on Advanced Applied Information Technologies, December 5, 2024, Khmelnytskyi, Ukraine - Zilina, Slovakia

* Corresponding author.
† These authors contributed equally.
s.gnatyuk@kai.edu.ua (S. Gnatyuk); v.sydorenko@ukr.net (V. Sydorenko); artem.polozhentsev@kai.edu.ua (A. Polozhentsev); baisholan@gmail.com (N. Baisholan).
0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-0139-0752 (A. Polozhentsev); 0000-0002-8134-0466 (N. Baisholan).

assessment, considering their impact on various aspects of the functioning of critical facilities, as well as the development of effective strategies to minimize risks.

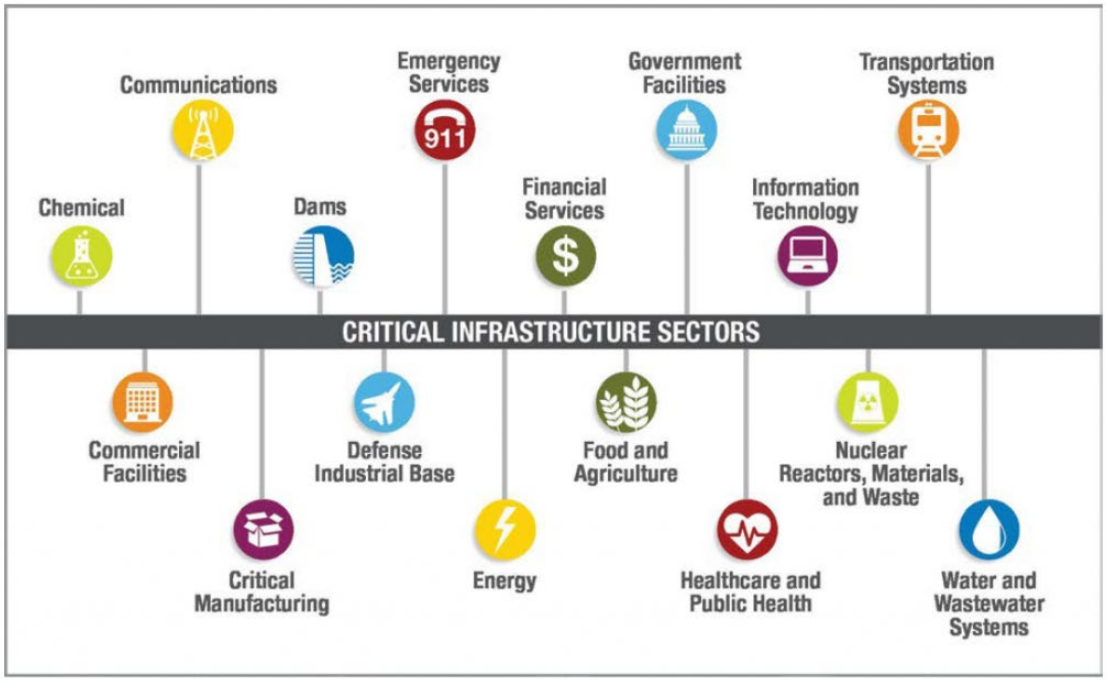


Figure 1: Critical information infrastructure of the state.

In order to achieve a high level of reliability and sustainability of IT systems, the article discusses the key stages of the developed method, including threat identification and assessment, prioritization using the pairwise comparison method (AHP), and synthesis of local and global priorities for IT security management. The described approach allows organizations to adapt existing methods to the specifics of their activities, thus ensuring more effective risk management and maintaining the stability of critical information infrastructures.

2. Literature review

Despite the importance of ensuring the IT security of CII, there is currently a lack of scientific research into the development and implementation of methods for prioritizing IT incidents, both internationally and domestically. Therefore, during the analysis, the authors investigated incident management approaches in different areas of CII.

Article [1] presents a systematic approach to risk assessment in telecommunications systems, with a particular focus on fifth-generation mobile networks (5G). The study provides an analysis of both standalone and non-standalone 5G networks, examining the migration process from 4G to 5G and identifying vulnerabilities inherent to both network generations. The main objective of the research is to classify potential threats using the STRIDE model [2] and derive a risk matrix based on the likelihood and impact of 12 threat scenarios affecting the radio access and network core. Also, the methodology [3] includes an overview of the 5G system specification, highlighting new security features compared to 4G, and analyzing residual vulnerabilities in non-standalone 5G deployments where legacy 4G protocols are still in use. To address these risks, the paper proposes a set of mitigations and security controls, offering a generic framework that can be adapted for different 5G implementations. This approach contributes to understanding security weaknesses in emerging telecommunications systems and provides a basis for developing more robust risk mitigation strategies.

Article [4] deals with the problem of managing cyber risks in information systems of critical infrastructure objects. The main objective of the study is to develop methods and models for risk assessment and management, in particular vector and integral risk models. The vector risk model uses a set of parameters to determine the level of risk to which the weighting factor is assigned,

and the total risk is calculated as the vector sum of the parameters, taking into account their weighting factors. This model makes it possible to identify the main risk components and to easily visualize and understand risks at different system levels. The integral risk model provides a comprehensive approach to risk assessment, taking into account the relationships between different parameters. In practice, these systems are used to monitor and manage cybersecurity in various critical infrastructure sectors, such as energy, transport and healthcare. The results of the study show that the proposed vector and integral risk models are effective tools for assessing and reducing cyber risks, providing reliable protection of critical infrastructure information systems from cyber threats.

Article [5] discusses mathematical methods to protect critical infrastructure from undesired events. The main objective of the study is to provide a template for analyzing and improving the protection and sustainability of critical infrastructure. Incident estimation includes models of the probability of failure of system components and the expected losses from such failures. For cyber security, vulnerability assessment methods and incident response times are considered. Sustainability metrics include the sustainability index, which measures the ability of the system to recover from failures, and the recovery target, which determines the maximum allowable system downtime. The use of these mathematical methods allows us to quantify incidents, evaluate the effectiveness of cybersecurity measures and improve cooperation between stakeholders, which confirms the practical value of the developed methods for effective management of critical infrastructure protection.

Article [6] examines the challenges organizations face in managing and responding to cybersecurity incidents through the use of Incident Response, Capability Maturity Models (CMMs). The study highlights that while maturity models such as NIST, CMMI, IRM3, and CERT-RMM provide guidelines for assessing incident response capabilities, they lack systematic methodologies for translating maturity assessment outcomes into actionable incident prioritization metrics. Key factors influencing incident prioritization include organizational preparedness, communication efficiency, and the integration of human and socio-technical elements into maturity assessments. The study also identifies gaps in existing CMMs, such as limited applicability across organizations, excessive complexity, and inadequate alignment with incident prioritization frameworks. Addressing these limitations, the research emphasizes the need for dynamic models and comprehensive guidelines that link maturity assessments with prioritization criteria, enabling organizations to refine their incident management processes in response to evolving threat landscapes and maturity levels.

Article [7] presents the development of an algorithm designed to prioritize cyber threats in the cybersecurity system, taking into account their high probability of implementation. The main objective of the study is to create an algorithm that includes a hierarchical model of a cybersecurity system with three levels: cybersecurity, threats and risks. The article discusses in detail the AHP method, which allows to evaluate and compare threat priorities. Key cyber threats such as Trojans, viruses and worms have the highest priority and require targeted mitigation measures. The results of the study confirm the practical value of the developed methodology, which helps to systematically prioritize threats and effectively manage cybersecurity.

As also explored in Articles [8, 9], recent advancements in cybersecurity research have emphasized the critical role of resilience in constructing robust IT infrastructures capable of resisting, restoring, and adapting to cyberattacks. The concept of resilience extends beyond traditional cybersecurity to address the dynamic challenges posed by evolving threats. This work highlights various techniques for enhancing resilience, including adaptive multi-agent systems, game-based simulation frameworks, and anomaly detection mechanisms. These approaches focus on ensuring continuity and stability in critical infrastructure through proactive threat detection and mitigation. For instance, methods such as adaptive distributed resilient observers and moving target defense paradigms have demonstrated effectiveness in countering sophisticated attacks like denial-of-service (DoS) and data injection. While these frameworks provide robust mechanisms for maintaining system resilience, they primarily address operational stability rather than the prioritization of IT incidents.

Thus, in Table. 1, it is proposed to compare the approaches described above that can be used to develop a method for prioritizing IT incidents according to the following criteria: ease of use (EU), focus on critical infrastructure (CI), objectivity (OB), possibility of application to IT incidents (IT).

Table 1
Comparison of approaches for prioritizing IT/security incidents

Approach / criterion	EU	CI	OB	IT
Method for risk assessment in telecommunications systems	-	+	+	-
Method for assessing cybersecurity risks of inf. OCI systems	-	+	+	-
Methodology for ranking cyberscenarios and critical objects	-	-	+	-
Incident Prioritization with Incident Response Management Maturity Capabilities	-	-	+	+
Method for assessing the priorities of a cyber security system	+	+	+	-
Resilience-based techniques for IT infrastructures	+	+	-	-

Thus, Table. 1 shows that the method developed by the authors of the study [7] is the best approach on the basis of which it is possible to develop a method for prioritizing IT incidents to ensure the security of CII, because it is easy to use, thanks to a clear hierarchical model that makes the incident assessment process understandable and accessible to users, it includes specific mechanisms for assessing and prioritizing threats specifically for CII, and the use of the hierarchical analysis method provides objectivity in the assessment of threats, as it allows threats to be systematically and transparently compared and ranked on the basis of established criteria.

Therefore, the purpose of this article is to develop and study a method for prioritizing IT incidents at CIIF.

To achieve this goal, it's necessary to solve the following tasks:

1) To analyze existing approaches to prioritizing IT incidents and identify their advantages and disadvantages.

2) To develop a method for IT incidents prioritization at the CIIF, based on the Hierarchy Analysis Method (hereafter referred to as AHP), in order to ensure the reliability and sustainability of the functioning of the CIIF.

3) To study the experimental method developed at CIIF for IT incidents prioritization.

3. Materials & methods

The method developed consists of the following steps:

Step 1. Definition of the IT Incident Management Structure of a Critical Information Infrastructure Facility.

At this step, it's necessary to create a structure for managing IT incidents, including the identification and classification of major incidents, such as problems with physical devices, software, security incidents, etc., as well as the creation of an appropriate hierarchical model.

Step 2. Evaluation of incidents and their priorities at both local and global levels in the IT security system.

At this step, it is necessary to assess the priority of each IT incident, taking into account its impact on different levels (local and global) of IT security, using the pairwise comparison method (AHP) [10-11] to assess the impact of each incident, calculating local and global threat priorities to determine the most critical ones for managing and minimizing risks.

Step 3. Comparison of elements of the IT security system at different levels to assess their impact and set priorities using the pairwise comparison method (AHP).

Step 3.1. Construction of pairwise comparison matrices

At this step, it's necessary to create a matrix of pairwise comparisons that allows to evaluate the relative importance of each criterion or alternative in the system. This step provides a framework

for further calculations. To do this, create a matrix A of size $n \times n$, where each element a_{ij} represents the ratio of importance between i and j criteria. The elements of the matrix are arranged as follows:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1i} \\ \vdots & \ddots & \vdots \\ a_{1j} & \cdots & a_{ij} \end{pmatrix} \quad (1)$$

where A – a matrix of paired comparisons, a_{ij} – elements of the matrix of paired comparisons.

Step 3.2. Normalization of paired comparison matrices

At this stage it's necessary to normalize the paired comparison matrices to ensure that the sum of all elements in each column of the matrix is 1. This allows to compare different criteria and their weights based on a single scale.

$$a'_{ij} = \frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} \quad (2)$$

where a'_{ij} normalized element of the paired comparison matrix, a_{ij} – the initial element of the matrix of paired comparisons.

After normalizing all the elements of the matrix, we obtain a normalized matrix A':

$$A' = \begin{pmatrix} a'_{11} & \dots & a'_{1i} \\ \vdots & \ddots & \vdots \\ a'_{1j} & \cdots & a'_{ij} \end{pmatrix} \quad (3)$$

where, A' - normalized pairwise comparison matrix, a'_{ij} - normalized element of the paired comparison matrix

Step 3.3. Calculation of weight vectors and Ax vector

In this step, we calculate the weight vectors W for each criterion based on a normalized matrix of paired comparisons A', which is necessary to determine the relative importance of each criterion and to further analyze their impact on the overall result.

$$W_i = \frac{1}{n} \sum_{j=1}^{n} a'_{ij} \quad (4)$$

where W_i - the weight coefficient for i-th criterion, a'_{ij} - normalized element of the paired comparison matrix, n – number of criteria.

To calculate the vector that represents the relative importance of each criterion and will be used for further calculations, we use the following formula:

$$W = \begin{pmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{pmatrix} \quad (5)$$

where W - are vectors of weights of comparison criteria.

Next, to assess the consistency of the matrix of paired comparisons and the accuracy of certain weight coefficients, which is critical for making informed decisions in the hierarchy analysis method, it is necessary to calculate the vector Ax:

$$Ax = A \times W \quad (6)$$

where A - initial matrix of paired comparisons, W - vector of weights.

So, the vector Ax helps us understand how each criterion affects the overall outcome, given the relative importance of each criterion.

Step 3.4. Calculation of the consistency index and ratio.

At this stage, it is necessary to calculate the consistency index and consistency ratio to check the consistency of the matrix of paired comparisons, which is an important step for evaluating the reliability of decisions made based on weighting factors.

To check the consistency of the matrix of paired comparisons, which ensures logical consistency and reliability of certain weighting coefficients, we calculate the largest eigenvalue:

$$\lambda_{\max} = \frac{1}{n}\sum_{i=1}^{n}\frac{(Ax)_i}{W_i} \tag{7}$$

where λ_{max} - the largest eigenvalue, n - number of criteria, Ax - elements of vectors, W_i - elements of the weight vector.

The consistency index determines how consistent the matrix of paired comparisons is:

$$CI = \frac{\lambda_{\max} - n}{n-1} \tag{8}$$

where CI -consistency index, λ_{max} - the largest eigenvalue, n - number of criteria.

$$CR = \frac{CI}{RI} \tag{9}$$

where CR – consistency ratio, CI - consistency index, RI - random consistency index, depends on the number of criteria and is determined by the table for the corresponding values n.

- If $CR < 0.1$, - the matrix of paired comparisons is considered consistent.
- If $CR \geq 0.1$, this means that the matrix has significant discrepancies and requires revising paired comparisons to achieve better consistency.

This step is crucial for ensuring the reliability and validity of decisions made, as it allows to identify and eliminate possible inconsistencies in the matrix of paired comparisons.

Step 4. Synthesis of local and global priorities for the IT security system

At this step, it is necessary to synthesize local and global priorities for the IT security system, which will determine the overall importance of each alternative solution, taking into account the weights of criteria and their priorities.

For each criterion C_i defining local priorities of alternatives A_j. Local priority of the alternative A_j by criterion C_i denoted as $W_{Ci, Aj}$.

Global priority alternatives A_j is calculated as the sum of the products of the weights of criteria and local priorities of the corresponding alternatives. The formula for calculating global priority is as follows:

$$G_{A_j} = \sum_{i=1}^{m}(W_{C_i} \times W_{C_i, A_j}) \tag{10}$$

where G_{A_j} – global priority of the alternative A_j, W_{C_i} – weight of the criterion C_i, W_{C_i, A_j} - local priority of the alternative A_j by criterion C_i, m – number of criteria.

After calculating the global priorities for each alternative, we obtain a vector of global priorities that allows us to determine the overall importance of each alternative in the IT security system and to draw informed conclusions about the selection of the highest priority alternative solutions for the IT security system. The alternative with the highest global priority is the most important and should be prioritized for implementation.

Step 5. Evaluation and adjustment of IT security priorities

At this step, it is necessary to calculate the final results of the priority assessment for the IT security system and adjust these priorities if necessary. This provides an accurate and informed definition of the most important aspects for protecting critical information infrastructure.

$$\begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{n1} & a'_{n2} & \cdots & a'_{nn} \end{pmatrix} \times \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} a'_{11}w_1 + a'_{12}w_2 + \cdots + a'_{1n}w_n \\ a'_{21}w_1 + a'_{22}w_2 + \cdots + a'_{2n}w_n \\ \vdots \\ a'_{n1}w_1 + a'_{n2}w_2 + \cdots + a'_{nn}w_n \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{pmatrix} \quad (11)$$

where a_{ij} – element of the matrix of paired comparisons, and i - line number, j – column number, a'_{ij} – normalized element of the paired comparison matrix, w_1, w_2,... w_n – weighting coefficients (priorities) defined for each criterion, Y_1, Y_2,... Y_n – results obtained after multiplying the normalized matrix by the vector of weighting coefficients.

Obtained results Y_1, Y_2,... Y_n reflect the relative importance of each criterion or alternative in the context of IT security. The analysis of these results allows us to determine which aspects require the greatest attention and resources to ensure effective protection.

Based on the results obtained and adjusted, decisions are made on the priority areas for IT incident protection. This helps to allocate resources efficiently and focus on the most important aspects of protecting critical information infrastructure.

The implementation scheme of the developed method is shown in Figure 2:

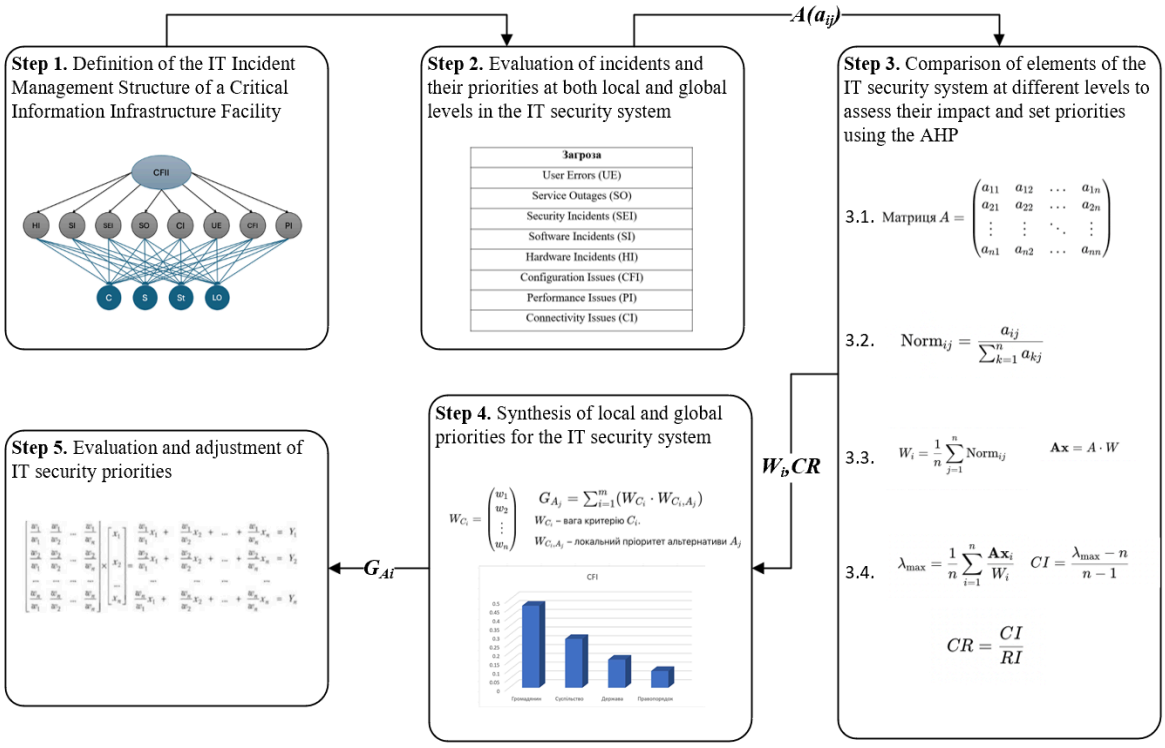


Figure 2: Implementation scheme for the prioritization of IT incidents on critical information infrastructure facilities.

4. Experimental study of the method

For an experimental study of the developed method, we will apply it to the 'Information services' sector, the 'mass media' sub-sector, which includes, for example, the provision of television and radio broadcasting services [12-13].

Step 1. In the presented model, the first level of the hierarchy has one objective: reliability and stability of the CIIF. Its priority value is assumed to be one.

Next, to form the second level of the hierarchy, it is proposed to apply the international standard ITIL [14] in accordance with the analysis carried out.

Therefore, the second level of the hierarchy includes different types of threats, classified according to ITIL:

- Hardware Incidents (HI);
- Software Incidents (SI);
- Security Incidents (SEI);
- Service Outages (SO);
- Connectivity Issues (CI);
- User Errors (UE);
- Configuration Issues (CFI);
- Performance Issues (PI).

The priorities of these threats are calculated using a matrix of pairwise comparisons of threats relative to the CIIF by comparing elements of the second level of the hierarchy with those of the first level [15].

The third level of the hierarchy covers the impact on citizens, society, the state and the rule of law. The impact of threats on these three categories is also assessed using a pairwise comparison matrix, which allows the priorities of threats for each category to be determined.

The structure of IT incident management in the CIIF [16], can be illustrated as presented in Fig. 3 (where C – citizen, S – society, St – state, LO – law and order):

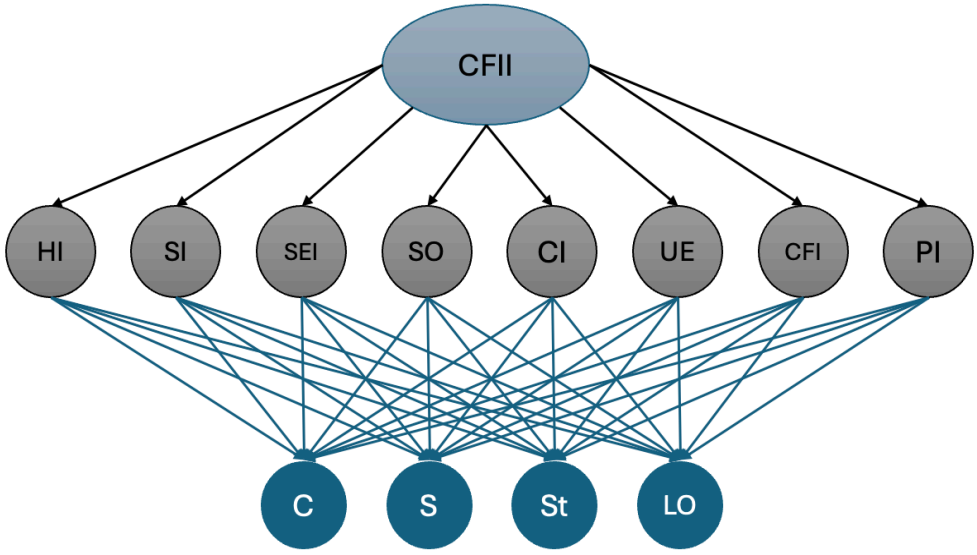


Figure 3: IT incident management structure at the Critical Information Infrastructure Facility.

Step 2. Estimates in the Saaty matrix are based on the relative importance of threats to the Reliability and Sustainability of CIIF. They take into account the potential impact of each threat on the overall level of security and functionality of the system.

Step 3. According to (1-9), we construct a matrix of pairwise comparisons, which is based on the scale of importance. The matrix has the following form (Table 2).

Global priorities show the relative strength, size and importance of each element of an IT security system [17]. Based on the calculations performed, User Errors (UE) has the highest local priority for IT security compared to other threats - 0.25. In second place is Service Outages (SO) with a global priority of 0.20. In third place is Security Incidents (SEI) with a global priority of 0.15.

Table 2
Matrix of pairwise comparisons of IT incidents on CIIF

	HI	SI	SEI	SO	CI	UE	CFI	PI
HI	1	3	2	4	5	6	7	3
SI	1/3	1	1/2	2	3	4	5	2
SEI	1/2	2	1	5	6	7	8	4
SO	1/4	1/2	1/5	1	3	4	2	1/2
CI	1/5	1/3	1/6	1/3	1	2	1/2	1/3
UE	1/6	1/4	1/7	1/4	1/2	1	3	1/2
CFI	1/7	1/5	1/8	1/2	2	1/3	1	1/4
PI	1/3	1/2	1/4	2	3	2	4	1

Software Incidents (SI) and Hardware Incidents (HI) are also important, with global priorities of 0.12 and 0.10 respectively. Configuration Issues (CFI) also deserve attention with a global priority of 0.08. For other threats, the global priorities are as follows Performance Issues (PI) – 0.06, Connectivity Issues (CI) – 0.04.

The global priority values obtained allow us to determine which threats are most critical to ensuring the reliability and sustainability of critical information infrastructures. Focusing on the highest priority threats helps to effectively manage IT security and minimize risks to citizens, society, government and public order [18] (Table 3).

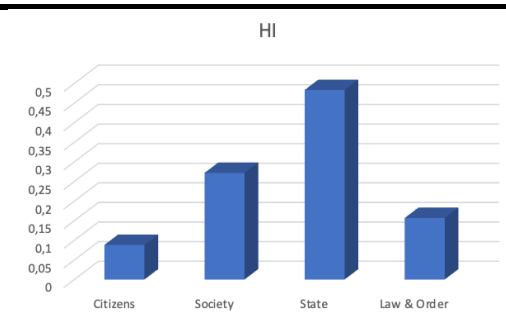
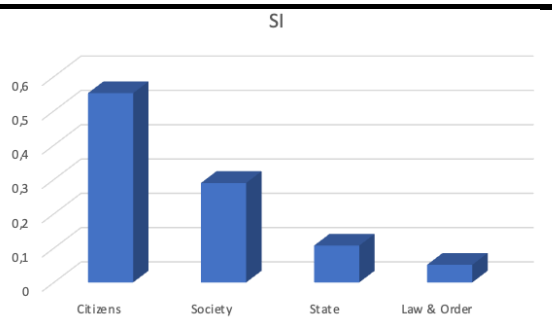
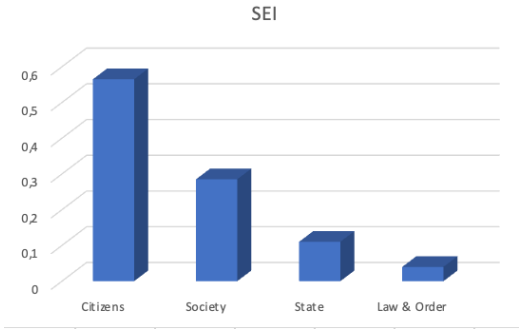
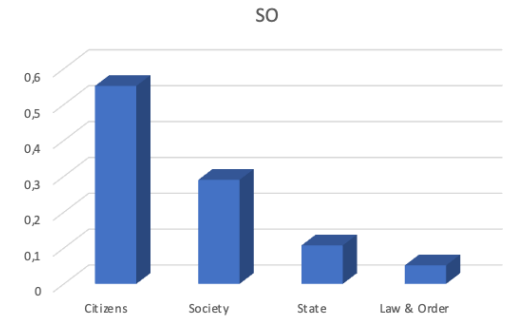
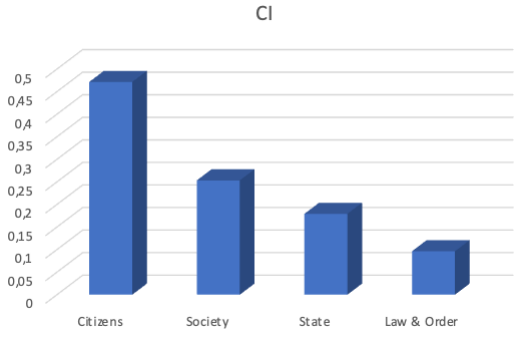
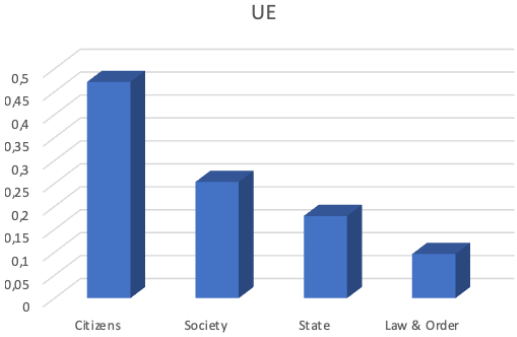
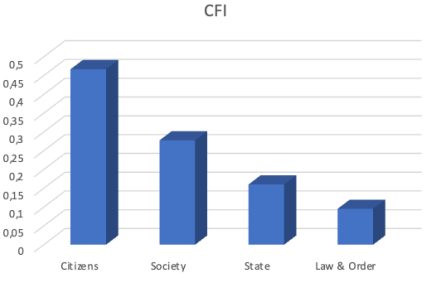
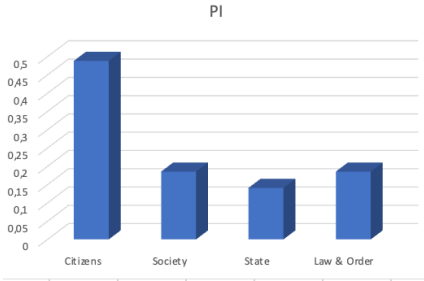
Table 3
Importance of global IT incident priorities CIIF

Threat	Global priority
UE	0.25
SO	0.20
SEI	0.15
SI	0.12
HI	0.10
CFI	0.08
PI	0.06
CI	0.04

The Paired Comparison Matrix allows to determine which of the threats are most critical to ensuring IT security. This helps to focus resources and efforts on the most important issues, minimizing the impact of potential threats on the system [19].

Step 4. The main task of this stage is to determine the local priorities of risks of objects of protection through the intermediate second level – threats, using pairwise comparison matrices for these threats, according to (10). Thus, using a group of pairwise comparison matrices for the above threats, we consistently form a set of local priorities of the third level regarding the risks of the individual, society and the state. The values of local priorities of risks of security objects for these threats are shown in Table. 4, taking into account [20].

Table 4
Importance of local priorities for IT incidents in CIIF

Hardware Incidents (HI) - problems with physical devices	Software Incidents (SI) - software problems
	
Security Incidents (SEI)	Service Outages (SO)
	
Connectivity Issues (CI)	User Errors (UE)
	
Configuration Issues (CFI)	Performance Issues (PI)
	

Step 5. Together with the matrices of the paired comparisons, we obtained measures of the estimates of the deviation from consistency, which are summarized in Table. 5, according to (11).

Therefore, it can be concluded that according to the conducted experiment, hardware incidents (HI) have the highest priority for the state (0.483), which emphasizes the need to support the physical infrastructure, software incidents (SI) and security incidents (SEI) are the most critical for citizens (0.552 and 0. 565 respectively), requiring attention to reliable software and cyber security; Service Outages (SO) have a significant impact on citizens and society, but less on the state and law and order; Performance

Issues (PI), User Errors (UE) and Configuration Issues (CFI) have a significant impact on citizens, requiring improvements in IT services and user training.

Table 5
Measures of deviation from consistency estimates

Levels	Priorities	n	Λmax	CR
1	RSCIP	8	8.57373	0.05812
2	HI	4	4.01452	0.005
2	SI	4	4.17244	0.05748
2	SEI	4	4.27255	0.09085
2	SO	4	4.17244	0.05748
2	CI	4	4.12326	0.04109
2	UE	4	4.03098	0.01033
2	CFI	4	4.03098	0.01033
2	PI	4	4.13199	0.04400

5. Conclusion

In conclusion, this study successfully achieved its key objectives by thoroughly analyzing international standards and practices such as ITIL, COBIT, ISO/IEC 20000, and the NIST Cybersecurity Framework. Through this analysis, the strengths and weaknesses of these approaches were identified, enabling the selection of the most relevant elements for the development of a new methodology. A notable finding is the limited scientific research available on IT incident prioritization, which highlights the relevance of this study. The ITIL framework, in particular, stood out for its structured, flexible, and service-oriented approach.

This paper develops a method that integrates international best practices with the Analytic Hierarchy Process (AHP). It effectively addresses the identification, assessment and prioritization of threats, incorporating both local and global priorities to improve IT security management. The approach allows for the consideration of different aspects of security, including their impact on citizens, society, the state and the rule of law, making it adaptable to different security contexts.

The practical value of the method was confirmed through experimental testing on real-world data. The results underscored its capacity to systematically prioritize IT threats, demonstrating that hardware incidents are of highest priority for state-level protection, while software and security incidents are of greater concern for citizens. These insights emphasize the importance of maintaining a resilient physical IT infrastructure and focusing on the development of reliable IT security software. Overall, this study contributes a significant advancement in IT incident management, providing a practical tool for improving IT security practices across different sectors.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Holtrup, G., Lacube, W., Percia David, D., Mermoud, A., Bovet, G., & Lenders, V. (2021). 5G system security analysis. arXiv preprint arXiv:2108.08700. https://arxiv.org/abs/2108.08700

[2] Holtrup, G., et al. (2023). Modeling 5G threat scenarios for critical infrastructure protection. In Proceedings of the 15th International Conference on Cyber Conflict: Meeting Reality (pp. 161–180). doi:10.23919/CyCon58705.2023.10
[3] R. Khan, et al., STRIDE-based Threat Modeling for Cyber-Physical Systems, IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe) (2017) 1–6.
[4] V.V. Mokhor, G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine, S.F. Honchar, & G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine. (2019). Evaluation of risks of cyber security of information systems of objects of critical infrastructure. Elektronnoe Modelirovanie, 41(6), 65–76.
[5] D. Jablanski. (2023). Method for Determining the State of Protection of Critical Information Infrastructure Objects from IT Risks. Scientific Research on Cybersecurity. URL: https://www.researchcybersecurity.com/state-protection-method/ (accessed: 01.06.2024).
[6] A. Gulay, & L. Maglaras. (2024). Alignment of Cybersecurity Incident Prioritisation with Incident Response Management Maturity Capabilities. arXiv preprint, arXiv:2410.02259. https://arxiv.org/pdf/2410.02259.
[7] A.B. Kaczynski, D.I. Varycheva, & S.V. Sviridenko. (2016). Effective IT Incident Management in critical information infrastructure. Information and Law, No. 2(17), pp. 114–126.
[8] S. Lysenko, D. Sokalskyi, & I. Mykhasko. (2022). Methods for cyberattacks detection in computer networks as a means of resilient IT-infrastructure construction: State-of-art. Computer Systems and Information Technologies, (3), 31–35. Khmelnytskyi National University. doi:10.31891/csit-2021-5-4
[9] S. Lysenko, & A. Kondratyuk. (2020). Technique for the risk assessing of the cyber-physical systems' information security based on the vulnerabilities' interconnect. Computer Systems and Information Technologies, (2), 54–57.
[10] T.L. Saaty, & L.G. Vargas. (2020). Applications in decision-making: Analytic hierarchy process—AHP. In Decision Making with the Analytic Hierarchy Process (pp. 129–152). Springer. doi:10.1007/978-3-030-39891-0_6.
[11] A.U. Khan, Y. Ali. (2020). Analytical Hierarchy Process (AHP) and Analytic Network Process Methods and Their Applications: A Twenty-Year Review from 2000–2019. International Journal of the Analytic Hierarchy Process, 12(3).
[12] Law of Ukraine on Critical Infrastructure. The Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed: 01.06.2024).
[13] Cabinet Of Ministers of Ukraine. (2020). Certain issues of critical infrastructure facilities: Resolution No. 1109 of October 9, 2020. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (accessed: 01.06.2024).
[14] PeopleCert. (2023). ITIL 4 Management Practices 2023. Retrieved from https://www.peoplecert.org
[15] S. Seo, D. Kim. (2020). Study on Inside Threats Based on Analytic Hierarchy Process. Symmetry, 12(8):1255. doi:10.3390/sym12081255
[16] S. Gnatyuk, V. Sydorenko, A. Polozhentsev, V. Sokolov. (2024). Method for managing IT incidents in critical information infrastructure facilities. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024), 3826, 326–333. https://ceur-ws.org/Vol-3826/short24.pdf
[17] S. Lipovetsky. (2021). Understanding the Analytic Hierarchy Process: by Konrad Kulakowski, Boca Raton, FL: Chapman and Hall/CRC, Taylor & Francis Group, 2021, 262 pp.
[18] M.I. Tariq, S. Ahmed, N.A. Memon, S. Tayyaba, M.W. Ashraf, M. Nazir, A. Hussain, V.E. Balas, & M.M. Balas. (2020). Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. Sensors, 20(5):1310.
[19] I. Canco, D. Kruja, & T. Iancu. (2021). AHP, a Reliable Method for Quality Decision Making: A Case Study in Business. Sustainability, 13(24):13932. doi:10.3390/su132413932
[20] ISACA. COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association (ISACA), Available at ISACA (2019).