Method for managing IT incidents in critical information infrastructure facilities

Sergiy Gnatyuk[1,†], Viktoria Sydorenko[1,†], Artem Polozhentsev[1,*,†] and Volodymyr Sokolov[2,†]

[1] National Aviation University, 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine
[2] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudryavska str., 04053 Kyiv, Ukraine

Abstract

Protecting Critical Information Infrastructure (CII) is essential in today's digitized world, where the growing number of cyber threats poses significant risks to national security, the economy, and public safety. CII includes vital sectors such as energy, transport, finance, and healthcare. Disruptions to these systems can have serious consequences, requiring effective identification, assessment, and management of IT threats. Despite the importance of IT security to CII, existing methods for managing IT threats remain underdeveloped. This paper presents a novel method for IT incident management in CII, combining the STRIDE model and TODIM multi-criteria decision-making. The method is designed to identify, assess, and prioritize threats, taking into account the criticality of CII objects at different levels. Through experimental validation, this method demonstrates its ability to improve CII security by providing a systematic approach to prioritizing and managing IT threats. This study provides a practical solution for improving CII protection against evolving cyber risks.

Keywords

critical infrastructure, critical information infrastructure facilities, cybersecurity, incident management, STRIDE, TODIM

1. Introduction

Protecting critical infrastructure facilities is one of the most important tasks for organizations and governments in today's digitized world. The growing number of cyber threats associated with the development of information technologies has increased the need to implement reliable security measures. Critical Information Infrastructure (CII) includes systems and networks that are vital to the functioning of society in the areas of energy, transport, finance, communications, and healthcare [1, 2].

The failure or compromise of such components can have serious consequences for national security, the economy and public welfare. To effectively protect CII, it is necessary to properly identify, assess and manage IT threats, especially in the context of limited defense resources. This highlights the important scientific task of developing and implementing an effective method for managing IT incidents in CII facilities (CIIF).

Despite the importance of ensuring the IT security of CII, there is currently a lack of scientific research on the development and implementation of IT threat management methodologies, both internationally and domestically (Fig. 1) [2]. However, during the analysis, the authors examined threat management approaches in various areas of CII.

Figure 1: The process of IT Incident Management

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
s.gnatyuk@nau.edu.ua (S. Gnatyuk);
v.sydorenko@ukr.net (V. Sydorenko);
artem.polozhentsev@nau.edu.ua (A. Polozhentsev);
v.sokolov@kubg.edu.ua (V. Sokolov)

0000-0003-4992-0564 (S. Gnatyuk);
0000-0002-5910-0837 (V. Sydorenko);
0000-0003-0139-0752 (A. Polozhentsev);
0000-0002-9349-7946 (V. Sokolov)

2. Literature review

In studies [4–6], the authors developed an algorithm for assessing cybersecurity threats to Learning Management Systems (LMS). By combining the STRIDE model with the TODIM multi-criteria decision support method and providing fuzzy sets, they evaluated LMS platforms, namely Moodle, Atutor, and Ilias. The study involved three cyber security experts who assessed security using linguistic variables, demonstrating the effectiveness of the algorithm in detecting and ranking cyber threats in LMS environments. This study is particularly relevant for cybersecurity professionals responsible for the security of educational technologies and provides a methodology that can be used to strengthen the security of LMSs.

In article [7], the authors explore the application of the STRIDE model for assessing cybersecurity threats in the critical infrastructure transportation industry. The article highlights how the integration of STRIDE with the Hazard Analysis and Risk Assessment (HARA) method, called the SAHARA approach, provides a comprehensive framework for assessing security risks in the early stages of development. This combined approach enables security threats to be identified and categorized, ensuring that appropriate countermeasures are implemented to protect automotive systems from advanced cyber-attacks, thereby supporting consistent and secure product development throughout the lifecycle.

The study [8] addresses the issues of improving security and privacy, as well as the vulnerability of 5G networks, with a focus on CI protection. Despite advances over previous generations, 5G networks still have technical security weaknesses that can be exploited. The paper uses the STRIDE threat classification model to identify and analyze eleven threat scenarios in the 5G ecosystem, highlighting the importance of implementing robust security measures to mitigate these risks.

The study [9] described that critical infrastructure and industrial control systems are complex cyber-physical systems. Ensuring the reliable operation of such systems requires comprehensive threat modeling during system design and validation. Also, the following articles [10, 11] present a comprehensive threat modeling methodology using STRIDE, a systematic approach to ensuring system security at the component level. The methodology is applied to a real-world testbed of a synchronous isolated system based on a synchro phasor. The study identifies the types of threats that can occur in each component of the system and how vulnerabilities in one component can compromise the security of the whole system. STRIDE has proven to be a simple and effective threat modeling methodology that simplifies the task for security analysts.

It has been found that there is currently no implemented method that would allow effective management of IT threats for CII. Therefore, the development of such a method is extremely necessary to ensure a more reliable protection against potential IT threats and to increase the level of security of Critical Information Systems (CIS). Thus, the purpose of this paper is to develop and experimentally study a method for managing IT threats for CII.

3. Analysis of international methodologies for IT threat modeling

Since the preliminary analysis of existing studies on the identification, assessment, and management of IT threats did not allow the identification of a formalized approach, the authors decided to develop their method for the management of IT threats for CIIF.

This requires conducting additional analysis of the effectiveness of international practices and threat modeling methodologies according to the following criteria Ease of Use (EU)—an assessment of the ease of use of the method in practice, Comprehensiveness (CM)—the extent to which the method covers all aspects of IT threat management, Integration with other systems (IS)—the extent to which the method allows integration with other security and management systems, CI focus (CI)—if the method takes into account the specifics of the ICS, Objectivity (OB)—the extent to which the method reduces subjectivity in the decision-making process, Time to Use (ET)—the time required to apply the method.

The STRIDE threat classification methodology [12] is a popular security threat analysis tool developed by Microsoft. The acronym stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. This methodology helps identify vulnerabilities in information systems, allowing developers and security professionals to take proactive measures to eliminate them. The benefits of STRIDE include its comprehensiveness in covering a wide range of threats, its clarity and structure with clearly defined threat categories, and its ability to integrate with other security methodologies and tools. However, in-depth knowledge of IT security is required to use this methodology effectively.

The National Institute of Standards and Technology's NIST SP 800-30 [13] standard provides a comprehensive approach to identifying, assessing, and managing risk while taking into account the specifics of an organization's processes and assets. The key benefits of NIST SP 800-30 are a comprehensive approach that covers all stages of risk management, from threat identification to response strategy development, and the recognition of the standard in many organizations. However, implementation of this standard can require significant resources and time and can be difficult for small organizations due to limited resources.

The international standard ISO/IEC 27005 [14] provides guidance on information security risk management and provides a structured approach to identifying, assessing, and managing risks. The advantages of ISO/IEC 27005 are its consistency with other ISO standards, which allows risk management to be integrated into an organization's overall management system and its structured approach. Disadvantages include the resources required to implement the standard and its complexity for small organizations, which may find it difficult to implement.

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology [15, 16] is designed to assess and manage information security risks by focusing on an organization's critical assets. It allows you to identify and protect the organization's most important assets and

perform a self-assessment using internal resources. However, OCTAVE requires significant involvement of staff at all levels of the organization and can be difficult to coordinate in large organizations.

The Control Objectives for Information and Related Technologies (COBIT) framework [17] is an IT governance framework that includes risk management aspects and ensures the integration of IT with business objectives. The benefits of COBIT include integration with business processes, which helps to align IT management with the overall business objectives of the organization, and a comprehensive approach that covers all aspects of IT management. However, implementing a framework can be resource-intensive, and small organizations may face difficulties due to insufficient resources for full implementation.

Table 1 compares approaches to prioritize IT threats according to the following criteria: EU is ease of use, CM is complexity, IS is integration with other systems, CI is focus on CI, OB is objectivity, and ET is time to application.

Table 1
IT Threat prioritization approaches

	EU	CM	IS	CI	OB	ET
STRIDE	+	+	+	-	+	+
NIST SP 800-30	-	+	-	+	-	-
ISO/IEC 27005	-	+	+	-	-	+
OCTAVE	-	+	-	-	+	+
COBIT	-	+	-	+	-	+

Based on the analysis of these criteria, the STRIDE approach is a highly effective and comprehensive approach to identifying IT threats. Its clear structure, ability to integrate with other methods, and emphasis on different types of threats make it an ideal tool for improving the security of information systems. STRIDE enables organizations not only to identify threats, but also to assess their criticality, develop appropriate protection methods, and ensure a comprehensive approach to risk management.

4. Analysis of decision-making methods

To prioritize IT threats, it is necessary to consider decision-making methodologies—approaches that help to analyze complex problems and select the best course of action, taking into account various possible alternatives. These methods include a range of techniques and tools to help evaluate different parameters and weight criteria to arrive at an objective, balanced decision [18].

The Analytic Hierarchical Process (AHP) [19], developed by Thomas Saaty in the 1980s, helps to break down a decision problem into a hierarchy of smaller components, including objectives, criteria, sub-criteria, and alternatives. By using mathematical principles to evaluate the importance of criteria and select the best option [20], AHP is intuitive and able to combine quantitative and qualitative criteria. However, the method can be subject to subjectivity in weighting and requires a significant amount of time and data for analysis.

TODIM [21] is a multicriteria decision analysis method based on the prospect theory of Daniel Kahneman and Amos Tversky. The method uses the principles of utility theory to model the preferences of a decision-maker under conditions of uncertainty and associated risks. The main steps of the method include identifying criteria and alternatives, evaluating alternatives for each criterion, assigning weights to the criteria, calculating the dominance of each alternative over the others based on the weights, using a prospective value function to account for risk attitudes, summing the prospective values to obtain a utility score, and selecting the alternative with the highest utility score. The method incorporates risk and uncertainty and is intuitive, but requires complex calculations and subjective judgement of weights.

The Technique of Options Selection and Review (TOPSIS) [22] determines the optimal alternative by selecting the alternative closest to the ideal point. The method takes into account the distances to the ideal (best) and anti-ideal (worst) solutions. TOPSIS is easy to implement and clearly identifies the best alternative, but it is sensitive to the relative values of the criteria and can be influenced by incorrect scaling.

Table 2 shows a comparison of the decision methods that can be used to assess IT threats. The analysis is based on the following criteria CI—CI applicability, FL—flexibility, SC—scalability, CR—risk and uncertainty consideration, EU—ease of use.

Table 2
Analysis of multi-criteria decision-making methods

	CI	FL	SC	CR	EU
AHP	+	+	+	-	+
TODIM	+	+	+	+	+
TOPSIS	-	-	+	-	+

Based on the analysis of these criteria, the TODIM approach is the most suitable for use in the area of CII. The method effectively takes into account risk and uncertainty, which is an important aspect of CII, and demonstrates a high degree of flexibility in considering different criteria.

5. Method for managing IT incidents in critical information infrastructure facilities

The method developed by the authors consists of 7 stages, each of which is described in more detail below.

Step 1: Identification of IT threats to CII.

The identification of IT threats is an important stage in the process of managing IT threats to CII. The purpose of this stage is to identify potential threats that could affect the normal operation of critical information systems. At this stage you can select threats according to various international approaches such as STRIDE, NIST SP 800-30, ISO/IEC 27005, OCTAVE, or COBIT, depending on the characteristics of the CII. The set of potential IT threats is called the U_i set:

$$U_i = \{U_1, U_2, \ldots, U_n\} \quad (1)$$

where U_i is a set of identified potential IT threats, $U_1, U_2, \ldots, U_n$ are potential IT threats.

Step 2: Define criteria for evaluating IT threats to CII.

For each threat U_i and each criterion k, let's introduce a set of evaluation criteria K:

$$K = \{k_1, k_2, \ldots, k_m\} \quad (2)$$

where K is a set of criteria against which IT threats are assessed, $k_1, k_2, \ldots, k_m$ —are specific assessment criteria.

Each potential threat U_i should be assessed against criteria K to determine its impact and priority.

Step 3. Collect and normalize data on IT threats to CII.

At this step, it is necessary to collect, assess, and normalize data on IT threats to CII. This process ensures an objective and balanced approach to threat assessment. Each threat Ui is evaluated according to the defined criteria K. For example, experts may evaluate the likelihood of a threat occurring, the potential damage, the complexity of implementation, etc. Each evaluation criterion k has a corresponding weight. Each evaluation criterion k has a corresponding weighting factor w_k, where the sum of all coefficients is 1:

$$\sum_{k=1}^{K} \omega_k = 1, \quad (3)$$

where K is the total number of criteria, w_k is the weighting factor for criterion k.

Step 4. Determine the weight of the CII IT threat criteria.

Determining the weighting factors for each IT threat assessment criterion is an important step that allows you to consider the relative importance of different aspects of the threat. This helps to ensure objectivity and balance in the IT threat assessment process. Each criterion is rated on a predetermined scale. In their paper, the authors suggest using a scale of 1 to 5, with 5 being the highest probability, damage, or complexity and 1 being the lowest. This scale is intuitive and easy to use, which simplifies the assessment process for experts. For each criterion, we calculate the average of the geometric scores provided by the experts as follows:

$$k = \left(\prod_{j=1}^{n} vk_j\right)^{1/n} \quad (4)$$

where vk_j is the evaluation of criterion k by expert j, n is the number of experts.

Next, at this stage, a vector of weighting coefficients should be created and calculated by normalizing the average geometric scores:

$$W = (W_1, W_2, \ldots, W_n)^T \quad (5)$$

where W_i is the weighting factor for each criterion i.

$$W_{jr} = \frac{W_j}{\sum_{r=1}^{n} W_r} \quad (6)$$

where W_j is the geometric mean for criterion j, W_r is the sum of geometric means for all criteria.

Step 5. Perform pairwise comparisons of alternative threats to CII.

In a pairwise comparison, the dominance of each threat over the others is determined using a prospective value function that takes into account the weights of the criteria and the ratings of the alternatives for each criterion.

$$Dom(U_i, U_j, k) = \omega_k \times \left(\frac{vU_i, k - vU_j, k}{1 + a \times vU_j, k} \right), \quad (7)$$

where U_i and U_j are the threats to be compared; k is the criterion by which the comparison is made; W_k is the weight of the criterion; vU_i,k and vU_j,k are the threat ratings by the criterion; α is a parameter reflecting the attitude toward risk.

Consideration of CI Categories

According to the Law of Ukraine "On Critical Infrastructure" [23], in particular, Article 10 "Categorization of CI", CI are divided into categories depending on their importance and potential impact on the security of the state or region. The introduction of the criticality variable C allows the integration of these categories as additional criteria into the multicriteria analysis according to the developed method, which increases the accuracy of the assessment of the potential impact of threats on different levels of criticality.

The criticality variable C takes values from 1 to 4, reflecting the level of criticality of the infrastructure object: Category I (C=1): Critical facilities of national importance. Disruption of their functioning can cause a national crisis. Category II (C=2): Critical facilities whose disruption could cause a regional crisis. Category III (C=3): Critical facilities whose disruption could cause a local crisis. Category IV (C=4): Essential facilities whose disruption could cause a local crisis.

Step 6. Obtain an integrative assessment of alternative IT threats to CII.

At this stage, it is necessary to calculate the value of the future value to obtain a utility score for each threat.

$$Score(U_i) = \sum_{j \neq i} \sum_{k=1}^{K} Dom(U_i, U_j, k) \quad (8)$$

where $Score(U_i)$ is the integrative utility score for threat a, U_i and U_j are the threats being compared, k is the criterion by which the comparison is made, and $Dom(U_i, U_j,k)$ is the prospective value function for determining the dominance of each threat over the others.

Step 7. Prioritize and make decisions about IT threats to CII.

At this step, it is necessary to prioritize the identified IT threats and make appropriate decisions on actions to eliminate or minimize them. This should be done by calculating the relative importance of each threat and ranking them based on the estimates obtained.

$$p(U_i) = \frac{Score(U_i)}{\sum_{i=1}^{n} Score(U_i)} \quad (9)$$

where $p(U_i)$ is the relative importance of each potential IT threat, and *Score(Ui)* is an integrative assessment of the utility for threat *a*.

Next, the IT threats should be ranked from highest to lowest. Threats with the highest scores are the most critical and require priority response. Based on the results of the threat ranking, decisions are made on the necessary measures to eliminate or minimize each threat. Measures may be technical, organizational, or procedural.

6. Experimental Study of the Method of IT Incident Management in CII

Let's apply this method to the CII sector "Digital Technologies", namely the sub-sector "Electronic Communications", according to [24–26].

Step 1: Identification of IT threats to CII

According to the STRIDE methodology, and analyzed studies [10–12, 27], the following IT threats were identified to improve the IT security of CII:

- Spoofing. The threat of interfering with the system by using false data or identity to gain unauthorized access. For example, a hacker could use forged certificates to gain access to an energy company's network.
- Tampering. Making unauthorized changes to data or system configurations. This can include changing logical control commands to OCI, which can lead to physical failures.
- Repudiation. The inability to trace or prove that a user's actions were performed. For example, the lack of audit logs can allow attackers to deny that malicious actions were taken on a water management network.
- Information disclosure. Unauthorized access to sensitive information. For example, leakage of classified information from government databases can have serious national security implications.
- Denial of Service (DoS). Attacks are designed to prevent the normal operation of a system, particularly by overloading resources. For example, a DoS attack on transportation infrastructure management systems could bring all traffic to a halt.
- Elevation of Privilege. A threat that allows an attacker to gain greater privileges than they have and use them to gain inappropriate access to systems or data. For example, an attacker could gain administrator privileges in health management systems and abuse those privileges.

Step 2: Define Criteria for Assessing IT Threats to CII

This stage involves a detailed definition of the criteria for assessing each IT threat to CII. The evaluation criteria are key parameters that allow a comprehensive analysis of threats and prioritization for further management. For each IT threat U_i and each criterion k, it is proposed to apply the following parameters according to (1, 2):

- Threat Probability (TP): An estimate of the likelihood that a specific IT threat will occur. This allows you to determine how often the threat can be expected to occur.
- Potential damage from the threat (P): An estimate of the potential damage that could be caused to CII if the threat is realized. Both financial loss and potential impact on the security and operation of the system are considered.
- Threat complexity (C): An assessment of the technical difficulty of implementing the threat by attackers. This includes an analysis of the knowledge, tools and resources required to carry out the attack.

Properly defining the criteria allows for a deeper and more comprehensive threat analysis, increasing the effectiveness of risk management and CII protection. The optimal number of criteria for assessing IT threats to CII depends on the complexity of the problem and the data available. According to [14, 28], the use of 3–7 criteria is standard practice to ensure a comprehensive analysis. This allows different aspects of threats and risks to be considered and provides a balanced approach to CII protection decision-making.

Step 3. Collect and normalize IT threat data for CII

This stage involves a detailed process of collecting, assessing, and normalizing IT threat data for CII. An important part of this phase is to determine the weighting factors for each assessment criterion, which will allow for an objective and balanced approach to threat assessment.

The weighting factors for assessing IT threats to CII should be determined based on their relative importance. The likelihood of a threat occurring was given a high coefficient because it has a significant impact on the risk of the threat being realized. The potential damage from the threat has the highest coefficient because the potential losses from the threat are critical to the functioning of the CII. The complexity of the threat realization received a lower coefficient due to its relatively lower importance compared to other criteria, but it is still important for assessing the technical aspects of protection [29].

By the previous steps, each evaluation criterion *k* has a corresponding weighting factor w_k, where the sum of all coefficients is 1 according to (3), as shown in Table 3 below:

Table 3
Table of IT threat assessment criteria

Criterion, k	Description	Weighting index, w_k
TP	The likelihood that the threat may materialize	0.4
P	Potential losses or damage that may be caused if the threat is realized	0.5
C	complexity of the technical implementation of the threat	0.1

Step 4. Determine the weight of the CII IT threat criteria.

A rating scale from 1 to 5 is used to further define the criteria, with 1 being the lowest level (low probability, minimal damage, low complexity) and 5 being the highest level (high probability, maximum damage, high complexity). These scores are then used to compare threats in pairs to determine their relative importance and criticality to CII. Based on these criteria, an integrative assessment and prioritization of threats is performed, which is the basis for management decisions on security and protection measures [30].

Therefore, according to (4, 5, 6), we will apply the above scale to evaluate the alternatives according to the specified criteria. Below is a table of alternatives evaluated by criteria (Table 4).

Table 4
Criteria-based alternatives evaluation

Threat	TP	P	C
Spoofing	2	4	3
Tampering	3	5	2
Repudiation	1	3	4
Information disclosure	4	5	2
Denial of Service	5	5	1
Elevation of Privilege	2	4	3

The values are then used to compare threats in pairs to determine their relative importance and criticality to the CII. This comparison helps determine which threats are the most serious and require priority protection measures. An integrative assessment and prioritization of threats based on the results is then performed, providing the basis for management decisions on security and protection measures for the CII.

Step 5. Perform pairwise comparisons of alternative threats to CII.

According to (7), in this step, the method of pairwise comparisons is used to determine the dominance of each threat over the others. This method allows the relative importance and criticality of each threat to be assessed by comparing them according to certain criteria. The application of the prospective value function takes into account the weights of the criteria and the scores of the alternatives for each criterion.

- Data Entry: After all threats have been evaluated according to the criteria defined in the previous step, the data is entered into specially developed software to perform the calculations.
- Determine the α parameter: The α parameter is set to account for risk attitudes. The value of α can take on any value depending on the specific situation but is usually between 0 and 1. Low values of α reduce the impact of the risk, while high values increase its significance.
- Pairwise comparison of threats: Each threat is compared to the others across all criteria. For each pair of threats, a dominance value is calculated using the formula above.
- Overall Dominance Calculation: After all threat pairs are compared for each criterion, a total dominance value is calculated for each threat. This value is used to rank and prioritize threats.

Thus, this phase provides a detailed and objective analysis of the threats, providing a reliable basis for management decisions regarding CII protection.

Step 6. Obtain an integrative assessment of alternative IT threats to CII.

To automate this process and increase the accuracy of the calculations, the developed IT Threat Management Methodology software application is used at this stage. This application integrates all the data, pairwise comparisons, and weighting factors to calculate the final utility scores. According to (8), we summarize the prospective values to obtain a utility score for each threat. Using the developed IT threat management software, the following result was obtained (Fig. 2).

0.02	0.5	0.2	0.3	Dom	Rank
S	2	4	3	2.406	3
T	3	5	2	-1.564	5
R	1	3	4	5.789	2
I	4	5	2	-1.004	4
D	5	5	1	9.145	1
E	2	4	3	-13.338	6

Figure 2: Result of using IT threat management software

Step 7. Prioritize and make decisions about IT threats to CII.

According to (9) and based on the analysis performed by the developed method, the threats were ranked according to their total dominance. Let us present the prioritization of threats, where threats with higher values of total dominance should be addressed as the most critical (Table 5):

Table 5
IT threat priorities for the CII sub-sector "Electronic communications"

Threat	Dom level	Priority
Spoofing	9.145	The highest
Tampering	5.789	High
Repudiation	2.406	Average
Information disclosure	−1.004	Medium
Denial of Service	−1.564	Low
Elevation of Privilege	−2.338	Low

Fig. 3 shows the results of the IT threat assessment for the CII sub-sector "electronic communications", according to Table 5.

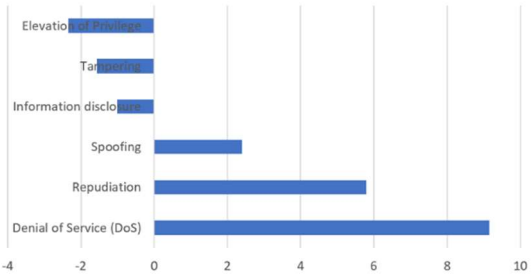

Figure 3: Results of the IT threat assessment

Thus, according to the results obtained with the help of the special software developed, the following recommendations have been made about IT threats [31]:

- Denial of Service (DoS): The most critical threat that needs to be addressed as a matter of priority is to reduce the risk of denial of service, which can lead to significant disruptions in CI operations. It is recommended to implement resilient systems against DoS attacks using load balancing and network-level protection techniques.
- Repudiation: Requires improved logging and auditing systems to ensure accountability and transparency of operations. Reliable mechanisms for logging and retaining user activity logs should be implemented, as well as regular audits to detect and prevent attempts to deny activity.
- Spoofing: It is necessary to strengthen authentication procedures and improve identification and verification systems to prevent unauthorized access. The use of multi-factor authentication and advanced user verification methods is recommended.
- Information disclosure: Data protection mechanisms should be strengthened, especially for sensitive information, to prevent unauthorized disclosure. Data encryption should be implemented both in transit and at rest, as well as monitoring and leak detection systems.
- Tampering: Protection should be provided against unauthorized interference with data, although this threat is not as critical as the others. Data integrity controls should be used and systems should be implemented to detect changes to data [32].
- Elevation of privilege: Although this is a serious threat, it has the lowest dominance score and can be addressed after more pressing issues. To prevent privilege escalation, it is necessary to implement the principle of least privilege, regularly review access rights, and use tools to detect and block attempts to elevate user privileges.

7. Conclusions

In conclusion, this paper has analyzed the existing methods of IT threat management at CIIF. It was found that the problem of IT threat management at CIIF has not been sufficiently studied, and the existing methods do not provide a complete solution to the problems of IT threat assessment for such facilities. Therefore, the authors have developed a new method for managing IT threats at CIIF by synthesizing the multi-criteria decision-making method TODIM and the threat model STRIDE, which allows them to effectively identify, assess, and prioritize threats, taking into account their probability, potential damage, and complexity of implementation. The developed method consists of the following stages: identification of threats, determination of evaluation criteria, data normalization, determination of criteria weights, pairwise comparison of alternative threats, obtaining an integrative evaluation, prioritization, and decision-making, and provides an effective approach to improving the level of CII security.

An experimental study of the developed method, conducted for the CII sub-sector "electronic communications", showed that the method effectively contributes to the management of IT threats by prioritizing these threats. This ensures a high level of CII security and allows the optimization of security measures to respond effectively to potential IT threats.

In addition, thanks to the special software developed, it was found that for the CII sub-sector "electronic communications", the threat of denial of service has the highest level of criticality. This indicates the need for priority action to neutralize it. In general, the prioritization of IT threats in the process of ensuring the protection of CII can ensure the effective allocation of resources and the application of the necessary measures to prevent potential attacks.

Further research will aim to optimize the method, in particular by:

- Determine normalized coefficients for selected threat criteria.
- Extend the recommendations for IT incident management according to the results obtained.
- Improving the method to allow the assessment of combined threats.

References

[1] O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 29–43.

[2] A. Zahynei, et al., Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 432–439.

[3] ITIL Incident Management: The Complete Guide URL: https://www.motadata.com/blog/itil-incident-management/

[4] T. Lechachenko, et al., Cybersecurity Assessments based on Combining TODIM Method and STRIDE Model for Learning Management Systems, in: Computer Information Technologies in Industry, vol. 3468 (2023) 250–256.
[5] T. Lechachenko, et al., Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model, in: Information Technologies: Theoretical and Applied Problems, vol. 3628 (2023).
[6] J. Wang, G. Wei, M. Lu, TODIM Method for Multiple Attribute Group Decision Making under 2-Tuple Linguistic Neutrosophic Environment, Symmetry, 10(10) (2018) 486. doi: 10.3390/sym10100486
[7] G. Macher, et al., Threat and Risk Assessment Methodologies in the Automotive Domain, Procedia Comput. Sci. 83 (2016) 1288–1294. doi: 10.1016/j.procs.2016.04.268.
[8] G. Holtrup, et al., Modeling 5G Threat Scenarios for Critical Infrastructure Protection, in: 15th International Conference on Cyber Conflict: Meeting Reality (2023) 161–180. doi: 10.23919/CyCon58705.2023.10.
[9] 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. doi: 10.1109/ISGTEurope.2017.8260283.
[10] M. Abomhara, M. Gerdes, G. M. Koien, A STRIDE-based Threat Model for Telehealth Systems, NISK (2015).
[11] A. Shostack, Experiences Threat Modeling at Microsoft, in: Modeling Security, vol. 413 (2024).
[12] Microsoft Corporation, "SDL Process Introduction", URL: http://msdn.microsoft.com/en-us/library/cc307406.aspx
[13] R. Ross, Guide for Conducting Risk Assessments, Special Publication (NIST SP) 800-30 Rev 1, National Institute of Standards and Technology, Gaithersburg, MD. Available at NIST (2012).
[14] International Organization for Standardization, ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks, ISO, Available at ISO (2022).
[15] R. A. Caralli, et al., Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University, Software Engineering Institute. Available at SEI CMU (2007).
[16] A. Shukla, E. A. Solbakken, R. Steen, On the Cyber-Emergency Preparedness in a Resilient Organization, in: 33rd European Safety and Reliability Conference (2023). doi: 10.3850/981-973-0000-00-0.
[17] ISACA, COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association (ISACA), Available at ISACA (2019).
[18] V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.
[19] T. L. Saaty, Decision Making with the Analytic Hierarchy Process, Int. J. Services Sci. 1(1) (2008) 83. doi: 10.1504/ijssci.2008.017590.
[20] H. Taherdoost, Decision Making using the Analytic Hierarchy Process (AHP); A Step by Step Approach, Int. J. Econom. Manag. Syst. (2017).
[21] B. Llamazares, An Analysis of the Generalized TODIM Method, European J. Operational Res. 269(3) (2018) 1041–1049. doi: 10.1016/j.ejor.2018.02.054.
[22] G. H. Tzeng, J. J. Huang, Multiple Attribute Decision Making: Methods and Applications, CRC press (2011).
[23] Law of Ukraine on Critical Infrastructure, Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/
[24] Cabinet of Ministers of Ukraine, Certain Issues of Critical Infrastructure Objects: Resolution No. 1109 dated October 9, 2020. URL: https://zakon.rada.gov.ua/laws/
[25] M. Al Hadidi, et al., Adaptive Regulation of Radiated Power Radio Transmitting Devices in Modern Cellular Network Depending on Climatic Conditions, Contemporary Engineering Sciences, 9(10) (2016) 473–485.
[26] M. Zaliskyi, et al., Statistical Data Processing During Wind Generators Operation, International Journal of Electrical and Electronic Engineering and Telecommunications, 8(1) (2019) 33–38.
[27] O. Solomentsev, et al., Sequential Procedure of Changepoint Analysis during Operational Data Processing, IEEE Workshop on Microwave Theory and Techniques in Wireless Communications, MTTW (2020) 168–171.
[28] X. Hu, et al., Statistical Techniques for Detecting Cyberattacks on Computer Networks based on an Analysis of Abnormal Traffic Behavior, Int. J. Comput. Netw. Inf. Secur. 12(6) (2020) 1–13.
[29] O. Solomentsev, et al., Data Processing Method for Deterioration Detection during Radio Equipment Operation, IEEE Microwave Theory and Techniques in Wireless Communications, MTTW (2019) 1–4.
[30] Z. Hassan, et al., Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems, in: IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (2018) 119–122.
[31] I. Ostroumov, N. Kuzmenko, Statistical Analysis and Flight Route Extraction from Automatic Dependent Surveillance-Broadcast Data, Integrated Communications, Navigation and Surveillance Conference (2022).
[32] Y. Averyanova, et al., UAS Cyber Security Hazards Analysis and Approach to Qualitative Assessment, Lecture Notes in Networks and Systems, 290 (2021) 258–265.