Application of tensor analysis for cybersecurity tasks in critical infrastructure*

Iaroslav Dorohyi[1,2], Vladyslav Kravchuk[1], Vasyl Tsurkan[2,3] and Iryna Berdychenko[4]

[1] Donetsk National Technical University, 76, Sambirska Str., Drohobych, Lviv region, 82111, Ukraine
[2] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Prospect Beresteiskyi (former Peremohy), Kyiv, Ukraine, 03056, Ukraine
[3] G. E. Pukhov Institute for Modeling in Energy Engineering of National Academy of Sciences of Ukraine, 15, Oleha Mudraka Str., Kyiv, 03164, Ukraine
[4] Black Sea National University named after Petro Mohyla, 10, 68 Desantnykiv Str., Mykolaiv, Mykolaiv region, 54000, Ukraine

Abstract

Cybersecurity of critical infrastructure is vital for the stability of modern society. With the growth of digital technologies and cyber threats, these infrastructures face increasing vulnerabilities. Effective threat detection and risk mitigation require modern analytical methods that assess and predict security levels throughout an infrastructure's lifecycle. Tensor analysis offers a powerful tool for modeling complex interrelations among critical components and evaluating vulnerabilities to cyber threats.

This article explores the use of tensor analysis in critical infrastructure cybersecurity. It introduces four-dimensional tensors to assess risks, threats, vulnerabilities, security measures, and resources, outlining a methodology for constructing tensor models. These models analyze parameters such as threat probability, resource significance, vulnerability levels, and the effectiveness of security measures. The study presents approaches for modeling threat impacts and calculating risk levels using tensors, emphasizing their utility in assessing and mitigating risks, even for "black-box" attack scenarios.

The results demonstrate that tensor analysis provides precise evaluations and recommendations for risk reduction, contributing to adaptive protection systems. Additionally, these findings can support the study of cybersecurity and critical infrastructure disciplines in higher education institutions, enhancing the practical understanding of risk management and security strategies.

Keywords

Critical infrastructure, tensor, tensor analysis, cybersecurity

Introduction

Critical infrastructure serves as the foundation for the functioning of modern society and the economy, encompassing energy systems, water supply, transportation, financial institutions, communication systems, and information technology. It ensures the continuity of life and the development of national economies and governmental structures. However, with the advancement of digital technologies and the increasing interconnectivity of various infrastructure sectors, the risks to its security are also rising. Modern cyber threats, particularly cyberattacks, can have catastrophic consequences for the functioning of critical assets and may even lead to significant economic and social losses. Considering these threats, the cybersecurity of critical infrastructure has become one of the most important priorities in state policies and scientific research.

Ensuring cybersecurity requires the development of new, effective methods for analyzing and monitoring the state of systems under protection. One such tool is tensor analysis. Tensors are multidimensional mathematical structures that enable the description of complex interrelations among different system elements. The application of tensors in cybersecurity analysis allows for the integration of various parameters such as risks, vulnerabilities, threats, resources, and protection measures into a unified mathematical model. This approach enables more accurate

*ITS-2025: Information Technologies and Security, December 11, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
yaroslav.dorohyi@donntu.edu.ua (I. Dorohyi); vladkrava15@ukr.net (V. Kravchuk);
v.v.tsurkan@gmail.com (V. Tsurkan); irinaberdychenko@gmail.com (I. Berdychenko);
0000-0003-3848-9852 (I. Dorohyi); 0009-0000-7929-6796 (V. Kravchuk);
0000-0003-1352-042X (V. Tsurkan); 0000-0002-6670-433X (I. Berdychenko);
© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-26
CEUR-WS.org/Vol-4337/paper7.pdf

forecasts and assessments of security levels for critical infrastructures, as well as effective identification of potential weaknesses within the system.

Risk assessment of cyber threats to critical infrastructure is an exceedingly complex task, as it requires accounting for a multitude of factors: the likelihood and criticality of threats, vulnerabilities, resource importance, and the effectiveness of protective measures. Tensor analysis enables the integration of all these parameters into a single model, which considers the interconnections and mutual influences among various elements. This approach facilitates comprehensive system monitoring and provides forecasts of potential consequences from various cyber threats.

One of the key aspects of this approach is modeling the impact of threats and protective measures on system vulnerabilities. Tensor analysis allows for an evaluation of how changes in threat parameters or vulnerabilities can affect the overall risk level for critical infrastructure resources. Specifically, it facilitates more accurate assessments of the probability of threat realization and the identification of potentially most vulnerable components of the infrastructure. Additionally, the tensor approach considers the influence of protective measures, which can reduce either the likelihood or the scale of a threat.

The article also explores the potential use of tensor analysis for modeling real-world cyberattack scenarios, such as "black-box" attacks, where the attacker lacks access to the internal system data but can manipulate parameters that are external to the user. Such models enable experiments with various parameters to assess the effectiveness of protective systems and to predict potential consequences of changes in these parameters.

Given the above, tensor analysis emerges as a powerful tool for comprehensive cybersecurity analysis of critical infrastructure. The application of such models enhances the effectiveness of risk prediction and management, ensuring a higher level of protection for critical assets against cyber threats. Tensor analysis enables the creation of more precise and dynamic security models that meet modern requirements and can adapt to new challenges in the field of cybersecurity.

In addition to practical applications, these results can be employed to improve the teaching of disciplines related to cybersecurity and critical infrastructure in higher education institutions. By incorporating tensor analysis into academic curricula, students can gain hands-on experience with advanced risk assessment techniques and better understand modern methodologies for securing vital infrastructure. This approach fosters the development of highly skilled professionals capable of addressing contemporary cybersecurity challenges effectively.

Research methodology

This study employs a combination of several research methods to analyze the cybersecurity of critical infrastructure, particularly tensor analysis methods for modeling complex interrelations among threats, resources, and protective measures. Classical scientific cognition methods, such as abstraction, analysis, and synthesis, were utilized to develop mathematical models, alongside modeling techniques for calculating risk tensors and the impact of threats.

Additionally, comparative analysis methods were applied to evaluate the effectiveness of different approaches to protecting critical systems. Forecasting methods were also employed to assess potential threats and vulnerabilities based on the developed models.

Literature review

The article [1] addresses the vulnerabilities of Internet of Things (IoT) systems in the context of critical infrastructure. It analyzes threats and security challenges at various levels of the IoT architecture, paying particular attention to anomaly detection, network security, and communication protocols affecting IoT environment security. The authors suggest future research directions to enhance IoT protection in critical infrastructure, focusing on implementing advanced technologies and methods to ensure data and communication security. This source is significant for understanding existing IoT vulnerabilities in critical sectors such as energy and transportation, where effective cybersecurity solutions are urgently needed.

The review [2] explores the latest trends in cybersecurity for protecting critical infrastructure. It emphasizes using advanced technologies such as artificial intelligence and blockchain to combat increasing cyber threats. The article highlights the importance of integrating these innovations to create effective protection mechanisms capable of adapting to new challenges. This research helps evaluate which technologies may be most effective for ensuring critical infrastructure resilience against cyber threats and offers forecasts for the field's future development.

The article [3] examines the potential of cybersecurity to enhance critical infrastructure resilience to cyber threats. The authors analyze various aspects of infrastructure adaptability and recovery after attacks, focusing on the importance of effective protection mechanisms. Specific approaches to building early detection and response systems for cyber threats are discussed. This work provides strategic recommendations for strengthening cybersecurity across different critical infrastructure sectors, from energy systems to transportation networks.

The study [4] focuses on using artificial intelligence to enhance critical infrastructure security. The authors describe the advantages and challenges of implementing AI for threat detection, protection automation, and real-time decision-making. One major challenge is ensuring the compatibility of AI solutions with existing security systems. The article also proposes future research directions to improve AI effectiveness in cybersecurity.

The work [5] presents a tensor-based mathematical model for assessing the resilience of critical infrastructures (such as energy, transportation, and utilities) against multifaceted threats, including cyberattacks, natural disasters, technological failures, and geopolitical conflicts. The authors emphasize a multidimensional approach that integrates technical, economic, environmental, social, and managerial factors across pre-disaster, crisis, and recovery phases. The proposed tensor framework captures interactions among infrastructure subsystems (generation, transportation, consumption), various resilience criteria (functionality, recovery time, threat resistance, adaptability, data security and protection, economic efficiency), and operational stages, while incorporating threat vectors to quantify disruption impacts and visualize vulnerabilities (e.g., via heatmaps). The model supports vulnerability identification, risk mitigation, strategic planning, and policy development for enhancing national security and system adaptability in the face of combined physical and cyber threats.

The review article [6] covers a wide range of topics related to cybersecurity, including vulnerabilities, threats such as ransomware and phishing, and protective mechanisms that can ensure information security. This article is an essential resource for professionals developing effective cybersecurity solutions. Given the growing number of cyber threats, this review helps understand which approaches are most effective in defending against diverse cyberattacks.

The study [7] examines IoT threats and attacks and effective countermeasures for securing such systems. Various types of attacks, from ransomware to attacks on physical devices, are discussed, with solutions proposed to neutralize them. This work is valuable for those integrating security systems in industrial IoT networks, where reliability and security requirements are exceptionally high.

The article [8] analyzes major cybersecurity vulnerabilities in Latin America, focusing on regional features and threats. The study examines how local factors influence cybersecurity strategies and proposes solutions to mitigate risks in these countries. This source is essential for understanding global and regional approaches to cybersecurity and adapting these methods to local threats.

The article [9] addresses challenges in critical infrastructure cybersecurity and offers solutions for overcoming them. The authors discuss diverse threats to infrastructure in sectors such as energy and water supply and provide recommendations for improving cybersecurity strategies. A key aspect is the emphasis on integrating new technologies to reduce the vulnerability of critical infrastructure systems to attacks.

The article [10] discusses the latest approaches to ensuring critical infrastructure cybersecurity, particularly in the energy sector and transportation systems. The authors stress the importance of integrating artificial intelligence and blockchain to enhance the security of critical infrastructures. They also focus on implementing solutions that enable timely detection of abnormal behavioral patterns and prevent potential cyber incidents. This review is a valuable resource for professionals

developing cybersecurity strategies in various critical sectors, as it offers clear insights into emerging trends and potential innovative solutions in this field.

The article [11] examines key cybersecurity challenges in smart grids, emphasizing the importance of ensuring reliable data and infrastructure protection in the energy sector. The authors propose various strategies to address threats such as malware and unauthorized access attempts. The focus is on using cryptography and authentication methods to strengthen network security.

The article [12] investigates cybersecurity issues in smart grids and the role of artificial intelligence in selecting the most effective protection methods. The authors apply a multi-criteria decision-making approach to evaluate different strategies for countering cyber threats. They specifically propose integrating machine learning algorithms to detect attacks and improve real-time protection efficiency.

The study [13] outlines major security issues in smart grids and suggests possible solutions for improving critical infrastructure protection. The focus is on anomaly detection in network operations, the use of encryption technologies, and the integration of multi-level protection systems. The article also highlights the importance of continuous monitoring and adaptive strategies in combating cyber threats.

The work [14] emphasizes both physical and cybersecurity aspects of smart grid infrastructure, particularly the importance of protecting not only digital but also physical system elements. The authors propose strategies for defending against physical attacks, such as sabotage, and cyberattacks that could significantly impact network integrity. Specific methods for securing interfaces and devices used in smart grids are discussed, as well as security challenges in automation processes that increase vulnerability to cyber threats.

The article [15] analyzes recent trends in ensuring the cyber-physical security of smart grids. Special attention is given to identifying and preventing new threats arising from integrating technologies such as IoT and AI. The authors discuss the importance of embedding protective mechanisms into various network components to enhance their reliability and resilience to attacks. The article also notes that integrating such technologies into critical infrastructures requires developing new security and resilience models capable of adapting to the ever-changing cyber threat landscape.

The article [16] proposes a methodology for qualitative evaluation of IT infrastructure elements' functionality, considering technical characteristics and operational conditions. The author developed a model for assessing the reliability and performance of IT system components, predicting potential failures, and optimizing their operation, emphasizing the universality of the approach for various types of infrastructure.

After a detailed analysis of literary sources covering key aspects of critical infrastructure cybersecurity, several parameters defining its security can be identified. Various studies emphasize the importance of identifying resources requiring protection, such as energy grids, transportation systems, and water supply management systems. Additionally, several threats and vulnerabilities jeopardizing the stability of these systems have been identified, including physical component attacks, malicious software, and more sophisticated attacks leveraging IoT and AI to penetrate security systems [1, 2, 4].

Research indicates that diverse protective measures have been developed based on these parameters and vulnerabilities. Recent advancements in cybersecurity focus on integrating cutting-edge technologies such as blockchain, machine learning, and artificial intelligence algorithms for effective anomaly detection and rapid threat response. An essential aspect is also the use of cryptography and other authentication methods to strengthen data protection and ensure network stability [5, 6, 9].

The following provides a detailed description of resource parameters, threats, vulnerabilities, and protective measures systematized during the literature analysis, which can be applied to develop recommendations for improving critical infrastructure cybersecurity, building cybersecurity models for critical infrastructure, and more.

Results

Classification of resource parameters in the context of risk management and information security

Resource parameters may vary depending on the modeling context and the type of resource (e.g., informational, financial, technical, etc.). However, most models related to risk management, information security, or resilience typically highlight several key resource characteristics:

1. ***Type of resource***. Determines the category to which the resource belongs. Examples include:
- *physical resource* – buildings, equipment, materials;
- *informational resource* – data, software, databases [1];
- *financial resource* – money, capital, loans [2];
- *human resource* – personnel, experts, skills;
- *infrastructure resource* – communications, power supply.

2. ***Resource criticality***. Assesses the importance of a resource for the functioning of a system or organization. It defines which resource takes priority under limited resources or increased risks:
- *critical resource* – essential for the uninterrupted operation of the system or execution of core activities [3, 5];
- *non-critical resource* – its absence or damage has minimal impact on operations.

3. ***Resource importance***. Indicates the degree of necessity of a resource for achieving specific goals or completing tasks:
- *high importance* – the resource is integral to achieving strategic goals;
- *low importance* – the resource is used for less critical or secondary tasks [4].

4. ***Resource availability***. Evaluates the level of access to a resource, including in the case of physical or technological constraints:
- *available* – the resource is consistently accessible for use [6, 7];
- *uncertain availability* – the resource is available but with restrictions;
- *non-renewable* – a resource that cannot be replenished (e.g., single-use materials).

5. ***Resource cost***. Defines the value or price of a resource, which may include acquisition, maintenance, servicing, and replacement costs:
- *high cost* – the resource is expensive to acquire or maintain;
- *low cost* – the resource is inexpensive or requires minimal expenses [8].

6. ***Resource resilience***. The property of a resource to withstand stressful situations or adverse impacts, including threats, vulnerabilities, attacks, or accidents:
- *resilient resource* – capable of withstanding adverse conditions without significant damage [9];
- *non-resilient resource* – loses its properties or functionality under external factors [10].

7. ***Resource efficiency***. The measure of resource productivity, indicating its ability to perform tasks with minimal expenditure:
- *high efficiency* – the resource operates with minimal costs per unit of output;
- *low efficiency* – the resource has high costs or does not perform its function effectively [11].

8. ***Resource life cycle***. The time period during which the resource remains effective and useful:
- *short-term resource* – has a limited lifespan or availability period;
- *long-term resource* – stable or has a prolonged lifespan [12].

9. ***Resource mobility***. The ability to move the resource or use it in various locations or conditions:
- *mobile resource* – easy to transport or use in different places;
- *immobile resource* – restricted to a specific location or environment [13].

10. ***Resource compatibility***. The ability to effectively use a resource in interaction with other components or systems:
- *compatible resource* – can be used in various environments or with other resources [14];
- *incompatible resource* – has limited compatibility with other system elements.

The resulting classification of parameters allows for a comprehensive analysis of resources in the context of risk modeling, resilience management, or security assurance, enabling informed decisions regarding their use, protection, and optimization.

Classification of threat parameters in cybersecurity modeling and risk management

Key aspects of threats used in cybersecurity modeling and risk management include the following parameters:

1. ***Type of threat***:
- *Malware* – programs or codes designed to harm systems (e.g., viruses, Trojans, rootkits) [1, 5];
- *Denial-of-Service (DoS/DDoS) attacks* – attacks aimed at blocking access to a resource [3];
- *Man-in-the-Middle (MITM) attacks* – attacks where an adversary intercepts or modifies communication between two parties [6, 7];
- *Phishing* – deceiving users to obtain their personal data (passwords, logins) [4];
- *Exploitation of software vulnerabilities* – exploits targeting flaws in code to infiltrate systems [8];
- *Social engineering* – manipulating individuals to gain access to information or resources [9].

2. ***Likelihood of threat occurrence***:
- *high likelihood* – the threat has a significant chance of realization due to the relevance of a vulnerability or the popularity of the attack [1, 5];
- *moderate likelihood* – the threat has a medium chance of realization, depending on specific conditions or context [10];
- *low likelihood* – the threat may occur only under exceptional circumstances or highly specific conditions [12].

3. ***Threat criticality***:
- *high criticality* – the threat can cause severe consequences for the organization, such as loss of vital data or functionality [8, 13];
- *moderate criticality* – the consequences of the threat may be important but not critical to the normal operation of the system [6];
- *low criticality* – the consequences of the threat are minimal and do not impact system or organizational performance [9].

4. ***Impact duration***:
- *short-term impact* – the threat has immediate but temporary effects, such as service delays [13];
- *long-term impact* – the consequences may be prolonged, such as system compromise or extended data loss [14].

5. ***Threat scope***:
- *global threat* – a threat that can affect the entire infrastructure or system [10];
- *local threat* – a threat affecting only a specific part of the system or resources [14];
- *targeted threat* – a threat focused on a specific vulnerability or system element [7].

6. ***Significance of vulnerabilities exploited by the threat***:
- *critical vulnerability* – the threat exploits a vulnerability that may lead to significant damage or data leaks [4, 5];
- *non-critical vulnerability* – the threat exploits less severe vulnerabilities with limited consequences [12].

7. ***Resources required to execute the threat***:
- high resource level – the threat requires substantial resources (financial, human, technical) to implement, such as complex DDoS attacks [3, 5];
- low resource level – the threat can be executed with simple or readily available tools [6].

8. ***System vulnerability to the threat***:

- high vulnerability – the system or resource is highly susceptible to the threat [13];
- low vulnerability – the system or resource is less sensitive to the threat [7].

9. ***Threat intensity***:

- *high intensity* – the attack has a significant impact in a short period, such as a massive DDoS attack [8];
- *low intensity* – the threat manifests gradually or with limited effect [12].

10. ***Number of attacks***:

- *scalable attacks* – the threat can be expanded and repeated from various points or at different stages [14];
- *single attacks* – the threat is singular or limited but may reoccur [12].

11. ***Reputational consequences***:

- *high reputational damage* – the threat may severely harm an organization's reputation due to data breaches or vulnerability exposure [9, 13];
- *low reputational damage* – the threat has a limited impact on the organization's image or trustworthiness [10].

This classification of threat parameters enables the creation of effective models for risk analysis, evaluation, and forecasting of potential threats to information systems, organizations, or critical infrastructures.

Classification of vulnerability characteristics in the context of cybersecurity and risk modeling

Key aspects of vulnerabilities used in cybersecurity modeling and risk management include the following parameters:

1. ***Type of vulnerability***:

- *technical vulnerabilities* – flaws in software or hardware components that can be exploited for unauthorized access or malicious actions. Examples include:
  - vulnerabilities in code (e.g., buffer overflows, SQL injections, vulnerabilities in libraries) [1, 5];
  - protocol vulnerabilities [6].
- *procedural vulnerabilities* – errors in organizational or administrative processes that can be exploited by attackers. Examples include:
  - insufficient user verification or weak security policies [5];
  - lack of access control policies [7].
- *human vulnerabilities* – mistakes made by individuals that can be exploited to carry out an attack. Examples include:
  - lack of employee awareness about threats, phishing attacks, social engineering [8].

2. ***Complexity of vulnerability***:

- *simple vulnerability* – a vulnerability that can be quickly identified and exploited using standard tools or methods [9];
- *complex vulnerability* – a vulnerability requiring advanced knowledge or specialized tools for identification and exploitation [10].

3. ***Potential impact***:

- *low impact* – exploitation of the vulnerability results in minor consequences, with minimal effect on confidentiality, integrity, or system availability [11];
- *moderate impact* – exploitation may lead to issues such as data loss or corruption, but without significant disruption to core functions [12];
- *high impact* – exploitation may cause serious consequences, such as loss of critical data, service unavailability, or complete system destruction [13].

4. ***Criticality of vulnerability***:

- *critical vulnerability* – a vulnerability that can compromise the functionality or security of critical infrastructure or system components [6, 7];

- *moderate criticality* – a vulnerability that may cause issues but is not decisive for the security of the entire system [8];
- *low criticality* – a vulnerability with minimal impact on system security [9].

5. ***Integration of vulnerability into the system***:

- *integrated vulnerability* – a vulnerability embedded in key system components or affecting the functionality of critical system or software elements [10];
- *independent vulnerability* – a vulnerability with limited impact on core system functions or relatively isolated from the primary infrastructure [11].

6. ***Ease of detection***:

- *easily detectable* – a vulnerability that can be identified using automated scanners or simple tools [12];
- *difficult to detect* – a vulnerability requiring advanced knowledge or specialized methods for identification, potentially part of complex systems or protected infrastructures [13].

7. ***Prevalence***:

- *widespread vulnerability* – a vulnerability found in many systems or components commonly used in the industry [5];
- *limited vulnerability* – a vulnerability occurring rarely or only in specific systems or environments [14].

8. ***Availability for exploitation***:

- *open vulnerability* – a vulnerability that is publicly known or for which exploits are already available [15];
- *closed vulnerability* – a vulnerability that is not widely known or for which exploits are not yet available [16].

9. ***Time of discovery***:

- *undiscovered vulnerability* – a vulnerability that has not yet been identified or documented [13];
- *discovered vulnerability* – a vulnerability for which public information is available regarding its existence and exploitation methods [9].

10. ***Time to remediation***:

- *immediately fixable* – a vulnerability that can be quickly addressed (e.g., through software updates or component replacement) [10];
- *time-consuming to fix* – a vulnerability requiring significant resources or time for remediation, such as changes to system architecture or components [11].

The defined characteristics help assess risks associated with vulnerabilities and support the development of defense strategies to reduce the likelihood of exploitation by attackers.

Classification of protection means against cyber threats and vulnerabilities in the context of cybersecurity

Key aspects of protection mean used in cybersecurity modeling and risk management include the following parameters:

1. ***Type of protection means***:

- *software tools* – tools that provide protection by analyzing, filtering, or modifying data:
  - antivirus programs;
  - intrusion detection systems (IDS);
  - DDoS protection tools;
  - firewalls;
  - encryption tools;
  - authentication and authorization systems (two-factor authentication, biometric systems).
- *hardware tools* – physical devices for protecting infrastructure:
  - hardware firewalls;

- secure servers and network components;
- encryption hardware.

• *organizational measures* – strategies, policies, and processes for protecting against cyber threats:
- access policies;
- security standards;
- user security training;
- access control for critical systems [1, 5].

2. ***Likelihood of triggering (effectiveness)***:

• *high effectiveness* – a protection tool with a high probability of detecting and responding to threats or vulnerabilities;

• *medium effectiveness* – a tool that works in most cases but may have some limitations or failures;

• *low effectiveness* – a tool that rarely works effectively or often generates false positives [1, 6].

3. ***Criticality of presence***:

• *critical tool* – without this tool, the system becomes extremely vulnerable to attacks and threats;

• *important tool* – a tool that significantly reduces risks but is not critically necessary;

• *auxiliary tool* – a tool that provides additional security but is not essential [4, 8].

4. ***Response speed***:

• *fast response* – a tool that can respond quickly to threats or vulnerabilities, protecting the system in real-time;

• *moderate response* – a tool that responds with some delay or after processing information;

• *slow response* – a tool that may require time to collect data or perform protective measures [10, 11].

5. ***Scalability***:

• *high scalability* – a protection tool that can easily be expanded for use in larger or more complex systems;

• *limited scalability* – a tool with limitations in use or unsuitable for rapid expansion;

• *low scalability* – a tool that is difficult or impossible to apply to large or distributed infrastructures [4, 12].

6. ***Ease of use***:

• *intuitive* – a tool with a simple interface that does not require special knowledge to manage;

• *complex to manage* – a tool that requires specialized knowledge or training for proper configuration and use;

• *high resource demands* – a tool that requires significant computational or human resources for configuration or management [11, 12].

7. ***Cost***:

• *high cost* – a tool requiring significant financial resources for purchase and maintenance;

• *medium cost* – a tool with an acceptable cost but may require additional maintenance expenses;

• *low cost* – inexpensive or free tools that can be used for basic protection [8, 10].

8. ***Updatability***:

• *easily updatable* – a tool that is regularly updated and always maintains the latest versions considering new threats;

• *updates depend on the user* – a tool requiring manual updates or updates at intervals;

• *not updatable* – a tool that does not receive updates or becomes obsolete over time [6, 10].

9. ***Integration with other systems***:

• *easy integration* – a tool that integrates easily with other security infrastructure components;

• *complex integration* – a tool with limited integration capabilities or requiring additional configurations for compatibility;

• *non-integrable* – a tool that cannot be integrated into the existing infrastructure [7, 8].

10. ***Compatibility***:

- *full compatibility* – a tool that is fully compatible with other system components and infrastructure;
- *limited compatibility* – a tool that may have compatibility restrictions with some components;
- *incompatibility* – a tool that does not function properly with other systems [5, 6].

The listed characteristics can help in selecting and evaluating the effectiveness of protection tools in the context of specific threats and vulnerabilities in systems to be protected.

Tensor model of cybersecurity for critical infrastructure

Using the classifications of parameters for resources, threats, vulnerabilities, and protection tools, we construct a 4-dimensional tensor model of cybersecurity for critical infrastructure.

First, we define the primary tensors:

- **resource tensor (R)** has four dimensions:
  - ***type of resource*** **(T_r)** – the category of the resource (e.g., information resource, software, hardware);
  - ***criticality of resource*** **(C_r)** – the degree of criticality of the resource for system operation;
  - ***importance of resource*** **(V_r)** – the resource's value to the organization;
  - ***availability of resource*** **(A_r)** – the likelihood of accessing the resource overall;
- **threat tensor (Z)** has four dimensions:
  - ***type of threat*** **(T_z)** – the category of the threat (e.g., cyberattack, natural disaster, human factor);
  - ***probability of occurrence*** **(P_z)** – the likelihood of the threat being realized;
  - ***criticality of threat*** **(C_z)** – the level of damage the threat can cause;
  - ***scope of threat*** **(S_z)** – the extent of the threat's impact on the overall system;
- **vulnerability tensor (V)** has four dimensions:
  - ***type of vulnerability*** **(T_v)** – the category of vulnerability (e.g., weak encryption, unknown software bugs);
  - ***complexity*** **(D_v)** – the complexity of exploiting the vulnerability;
  - ***potential impact on resources*** **(I_v)** – the effect of the vulnerability on organizational resources;
  - ***criticality of vulnerability*** **(C_v)** – the level of harm the vulnerability can cause;
- **protection tools tensor (G)** has four dimensions:
  - ***type of protection tool*** **(T_g)** – the category of protection tool (e.g., antivirus, firewall);
  - ***probability of activation*** **(P_g)** – the likelihood that the protection tool will activate in the event of a threat;
  - ***criticality of tool*** **(C_g)** – the importance of having the protection tool;
  - ***cost of tool*** **(C_{g_v})** – the expense of implementing the protection tool.

Thus, the key elements of the mathematical model are:

- resource tensor **(R)** describes various characteristics of resources that require protection. Each resource is evaluated using the following dimensions (1):

$$R_{i,j,k,l} = f\left(T_r, C_r, V_r, A_r\right), \quad (1)$$

where:

i – index of resource type T_r;

j – index of criticality C_r;

k – index of importance V_r;

l – index of resource availability A_r;

• threat tensor (Z) considers threat type, probability, criticality, and scope. Threats are evaluated through these dimensions (2):

$$Z_{i,j,k,l} = f\left(T_z, P_z, C_z, S_z\right), \quad (2)$$

where:

i – index of threat type T_z;

j – index of probability P_z;

k – index of criticality C_z;

l – index of threat scope S_z;

• vulnerability tensor (V) evaluates aspects of system vulnerabilities, including complexity, potential impact on resources, and criticality (3):

$$V_{i,j,k,l} = f\left(T_v, D_v, I_v, C_v\right), \quad (3)$$

where:

i – index of vulnerability type T_v;

j – index of complexity D_v;

k – index of potential impact I_v;

l – index of vulnerability criticality C_v;

• protection tools tensor (G) evaluates the effectiveness and importance of protection tools in terms of activation probability and criticality:

$$G_{i,j,k,l} = f\left(T_g, P_g, C_g, C_{g_v}\right), \quad (4)$$

where:

i – index of protection tool type T_g;

j – index of activation probability P_g;

k – index of criticality C_g;

l – index of cost C_{g_v}.

To facilitate working with the model, several additional tensors are constructed:

• threat impact tensor (G) defines how specific threats affect resources, considering probability, criticality, and scope (5):

$$I_{i,j,k,l} = f\left(Z_{i,j,k,l} \cdot R_{i,j,k,l}\right), \quad (5)$$

where:

$R_{i,j,k,l}$ – resource tensor;

$Z_{i,j,k,l}$ – threat tensor;

• risk tensor (R_r) evaluates the likelihood of specific threats exploiting vulnerabilities for certain resources, considering protection tools (6):

$$R_r = f\left(I_{i,j,k,l} \cdot V_{i,j,k,l} \cdot G_{i,j,k,l}\right), \quad (6)$$

where:

$I_{i,j,k,l}$ – threat impact tensor;

$V_{i,j,k,l}$ – vulnerability tensor;

$G_{i,j,k,l}$ – protection tools tensor.

Example of model application

The following demonstrates the application of the developed model using an imaginary critical infrastructure with dimensions 2x2x2x2 (2 resources, threats, vulnerabilities, and protective measures). The tensors for the task are described as follows.

For each resource, parameters such as criticality, value, and availability are considered.

The structure of the resource tensor (R) is as follows:

$$R_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}R_{1,1,1,1} & R_{1,1,1,2}\\ R_{1,1,2,1} & R_{1,1,2,2}\end{bmatrix} & \begin{bmatrix}R_{1,2,1,1} & R_{1,2,1,2}\\ R_{1,2,2,1} & R_{1,2,2,2}\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}R_{2,1,1,1} & R_{2,1,1,2}\\ R_{2,1,2,1} & R_{2,1,2,2}\end{bmatrix} & \begin{bmatrix}R_{2,2,1,1} & R_{2,2,1,2}\\ R_{2,2,2,1} & R_{2,2,2,2}\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

Let the following tensor be given:

$$R_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}1 & 0.9\\ 0.85 & 0.8\end{bmatrix} & \begin{bmatrix}0.95 & 0.9\\ 0.85 & 0.75\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.85 & 0.8\\ 0.75 & 0.7\end{bmatrix} & \begin{bmatrix}0.8 & 0.75\\ 0.7 & 0.65\end{bmatrix}\end{bmatrix}\end{bmatrix}$$

Each index in the tensor $R_{i,j,k,l}$ indicates a value that characterizes a specific resource (depending on its type) in the context of three key parameters: criticality, importance, and availability:

1. i **(resource type)**:
   - $i=$ 1: informational resource.
   - $i=$ 2: hardware resource.
2. j**(resource criticality)**:
   - $j=$ 1*: critical resource.*
   - $j=$ 2*: non-critical resource.*
3. k **(resource importance)**:
   - $k=$ 1*: important resource.*
   - $k=$ 2*: less important resource.*
4. l **(resource availability)**:
   - $l=$ 1*: accessible resource.*
   - $l=$ 2*: less accessible resource.*

For example:

- 1 (for $R_{1,1,1,1}$): a high value for a resource that is highly critical, important, and accessible (e.g., a very important informational resource with high significance and availability for use).
- 0.65 (for $R_{2,2,2,2}$): a hardware resource with low criticality, lesser importance, and a low level of accessibility.

For each vulnerability, the parameters considered are criticality, potential impact, and exploitation complexity.

Structure of the vulnerability tensor (V)**:**

$$V_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}V_{1,1,1,1} & V_{1,1,1,2}\\ V_{1,1,2,1} & V_{1,1,2,2}\end{bmatrix} & \begin{bmatrix}V_{1,2,1,1} & V_{1,2,1,2}\\ V_{1,2,2,1} & V_{1,2,2,2}\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}V_{2,1,1,1} & V_{2,1,1,2}\\ V_{2,1,2,1} & V_{2,1,2,2}\end{bmatrix} & \begin{bmatrix}V_{2,2,1,1} & V_{2,2,1,2}\\ V_{2,2,2,1} & V_{2,2,2,2}\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

Let the following vulnerability tensor be given:

$$V_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}0.85 & 0.8\\ 0.75 & 0.7\end{bmatrix} & \begin{bmatrix}0.9 & 0.85\\ 0.8 & 0.75\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.95 & 0.9\\ 0.85 & 0.8\end{bmatrix} & \begin{bmatrix}0.8 & 0.75\\ 0.7 & 0.65\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

The tensor has four dimensions:

1. i – type of vulnerability (1 – weak encryption, 2 – hardware vulnerability).
2. j – criticality of the vulnerability (1 – highly critical, 2 – less critical).

3. k – nature of the attack (1 – cyberattack, 2 – social engineering).
4. l – probability of exploitation (1 – high, 2 – low).

For example:

- $V_{1,1,1,1}=0.85$: for a highly critical weak encryption vulnerability exploited through a cyberattack with a high probability of exploitation, the vulnerability level is 0.85.
- $V_{1,1,1,2}=0.8$: for a highly critical weak encryption vulnerability exploited through a cyberattack with a low probability of exploitation, the vulnerability level is 0.8.

For each protective measure, the parameters of criticality, probability, and scale are considered.

The structure of the protection tensor (G):

$$G_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}G_{1,1,1,1} & G_{1,1,1,2}\\ G_{1,1,2,1} & G_{1,1,2,2}\end{bmatrix} & \begin{bmatrix}G_{1,2,1,1} & G_{1,2,1,2}\\ G_{1,2,2,1} & G_{1,2,2,2}\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}G_{2,1,1,1} & G_{2,1,1,2}\\ G_{2,1,2,1} & G_{2,1,2,2}\end{bmatrix} & \begin{bmatrix}G_{2,2,1,1} & G_{2,2,1,2}\\ G_{2,2,2,1} & G_{2,2,2,2}\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

Let the following protection tensor be given (7):

$$G_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}0.95 & 0.9\\ 0.85 & 0.8\end{bmatrix} & \begin{bmatrix}0.9 & 0.85\\ 0.8 & 0.75\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.92 & 0.88\\ 0.85 & 0.8\end{bmatrix} & \begin{bmatrix}0.85 & 0.8\\ 0.75 & 0.7\end{bmatrix}\end{bmatrix}\end{bmatrix}. \quad (7)$$

The tensor has four dimensions:

1. i – type of protection (1 – antivirus, 2 – firewall).
2. j – probability of activation (1 – high, 2 – low).
3. k – criticality of presence (1 – critical, 2 – less critical).
4. l – cost of the protection (1 – high, 2 – low).

For example:

- $G_{1,1,1,1}=0.95$: an antivirus with a high probability of activation, critical presence, and high cost has a protection level of 0.95.

For each threat, the following parameters are considered: criticality, probability, and scale.

The structure of the threat tensor (Z):

$$Z_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}Z_{1,1,1,1} & Z_{1,1,1,2}\\ Z_{1,1,2,1} & Z_{1,1,2,2}\end{bmatrix} & \begin{bmatrix}Z_{1,2,1,1} & Z_{1,2,1,2}\\ Z_{1,2,2,1} & Z_{1,2,2,2}\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}Z_{2,1,1,1} & Z_{2,1,1,2}\\ Z_{2,1,2,1} & Z_{2,1,2,2}\end{bmatrix} & \begin{bmatrix}Z_{2,2,1,1} & Z_{2,2,1,2}\\ Z_{2,2,2,1} & Z_{2,2,2,2}\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

Let the following threat tensor be given (8):

$$Z_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}0.9 & 0.85\\ 0.8 & 0.75\end{bmatrix} & \begin{bmatrix}0.7 & 0.65\\ 0.6 & 0.55\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.8 & 0.75\\ 0.7 & 0.65\end{bmatrix} & \begin{bmatrix}0.6 & 0.55\\ 0.5 & 0.45\end{bmatrix}\end{bmatrix}\end{bmatrix}. \quad (8)$$

The tensor has four dimensions:

1. i – type of threat (1 – cyberattack, 2 – human factor).
2. j – probability of occurrence (1 – high, 2 – low).
3. k – criticality (1 – critical, 2 – less critical).
4. l – scale of the threat (1 – local impact, 2 – global impact).

For example:

- $Z_{1,1,1,1}=0.9$: a critical cyberattack with a high probability of occurrence and local impact has a threat level of 0.9.

To construct the threat impact tensor (I), which shows how a threat affects resources, considering the probability, criticality, and scale of the threat, as well as resource characteristics, we use formula (5).

We apply the element-wise product $Z_{i,j,k,l} \cdot R_{i,j,k,l}$ and consider the dependency $f(x)=x$ (in our example).

$$I_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}0.9\times1 & 0.85\times0.9\\ 0.8\times0.85 & 0.75\times0.8\end{bmatrix} & \begin{bmatrix}0.7\times0.95 & 0.65\times0.9\\ 0.6\times0.85 & 0.55\times0.75\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.8\times0.85 & 0.75\times0.8\\ 0.7\times0.75 & 0.65\times0.7\end{bmatrix} & \begin{bmatrix}0.6\times0.8 & 0.55\times0.75\\ 0.5\times0.7 & 0.45\times0.65\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

After the calculation, we obtain the following threat impact tensor:

$$I_{i,j,k,l}=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}0.9 & 0.765\\ 0.68 & 0.6\end{bmatrix} & \begin{bmatrix}0.665 & 0.585\\ 0.51 & 0.4125\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.68 & 0.6\\ 0.525 & 0.455\end{bmatrix} & \begin{bmatrix}0.48 & 0.4125\\ 0.35 & 0.2925\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

Next, we calculate the risk tensor using the formula (6).

$$R_r=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}0.9\times0.85\times0.95 & 0.765\times0.8\times0.9\\ 0.68\times0.75\times0.85 & 0.6\times0.7\times0.8\end{bmatrix} & \begin{bmatrix}0.665\times0.9\times0.92 & 0.585\times0.85\times0.88\\ 0.51\times0.8\times0.85 & 0.4125\times0.75\times0.8\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.68\times0.95\times0.92 & 0.6\times0.9\times0.88\\ 0.525\times0.85\times0.85 & 0.455\times0.8\times0.8\end{bmatrix} & \begin{bmatrix}0.48\times0.8\times0.85 & 0.4125\times0.75\times0.8\\ 0.35\times0.7\times0.75 & 0.2925\times0.65\times0.7\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

After the calculation, we obtain the following risk tensor:

$$R_r=\begin{bmatrix}\begin{bmatrix}\begin{bmatrix}0.7245 & 0.5484\\ 0.4238 & 0.336\end{bmatrix} & \begin{bmatrix}0.5483 & 0.4362\\ 0.4344 & 0.2475\end{bmatrix}\end{bmatrix}\\ \begin{bmatrix}\begin{bmatrix}0.5926 & 0.4752\\ 0.3784 & 0.2912\end{bmatrix} & \begin{bmatrix}0.3264 & 0.2475\\ 0.1838 & 0.1335\end{bmatrix}\end{bmatrix}\end{bmatrix}.$$

The risk tensor R_r reflects the probability of the realization of risks associated with specific threats, resources, vulnerabilities, and protection measures. Each element of the tensor R_r corresponds to the risk probability for a specific combination of these factors.

For example:

- $R_{r,1,1,1,1}=0.7245$ indicates a high risk of a cyberattack on an information resource due to the vulnerability "weak encryption" in the presence of antivirus software.
- $R_{r,2,2,2,2}=0.1335$ indicates a low risk of human factor exploitation on a hardware resource with an existing hardware vulnerability and the presence of a firewall.

Modeling of the “black box” attack. To model the "black box" attack, we will modify our initial data from the protection tensor (7) and threat tensor (8).

Changes made to the data for simulating the "black box" attack:

1. Increase the values for certain elements of the threat tensor, for example:

- $Z'_{1,1,1,1}=1.0$ (the probability of the threat has increased to 1).
- $Z'_{2,2,2,2}=0.7$ (the probability has increased).

2. Decrease the values for certain elements of the protection tensor, for example:

- $G'_{1,1,1,1}=0.7$ (protection has decreased).
- $G'_{2,2,2,2}=0.6$ (protection has decreased).

Using formulas (5) and (6) for calculation, we obtain the following results:

$$I'_{i,j,k,l} = \begin{bmatrix} \begin{bmatrix} \begin{bmatrix} 1 & 0.765 \\ 0.68 & 0.6 \end{bmatrix} & \begin{bmatrix} 0.665 & 0.585 \\ 0.51 & 0.4125 \end{bmatrix} \end{bmatrix} \\ \begin{bmatrix} \begin{bmatrix} 0.68 & 0.6 \\ 0.525 & 0.455 \end{bmatrix} & \begin{bmatrix} 0.48 & 0.4125 \\ 0.35 & 0.455 \end{bmatrix} \end{bmatrix} \end{bmatrix},$$

$$R'_r = \begin{bmatrix} \begin{bmatrix} \begin{bmatrix} 0.595 & 0.5508 \\ 0.4335 & 0.336 \end{bmatrix} & \begin{bmatrix} 0.5382 & 0.4246 \\ 0.3264 & 0.232 \end{bmatrix} \end{bmatrix} \\ \begin{bmatrix} \begin{bmatrix} 0.595 & 0.4752 \\ 0.3793 & 0.2912 \end{bmatrix} & \begin{bmatrix} 0.3264 & 0.2475 \\ 0.1838 & 0.177 \end{bmatrix} \end{bmatrix} \end{bmatrix}.$$

As seen from the simulation results, the deteriorated parameters during the attack reduced the risk of the attack, indicating the need for improvement in the tensor model.

To find the optimal model, further research on the mutual influence between model elements should be conducted. As a further development of the models, the following studies can be proposed:

1. Addition of an adaptive defense parameter.

Expand the model by considering the adaptability of the defense system, which reduces the impact of attacks on threats. For this, a new coefficient $A_{i,j,k,l}$ – the adaptability of the defense – will be introduced. It models the initial threat level, forming a new threat tensor in the following form:

$$Z'_{i,j,k,l} = Z_{i,j,k,l} \cdot \left(1 - A_{i,j,k,l}\right)$$

where $0 \le A_{i,j,k,l} \le 1$ (the higher $A_{i,j,k,l}$, the more effective the reduction).

2. Considering the reverse impact of defense measures on threats.

Defense measures can not only neutralize vulnerabilities but also actively reduce the level of threats. We will update the model so that the threat level changes according to the effectiveness of the defense ($G_{i,j,k,l}$):

$$Z'_{i,j,k,l} = Z_{i,j,k,l} \cdot \left(1 - \alpha\, G_{i,j,k,l}\right),$$

where α is the coefficient of the defense's impact on the threat ($0 \le \alpha \le 1$).

3. Evaluating the threat tensor through the time aspect.

The threat decreases over time due to the implementation of protective measures. To model this, we add a time dynamics function:

$$Z'_{i,j,k,l}(t) = Z_{i,j,k,l} \cdot e^{-\beta t},$$

where β is the threat decay coefficient and t is the time after the threat is detected.

The proposed changes allow modeling a more dynamic reduction of threats and accounting for the active contribution of protection. These approaches can be used together or separately, depending on the specifics of the task.

Conclusions

The article explores the potential applications of tensor analysis for addressing cybersecurity challenges in critical infrastructure. The use of tensors allows for a comprehensive evaluation of the interrelationships between various aspects of infrastructure security, such as resources, threats, vulnerabilities, and protection measures, enabling a more precise and detailed risk analysis. The developed methods and approaches facilitate the creation of models that not only account for current conditions but also consider possible changes in the threat environment, making these models adaptive to new challenges.

In particular, the article demonstrates how four-dimensional tensors can be used to model complex interactions between different cybersecurity parameters, such as the probability of a threat, the importance and criticality of resources, the level of vulnerability, and the effectiveness

of protection measures. This approach enables a deeper analysis of the impact of each of these parameters on the overall risk level for critical infrastructure assets.

Special attention is given to the use of algorithms for constructing threat and risk impact tensors, as well as for comparing results before and after changes in protection parameters. The article explains how changes in parameters, such as the probability of a threat or the effectiveness of protection measures, can significantly alter the risk level, allowing for real-time adaptation of protection strategies. Methods for modeling "black box" attacks, where the attacker has no access to the system's internal parameters but can influence external parameters, were also analyzed. This approach helps to account for real-world attack scenarios, which are becoming increasingly common in modern cybersecurity threats.

The study concludes that tensor analysis is a powerful tool for comprehensive cybersecurity risk assessment of critical infrastructure. Using this approach ensures more accurate vulnerability assessments of infrastructure, the development of adaptive protection systems, and the implementation of appropriate measures to reduce risks.

Additionally, the results obtained have significant potential for educational purposes. They can be utilized in higher education to enhance the teaching of subjects related to cybersecurity and critical infrastructure. By incorporating tensor analysis into academic programs, students can gain practical insights into advanced risk assessment techniques and adaptive protection strategies, fostering the development of professionals equipped to address modern cybersecurity challenges effectively.

Further development of the research

The further development of the research on the application of tensor analysis for cybersecurity in critical infrastructure will focus on integrating machine learning and artificial intelligence methods to create adaptive systems capable of predicting new threats and responding to them. An important direction will be the development of algorithms for real-time monitoring and automatic adjustment of protection parameters, which will enhance security management efficiency.

Additionally, it is necessary to improve models to account for a broader range of factors – not only technical but also organizational, legal, and economic aspects – to create more accurate threat forecasts.

Another promising direction is the testing of models on real-world scenarios and critical infrastructures to assess the effectiveness of various protection strategies. This will help identify shortcomings in existing methods and improve them. Integration with cutting-edge technologies will provide the opportunity to create more resilient protection systems for critical infrastructures.

Declaration on Generative AI

During the preparation of this work, the authors used GPT-4.0 and Grammarly in order to: Grammar and spelling check. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the publication’s content.

References

[1] Y. Zhang, L. Zhao, and Z. Liu, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things," Sensors, vol. 23, no. 8, p. 4117, 2023. DOI: 10.3390/s23084117.

[2] P. Kumar and A. Singh, "Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review," Cybersecurity and Infrastructure Technology Research Journal, vol. 5, no. 3, pp. 872, 2023. DOI: 10.51594/csitrj.v5i3.872.

[3] R. Patel and A. Shah, "Cybersecurity capabilities for critical infrastructure resilience," International Journal of Cybersecurity, vol. 5, no. 6, pp. 91-102, 2021. DOI: 10.1108/ICS-06-2021-0091.

[4] J. C. Macdonald and F. W. Wang, "AI for Critical Infrastructure Security: Concepts, Challenges, and Future Directions," Journal of Artificial Intelligence, vol. 17, pp. 746-768, 2024. DOI: 10.10574268.

[5] I. Dorohyi, V. Kravchuk, and V. Tsurkan, "A tensor-based model for assessing resilience of critical infrastructure," in Proc. ITS-2024: Information Technologies and Security, Kyiv, Ukraine, Dec. 2024, CEUR Workshop Proceedings, vol. 4068, pp. 109-124, 2024. ISSN: 1613-0073. Available: https://ceur-ws.org/Vol-4068/paper9.pdf.
[6] M. E. Brown and T. S. Kumar, "A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things," Technologies, vol. 11, no. 6, pp. 161, 2023. DOI: 10.3390/technologies11060161.
[7] C. Martinez and J. Fernandez, "A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America," Informatics, vol. 10, no. 3, pp. 71, 2023. DOI: 10.3390/informatics10030071.
[8] L. S. Chan, M. Lee, and J. Yang, "Cybersecurity of Critical Infrastructures: Challenges and Solutions," Sensors, vol. 22, no. 14, pp. 5105, 2023. DOI: 10.3390/s22145105.
[9] P. Kumar and A. Singh, "Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review," Cybersecurity and Infrastructure Technology Research Journal, vol. 5, no. 3, pp. 872, 2023. DOI: 10.51594/csitrj.v5i3.872.
[10] K. J. He, J. Liu, and H. W. Song, "Cyber Security in Smart Grid: Challenges and Solutions," Proceedings of the IEEE Conference on Communications and Wireless Computing, pp. 1-5, 2020. DOI: 10.1109/CCWC47524.2020.9036484.
[11] F. P. Alonso and D. M. Garcia, "Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence," Journal of Cybersecurity and Privacy, vol. 3, no. 4, pp. 31, 2023. DOI: 10.3390/jcp3040031.
[12] R. K. Sharma and N. J. Patel, "Smart Grid Cyber Security Enhancement: Challenges and Solutions–A Review," Sustainability, vol. 14, no. 21, pp. 14226, 2023. DOI: 10.3390/su142114226.
[13] A. T. Johnson and S. Y. Li, "Cyber–Physical Security of a Smart Grid Infrastructure," IEEE Transactions on Smart Grids, vol. 3, no. 2, pp. 1061-1070, 2012. DOI: 10.1109/TSG.2012.6016202.
[14] X. P. Li and Y. W. Zhang, "Trends in Smart Grid Cyber-Physical Security: Components, Threats, and Solutions," IEEE Transactions on Smart Grids, vol. 13, no. 1, pp. 50-62, 2023. DOI: 10.1109/TSG.2023.10713384.
[15] S. Telenyk, O. Rolick, M. Bukasov, Y. Dorogiy, D. Halushko and A. Pysarenko, "Qualitative evaluation method of IT-infrastructure elements functioning," 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, 2014, pp. 165-169, doi: 10.1109/BlackSeaCom.2014.6849031.