НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

МАТЕРІАЛИ XXV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ВИПУСК 25

Київ – 2025

Рекомендовано до друку Вченою радою
Інституту проблем реєстрації інформації НАН України
(протокол № 9 від 23 грудня 2025 р.)

Інформаційні технології та безпека. Матеріали XXV Міжнародної науково-практичної конференції ІТБ-2025. – Київ: Інжиніринг. – 285 с. ISBN: 978-617-8180-04-1

До збірника увійшли матеріали доповідей, представлених на XXV Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2025, 11 грудня 2025 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням створення і впровадження інформаційних технологій, актуальним проблемам забезпечення інформаційної та кібербезпеки, протидії інформаційним операціям і кібертероризму, інтелектуальним технологіям підтримки прийняття рішень, проведенню аналітичних досліджень на основі сучасних методів інтелектуального аналізу даних.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

ISBN 978-617-8180-04-1

UDC 351.865

APPLICATION OF TENSOR ANALYSIS FOR CYBERSECURITY TASKS IN CRITICAL INFRASTRUCTURE

Iaroslav Dorohyi[1][0000-0003-3848-9852], Vladyslav Kravchuk[2][0009-0000-7929-6796], Vasyl Tsurkan[3][0000-0003-1352-042X], Iryna Berdychenko[4][0000-0002-6670-433X]

[1] *Donetsk National Technical University, Drohobych, Ukraine*
[2] *Donetsk National Technical University, Drohobych, Ukraine*
[3] *Institute of Special Communications and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine,*
[4] *Petro Mohyla Black Sea National University, Mykolaiiv, Ukraine*
[1] cisco.rna@gmail.com
[2] vladkrava15@ukr.net,
[3] v.v.tsurkan@gmail.com,
[4] irinaberdychenko@gmail.com,

Cybersecurity of critical infrastructure is essential for societal stability. As digitalization increases, so do vulnerabilities and risks. Tensor analysis provides an effective means to model complex interdependencies among system components and assess exposure to cyber threats. This study proposes a tensor-based methodology for evaluating risks, vulnerabilities, and protective measures using multidimensional data structures.

Keywords: Critical infrastructure, tensor, tensor analysis, cybersecurity.

Introduction

Critical infrastructure [1] underpins the functioning of modern society and the economy, including energy, transport, finance, communication, and IT systems. As digitalization and interconnectivity grow, so do cybersecurity risks, making their protection a top priority. Tensor analysis [2] offers an effective approach for modeling complex interdependencies among system elements, integrating risks, vulnerabilities, threats, and protective measures into a unified analytical model. This multidimensional

method enhances the accuracy of risk assessment, identifies critical vulnerabilities, and evaluates the impact of threats and defenses, including in “black-box” attack scenarios.

Findings

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):

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

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

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

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

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

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

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

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):

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

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

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

Modelling of the "black box" attack. To model the "black box" attack, we need to modify our initial data from the protection tensor (4) and threat tensor (2).

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

1. Increase the values for certain elements of the threat tensor, for example: $Z'_{1,1,1,1} = 1.0$, $Z'_{2,2,2,2} = 0.7$.

2. Decrease the values for certain elements of the protection tensor, for example: $G'_{1,1,1,1} = 0.7$, $G'_{2,2,2,2} = 0.6$.

Using formulas (5) and (6) for calculation, we obtain the new results for tensors $I'_{i,j,k,l}$ and R'_r and as result we can evaluate them.

Conclusions

The article examines the use of tensor analysis to address cybersecurity challenges in critical infrastructure by modeling complex interrelations among resources, threats, vulnerabilities, and protection measures for more accurate and adaptive risk assessment. Using four-dimensional tensors, the approach captures the influence of threat probability, resource criticality, vulnerability levels, and defense effectiveness on overall risk. It also enables real-time adjustment of protection strategies and supports modeling of "black-box" attack scenarios reflecting real-world threats.

References

1. Dorohyi, I., Mokhor, V., Kozliuk, I., & Tsurkan, V. (2015). *Krytychna infrastruktura: vrazlyvosti, zahrozy, ryzyky* [Critical infrastructure: vulnerabilities, threats, risks]. In *Tezy dopovidei II mizhnarodnoi naukovo-praktychnoi konferentsii «Informatsiini tekhnolohii ta vzaiemodii»* (pp. 46–47). Kyiv, Ukraine.
2. Dorohyi, I., Kravchuk, V., & Tsurkan, V. (2024). Tensor model for representing critical infrastructure. In *Selected Papers of the XXIV International Scientific and Practical Conference "Information Technologies and Security" (ITS 2024), Kyiv, Ukraine, December 19, 2024* (Vol. 4068, pp. 109–124). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-4068/ (ISSN 1613-0073)