PROCEEDINGS

1ST INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «RESILIENT SYSTEMS: SECURE DIGITAL TECHNOLOGIES AND CRITICAL INFRASTRUCTURE» (RS-2025)

June 27, 2025

Drohobych, 2025

UDC 004.56/004.08/519.6
DOI: 10.5281/ZENODO.15775240

CONFERENCE ORGANIZING:

Donetsk National Technical University
G. E. Pukhov Institute for Modeling Problems in Energy Engineering, NAS of Ukraine
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Cherkasy State Technological University
Ternopil Ivan Puluj National Technical University
State University "Zhytomyr Polytechnic"
Lviv State University of Life Safety
National Aerospace University "Kharkiv Aviation Institute"
Berdyansk State Pedagogical University
Odesa National University of Economics
State Service for Special Communications and Information Protection of Ukraine
National Bank of Ukraine
University of Zielona Góra (Poland)
Academy of Silesia (Poland)
State University of Western Paraná (Brazil)
Copenhagen Business School (Denmark)

Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference. Drohobych: Donetsk National Technical University, 2025. 184 pp.

The proceeding contains materials of the conference on theoretical and practical problems of AI, cybersecurity and critical infrastructures.

Recommended for publication by the Academic Council of the State Higher Educational Institution 'Donetsk National Technical University'

The materials are submitted in the author's edition

ORGANIZING COMMITTEE

Chair of the Organizing Committee:

Iaroslav DOROHYI – DSc, Professor, Head of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Deputy Chair of the Organizing Committee:

Mykyta ALEKSANDROV – PhD**,** Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Members of the Organizing Committee:

Yevhen BASHKOV – DSc, Professor, Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Tetiana ALTUKHOVA – CSc, Associate Professor, Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Iryna NAZAROVA – CSc, Associate Professor, Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Yelyzaveta YEZHOVA – Assistant Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Dmytro KHOMA – Assistant Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

PROGRAM COMMITTEE

Chair of the Program Committee:

Yaroslav DOROHYI – DSc, Professor, Head of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Deputy Chair of the Program Committee:

Yevhen BASHKOV – DSc, Professor, Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Members of the Program Committee:

Volodymyr MOKHOR – Corresponding Member of NASU, DSc, Professor, Director, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Oleksandr CHEMERYS – DSc, Professor, Deputy Director for Research, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Serhii HILHURT – DSc, Senior Researcher, Head of the Department of Mathematical and Econometric Modeling, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Dmytro LANDE – DSc, Professor, Head of the Department of Information Security, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” (Ukraine).

Anatolii CHEPYNOHA – CSc, Associate Professor, Dean of the Faculty of Information Technologies and Systems, Cherkasy State Technological University (Ukraine).

Roman PROSKUROVSKYI – CSc, Associate Professor, Head of the Critical Infrastructure Protection Division, National Bank of Ukraine (Ukraine).

Oleksandr BAKALYNSKYI – CSc, Senior Researcher, Senior Specialist of the Critical Infrastructure Protection Department, National Bank of Ukraine (Ukraine).

Serhii MARTSENKO – CSc, Associate Professor, Associate Professor of the Department of Computer Science, Ternopil Ivan Puluj National Technical University (Ukraine).

Andrii YEFIMENKO – CSc, Associate Professor, Head of the Department of Computer Engineering and Cybersecurity, State University “Zhytomyr Polytechnic” (Ukraine).

Maryna HRAF – PhD, Associate Professor, Head of the Department of Computer Science, State University “Zhytomyr Polytechnic” (Ukraine).

Nataliia MASLOVA – CSc, Associate Professor, Department of Information Security Management, Lviv State University of Life Safety (Ukraine).

CONTENTS

SECTION 1: ARTIFICIAL INTELLIGENCE

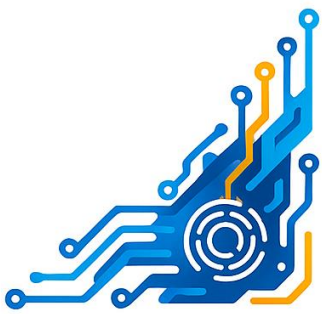
SECTION 2: CYBERSECURITY AND CRITICAL INFRASTRUCTURE

SECTION 3: INFORMATION TECHNOLOGIES

SECTION 4: COMPUTER AND MATHEMATICAL MODELING

Oleksandr Shtepa

SECTION 5: DIGITAL SYSTEMS



ANALYSIS OF MODERN METHODS FOR MODELING CRITICAL INFRASTRUCTURE IN CYBERSECURITY

Vladyslav Kravchuk, Iaroslav Dorohyi, Vasyl Tsurkan

АНАЛІЗ СУЧАСНИХ МЕТОДІВ МОДЕЛЮВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КІБЕРБЕЗПЕЦІ

Кравчук В.С.[1], Дорогий Я.Ю.[1,2,3], Цуркан В.В.[2,4]
[1] Донецький національний технічний університет
[2] Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
[3] Київський національний університет імені Тараса Шевченка
[4] Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(Україна)

Анотація. У статті проведено компаративний аналіз сучасних методів моделювання критичної інфраструктури в контексті кібербезпеки, зокрема FMEA, HAZOP, Checklist, SWIFT та тензорного аналізу. Досліджено їхні переваги, обмеження та застосування в енергетичному, транспортному та державному секторах.

Ключові слова: кібербезпека, критична інфраструктура, моделювання, FMEA, HAZOP, Checklist, SWIFT, тензорний аналіз.

Вступ. Критична інфраструктура, що охоплює енергетичні мережі, транспортні системи, державні інформаційні ресурси та інші ключові об’єкти, є основою функціонування сучасного суспільства. У контексті зростання кіберзагроз, таких як атаки на SCADA-системи, DDoS-атаки чи витоки даних, захист критичної інфраструктури набуває стратегічного значення. Згідно з дослідженнями, кількість кібератак на критичну інфраструктуру зросла на 140% у період з 2018 по 2023 роки [1], що підкреслює необхідність розробки ефективних методів моделювання та аналізу ризиків. Моделювання в кібербезпеці дозволяє не лише ідентифікувати вразливості, а й прогнозувати потенційні загрози, планувати реагування та забезпечувати стійкість систем.

Сучасні методи моделювання, такі як FMEA (Failure Mode and Effect Analysis), HAZOP (Hazard and Operability Analysis), Checklist, SWIFT (Structured What-If Technique) та тензорний аналіз, пропонують різні підходи до оцінки безпеки. FMEA забезпечує детальний аналіз впливу відмов, HAZOP систематично виявляє небезпеки, Checklist пропонує швидкий аудит за стандартами, SWIFT використовує експертні сценарії, а тензорний аналіз дозволяє обробляти багатовимірні дані для виявлення аномалій [2-7]. Кожен метод має унікальні переваги, але їхня ефективність залежить від контексту застосування, типу інфраструктури та доступних ресурсів.

Ця стаття має на меті провести компаративний аналіз сучасних методів моделювання критичної інфраструктури (FMEA, HAZOP, Checklist, SWIFT, тензорний аналіз), оцінити їхні сильні та слабкі сторони, а також проаналізувати приклади застосування в енергетичному, транспортному та державному секторах.

Сучасні методи моделювання.

1. FMEA – це систематичний метод, який використовується для ідентифікації потенційних режимів відмов у системах та оцінки їхнього впливу. У контексті кібербезпеки

критичної інфраструктури FMEA допомагає визначити вразливості, оцінити їхні наслідки та визначити пріоритети для захисту. Наприклад, у системах автоматизованого управління технологічними процесами FMEA може виявити точки, де кібератака може призвести до збою [2].

FMEA забезпечує детальний аналіз впливу відмов, що дозволяє чітко визначити критичні точки системи, але через статичний підхід метод менш ефективний для динамічних загроз, таких як реагування на кіберінциденти. Він широко застосовується для оцінки ризиків у складних системах, зокрема в енергетичних мережах.

2. HAZOP – це структурований метод для виявлення небезпек та проблем у процесах. У кібербезпеці він адаптується для аналізу вразливостей у системах управління критичної інфраструктури, таких як енергетичні чи транспортні мережі. HAZOP дозволяє систематично оцінити, як відхилення від нормального функціонування можуть призвести до кіберзагроз [3].

HAZOP охоплює широкий спектр потенційних загроз, включаючи неочевидні, але потребує значних ресурсів і часу для проведення аналізу. Метод є ефективним для великих інфраструктурних систем, де необхідний комплексний підхід до оцінки ризиків.

3. Checklist – це простий метод, який використовує списки відомих вразливостей або стандартів безпеки для оцінки стану системи. У кібербезпеці він застосовується для швидкого аудиту, наприклад, перевірки відповідності стандартам ISO/IEC 27001 [4].

Checklist вирізняється швидкістю та простотою реалізації, але не охоплює нові чи нестандартні загрози. Метод застосовується для регулярних перевірок безпеки в аеропортах та державних системах.

4. SWIFT – це гнучкий метод, який передбачає експертні обговорення для виявлення ризиків за допомогою сценаріїв "Що якщо". У кібербезпеці він дозволяє виявляти неочевидні загрози шляхом залучення експертів [5].

SWIFT вирізняється гнучкістю та здатністю виявляти широкий спектр ризиків, але залежить від якості експертів, що може призводити до суб’єктивності. Метод застосовується для аналізу складних систем, зокрема транспортних мереж.

5. Тензорний аналіз використовується для моделювання багатовимірних даних і складних взаємозв’язків у кіберфізичних системах. У кібербезпеці він допомагає виявляти аномалії та прогнозувати загрози шляхом аналізу великих обсягів даних, наприклад, мережевого трафіку чи поведінки системи [6-7].

Тензорний аналіз здатний обробляти багатовимірні дані, виявляти складні взаємозв’язки та аномалії, але характеризується високою обчислювальною складністю та вимагає спеціалізованих знань для реалізації. Метод застосовується для аналізу безпеки в кіберфізичних системах, таких як системи управління енергомережами чи IoT-мережі.

Компаративний аналіз методів. Дослідження [1] оцінює ці методи за п’ятьма критеріями: ідентифікація ризиків, реагування на кіберінциденти, відновлення, захист і стійкість. Нижче наведено порівняльну таблицю розглянутих методів (табл. 1).

Таблиця 1 – Порівняльна характеристика методів

Метод	**Ідентифікація ризиків**	**Реагування на інциденти**	**Відновлення**	**Захист**	**Стійкість**
FMEA	Висока (детальний аналіз відмов)	Низька (статичний метод)	Низька (не орієнтований на відновлення)	Середній	Середня

Метод	Ідентифікація ризиків	Реагування на інциденти	Відновлення	Захист	Стійкість
HAZOP	Висока (систематичний аналіз)	Середня (може планувати реагування)	Середня	Високий	Висока
Checklist	Середня (обмежена стандартами)	Низька (не динамічний)	Низька	Середній	Низька
SWIFT	Висока (експертний підхід)	Середня (залежить від сценаріїв)	Середня	Високий	Висока
Тензорний аналіз	Висока (аналіз багатовимірних даних)	Висока (виявлення аномалій у реальному часі)	Високий (орієнтований на відновлення)	Високий	Висока

Аналіз показує, що HAZOP та SWIFT є найбільш універсальними методами, оскільки вони охоплюють широкий спектр критеріїв і ефективно застосовуються до складних систем. FMEA забезпечує детальний аналіз впливу відмов, але її гнучкість обмежена для динамічних загроз. Checklist підходить для базового аудиту безпеки, проте не забезпечує комплексного захисту. Тензорний аналіз вирізняється високою ефективністю в ідентифікації ризиків і реагуванні на інциденти завдяки обробці багатовимірних даних, але його обмеженням є висока обчислювальна складність.

Кейси застосування. Дослідження [1] включає кейси застосування методів на реальних системах критичної інфраструктури, хоча деталі обмежені у відкритих джерелах. Нижче наведено приклади, засновані на загальних практиках:

У енергетичному секторі HAZOP застосовується для аналізу вразливостей у системах управління електромережами, зокрема для виявлення ризиків атак на SCADA-системи [8], тоді як FMEA використовується для оцінки впливу кібератак на АСУ ТП, наприклад, у теплових електростанціях [9]. У транспортній інфраструктурі SWIFT допомагає оцінювати ризики в системах управління рухом, таких як залізничні мережі, де аналізуються сценарії атак на сигнальні системи [10], а Checklist застосовується для регулярних аудитів безпеки в аеропортах, перевіряючи відповідність стандартам [11]. У державних інформаційних системах FMEA та HAZOP використовуються для оцінки вразливостей у державних реєстрах, таких як Єдиний державний реєстр, для захисту від атак типу DDoS чи витоку даних [12].

Висновки. Методи FMEA, HAZOP, Checklist та SWIFT є основними інструментами для моделювання критичної інфраструктури в кібербезпеці. HAZOP та SWIFT виділяються своєю універсальністю, тоді як FMEA ефективна для детального аналізу, Checklist – для швидких аудитів, а тензорний аналіз – здатністю обробляти багатовимірні дані для виявлення аномалій. Практичні кейси підтверджують їхню ефективність у різних секторах, хоча деталі їх використання в джерелах наведено обмежено.

ЛІТЕРАТУРА

1. Шульга В. П., Іванченко Е. В., Вишневська Н. С., Бербер А. С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави // Ukrainian Scientific Journal of Information Security. 2024. № 1. С. 95–99. DOI: 10.31673/2409-7292.2024.030001.
2. Stamatis D. H. Failure Mode and Effect Analysis: FMEA From Theory to Execution / D. H. Stamatis. Milwaukee, Wisc. : ASQC Quality Press, 1995. 494 с. URL: https://surl.li/mcubkp.
3. Center for Chemical Process Safety. Guidelines for Hazard Evaluation Procedures / Center for Chemical Process Safety. 3rd ed. Hoboken, NJ : Wiley, 2008. 576 с. DOI: 10.1002/9780470924891. URL: https://surl.li/dtlxux.
4. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements. Geneva : International Organization for Standardization, 2022. URL: https://surl.li/llkcev.
5. Bahr N. System Safety Engineering and Risk Assessment: A Practical Approach / N. Bahr. 2nd ed. Boca Raton, FL : CRC Press, 2015. 444 с. DOI: 10.1201/b17854.
6. Kolda T. G., Bader B. W. Tensor Decompositions and Applications // SIAM Review. 2009. Vol. 51, No. 3. P. 455–500. DOI: 10.1137/07070111X.
7. Dorohyi I., Tsurkan V., Kravchuk V. Tensor model for describing critical infrastructure / I. Dorohyi, V. Tsurkan, V. Kravchuk // «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 12 грудня 2024 р. / ДВНЗ «ДонНТУ; відп. ред. Г.В. Ступак. Дрогобич: ДВНЗ «ДонНТУ», 2024. с. 53-55. doi: 10.5281/zenodo.14744625. URL: surl.li/ettdno.
8. Кібербезпека енергетики: матеріали науково-практичної конференції / ІПМЕ ім. Г. Є. Пухова НАН України. Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2022. 120 с. URL: https://surli.cc/lfcddz.
9. Єрмак Д. М., Загоруйко Л. В. Огляд методів та способів підвищення безпеки експлуатації об'єктів критичної інфраструктури від кібератак // Прикладні аспекти сучасних міждисциплінарних досліджень. 2024. С. 219–220. DOI: 10.32782/2617-1236-2024-219. URL: https://surli.cc/nhspmq.
10. Аналіз світових практик захисту критичної інфраструктури // Cybersecurity Journal. 2022. № 3. С. 45–50. URL: https://surl.li/bypkqi.
11. Детальний аналіз об'єктів критичної інфраструктури // SmartTender Blog. 2022. URL: https://surl.lu/dsfrnj.
12. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 23 трав. 2019 р. № 518 // Офіційний вісник України. 2019. № 45. С. 1523. URL: https://surl.li/seyzwz.