RESILIENCE AND SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES

Oleksandr Nestorenko, Iryna Verbenets

СТІЙКІСТЬ І БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Несторенко О.В.
Сілезька академія (Польща)

Вербенець І. О.
Бердянський державний педагогічний університет (Україна)

Анотація. У дослідженні проаналізовано сучасні підходи до забезпечення стійкості та безпеки об'єктів критичної інфраструктури (КІ) України в умовах повномасштабної збройної російської агресії. Проаналізовано роль інформаційно-аналітичних систем, кібербезпеки, автономності енергопостачання та технологій штучного інтелекту у протидії загрозам. Наголошено на важливості інтегрованого підходу, що охоплює як фізичну, так і цифрову компоненти безпеки. Зроблено посилання на ключові джерела, які висвітлюють правові, технічні та управлінські аспекти теми.

Вступ. Поняття критичної інфраструктури охоплює об'єкти, системи та сервіси, від стабільного функціонування яких залежить національна безпека, обороноздатність, економіка та основні сфери життєдіяльності суспільства. В умовах російсько-української війни її вразливість стала одним із ключових викликів для держави. Цілеспрямовані удари по енергетичних об'єктах, транспортних мережах, системах зв'язку та водопостачання спричинили необхідність переосмислення традиційних підходів до захисту та управління інфраструктурою. У контексті нових викликів безпеки, зокрема гібридних загроз, що включають поєднання кібер- і фізичних атак, мають бути переглянуті правові умови функціонування критичної інфраструктури [1].

Актуальність досліджень. Останні події, пов'язані з гібридними загрозами, включаючи кібератаки, природні катаклізми та воєнні дії, вказують на необхідність впровадження адаптивних і динамічних систем захисту, здатних оперативно реагувати на зміни ситуації в режимі реального часу.

Постановка задачі. Метою дослідження є аналіз сучасних технологій, що сприяють підвищенню стійкості КІ, та визначення перспективних напрямів розвитку інформаційних та аналітичних засобів для забезпечення її безпеки.

Результати досліджень. Повномасштабна війна суттєво трансформувала характер загроз. На зміну традиційним сценаріям приходять високотехнологічні способи дестабілізації, зокрема кібератаки на об'єкти енергетики, інформаційні системи управління, транспортну логістику та фінансову сферу. Одночасно з цим – ракетні удари зумовлюють руйнування фізичної інфраструктури, що вимагає створення динамічних і адаптивних систем моніторингу та реагування. Значна частина вітчизняних установ, включно з

університетами та державними підприємствами, змушена була переміститися або змінити форму роботи [2]. Досвід цифрової трансформації переміщених вищих навчальних закладів свідчить про необхідність гнучких моделей управління інфраструктурою в умовах воєнного стану.

У межах дослідження проведено системний аналіз сучасних підходів до підвищення стійкості КІ, зокрема таких компонентів: інформаційно-аналітичних систем для моніторингу стану об'єктів; застосування SCADA-систем і сенсорних мереж; моделей машинного навчання для прогнозування ризиків; забезпечення енергетичної автономності; захисту кіберпростору та інформаційних мереж; створення резервних каналів управління та зв'язку.

Міська інфраструктура залишається однією з найбільш вразливих складових КІ. Ефективне управління міською інфраструктурою прямо впливає на її конкурентоспроможність і стійкість до зовнішніх впливів [3]. Ці підходи набули нового значення в умовах бойових дій, коли навіть локальні інциденти можуть спричинити масштабні гуманітарні наслідки. Кібербезпека об'єктів КІ – одна з ключових умов стійкості систем. Комплексне оцінювання кіберзагроз на основі вразливостей об'єктів КІ з урахуванням їхньої галузевої специфіки є важливим інструментом підвищення загальної безпеки. Одним з ефективних інструментів є впровадження систем виявлення аномалій із використанням штучного інтелекту.

В умовах частих атак на енергетичну інфраструктуру особливого значення набуває створення резервних джерел живлення, локальних енергетичних систем та забезпечення автономності об'єктів [4]. Це дозволяє не лише відновлювати функціонування після інцидентів, але й забезпечувати базовий рівень життєдіяльності навіть під час масштабних атак. Інноваційні моделі розвитку, що застосовуються у сфері інвестицій та інфраструктурного планування, можуть бути адаптовані для потреб відновлення зруйнованої інфраструктури. Це стосується, зокрема, туристичних або курортних міст, які зазнали пошкоджень, проте мають стратегічне значення для економіки [5].

Успішна протидія загрозам критичній інфраструктурі України в умовах війни можлива лише за умови поєднання технічних, правових, організаційних і цифрових інструментів. Необхідним є перехід до гібридної моделі захисту, яка інтегрує фізичну безпеку, кіберзахист, автономне енергоживлення та адаптивні моделі управління на основі аналізу великих даних. З огляду на динаміку загроз, подальші дослідження мають бути зосереджені на розробці інтелектуальних систем адаптивного реагування з високим рівнем самонавчання. У свою чергу, нормативно-правове забезпечення має враховувати реалії воєнного часу та нові стандарти безпеки.

Висновки. У ході дослідження було встановлено, що забезпечення стійкості та безпеки об'єктів критичної інфраструктури в умовах збройного конфлікту вимагає комплексного, системного підходу, який охоплює правові, технічні, організаційні та цифрові аспекти. Війна в Україні продемонструвала вразливість ключових інфраструктурних об'єктів до комбінованих загроз – фізичних атак, кіберзлочинності та інформаційних впливів. Особливої актуальності набуває розвиток інформаційно-аналітичних систем, здатних забезпечувати моніторинг стану КІ в режимі реального часу, виявляти аномалії за допомогою технологій штучного інтелекту та забезпечувати своєчасне реагування. Не менш важливим є формування гібридної моделі захисту, яка поєднує фізичну безпеку, кіберзахист, автономне енергоживлення та резервні канали управління. Успішна протидія загрозам вимагає не лише інженерних рішень, а й належного нормативно-правового забезпечення. Правова база, що регулює захист КІ, повинна бути адаптована до

умов гібридної війни та враховувати нові виклики, зокрема у сфері кібербезпеки та енергетичної автономії.

Подальші наукові розвідки мають бути спрямовані на створення інтелектуальних систем адаптивного реагування, що здатні навчатися в процесі функціонування, враховувати специфіку кожного об'єкта КІ та забезпечувати проактивне управління ризиками. Забезпечення стійкості КІ – це не лише технічне завдання, а питання національної безпеки, соціальної стабільності та виживання держави в умовах воєнних дій. Саме тому модернізація підходів до захисту інфраструктури повинна стати одним із пріоритетів державної політики України у післявоєнний період.

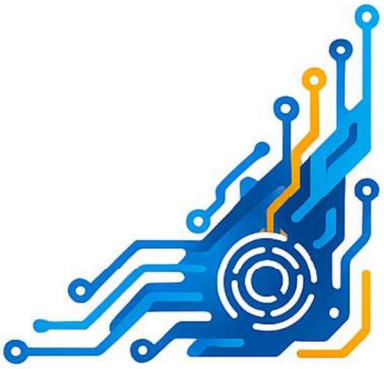
ЛІТЕРАТУРА

1. Солопова І. В. Правові умови захисту об'єктів критичної інфраструктури в Україні: проблеми та перспективи // Південноукраїнський правничий часопис. – 2021. – № 2. – С. 119–125. – DOI: https://doi.org/10.32850/sulj.2021.2.20.
2. Alieksieieva H., Kravchenko N., Horbatiuk L., Nestorenko T., Zhyhir V., Kalinichenko A., Glazova Y. Digital transformation of relocated higher education institutions in Ukraine under martial law // Problems and Perspectives in Management. – 2025. – 23 (2-si). – P.71-85. – DOI: https://doi.org/10.21511/ppm.23(2-si).2025.06
3. Nestorenko T. City infrastructure in the context of its competitiveness // Collection of scientific papers. Economic sciences. – 2007. – Vol. 59. – T. 72. – P. 70-76. – URL: https://lib.chmnu.edu.ua/pdf/naukpraci/economy/2007/72-59-13.pdf.
4. Мурасов Р., Мельник Я. Оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України // Сучасні інформаційні технології у сфері безпеки та оборони. – 2024. – № 46 (1). – С. 41–44. – DOI: https://doi.org/10.33099/2311-7249/2023-46-1-41-44.
5. Nestorenko T., Koinash M., Nestorenko O., Symonenko D. Modelling of innovative and investment processes in resort cities and destinations // Development Service Industry Management. – 2024. – № 4. – P. 351–357. DOI: https://doi.org/10.31891/dsim-2024-8(54).

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

CONTENTS

SECTION 1: ARTIFICIAL INTELLIGENCE

SECTION 2: CYBERSECURITY AND CRITICAL INFRASTRUCTURE