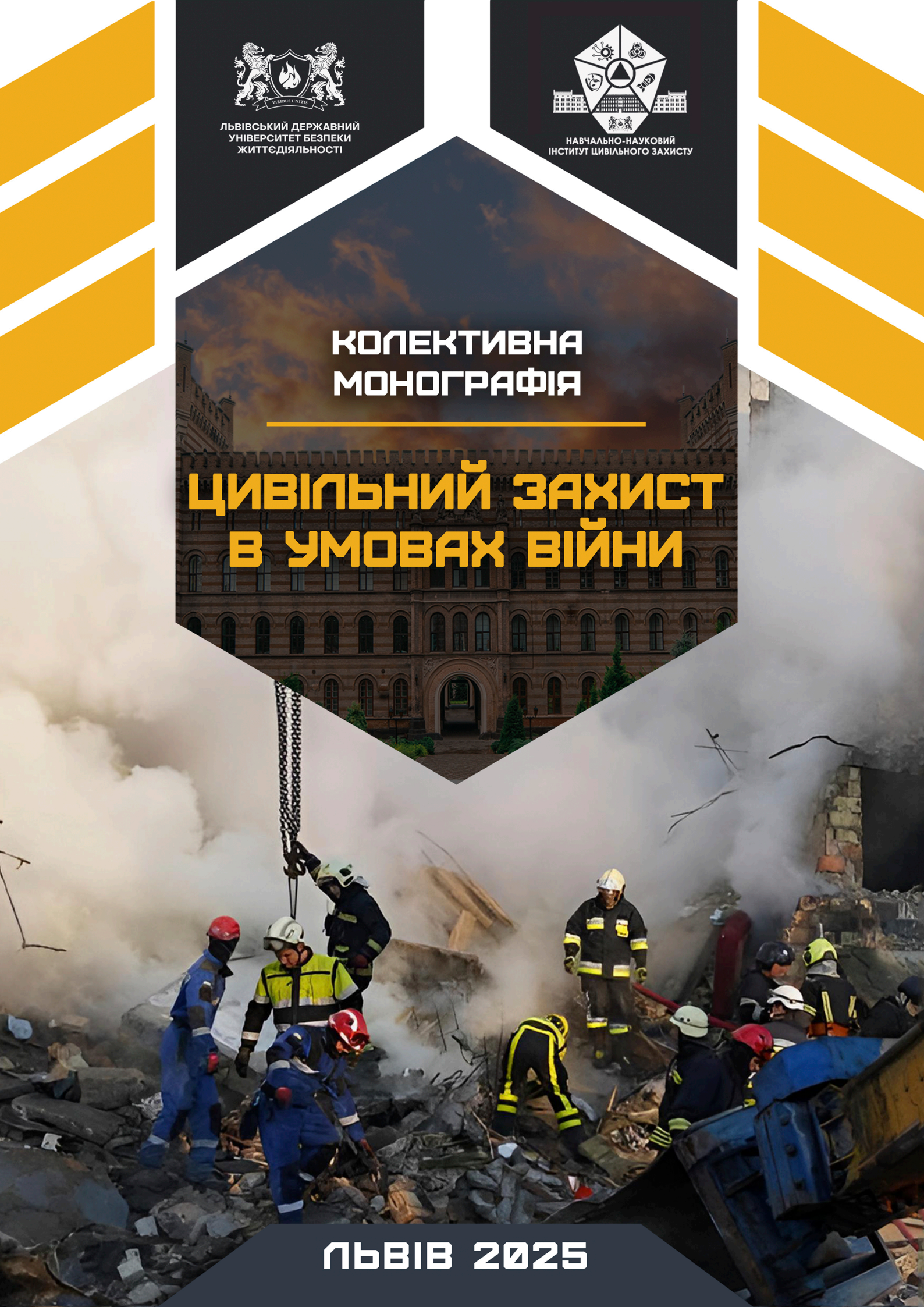
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЦИВІЛЬНОГО ЗАХИСТУ

КОЛЕКТИВНА МОНОГРАФІЯ

ЦИВІЛЬНИЙ ЗАХИСТ В УМОВАХ ВІЙНИ



ЛЬВІВ 2025

Львівський державний університет безпеки життєдіяльності

ЦИВІЛЬНИЙ ЗАХИСТ В УМОВАХ ВІЙНИ

CIVIL PROTECTION IN TIMES OF WAR

Львів 2025

УДК 614.8:355.58:351.78(477)
Ц58

Рецензенти: **Шевченко Роман Іванович** – доктор технічних наук, професор, заступник начальника центру – начальник відділу організації науково-дослідної діяльності науково-інноваційного центру Національного університету цивільного захисту України.
Авраменко Олександр Васильович – доктор технічних наук, доцент, професор кафедри логістики Повітряних Сил інституту авіації та протиповітряної оборони Національного університету оборони України.
Рогуля Андрій Олексійович – кандидат наук з державного управління, начальник навчально-методичного центру цивільного захисту та безпеки життєдіяльності Львівської області.
Зачко Олег Богданович – доктор технічних наук, професор, Заслужений діял науки і техніки України, професор кафедри права та менеджменту у сфері цивільного захисту Львівського державного університету безпеки життєдіяльності.

Редакційна колегія колективної монографії:

Бондар Дмитро Володимирович – кандидат наук з державного управління, доцент, ректор Львівського державного університету безпеки життєдіяльності.

Технічний редактор:

Яковчук Роман Святославович – доктор технічних наук, доцент, начальник навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності.

Рекомендовано до друку Вченою радою Львівського державного університету безпеки життєдіяльності
(протокол №1 від 27.08.2025 р.)

Цивільний захист в умовах війни: колективна монографія / за загальною редакцією Дмитра Бондаря. Львів: ЛДУБЖД, 2025. 524с.

Колективна монографія **«Цивільний захист в умовах війни»** присвячена аналізу сучасних викликів та пошуку ефективних рішень у сфері безпеки населення під час збройної агресії проти України. У ній досліджуються питання адаптації захисних споруд для осіб з інвалідністю та маломобільних груп, удосконалення системи евакуації та оповіщення, реагування на радіаційні, хімічні та техногенні загрози. Значна увага приділена командно-штабним навчанням, міжнародному досвіду та інноваційним підходам у сфері цивільного захисту. Автори систематизують проблеми координації органів влади та ДСНС, виявляють недоліки нормативної бази й організаційних процедур, пропонують моделі управління та алгоритми дій у кризових ситуаціях. Теоретична цінність праці полягає в розвитку наукових засад безпеки, зокрема у контексті воєнних загроз, а практична – у створенні конкретних рекомендацій для органів влади, рятувальних служб, військових та місцевих громад. Монографія поєднує наукові підходи, результати моделювання та аналіз реальних кейсів, що забезпечує її прикладне значення. Запропоновані рішення спрямовані на формування безбар'єрного середовища, стійкої системи реагування та ефективного управління надзвичайними ситуаціями. Видання має як наукову, так і практичну цінність для фахівців цивільного захисту, представників державних і місцевих органів влади, освітніх закладів та міжнародних партнерів.

ISBN 978-617-8654-10-8

БЕЗПЕКОЮ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ, ЩО ОХОРОНЯЄТЬСЯ, ВІД ТЕРОРИСТИЧНОГО НАЗЕМНОГО І ПОВІТРЯНОГО ПРОНИКНЕННЯ НА ОБ'ЄКТ..... 348

Рустам МУРАСОВ. МЕТОДИКА ОЦІНЮВАННЯ ЗАГРОЗ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ЗОНІ ВЕДЕННЯ БОЙОВИХ ДІЙ..... 367

Роман ЯКОВЧУК, Андрій ГАВРИСЬ, Вікторія ФІЛІППОВА, Назарій ТУР. КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ..... 380

Ярослав БАЛЛО, Вадим НІЖНИК, Дмитро СЕРЕДА, Олександр ТЕСЛЕНКО, Роман ПАЛЬЧИКОВ. ПРОГНОЗУВАННЯ РИЗИКІВ ТА ЗАБЕЗПЕЧЕННЯ ПРОТИПОЖЕЖНОГО ЗАХИСТУ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ..... 397

Батир ХАЛМУРАДОВ, Олег ТРЕТЬЯКОВ, Євген ЛІНЧЕВСЬКИЙ. ІНЖЕНЕРНИЙ, ФІЗИЧНИЙ ТА ВНУТРІШНІЙ ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ..... 417

Василь КАРАБИН, Роман ЯКОВЧУК, Андрій ТАРНАВСЬКИЙ. ІННОВАЦІЙНА КОНЦЕПЦІЯ ПІДГОТОВКИ КАДРІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ..... 433

РОЗДІЛ 4. РОЗВИТОК ІННОВАЦІЙ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Дмитро БОНДАР, Василь ПОПОВИЧ, Ростислав ГРИНИК. ІННОВАЦІЙНІ ІТ-СИСТЕМИ ЛЬВІВСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ ДЛЯ ЦИВІЛЬНОГО ЗАХИСТУ: RSP, «Я – ДОБРОВОЛЕЦЬ» ТА QRESCUE..... 452

Ігор ГЕТАЛО, Дмитро ЯДЧЕНКО, Ілля ЖИДЕНКО, Дмитро ДОБРЯК, Владислав РУЖИН. ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ ТА НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ ПІД ЧАС ЛІКВІДАЦІЇ НАСЛІДКІВ НАДЗВИЧАЙНИХ СИТУАЦІЙ ВНАСЛІДОК ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ..... 461

Василь ЗАВОДЮК, Назарій БУРАК, Орест ШОПСЬКИЙ. ІННОВАЦІЙНІ РІШЕННЯ В СИСТЕМІ ОПОВІЩЕННЯ НАСЕЛЕННЯ ПРО НАДЗВИЧАЙНІ СИТУАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ..... 473

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Роман ЯКОВЧУК
доктор технічних наук, доцент, начальник навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності,
r.yakovchuk@ldubgd.edu.ua, ORCID: 0000-0001-5523-5569

Андрій ГАВРИСЬ
кандидат технічних наук, доцент, заступник начальника кафедри цивільного захисту Львівського державного університету безпеки життєдіяльності,
Havrys.AND@gmail.com, ORCID: 0000-0003-2527-7906

Вікторія ФІЛІППОВА
ад'юнкт денної форми здобуття освіти докторантури-ад'юнктури Львівського державного університету безпеки життєдіяльності,
filippova99@ukr.net, ORCID: 0000-0003-0771-1975

Назарій ТУР
здобувач четвертого (освітньо-наукового) рівня вищої освіти Львівського державного університету безпеки життєдіяльності,
rptb2020@gmail.com, ORCID: 0000-0002-0557-5351

У дослідженні розглядаються проблеми захисту об'єктів критичної інфраструктури (ОКІ) України в умовах повномасштабної збройної агресії. Проведено інформаційно-аналітичний огляд атак на інфраструктурні об'єкти за період 2022-2024 років із використанням різних видів озброєння.

Обґрунтовано необхідність комплексного підходу до безпеки, що охоплює організаційні, технічні, інформаційні та кадрові компоненти.

Представлено узагальнену блок-схему заходів із захисту критичної та енергетичної інфраструктури та запропоновано інтеграцію міжнародного досвіду до національних рішень.

Мета дослідження: сформувати науково обґрунтований підхід до зміцнення захисту об'єктів критичної інфраструктури України в умовах воєнного стану шляхом аналізу сучасних загроз, статистичних тенденцій атак, систем ризик-менеджменту та практик міжнародного досвіду.

Методи дослідження: інформаційно-аналітичний метод, порівняльний аналіз, системний аналіз, методи ризик-менеджменту.

Результати: на основі дослідження встановлено, що з 2022 до 2024 року понад 2110 об'єктів критичної інфраструктури зазнали уражень, з яких 425 – об'єкти енергетики; найбільш поширені загрози: ракетні обстріли, удари БпЛА, кібератаки; запропоновано структуру інтегрованого підходу до захисту, що включає: прогнозування загроз, раннє виявлення, інженерний та цифровий захист; узагальнено міжнародні практики управління стійкістю, сформовано блок-схеми стратегічного захисту критичної та енергетичної інфраструктури [1].

Теоретична цінність дослідження: теоретична цінність полягає у розвитку концептуального підходу до аналізу системи захисту об'єктів критичної інфраструктури як складної соціотехнічної системи в умовах гібридної війни. Узагальнено положення щодо мультидисциплінарного ризик-менеджменту.

Практична цінність дослідження: практичні результати можуть бути використані при розробці державних програм із захисту критичних об'єктів; у процесі модернізації систем енергозабезпечення; під час планування оборонних інженерних заходів на об'єктах а також при підготовці персоналу.

Оригінальність: дослідження об’єднує статистичні дані про ураження критичної інфраструктури, блок-схемне відображення заходів безпеки та міжнародні підходи до управління ризиками, створюючи цілісну модель захисту у воєнних умовах.

Обмеження дослідження: деякі обмеження пов’язані з неповнотою або засекреченістю статистичних даних про ураження військових та інших об’єктів.

Майбутні дослідження: перспективним напрямом подальших досліджень є створення математичних моделей для прогнозування деструктивного ефекту на інфраструктуру.

Ключові слова: критична інфраструктура, воєнний стан, енергетична безпека, ризик-менеджмент, системний аналіз, обстріли.

COMPREHENSIVE PROTECTION SYSTEM FOR UKRAINE'S CRITICAL INFRASTRUCTURE UNDER MARTIAL LAW

Roman YAKOVCHUK
Doctor of Technical Sciences, Associate Professor, Head of the Educational and Scientific Institute of Civil Protection, Lviv State University of Life Safety,
r.yakovchuk@ldubgd.edu.ua, ORCID: 0000-0001-5523-5569

Andrii HAVRYS
PhD in Technical Sciences, Associate Professor, Deputy Head of the Department of Civil Protection, Lviv State University of Life Safety,
Havrys.AND@gmail.com, ORCID: 0000-0003-2527-7906

Viktoriia FILIPPOVA
Adjunct of the Full-Time Doctoral (PhD) Program, Lviv State University of Life Safety,
filippova99@ukr.net, ORCID: 0000-0003-0771-1975

Nazarii TUR
Graduate of the third (educational and scientific) level of higher education at the Lviv State University of Life Safety,
rptb2020@gmail.com, ORCID: 0000-0002-0557-5351

The article addresses the challenges of protecting critical infrastructure facilities in Ukraine under conditions of full-scale armed aggression. An information and analytical overview of attacks on infrastructure objects during 2022-2024 is provided, covering the use of various types of weaponry, including missiles, Shahed-136 drones, aerial bombs, and S-300/S-400 systems.

The necessity for a comprehensive security approach is substantiated-one that integrates organizational, technical, informational, and human resource components.

A generalized block diagram of measures for the protection of critical and energy infrastructure is presented, including automated monitoring systems, cybersecurity solutions, engineering shelters, and intelligent risk management tools.

The integration of international practices into national protection systems is proposed.

Purpose: to develop a scientifically grounded approach to strengthening the protection of Ukraine’s critical infrastructure under martial law through the analysis of current threats, statistical trends of attacks, risk management systems, and international practices.

Method: information and analytical method, comparative analysis, systems analysis, and risk management methodologies.

Findings: the study established that over 2,110 critical infrastructure facilities were damaged between 2022 and 2024, including 425 energy sector objects.

The most common threats were missile strikes, UAV attacks, and cyber incidents.

An integrated protection framework is proposed, which includes threat forecasting, early detection, engineering and digital protection.

International resilience management practices have been generalized (ISO 31000, cybersecurity models, blockchain-based solutions, etc.).

Strategic protection block diagrams for critical and energy infrastructure have been developed (Figures 5-6).

Theoretical significance: the theoretical value lies in the development of a conceptual framework for analyzing critical infrastructure protection as a complex sociotechnical system in the context of hybrid warfare. Key principles of multidisciplinary risk management have been summarized.

Practical implicstions: the practical findings can be used in the development of state programs for the protection of critical assets, in the modernization of energy supply systems, in the planning of engineering defense measures, and in personnel training.

Originality: this study combines statistical data on infrastructure damage, block-diagram representations of protective measures, and international risk management practices to form an integrated protection model under conditions of war.

Research Limitations: some limitations are due to the incompleteness or confidentiality of statistical data on the damage to military infrastructure.

Future Research: a promising direction for further research is the development of mathematical models to forecast the destructive impact on infrastructure.

Keywords: critical infrastructure, martial law, energy security, risk management, systems analysis, missile attacks.

Вступ

У XXI столітті критична інфраструктура постає не лише як сукупність об’єктів технічного забезпечення, а як складна соціотехнічна система, від надійності якої залежить стабільність функціонування держави в умовах надзвичайних ситуацій. Особливої актуальності ця проблема набуває в Україні – країні, яка з 2022 року є об’єктом збройної агресії з боку російської федерації. Масовані атаки на об’єкти енергетики, транспорту, комунального господарства, медицини та зв’язку показали, що критична інфраструктура стала не лише інженерною, але й стратегічною мішенню, виведення з ладу якої призводить до серйозних соціальних і гуманітарних криз.

Особливість сучасної війни полягає у її гібридному характері, що поєднує фізичні атаки із кібератаками, інформаційними впливами, економічним тиском. У цьому контексті критична інфраструктура стає вразливою з усіх боків – як до прямих ракетних ударів, так і до цифрових збоїв, диверсій, знищення ланцюгів постачання, перешкод у логістиці та комунікаціях. Більше того, об’єкти інфраструктури нерідко стають інструментом для створення тиску на цивільне населення, що свідчить про наявність цілеспрямованої стратегії ворога щодо ескалації соціальної напруги.

Український досвід, на жаль, уже продемонстрував масштабні наслідки таких дій. У періоди осінньо-зимових кампаній 2022-2024 років сотні населених пунктів залишались без світла, тепла і зв’язку внаслідок ударів по енергетичних об’єктах. Деякі регіони втрачали доступ до питної води через порушення роботи насосних станцій. Було уражено великі об’єкти паливно-енергетичного комплексу, трансформаторні підстанції, магістральні лінії, диспетчерські центри. Наслідки таких атак проявляються не лише в економічному вимірі, а й у сфері гуманітарної безпеки, охорони здоров’я, соціальної стабільності.

Окрім фізичних загроз, особливе занепокоєння викликають кібератаки, які дедалі частіше супроводжують ракетні обстріли. Відомо про численні випадки спроб втручання у роботу SCADA-систем, злам операторських серверів, саботаж енергетичних процесів. У 2023-2024 роках було зафіксовано складні багаторівневі атаки на цифрові системи управління інфраструктурою, які поєднували елементи соціальної інженерії, шкідливого програмного забезпечення та DDoS-кампаній. Така багатовекторність загроз вимагає перегляду традиційного підходу до безпеки – від простої охорони об’єктів до формування цілісної

- інформаційно-аналітичні (моделювання ризиків, системи раннього виявлення).
- Водночас, адаптація міжнародного досвіду вимагає врахування українських реалій:
- асиметричність загроз: Україна стикається з ракетними та дроновими атаками майже щодня, що потребує не лише стійкості, а й мобільності захисту;
- ресурсні обмеження: необхідність формувати рішення, які можуть бути ефективними навіть при обмеженому фінансуванні;
- високий ступінь непередбачуваності: агресор постійно змінює тактику.

Крім того, важливим чинником є людський ресурс – як на рівні оперативного персоналу об'єктів, так і на рівні управлінських рішень. Необхідна підготовка кадрів, які володіють навичками кризового управління, розумінням технологій кіберзахисту та системного аналізу загроз.

Таким чином, сучасна система захисту критичної інфраструктури має бути динамічною, адаптивною, технологічно гнучкою та глибоко інтегрованою в загальнонаціональну систему безпеки.

Висновки

В дослідженні проаналізовано захист об'єктів критичної інфраструктури України під час військового конфлікту, підкреслюючи складність сучасних загроз і необхідність комплексного підходу.

У роботі чітко підкреслено, що критична інфраструктура є основою життєдіяльності країни, тому що забезпечує функціонування економіки, транспорту, зв'язку та комунальних послуг для населення. Модернізація об'єктів інфраструктури, використання систем моніторингу та посилення фізичного захисту значно підвищують стійкість до атак, включаючи ракетні та кібернетичні загрози.

Також авторами доведено, що захист енергетичних об'єктів є пріоритетом, оскільки енергетичний сектор України є стратегічно важливою частиною інфраструктури, а знищення чи пошкодження об'єктів енергетики призводить до знеструмлення великих регіонів, що в свою чергу паралізує роботу інших важливих установ. Ураження цих об'єктів може ускладнити логістику, ремонт техніки, виробництво зброї та інші оборонні процеси. Відсутність електроенергії та тепла в умовах холодної погоди створює серйозні проблеми для здоров'я громадян України.

У підсумку, в умовах безпрецедентного зростання атак та техногенних загроз, запропоновані заходи покликані не лише підвищити стійкість інфраструктури до руйнувань, але й сприяти стабільності держави та безпеці її громадян. Досвід, отриманий з аналізу міжнародних практик, дозволяє Україні адаптувати ефективні стратегії для захисту критичної інфраструктури, а також розробляти національні підходи, що враховують специфіку сучасного конфлікту та необхідність оперативного реагування. Ці висновки та рекомендації можуть слугувати фундаментом для подальших наукових та прикладних досліджень, спрямованих на формування комплексної системи захисту об'єктів критичної інфраструктури у контексті глобальної та національної безпеки.

Список використаних джерел

1. Статистика повітряних тривог. URL: https://air-alarms.in.ua/?from=2022-02-24&to=2024-08-30#statistic.

2. Закон України від 16 листопада 2021 року №1882-IX «Про критичну інфраструктуру».

3. Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури».

4. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT).

5. Havrys, A., Filippova, V., & Tur, N. (2024). Інформаційний аналіз систем захисту об'єктів критичної інфраструктури в період дії воєнного стану. Вісник Львівського

державного університету безпеки життєдіяльності, 30, 173-187. https://doi.org/https://doi.org/10.32447/20784643.30.2024.17.

6. Герасименко О.М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. № 84(3).

7. Іваницька О., Возненко О. Управління ризиками об'єктів критичної інфраструктури. Фінанси України. 2024. № 6. С. 93–107.

8. Арсенович Л.А. Підготовка фахівців у сфері захисту критичної інфраструктури. Таврійський науковий вісник. Серія: Публічне управління та адміністрування. 2023. № 5. С. 3–14.

9. Скіцько О., Ширшов Р. Система управління інформаційною безпекою як інструмент підвищення рівня захисту об'єктів КІ. Міжнародний науковий журнал інженерії та сільського господарства. 2023. № 2(6). С. 12–22.

10. George S., Baskar T., Srikaanth P. B. Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. Partners Universal International Innovation Journal. 2024. Vol. 2(1). P. 51–75.

11. Bjarte R., Lange D., Marianthi T., Pursiainen C. From risk management to resilience management in critical infrastructure. Journal of Management in Engineering. 2020. Vol. 36(4).

12. Govea J., Gaibor-Naranjo W., Villegas-Ch W. Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. Computer. 2024. Vol. 13. P. 122.

13. Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection. 2015. Vol. 8. P. 53–66.

14. Pursiainen C., Kytömaa E. From European critical infrastructure protection to the resilience of European critical entities. Sustainable and Resilient Infrastructure. 2022. Vol. 8(1). P. 85–101.

15. Lifshitz Sherzer G., Urlainis A., Moya S., Shohet I. Seismic Resilience in Critical Infrastructures: A Power Station Preparedness Case Study. Applied Sciences. 2024. Vol. 14. P. 3835.

16. Чумаченко С.М., Кутовий О.П., Попель В.А., Гуйдра О.Г., Заїка Н.В., Мурасов Р.К. Науково-методичний підхід щодо оцінювання безпеки критичної інфраструктури на основі комплексу засобів захисту її об'єктів від БПЛА і крилатих ракет. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2023. № 1

17. Казьмірук С.Д., Леонов Б.Д., Омельян О.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури на основі використання штучного інтелекту в умовах воєнного стану. Юридичний науковий електронний журнал. 2024. № 6.

18. Коцюруба В.І., Білик А.С. Захист КІ від ракетних ударів через підземне розташування. Ядерна та радіаційна безпека. 2023. № 2(98). С. 69–79.

References

1. Air Raid Statistics. URL: https://air-alarms.in.ua/?from=2022-02-24&to=2024-08-30#statistic

2. Law of Ukraine of November 16, 2021, No. 1882-IX "On Critical Infrastructure".

3. Resolution of the Cabinet of Ministers of Ukraine dated July 22, 2022, No. 821 "On Approval of the Procedure for Monitoring the Security Level of Critical Infrastructure Facilities".

4. DSTU ISO 31000:2018 Risk Management. Principles and Guidelines (ISO 31000:2018, IDT).

5. Havrys, A., Filippova, V., & Tur, N. (2024). Information Analysis of Protection Systems for Critical Infrastructure Facilities During Martial Law. Bulletin of the Lviv State University of Life Safety, 30, 173–187. https://doi.org/10.32447/20784643.30.2024.17

6. Herasymenko, O. M. (2024). Threats to critical infrastructure facilities in Ukraine under martial law. Scientific Bulletin of Uzhhorod National University. Law Series, 84(3). [In Ukrainian].

7. Ivanytska, O., & Voznenko, O. (2024). Risk management of critical infrastructure facilities. Finance of Ukraine, 6, 93–107. [In Ukrainian].

8. Arsenovych, L. A. (2023). Training specialists in the field of critical infrastructure protection. Tavriya Scientific Bulletin. Public Administration and Administration Series, 5, 3–14. [In Ukrainian].

9. Skitsko, O., & Shyrshov, R. (2023). Information security management system as a tool for improving the protection of critical infrastructure facilities. International Scientific Journal of Engineering and Agriculture, 2(6), 12–22. [In Ukrainian].

10. George, S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51–75.

11. Bjarte, R., Lange, D., Marianthi, T., & Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. Journal of Management in Engineering, 36(4).

12. Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Securing critical infrastructure with blockchain technology: An approach to cyber-resilience. Computer, 13, 122.

13. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53–66.

14. Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities. Sustainable and Resilient Infrastructure, 8(1), 85–101.

15. Lifshitz Sherzer, G., Urlainis, A., Moya, S., & Shohet, I. (2024). Seismic resilience in critical infrastructures: A power station preparedness case study. Applied Sciences, 14, 3835.

16. Chumachenko, S. M., Kutovyi, O. P., Popel, V. A., Huidera, O. H., Zaika, N. V., & Murasov, R. K. (2023). Scientific-methodical approach to assessing the security of critical infrastructure based on integrated protection tools against UAVs and cruise missiles. Scientific Notes of V. I. Vernadsky Taurida National University. Technical Sciences Series, 1. [In Ukrainian].

17. Kazmiruk, S. D., Leonov, B. D., & Omelian, O. S. (2024). Ensuring cybersecurity of critical infrastructure objects using artificial intelligence under martial law conditions. Legal Scientific Electronic Journal, 6. [In Ukrainian].

18. Kotsiuruba, V. I., & Bilyk, A. S. (2023). Protection of critical infrastructure from missile strikes through underground placement. Nuclear and Radiation Safety, 2(98), 69–79. [In Ukrainian].

колективна монографія

ЦИВІЛЬНИЙ ЗАХИСТ В УМОВАХ ВІЙНИ

CIVIL PROTECTION IN TIMES OF WAR

Літературний редактор	**Галина ПАДИК**
Технічний редактор	**Роман ЯКОВЧУК**
Комп’ютерна верстка	**Маріанна КЛИМУС**
Друк	**Назарій ПЕТРОЛЮК**

Підписано до друку 04.09.2025 р.
Формат 60х84/12. Гарнітура Times New Roman.
Папір офсетний. Ум. Друк. арк. 43,6. Тираж 100.

Друк ЛДУБЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
Тел. /факс: (032)233-24-79
E-mail: vnrd@ldubgd.edu.ua
Свідоцтво суб’єкта видавничої справи ДК №7249 від 09.02.2021 р.

ЗАПОБІГТИ

ВРЯТУВАТИ

ДОПОМОГТИ

ISBN 978-617-8654-10-8