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

за загальною редакцією Дмитра Бондаря

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

ІННОВАЦІЙНА КОНЦЕПЦІЯ ПІДГОТОВКИ КАДРІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Василь КАРАБИН
доктор технічних наук, професор, професор кафедри цивільного захисту Львівського державного університету безпеки життєдіяльності,
vasyl.karabyn@gmail.com, ORCID: 0000-0002-8337-5355

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 ТАРНАВСЬКИЙ
кандидат технічних наук, доцент, доцент кафедри цивільного захисту Львівського державного університету безпеки життєдіяльності,
andry090880@ukr, ORCID: 0000-0002-4625-2022

Мета дослідження: обґрунтувати потреби у впровадженні цілісної, багаторівневої моделі підготовки фахівців у сфері цивільного захисту з акцентом на захист критичної інфраструктури. Ключовим завданням такої системи є не лише формування теоретичних знань, а й розвиток практичних компетентностей для роботи в реальному полі ризику.

Методи дослідження: у роботі використано комплексний міждисциплінарний підхід, що включає аналіз наукової літератури, порівняльний аналіз міжнародних і національних освітніх практик, контент-аналіз нормативно-правових актів, а також експертні інтерв'ю з представниками ДСНС України, МВС, державних підприємств та освітніх закладів. Особливу увагу приділено аналізу компетентнісних моделей, модульних освітніх програм, симуляційних тренінгів і практико-орієнтованого навчання. Дослідження також спирається на аналіз кейсів із впровадження інноваційних освітніх технологій у країнах ЄС та НАТО.

Результати: розроблено концепцію багаторівневої системи підготовки фахівців для захисту КІ, яка охоплює бакалаврські, магістерські та програми підвищення кваліфікації. Визначено ключові компетентності, необхідні для сучасних фахівців: аналітичні, прогностичні, організаційні, комунікативні, а також вміння працювати з сучасними технологіями моніторингу, реагування та управління ризиками. Доведено, що впровадження такої системи підготовки сприятиме підвищенню рівня безпеки об'єктів КІ, зменшенню втрат у надзвичайних ситуаціях, формуванню кадрового резерву для ДСНС України, МВС, держпідприємств і підвищенню стійкості держави до гібридних загроз.

Теоретична цінність дослідження: полягає у розвитку концепції міждисциплінарної підготовки фахівців для сфери цивільного захисту та захисту КІ, а також у систематизації сучасних освітніх моделей і підходів, що застосовуються у провідних країнах світу. Дослідження пропонує нову парадигму формування компетентностей, яка враховує як національні, так і міжнародні стандарти, інтегруючи елементи ризик-менеджменту, кризового управління, кібербезпеки та інституційної взаємодії.

Оригінальність: розробка цілісної моделі багаторівневої підготовки фахівців, яка враховує сучасні виклики для КІ, а також у пропозиції механізмів інтеграції європейських освітніх стандартів у національну систему освіти. Вперше запропоновано структуру освітніх програм, яка поєднує теоретичну підготовку, практичні тренінги, симуляційні навчання та партнерство з роботодавцями для формування професійної спільноти у сфері захисту КІ.

Практична цінність: можливість використання запропонованої моделі для розробки та впровадження нових освітніх програм у закладах вищої освіти, підвищення кваліфікації персоналу ДСНС України, МВС, держпідприємств та приватного сектору. Результати

дослідження можуть бути використані для удосконалення нормативно-правової бази, розробки стандартів професійної підготовки, а також для підвищення рівня безпеки та стійкості критичної інфраструктури України в умовах сучасних загроз.

Ключові слова: цивільний захист; критична інфраструктура; підготовка кадрів; модульна освітня програма; міжвідомча взаємодія.

INNOVATIVE CONCEPT OF PERSONNEL TRAINING TO ENSURE THE SAFETY AND RESILIENCE OF CRITICAL INFRASTRUCTURE

Vasyl KARABYN
Dr.Eng., Professor, Department of Civil Protection, Lviv State University of Life Safety,
vasyl.karabyn@gmail.com, ORCID: 0000-0002-8337-5355

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 TARNAVSKYI
Ph.D., Associate Professor, Department of Civil Protection, Lviv State University of Life Safety,
andry090880@ukr.net, ORCID: 0000-0002-4625-2022

Purpose of the Study: this monograph subsection aims to substantiate the need for implementing an integrated, multi-level model of specialist training in the field of civil protection, with a focus on safeguarding critical infrastructure. The key objective of this system is not only to impart theoretical knowledge but also to develop practical competencies required to operate effectively in real risk environments.

Research Methods: a comprehensive interdisciplinary approach was employed, including analysis of scientific literature; comparative review of international and national educational practices; content analysis of legal and regulatory documents; and expert interviews with representatives of the State Emergency Service (DSNS), Ministry of Internal Affairs (MIA), state-owned enterprises, and educational institutions. Special attention was given to competency frameworks, modular educational programs, simulation-based training, and practice-oriented learning. The study also draws on case analyses of innovative educational technology implementations in EU and NATO member states.

Results: a multi-level training system for critical infrastructure specialists was developed, encompassing bachelor's, master's, and continuing professional development programs. Key competencies required of modern practitioners were identified: analytical and forecasting abilities; organizational and communication skills; and proficiency with advanced monitoring, response, and risk-management technologies. It was demonstrated that implementing this training model will enhance the security of critical infrastructure facilities, reduce losses during emergencies, build a personnel reserve for DSNS, MIA, and state enterprises, and increase the nation's resilience to hybrid threats.

Theoretical Value: the study advances the concept of interdisciplinary training for civil protection and critical infrastructure defense specialists, and systematically organizes contemporary educational models and approaches used in leading countries. It offers a new paradigm for competency development that integrates national and international standards, blending elements of risk management, crisis governance, cybersecurity, and institutional cooperation.

Originality: the research introduces a holistic multi-level training model that addresses current critical infrastructure challenges and proposes mechanisms for integrating European educational standards into the national system. For the first time, an educational program structure is presented that combines theoretical instruction, practical drills, simulation-based learning, and employer partnerships to cultivate a professional community dedicated to critical infrastructure protection.

Practical Value: the proposed model can be applied to design and implement new curricula in higher-education institutions, as well as to upgrade the qualifications of personnel within DSNS, MIA, state enterprises, and the private sector. Study outcomes may inform improvements to the legal and regulatory framework, the development of professional training standards, and measures to enhance the safety and resilience of Ukraine's critical infrastructure in the face of contemporary threats.

Keywords: civil protection; critical infrastructure; personnel training; modular educational program; interagency cooperation.

Вступ

Критична інфраструктура є основою функціонування сучасної держави, забезпечуючи сталість соціальних, економічних і політичних процесів. До об'єктів критичної інфраструктури належать енергетичні системи, транспорт, зв'язок, водопостачання, охорона здоров'я, фінансові установи, а також інформаційно-комунікаційні технології. В умовах глобальної нестабільності та зростання кількості загроз, питання захисту критичної інфраструктури набуває особливої актуальності. Сучасні виклики, такі як війна, кіберзагрози та техногенні катастрофи, вимагають комплексного підходу до підготовки фахівців, здатних ефективно реагувати на ці ризики та забезпечувати безперервність функціонування життєво важливих систем.

Збройні конфлікти, особливо в умовах сучасної гібридної війни, суттєво впливають на безпеку критичної інфраструктури. Військові дії супроводжуються цілеспрямованими атаками на енергетичні, транспортні, водопостачальні та інші об'єкти, від яких залежить життєдіяльність населення та економіки. Досвід останніх років, зокрема війна в Україні, показав, що противник активно використовує удари по енергетичних системах, мостах, залізничних вузлах, об'єктах зв'язку для дестабілізації ситуації в тилу, створення паніки та зниження обороноздатності держави. Руйнування таких об'єктів призводить до масштабних соціальних, економічних і гуманітарних наслідків, а також може створювати "каскадний ефект", коли пошкодження одного сектору тягне за собою збої в інших сферах життєдіяльності [1].

На особливу увагу заслуговує питання захисту об'єктів паливно-енергетичного комплексу [2-5], які часто стають першочерговою ціллю під час воєнних дій. Знищення або пошкодження електростанцій, підстанцій, ліній електропередачі може спричинити відключення цілих регіонів від електропостачання, що унеможливлює нормальне функціонування лікарень, водоканалів, транспорту, підприємств та інших важливих об'єктів. Водночас, атаки на транспортну інфраструктуру ускладнюють евакуацію населення, постачання гуманітарної допомоги та переміщення військ [1].

З розвитком цифрових технологій та зростанням рівня автоматизації управління об'єктами критичної інфраструктури, зростає і ризик кібератак. Кіберзагрози стали невід'ємною частиною сучасних гібридних конфліктів, оскільки атаки на інформаційні системи можуть бути не менш руйнівними, ніж фізичне знищення об'єктів. Критична інфраструктура часто є основною мішенню для кібератак, спрямованих на виведення з ладу енергетичних систем, транспортних вузлів, водопостачання, фінансових установ та інших життєво важливих сфер [6]. Зловмисники використовують складні методи проникнення в інформаційні системи, зокрема фішинг, соціальну інженерію, шкідливе програмне забезпечення, а також атаки типу "відмова в обслуговуванні" (DDoS). Наслідком таких атак може стати зупинка енергопостачання, порушення роботи транспорту, банківських систем, а також витік або знищення важливої інформації. Особливо небезпечними є атаки на системи автоматизованого управління (SCADA), які використовуються для моніторингу та контролю технологічних процесів на об'єктах енергетики, водопостачання, транспорту [6]. В останні роки фіксується зростання кількості цілеспрямованих кібератак на критичну інфраструктуру різних країн. Наприклад, у 2022 році в Україні було зафіксовано низку потужних кібератак на енергетичний сектор, що супроводжувалися фізичними ударами по об'єктах інфраструктури. Це свідчить про інтеграцію кібер- та фізичних атак у межах гібридної війни. Для ефективного протистояння таким загрозам необхідно не лише впроваджувати сучасні засоби кіберзахисту,

Значним суспільним ефектом є зменшення втрат у надзвичайних ситуаціях. Завдяки високому рівню професійної підготовки, фахівці будуть здатні організовувати ефективне реагування на кризові події, координувати евакуаційні заходи, проводити ліквідацію наслідків аварій та катастроф. Це дозволить мінімізувати людські жертви, зменшити матеріальні збитки та знизити негативний вплив на навколишнє середовище. Крім того, швидке відновлення роботи об'єктів КІ після надзвичайних подій сприятиме стабілізації економіки та підтримці життєдіяльності населення.

Особливе значення має формування кадрового резерву для ключових державних структур, таких як ДСНС України, МВС, а також для державних підприємств, що відповідають за експлуатацію та безпеку КІ. Наявність підготовлених, мобільних та адаптивних фахівців дозволить оперативно реагувати на нові виклики, підсилювати існуючі підрозділи та забезпечувати безперервність функціонування систем безпеки. Це особливо актуально в умовах зростання складності загроз, що вимагає високої готовності та професіоналізму персоналу.

Крім того, створення такої системи підготовки сприятиме підвищенню рівня міжвідомчої та міжсекторальної взаємодії. Фахівці нового покоління будуть володіти навичками координації дій між різними державними органами, приватним сектором та міжнародними партнерами, що є критично важливим для ефективного управління ризиками та кризовими ситуаціями на національному рівні. Такий підхід сприятиме формуванню єдиної системи безпеки, здатної швидко адаптуватися до нових викликів.

Суспільний ефект від реалізації програми також полягає у підвищенні довіри громадян до системи безпеки та захисту. Кваліфіковані фахівці, які діють професійно і оперативно, сприяють зменшенню паніки, підвищенню рівня обізнаності населення щодо заходів безпеки та формуванню культури безпеки в суспільстві. Це, у свою чергу, зміцнює соціальну згуртованість та підвищує загальну стійкість держави до різних загроз.

Важливо також відзначити, що створення системи підготовки фахівців нового покоління сприятиме розвитку науково-дослідницької діяльності у сфері захисту КІ. Це дозволить впроваджувати інноваційні технології, розробляти нові методики оцінки ризиків та управління безпекою, а також підвищувати ефективність існуючих систем захисту. Такий науково-практичний потенціал буде важливим ресурсом для держави у забезпеченні її безпеки та конкурентоспроможності.

Отже, очікувані результати реалізації системи підготовки фахівців нового покоління у сфері захисту критичної інфраструктури є багатогранними і мають суттєвий вплив на безпеку, економіку та соціальну стабільність країни. Вони включають:

–Створення високоефективної системи підготовки фахівців, що відповідає сучасним викликам і стандартам;

–Підвищення рівня безпеки та стійкості ОКІ, що знижує ризики виникнення надзвичайних ситуацій;

–Зменшення людських, матеріальних та екологічних втрат у разі надзвичайних ситуацій завдяки оперативному та професійному реагуванню;

–Формування кадрового резерву для ключових державних структур та підприємств, що забезпечує гнучкість і оперативність у реагуванні на загрози;

–Посилення міжвідомчої та міжнародної співпраці у сфері безпеки;

–Підвищення рівня довіри населення до системи захисту та формування культури безпеки;

–Розвиток науково-дослідницьких і інноваційних процесів у сфері захисту КІ.

–У підсумку, реалізація комплексної системи підготовки фахівців нового покоління створює міцний фундамент для забезпечення національної безпеки, ефективного управління ризиками та сталого розвитку країни в умовах сучасних викликів і загроз.

Висновки

1. Сучасні загрози критичній інфраструктурі України носять комплексний характер: від прямих військових дій та гібридних атак до кіберінцидентів і техногенних аварій. Це потребує перегляду традиційних підходів до підготовки фахівців із захисту КІ – від теоретичного

вивчення стандартів до відпрацювання практичних навичок у наближених до реальності кризових сценаріях. Водночас інтеграція автоматизованих систем моніторингу з аналітично-прогностичними інструментами доводить свою ефективність у своєчасному виявленні вразливостей і зменшенні масштабу потенційних наслідків.

2. Європейські стандарти та стандарти НАТО (зокрема ISO 27001 і Directive (EU) 2022/2557) можуть і повинні бути адаптовані до українського контексту з урахуванням особливостей взаємодії держструктур та громадського сектору. Саме за умови чіткої регламентації міжвідомчої взаємодії й регулярного обміну інформацією між ДСНС України, поліцією, операторами енергомереж та кіберслужбами стає можливим швидке й скоординоване реагування на інциденти.

3. Модульна структура освітньої програми, показує свою практичну доцільність: учасники тренінгів одночасно розвивають аналітичні здібності, навички роботи з SCADA-системами, розуміння принципів управління безперервністю діяльності та комунікацію в кризових умовах. Така покрокова побудова навчального процесу дозволяє ефективно оцінювати прогрес і коригувати програму відповідно до динаміки загроз.

4. Дослідження підкреслює необхідність створення механізмів постійного моніторингу якості підготовки кадрів і динамічного оновлення стандартів програми за допомогою системи KPI. Це забезпечить гнучкість – вчасне впровадження нових модулів для протидії надзвичайним ситуаціям. Лише завдяки такому проактивному підходу Україна зможе підтримувати стійкість своєї критичної інфраструктури перед обличчям невпинно зростаючих викликів.

Список використаних джерел

1. Koval, V. V., & Shapoval, O. V. (2020). The system of state protection of critical infrastructure of Ukraine: genesis, current state and prospects for optimization in terms of further national security. Chas Prava (Time of Law), (4), 146–153. https://chasprava.com.ua/index.php/journal/article/view/592

2. Kochmar, I., Karabyn, V. (2023). Water Extracts from Waste Rocks of the Coal Industry of Chervonograd Mining Area (Ukraine): Problems of Environmental Safety and Civil Protection. Ecological Engineering & Environmental Technology, 24(1), 247-255. https://doi.org/10.12912/27197050/155209

3. Kochmar, I., Karabyn , V., Stepova, K., Stadnik, V., & Sozanskyi, M. (2024). Thermal Impact on Heavy Metal Bioavailability in Burnt Rocks of Waste Heap of Chervonohradska Coal-preparation Plant (Lviv Region, Ukraine). Geomatics and Environmental Engineering, 18(1), 117–133. https://doi.org/10.7494/geom.2024.18.1.117

4. Kochmar, I., Karabyn, V., Kordan, V. (2024). Ecological and geochemical aspects of thermal effects on argillites of the Lviv-Volyn coal basin spoil tips. Scientific Bulletin of National Mining University, 3, 100-107. https://doi.org/10.33271/nvngu/2024-3/100

5. Karabyn V. and Kochmar I. (2025). Distribution of different forms of manganese in coal mining waste: A case study of the Vizeyska mine, Ukraine IOP Conf. Ser.: Earth Environ. Sci. 1499 012045 DOI 10.1088/1755-1315/1499/1/012045

6. Sweeney, D. (2021). Staring Down the Digital Fulda Gap: Path Dependency as a Cyber Defense Vulnerability. arXiv preprint arXiv:2112.02773. https://arxiv.org/ftp/arxiv/papers/2112/2112.02773.pdf

7. Shuryhin, V., Rak, Y., & Karabyn, V. (2020). Analysis of factors and development of methods for managing the environmental and civil safety of transboundary transportation of oil and oil products through pipelines. ScienceRise, (5 (70) Special), 51-56.

8. Kuzyk, A., Karabyn, V., Shuryhin, V., Sushko, Y., Stepova, K., Karabyn, O. (2023). The River System Pollutant Migration in the Context of the Sudden One-Time Discharge with Consideration of the Bottom Sediments Influence (Case of Benzene Migration in the Stryi River, Ukraine). Ecological Engineering & Environmental Technology, 24(1), 46-54. https://doi.org/10.12912/27197050/154909

9. Shuryhin, V., Karabyn, V., Kuzyk, A. (2023). Prediction of Benzene Migration Parameters Resulting from Continuous Flow in a Mountain River. Ecological Engineering & Environmental Technology, 24(8), 73-81. https://doi.org/10.12912/27197050/171529

10. Papastergiou, S., & Tsiakas, K. (2025). Towards the Design of Cyber Range Training Programs for Enhanced Preparedness: Investigating the Training Needs in Critical Infrastructures. 2025 IEEE International Conference on Cyber Security and Resilience (CSR), 1-8. https://ieeexplore.ieee.org/document/11016646/

11. Raj, P. (2025). Vocational and Skill-Based Education in India: A Critical Review of NEP 2020's Implementation and Challenges. MORFAI: Multidisciplinary Online Research Forum for Advancement & Innovation, 5(1), 1-15. https://radjapublika.com/index.php/MORFAI/article/view/2626

12. Klymenko, O., & Zakharchenko, L. (2021). Strengthening the protection of critical infrastructure: domestic realities and international cooperation. National Institute for Strategic Studies. http://npndfi.org.ua/?page_id=774&lang=en&aid=1063

13. Верховна Рада України. (2021). Закон України "Про критичну інфраструктуру". https://zakon.rada.gov.ua/laws/show/1882-20#Text

14. Koval, V., & Shapoval, O. (2022). Usage of Open-Source Intelligence for Security of Critical Infrastructure. Information Security of Critical Infrastructure, 2, 24-32. https://ists.knu.ua//article/view/3747

15. OECD. (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing. https://doi.org/10.1787/6efc8d9f-en

16. Формування системи освіти, підготовки та перепідготовки персоналу у сфері захисту критичної інфраструктури: аналіт. доп. / О.М. Суходоля. Київ: Національний інститут стратегічних досліджень, 2025. 92 с. DOI: https://doi.org/10.53679/NISS-analytrep.2025.01.

17. Sari, A. R., & Sari, R. F. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. Journal of Computer and Communications, 9, 69–90. https://www.scirp.org/journal/doi.aspx?doi=10.4236/jcc.2021.98006

18. European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333/164. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

19. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. https://www.iso.org/standard/75106.html

20. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. https://www.iso.org/standard/27001

21. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

22. NATO. (2023). Resilience and Article 3. https://www.nato.int/cps/en/natohq/topics_132722.htm

23. UNDRR. (2017). Build Back Better in recovery, rehabilitation and reconstruction. United Nations Office for Disaster Risk Reduction. https://www.undrr.org/terminology/build-back-better

References

1. Koval, V. V., & Shapoval, O. V. (2020). The system of state protection of critical infrastructure of Ukraine: genesis, current state and prospects for optimization in terms of further national security. Chas Prava (Time of Law), (4), 146–153. https://chasprava.com.ua/index.php/journal/article/view/592

2. Kochmar, I., Karabyn, V. (2023). Water Extracts from Waste Rocks of the Coal Industry of Chervonograd Mining Area (Ukraine): Problems of Environmental Safety and Civil Protection.

Ecological Engineering & Environmental Technology, 24(1), 247-255. https://doi.org/10.12912/27197050/155209

3. Kochmar, I., Karabyn , V., Stepova, K., Stadnik, V., & Sozanskyi, M. (2024). Thermal Impact on Heavy Metal Bioavailability in Burnt Rocks of Waste Heap of Chervonohradska Coal-preparation Plant (Lviv Region, Ukraine). Geomatics and Environmental Engineering, 18(1), 117–133. https://doi.org/10.7494/geom.2024.18.1.117

4. Kochmar, I., Karabyn, V., Kordan, V. (2024). Ecological and geochemical aspects of thermal effects on argillites of the Lviv-Volyn coal basin spoil tips. Scientific Bulletin of National Mining University, 3, 100-107. https://doi.org/10.33271/nvngu/2024-3/100

5. Karabyn V. and Kochmar I. (2025). Distribution of different forms of manganese in coal mining waste: A case study of the Vizeyska mine, Ukraine IOP Conf. Ser.: Earth Environ. Sci. 1499 012045 DOI 10.1088/1755-1315/1499/1/012045

6. Sweeney, D. (2021). Staring Down the Digital Fulda Gap: Path Dependency as a Cyber Defense Vulnerability. arXiv preprint arXiv:2112.02773. https://arxiv.org/ftp/arxiv/papers/2112/2112.02773.pdf

7. Shuryhin, V., Rak, Y., & Karabyn, V. (2020). Analysis of factors and development of methods for managing the environmental and civil safety of transboundary transportation of oil and oil products through pipelines. ScienceRise, (5 (70) Special), 51-56.

8. Kuzyk, A., Karabyn, V., Shuryhin, V., Sushko, Y., Stepova, K., Karabyn, O. (2023). The River System Pollutant Migration in the Context of the Sudden One-Time Discharge with Consideration of the Bottom Sediments Influence (Case of Benzene Migration in the Stryi River, Ukraine). Ecological Engineering & Environmental Technology, 24(1), 46-54. https://doi.org/10.12912/27197050/154909

9. Shuryhin, V., Karabyn, V., Kuzyk, A. (2023). Prediction of Benzene Migration Parameters Resulting from Continuous Flow in a Mountain River. Ecological Engineering & Environmental Technology, 24(8), 73-81. https://doi.org/10.12912/27197050/171529

10. Papastergiou, S., & Tsiakas, K. (2025). Towards the Design of Cyber Range Training Programs for Enhanced Preparedness: Investigating the Training Needs in Critical Infrastructures. 2025 IEEE International Conference on Cyber Security and Resilience (CSR), 1-8. https://ieeexplore.ieee.org/document/11016646/

11. Raj, P. (2025). Vocational and Skill-Based Education in India: A Critical Review of NEP 2020's Implementation and Challenges. MORFAI: Multidisciplinary Online Research Forum for Advancement & Innovation, 5(1), 1-15. https://radjapublika.com/index.php/MORFAI/article/view/2626

12. Klymenko, O., & Zakharchenko, L. (2021). Strengthening the protection of critical infrastructure: domestic realities and international cooperation. National Institute for Strategic Studies. http://npndfi.org.ua/?page_id=774&lang=en&aid=1063

13. Verkhovna Rada Ukrainy. (2021). Zakon Ukrainy "Pro krytychnu infrastrukturu". https://zakon.rada.gov.ua/laws/show/1882-20#Text

14. Koval, V., & Shapoval, O. (2022). Usage of Open-Source Intelligence for Security of Critical Infrastructure. Information Security of Critical Infrastructure, 2, 24-32. https://ists.knu.ua//article/view/3747

15. OECD. (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing. https://doi.org/10.1787/6efc8d9f-en

16. Formuvannia systemy osvity, pidhotovky ta perepidhotovky personalu u sferi zakhystu krytychnoi infrastruktury: analit. dop. / O.M. Sukhodolia. Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen, 2025. 92 s. DOI: https://doi.org/10.53679/NISS-analytrep.2025.01

17. Sari, A. R., & Sari, R. F. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. Journal of Computer and Communications, 9, 69–90. https://www.scirp.org/journal/doi.aspx?doi=10.4236/jcc.2021.98006

18. European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive

2008/114/EC. Official Journal of the European Union, L 333/164. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

19. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. https://www.iso.org/standard/75106.html

20. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. https://www.iso.org/standard/27001

21. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

22. NATO. (2023). Resilience and Article 3. https://www.nato.int/cps/en/natohq/topics_132722.htm

23. UNDRR. (2017). Build Back Better in recovery, rehabilitation and reconstruction. United Nations Office for Disaster Risk Reduction. https://www.undrr.org/terminology/build-back-better