Інтегрований підхід до підготовки фахівців із захисту критичної інфраструктури в Україні

An Integrated Approach to Training Specialists in Critical Infrastructure Protection in Ukraine

Роман Яковчук [A]

Corresponding author: д.тех.н., доцент, начальник факультету цивільного захисту Львівського державного університету безпеки життєдіяльності, e-mail: yakovchukrs@ukr.net, ORCID: 0000-0001-5523-5569

Василь Карабин [A]

д.тех.н., професор, професор кафедри цивільного захисту, e-mail: vasyl.karabyn@gmail.com, ORCID: 0000-0002-8337-5355

Андрій Тарнавський [A]

к.тех.н., доцент, доцент кафедри цивільного захисту, e-mail: andry090880@ukr.net, ORCID: 0000-0002-4625-2022

Roman Yakovchuk [A]

Corresponding author: DSc, Associate Professor, Head of the Faculty of Civil Protection, Lviv State University of Life Safety, e-mail: yakovchukrs@ukr.net, ORCID: 0000-0001-5523-5569

Vasyl Karabyn [A]

DSc, Professor, Professor of the Department of Civil Protection, Lviv State University of Life Safety, e-mail: vasyl.karabyn@gmail.com, ORCID: 0000-0002-8337-5355

Andrii Tarnavskyi [A]

Candidate of Technical Sciences, Associate Professor, e-mail: andry090880@ukr.net, ORCID: 0000-0002-4625-2022

[A] Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

[A] Lviv State University of Life Safety, Lviv, Ukraine

Received: April 20, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.13

Мета роботи: Визначити ключові компетентності, оптимальні методи організації навчальних заходів та структуру й зміст освітньої програми підвищення кваліфікації фахівців із захисту критичної інфраструктури з урахуванням воєнних та техногенних загроз з метою підвищення стійкості та готовності критичних об'єктів до кризових ситуацій..

Метод дослідження: Контент-аналіз, SWOT-аналіз, метод Дельфі.

Результати дослідження: Ідентифіковано 6 ключових компетентностей фахівців із захисту критичної інфраструктури; підтверджено високу релевантність і практичну ефективність чотиримодульної програми; розроблено рекомендації щодо оптимізації змісту та форм навчання.

Теоретична цінність дослідження: Запропоновано адаптовану модель компетенцій фахівця у сфері захисту критичної інфраструктури з урахуванням концепції стійкості та міждисциплінарного підходу, що розширює наукові уявлення про професійну підготовку в умовах гібридних загроз.

Практична цінність дослідження: Озвучені методичні рекомендації та інструментарій оцінки (опитувальник, гайд-інтерв'ю, SWOT-аналіз) можуть бути використані університетами й практичними службами для розробки та вдосконалення власних програм підвищення кваліфікації.

Оригінальність дослідження: Інтегровано кількісні та якісні методи оцінки професійної підготовки фахівців у контексті воєнних та техногенних ризиків в Україні; унікальність підходу полягає в поєднанні міжнародних стандартів НАТО/ЄС із локальними умовами та реаліями сучасної війни.

Тип статті: Теоретичний, описовий, практичний, методичний.

Ключові слова: цивільний захист, критична інфраструктура, підготовка кадрів, воєнні загрози.

Purpose: to identify the key competencies, optimal methods for organizing training activities, and the structure and content of a continuing professional development program for critical infrastructure protection specialists, taking into account military and technological threats, in order to enhance the resilience and preparedness of critical facilities for crisis situations.

Method: content analysis, SWOT analysis, Delphi method.

Findings: six key competencies of critical infrastructure protection specialists were identified; the high relevance and practical effectiveness of the four-module program were confirmed; recommendations were developed to optimize content and instructional formats.

Theoretical implications: an adapted competency model for civil protection of critical infrastructure was proposed, incorporating the concept of resilience and an interdisciplinary approach, thereby expanding academic understanding of professional training under hybrid threat conditions.

Practical implications: the methodological recommendations and assessment tools (questionnaire, interview guide, SWOT analysis) presented can be used by universities and operational agencies to develop and refine their own professional development programs.

Originality: quantitative and qualitative methods were integrated to evaluate specialist training in the context of military and technological risks in Ukraine; the uniqueness of the approach lies in combining NATO/EU standards with local conditions and the realities of modern warfare.

Paper type: Theoretical, descriptive, practical, methodical.

Key words: civil protection, critical infrastructure, personnel training, military threats.

Вступ

Захист критичної інфраструктури є важливим завданням цивільного захисту, особливо у час збройної агресії рф. У сучасних умовах об'єкти критичної інфраструктури (ОКІ) – від об'єктів енергетики до водопостачальних мереж – стають мішенями як для фізичних, так і для

кіберзагроз, що вимагає комплексного посилення захисту з боку держави та залучених структур. Знищення або виведення з ладу таких об'єктів призводить до серйозних наслідків для безпеки, стабільності та життєзабезпечення населення.

Крім традиційних загроз важливим фактором уразливості КІ є воєнні та техногенні ризики. Так, при ракетних ударах на енергетичні об'єкти та мережі України у серпні 2024 року було задіяно понад 200 ракет та безпілотників, що спричинило знеструмлення понад мільйон домогосподарств, вихід з ладу гідротехнічних споруд і об'єктів водопостачання, а також перебої в роботі систем теплопостачання [1]. Додаткову небезпеку становлять аварійні скиди шкідливих речовин у річкові системи Це обґрунтовує потребу в міждисциплінарному підході, внаслідок чого міграція вуглеводневих сполук спостерігається на десятки кілометрів, що може поширювати токсичне забруднення до водоочисних споруд та елементів водопостачальної інфраструктури [2, 3]. Транспортування нафтопродуктів транскордонними трубопроводами створює додаткові екологічні загрози. Аналіз факторів та розробка методів управління безпекою цього процесу дозволяють знизити ймовірність аварій та мінімізувати наслідки для населення і довкілля [4].

Таким чином, сучасна система захисту критичної інфраструктури має враховувати не лише фізичні та кібернетичні загрози, але й складні взаємодії з навколишнім середовищем та процеси, що відбуваються як у гідросфері, так і в геосфері. Це обґрунтовує потребу в міждисциплінарному підході, який поєднує інженерні рішення, екологічний нагляд і стратегічне планування.

Теоретичні основи дослідження

Захист критичної інфраструктури (КІ) в умовах сучасних безпекових викликів розглядається як багатовимірна система заходів, що охоплює організаційні, технічні, правові, інформаційні та кадрові аспекти. Теоретичним підґрунтям для розбудови такої системи є концепції сталості, ризик-менеджменту та управління у кризових ситуаціях.

Ключовим положенням сучасних теорій управління критичною інфраструктурою є визнання її міжгалузевої взаємозалежності, коли пошкодження одного елемента може спричинити ланцюгову реакцію в інших секторах, що забезпечують життєдіяльність населення, економічну стабільність та національну безпеку. Відтак, у сучасних дослідженнях акцентовано увагу на необхідності системного підходу до захисту КІ, що включає комплексну оцінку вразливостей, ідентифікацію критичних функцій та планування заходів із забезпечення стійкості в умовах багаторівневих загроз (OECD, 2019) [5].

Український науково-освітній простір активно інтегрує ці підходи. Вітчизняні дослідники зазначають, що ключовим чинником ефективного захисту об'єктів КІ є кваліфікований персонал, здатний діяти в умовах надзвичайних ситуацій, реалізовувати превентивні заходи та координувати взаємодію між суб'єктами захисту (Суходоля, 2025) [6]. Це узгоджується з міжнародними підходами, згідно з якими підготовка персоналу є однією з трьох основ стратегії зміцнення стійкості поряд із технологічними рішеннями та належним управлінням.

Особливого значення в теоретичному обґрунтуванні набуває розуміння феномену "стійкості" (resilience), яка визначається як здатність системи протистояти зовнішнім загрозам, адаптуватися до них та швидко відновлюватися. Цей підхід став домінантним у документах НАТО та ЄС, де підкреслюється необхідність переходу від реактивної до проактивної моделі захисту, орієнтованої на запобігання порушенням функціонування КІ [7].

У контексті українських реалій, пов'язаних із повномасштабною війною та гібридними загрозами, розвиток національної системи захисту КІ має спиратися не лише на правову базу, а й на чітко окреслені освітньо-кваліфікаційні вимоги до фахівців. Саме тому освітні програми підвищення кваліфікації, такі як реалізована у Львівському державному університеті безпеки

життєдіяльності, є не лише педагогічною інновацією, а й елементом національної стратегії зміцнення обороноздатності держави [8].

У підсумку теоретичні основи дослідження захисту критичної інфраструктури базуються на концепціях стійкості, міждисциплінарної взаємодії та інституційної готовності, які мають бути реалізовані через системну освітню політику, технологічну модернізацію та стратегічне управління.

Постановка проблеми

Забезпечення безпеки та безперебійного функціонування критичної інфраструктури значною мірою залежить від рівня підготовленості фахівців, які залучені до здійснення заходів щодо захисту ОКІ, та їхньої компетенції [9]. Зовнішні та внутрішні загрози, що зростають у безпековому середовищі України, підсилюють необхідність підвищення професійної підготовки фахівців, які в умовах протидії збройній агресії займаються виявленням, запобіганням і нейтралізацією загроз для ОКІ, а також ліквідацією наслідків надзвичайних ситуацій у разі їх виникнення на таких об'єктах [8]. Тому підвищення кваліфікації спеціалістів у сфері захисту критичної інфраструктури набуває не лише освітнього, а й стратегічного значення для державної безпеки. Системна професійна підготовка має забезпечити здатність оперативно реагувати на загрози, впроваджувати превентивні заходи та діяти ефективно в умовах кризових ситуацій.

Мета дослідження – визначити ключові компетентності, оптимальні методи організації навчальних заходів та структуру й зміст освітньої програми підвищення кваліфікації фахівців із захисту критичної інфраструктури з урахуванням воєнних та техногенних загроз з метою підвищення стійкості та готовності критичних об'єктів до кризових ситуацій.

Методологія дослідження

Методологія дослідження спрямована на всебічну оцінку ефективності освітньої програми підвищення кваліфікації фахівців із захисту критичної інфраструктури та складається з трьох взаємопов'язаних етапів: підготовчого, експериментального і аналітичного.

1. Підготовчий етап. На цьому етапі проведено контент-аналіз ключових нормативно-правових документів, що визначають вимоги до стійкості критичних об'єктів (Directive (EU) 2022/2557) та національних планів захисту КІ [9]. Вивчено наукові підходи до організації навчальних програм із безпеки КІ, зокрема на основі аналітичної доповіді Суходолі (2025) [6] та методичних рекомендацій міжнародних організацій. Результатом стало формування теоретико-методичного каркасу, в межах якого розроблено інструментарій дослідження: опитувальник, гайд-інтерв'ю для експертів і форму для SWOT-аналізу.

2. Експериментальний етап. Для збору даних застосовано змішану (mixed-methods) стратегію відповідно до рекомендацій Creswell та Creswell (2018) [10]. Використано чотири основні методи:

- **Контент-аналіз** програм та навчальних матеріалів (загалом 24 документи державного та університетського рівня);
- **Метод Дельфі** (дві хвилі опитування 10 експертів із різних секторів КІ) для узгодження ключових компетентностей і додаткових тем на навчальних модулях. Метод Дельфі обрано через здатність досягати консенсусу серед експертів без прямого впливу групової динаміки, що критично важливо для оцінки професійних компетенцій та можливості анонімного уточнення позицій експертів у кількох ітераціях, що зменшує ризик упереджень;
- **Фокус-групи** (3 групи по 6-8 учасників) для глибинного обговорення організаційних та методичних аспектів проведення занять. Фокус-групи застосовані для виявлення

неочевидних проблем у організації занять через групову дискусію, глибинного розуміння контексту воєнних та техногенних загроз через відкрите обговорення кейсів.

3. Аналітичний етап. Зібрані кількісні дані проаналізовано з використанням описової статистики та рейтингового оцінювання. Якісний масив (відкриті відповіді, інтерв'ю, фокус-групи) оброблено за допомогою тематичного аналізу і SWOT-аналізу сильних і слабких сторін програми. Аналітичну частину доповнено порівняльним аналізом із рекомендаціями CER Directive щодо інституційної готовності та процедури реагування на кризові ситуації [7].

Вибірка і етичні аспекти. У вибірку включено фахівців із підрозділів цивільного захисту різного рівня: від локальних рятувальних служб до представників державних органів. Дані респондентів анонімізовані згідно з етичними стандартами наукових досліджень.

Застосована методологія забезпечила інтеграцію кількісних та якісних даних, що дозволило виявити як загальні тенденції сприйняття програми, так і глибинні побажання й застереження фахівців. Такий підхід створює надійну основу для подальшої модернізації змістових модулів та вдосконалення форм навчання фахівців із захисту критичної інфраструктури.

Результати

Основною метою підвищення кваліфікації осіб, які залучаються до здійснення заходів захисту ОКІ, є забезпечення особистісного та професійно-діяльнісного самовдосконалення на основі активізації їхньої базової освіти, набутого професійного та життєвого досвіду відповідно до індивідуально-особистих інтересів, соціальних запитів держави щодо ефективного виконання посадово-функціональних обов'язків.

Підходи щодо захисту критичної інфраструктури мають спільні і відмінні риси в Україні і країнах Європейського союзу (табл. 1).

Таблиця 1 – Порівняння міжнародних та українських підходів до захисту захисту критичної інфраструктури (укладено за матеріалами [6, 11-18])

Критерій	Українські стандарти	Міжнародні стандарти
Правова база	Закон України від 16.11.2021 № 1882-IX "Про критичну інфраструктуру"	Директива ЄС 2022/2557, ISO 27001/22301, стандарти НАТО
Стійкість (resilience)	Інтеграція концепції через міждисциплінарний підхід	Проактивне управління ризиками, адаптація до гібридних загроз (ISO 22301, НАТО)
Кібербезпека	Регулюється окремими законами (наприклад, "Про кібербезпеку")	ISO 27001 для інформаційної безпеки, Framework for Improving Critical Infrastructure Cybersecurity (NIST)
Механізми реалізації	Паспорти безпеки, проекти загроз, категоризація об'єктів	Системи менеджменту безпеки (ISO), планування безперервності бізнесу (ISO 22301)
Взаємодія секторів	Державно-приватне партнерство, міжвідомча координація	Координація через NATO-EU Task Force, транснаціональні протоколи
Освіта та підготовка	Освітньо-професійні програми за першим (бакалаврським), другим (магістерським) рівнями вищої освіти. Освітні програми підвищення кваліфікації	Сертифікаційні програми ISO, навчання в рамках NATO Centres of Excellence

Водночас в ЄС і в Україні є розуміння важливості якісної підготовки кадрів у напрямі стійкості та захисту об'єктів критичної інфраструктури.

Для підвищення рівня кваліфікації персоналу ОКІ у Львівському державному університеті безпеки життєдіяльності розроблена Освітня програма підвищення кваліфікації "Захист об'єктів критичної інфраструктури".

Метою цієї освітньої програми підвищення кваліфікації є підготовка посадових осіб, які залучені до здійснення заходів захисту ОКІ, вивчення теоретичних основ та практичних заходів щодо організації захисту ОКІ, функціонування загальної системи захисту та забезпечення безпеки та стійкості критичної інфраструктури України.

Освітня програма спрямована на формування компетентностей у посадових осіб, відповідальних за захист критичної інфраструктури, нових знань, умінь та навичок, спрямованих на створення і організацію безпеки критичної інфраструктури, зокрема:

забезпечення функціональності, безперервності роботи, цілісність і стійкість критичної інфраструктури;

набуття теоретичних основ та поглиблення набутих теоретичних знань щодо законодавчої бази у сфері захисту критичної інфраструктури;

формування практичних умінь з порядку визначення критичності окремих елементів ОКІ;

порядку влаштування, оцінки і підтримання інженерного захисту окремих критичних елементів;

опанування методики проведення моніторингу рівня безпеки ОКІ;

реагування на надзвичайні ситуації та ліквідацію їх наслідків на ОКІ.

Освітня програма складається з чотирьох змістових модулів, які логічно побудовані та охоплюють увесь спектр необхідних знань і навичок (рис. 1).

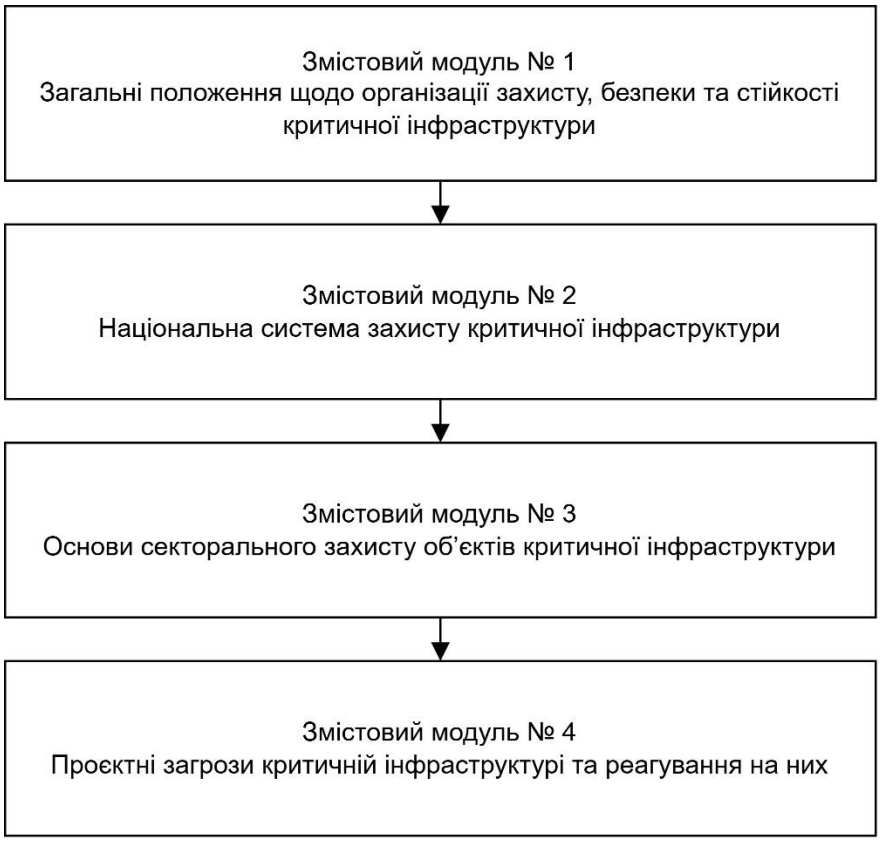

Рисунок 1 – Схема змістових модулів освітньої програми підвищення кваліфікації "Захист об'єктів критичної інфраструктури" у Львівському державному університеті безпеки життєдіяльності

Змістовий модуль № 1 "Загальні положення щодо організації захисту, безпеки та стійкості критичної інфраструктури" зосереджений на організаційних та правових аспектах

захисту критичної інфраструктури, основних засадах державної політики у сфері захисту критичної інфраструктури, стійкості критичної інфраструктури, ознайомленні з міжнародним досвідом захисту ОКІ.

Змістовий модуль № 2 "Національна система захисту критичної інфраструктури" детально розглядає національну систему захисту ОКІ, основні функції уповноваженого органу у сфері захисту критичної інфраструктури України, діяльність функціональних та секторальних органів у сфері захисту критичної інфраструктури, порядок взаємодії між суб'єктами захисту критичної інфраструктури.

Змістовий модуль № 3 "Основи секторального захисту об'єктів критичної інфраструктури" охоплює комплекс знань і практичних навичок, необхідних для організації захисту об'єктів у різних секторах критичної інфраструктури, порушення функціонування яких призводить до порушення життєво важливих функцій та послуг. У модулі розглядаються питання запобігання посяганням на ОКІ у контексті їх секторальної приналежності, моніторингу, інженерного захисту ОКІ. Особливу увагу приділено основним аспектам енергетичної безпеки держави та особливостям забезпечення паливно-енергетичного сектору, секторів транспорту, промисловості, систем життєзабезпечення, громадської безпеки, соціального захисту, державного матеріального резерву, державної влади та місцевого самоврядування, захисту інформації, інформаційного медіа сектору, цифрових технологій. Основний акцент робиться на актуальності захисту критичної інфраструктури в умовах гібридної технології ведення війни, повномасштабної війни, а також терористичних загроз в Україні.

Змістовий модуль № 4 "Проєктні загрози критичній інфраструктурі та реагування на них" зосереджений на проєктних загрозах для критичної інфраструктури, організації реагування на кризові ситуації в умовах воєнного стану. Особливу увагу зосереджено на реагуванні на надзвичайні ситуації, пов'язані з радіаційною та хімічною небезпекою, кіберзагрозах для ОКІ та їх усуненні, синергії фізичного та кіберзахисту на ОКІ.

У результаті навчання слухачі опанують такі вміння:

ідентифікувати та здійснювати категоризацію ОКІ;

здійснювати планування, розроблення та впровадження заходів захисту критичної інфраструктури;

визначати критичні елементи ОКІ;

визначати можливі загрози для критичної інфраструктури;

оцінювати вразливість ОКІ;

визначати рівень захисту та планувати заходи захисту ОКІ;

розробляти паспорти безпеки ОКІ;

прогнозувати і оцінювати обстановку в зоні кризової ситуації на ОКІ та тактичні можливості підрозділів, що залучаються до ліквідації наслідків аварійної ситуації;

розробляти плани взаємодії та підтримувати життєво важливі функції на випадок порушення функціонування об'єктів критичної енергетичної інфраструктури.

Освітня програма підвищення кваліфікації "Захист об'єктів критичної інфраструктури" є своєчасною відповіддю на виклики, з якими сьогодні стикається Україна. Війна яскраво продемонструвала, наскільки вразливими є ОКІ перед військовими атаками, гібридними загрозами та надзвичайними ситуаціями природного і техногенного характеру. Саме тому підготовка фахівців, які здатні забезпечити захист ключових об'єктів країни, стала не просто актуальною, а життєво необхідною.

Особливо важливим є міжнародний контекст цієї програми. У рамках підвищення кваліфікації враховано кращі практики країн-членів ЄС і стандартів НАТО у сфері захисту критичної інфраструктури. Це дає змогу адаптувати підготовку фахівців до сучасних вимог, а також інтегрувати Україну у спільний безпековий простір.

Навчальний план програми передбачає 90 академічних годин (3 ECTS-кредити), з них: 60 годин на теоретичні та практичні заняття та 30 годин на самостійну роботу.

Учасники програми отримуватимуть відповідний сертифікат про підвищення кваліфікації, що визнається державними органами.

Освітня програма підвищення кваліфікації може бути корисною не лише для вітчизняних фахівців, які залучені до здійснення заходів захисту критичної інфраструктури, але й для посадових осіб та персоналу, який відповідає за охорону, безпеку та захист ОКІ, а також представників екстрених служб з реагування на надзвичайні ситуації Європейського Союзу.

Висновки

У результаті комплексного дослідження було визначено ключові компетентності фахівців із захисту критичної інфраструктури, зокрема:

забезпечення функціональності, безперервності роботи, цілісність і стійкість критичної інфраструктури;

набуття теоретичних основ та поглиблення набутих теоретичних знань щодо законодавчої бази у сфері захисту критичної інфраструктури;

формування практичних умінь з порядку визначення критичності окремих елементів ОКІ;

порядку влаштування, оцінки і підтримання інженерного захисту окремих критичних елементів;

опанування методики проведення моніторингу рівня безпеки ОКІ;

реагування на надзвичайні ситуації та ліквідацію їх наслідків на ОКІ.

Застосування змішаної методології (контент-аналіз, Delphi, фокус-групи, анкетування) дозволило верифікувати структуру освітньої програми та підтвердити її ефективність. Експертне коло високо відзначило інтерактивні формати викладання й акцент на практичних навичках. SWOT-аналіз виявив сильні сторони програми (інтеграція міжнародних стандартів, міждисциплінарний підхід) та слабкі – необхідність оновлення кейсів під поточні воєнні реалії.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. IEA. Інтернет джерело. URL : https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack?utm_source
2. Shuryhin, V. (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*. URL : https://www.ecoeet.com/The-River-System-Pollutant-Migration-in-the-Context-of-the-Sudden-One-Time-Discharge%2C154909%2C0%2C2.html
3. Карабин В.В. (2015). Закономірності зміни макрокомпонентного хімічного складу вод ріки Білий Черемош. *Збірник наукових праць УкрДГРІ*. (1), С. 114-121.
4. 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), 51-56. https://doi.org/10.21303/2313-8416.2020.001484

5. Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience*. OECD Publishing. URL : https://www.oecd.org/publications/good-governance-for-critical-infrastructure-resilience-7a74ebc3-en.htm
6. 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. https://doi.org/10.53679/NISS-analytrep.2025.01.
7. European Commission. (2022). *Directive on the resilience of critical entities (CER Directive)*. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557
8. Яковчук Р.С., Тарнавський А.Б., Карабин В.В. Перспективи підготовки фахівців у галузі захисту критичної інфраструктури України // Екологічна безпека в умовах війни: збірник тез доповідей V Міжнародної науково-практичної конференції, м. Львів, 21 листопада 2024 р. Львів: ЛДУ БЖД, 2024. С. 211-213.
9. Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України від 19.09.2023 № 825-р.
10. Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE. URL : https://us.sagepub.com/en-us/nam/research-design/book255675
11. Верховна Рада України. (2021). Закон України "Про критичну інфраструктуру". URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text
12. 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. URL : https://eur-lex.europa.eu/eli/dir/2022/2557/oj
13. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. URL : https://www.iso.org/standard/75106.html
14. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. URL : https://www.iso.org/standard/27001
15. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. URL : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
16. NATO. (2023). Resilience and Article 3. URL : https://www.nato.int/cps/en/natohq/topics_132722.htm
17. OECD. (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing. https://doi.org/10.1787/6efc8d9f-en
18. UNDRR. (2017). Build Back Better in recovery, rehabilitation and reconstruction. United Nations Office for Disaster Risk Reduction. URL : https://www.undrr.org/terminology/build-back-better

References

1. IEA. Інтернет джерело. Available from : https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack?utm_source
2. Shuryhin, V. (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*. Available from : https://www.ecoeet.com/The-River-System-Pollutant-Migration-in-the-Context-of-the-Sudden-One-Time-Discharge%2C154909%2C0%2C2.html

3. Karabyn, V.V. (2015). Zakonomirnosti zminy makrokomponentnoho khimichnoho skladu vod riky Bilyi Cheremosh. *Zbirnyk naukovykh prats UkrDGRI*. (1), 114–121.
4. 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), 51-56. https://doi.org/10.21303/2313-8416.2020.001484
5. Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience*. OECD Publishing. Available from : https://www.oecd.org/publications/good-governance-for-critical-infrastructure-resilience-7a74ebc3-en.htm
6. 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. https://doi.org/10.53679/NISS-analytrep.2025.01
7. European Commission. (2022). *Directive on the resilience of critical entities (CER Directive)*. Available from : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557
8. Yakovchuk R.S., Tarnavskyi A.B., Karabyn V.V. Perspektyvy pidhotovky fakhivtsiv u haluzi zakhystu krytychnoi infrastruktury Ukrainy // Ekolohichna bezpeka v umovakh viiny: zbirnyk tez dopovidei V Mizhnarodnoi naukovo-praktychnoi konferentsii, m. Lviv, 21 lystopada 2024 r. Lviv: LDU BZhD, 2024. S. 211–213.
9. Natsionalnyi plan zakhystu ta zabezpechennia bezpeky ta stiikosti krytychnoi infrastruktury: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 19.09.2023 № 825-r.
10. Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE. Available from : https://us.sagepub.com/en-us/nam/research-design/book255675
11. Verkhovna Rada Ukrainy. (2021). Zakon Ukrainy “Pro krytychnu infrastrukturu”. Available from : https://zakon.rada.gov.ua/laws/show/1882-20#Text
12. 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. Available from : https://eur-lex.europa.eu/eli/dir/2022/2557/oj
13. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Available from : https://www.iso.org/standard/75106.html
14. 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
15. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Available from : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
16. NATO. (2023). Resilience and Article 3. Available from : https://www.nato.int/cps/en/natohq/topics_132722.htm
17. OECD. (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing. https://doi.org/10.1787/6efc8d9f-en
18. UNDRR. (2017). Build Back Better in recovery, rehabilitation and reconstruction. United Nations Office for Disaster Risk Reduction. Available from : https://www.undrr.org/terminology/build-back-better