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

РОЗДІЛ 4. РОЗВИТОК ІННОВАЦІЙ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

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,

а й готувати фахівців, здатних оперативно реагувати на інциденти, аналізувати ризики та забезпечувати стійкість інформаційних систем [6].

Окрім воєнних і кіберзагроз, критична інфраструктура залишається вразливою до техногенних катастроф, які можуть бути спричинені як навмисними діями, так і випадковими або природними чинниками. Зростання технологічної складності об'єктів підвищує ризик виникнення аварій, які можуть мати катастрофічні наслідки для населення, довкілля та економіки держави. Особливо небезпечними є аварії на об'єктах енергетики, хімічної промисловості, транспортних системах [7], водопостачання [8, 9] де навіть незначна несправність може призвести до масштабних руйнувань, забруднення навколишнього середовища та загибелі людей [1].

Прикладами таких катастроф є вибухи на хімічних заводах, аварії на атомних електростанціях, транспортні катастрофи, які часто супроводжуються значними людськими жертвами та економічними втратами. В умовах війни ризик техногенних катастроф зростає внаслідок цілеспрямованих атак на промислові об'єкти, а також через зниження рівня технічного обслуговування, дефіцит кадрів і ресурсів для підтримки безпеки. У таких умовах особливо важливою є підготовка фахівців, які володіють знаннями з управління ризиками, аварійного реагування, ліквідації наслідків катастроф та відновлення функціонування об'єктів критичної інфраструктури [1].

У сучасних умовах критична інфраструктура стає дедалі більшою мішенню для різноманітних загроз – від фізичних атак до складних кібератак і техногенних катастроф. З огляду на це, зростає потреба у фахівцях, які володіють міждисциплінарними знаннями та практичними навичками для забезпечення її стійкості та безпеки. Зокрема, для секторів енергетики, транспорту, зв'язку, охорони здоров'я та водопостачання необхідні спеціалісти, здатні не лише реагувати на надзвичайні ситуації, а й здійснювати превентивний аналіз ризиків, розробляти стратегії захисту та впроваджувати сучасні технології для підвищення рівня безпеки об'єктів [10].

В умовах постійного зростання складності загроз особливої ваги набуває міждисциплінарна підготовка фахівців, які здатні працювати на стику різних галузей знань, аналізувати ситуацію у реальному часі, приймати ефективні рішення та координувати дії різних служб у надзвичайних ситуаціях. Саме тому сучасна система підготовки фахівців із захисту критичної інфраструктури повинна враховувати новітні виклики та забезпечувати формування відповідних компетентностей [6].

У таких умовах особливої ваги набуває підготовка фахівців, які здатні швидко оцінювати загрози, здійснювати моніторинг стану об'єктів та організовувати ефективне реагування на надзвичайні ситуації [1].

Зростання попиту на таких фахівців підтверджується й глобальними тенденціями у сфері професійної освіти. Досвід впровадження навичково-орієнтованих освітніх програм у різних країнах демонструє, що інтеграція практичного навчання, стажувань та співпраці з роботодавцями дозволяє формувати конкурентоспроможних спеціалістів, які готові до роботи у складних і динамічних умовах. Системи освіти, які акцентують на розвитку практичних навичок і адаптації до швидких змін у технологіях, дають змогу краще відповідати потребам сучасного ринку праці, зокрема у сфері захисту критичної інфраструктури [11].

Особливої уваги потребує підготовка кадрів для роботи з новітніми технологіями, такими як системи автоматизованого управління, штучний інтелект, засоби моніторингу та реагування на інциденти. Від фахівців очікується не лише глибоке розуміння технічних аспектів, а й здатність до швидкого прийняття рішень у кризових ситуаціях, вміння працювати в міждисциплінарних командах і комунікувати з різними стейкхолдерами. Для цього важливо впроваджувати спеціалізовані тренінги, симуляційні навчання та використання кіберполігонів, які дозволяють відпрацьовувати дії у реалістичних сценаріях [10].

Водночас, дедалі більшої ваги набуває питання безперервного професійного розвитку та підвищення кваліфікації діючих фахівців. Зміни у законодавстві, поява нових технологій і методів атак вимагають регулярного оновлення знань і навичок. Ефективними інструментами для цього є короткострокові курси, онлайн-навчання, сертифікаційні програми, а також участь

у міжнародних освітніх проєктах. Такий підхід дозволяє забезпечити гнучкість і мобільність професійної підготовки, швидко реагувати на нові виклики і підтримувати високий рівень компетентності персоналу.

Значну роль у підготовці фахівців відіграють партнерства між закладами освіти, державними структурами та приватним сектором. Саме завдяки тісній співпраці з роботодавцями можливо адаптувати навчальні програми до реальних потреб ринку праці, впроваджувати сучасні технології у навчальний процес і забезпечувати студентам можливість проходження практики на об'єктах критичної інфраструктури. Такі партнерства сприяють не лише підвищенню якості підготовки, а й формуванню професійних спільнот, які об'єднують фахівців різних галузей для спільного вирішення актуальних проблем безпеки [11].

Окремим викликом залишається забезпечення різноманітності та інклюзивності у підготовці фахівців. Сучасні дослідження наголошують на необхідності врахування різних професійних і освітніх траєкторій, розробки програм для людей із різним рівнем базової підготовки, а також підтримки безперервного навчання протягом усього життя. Це дозволяє залучати до сфери захисту критичної інфраструктури фахівців із суміжних галузей, розширювати кадровий резерв і забезпечувати стійкість системи у довгостроковій перспективі.

Зростання потреби у фахівцях для захисту критичної інфраструктури також пов'язане з глобальними тенденціями щодо підвищення вимог до безпеки та стійкості державних і приватних систем. Сучасні стандарти управління ризиками, кібербезпеки, реагування на надзвичайні ситуації вимагають від персоналу не лише технічних знань, а й навичок стратегічного планування, аналітики, комунікації та лідерства. Тому освітні програми мають бути спрямовані на формування комплексних компетентностей, які дозволяють ефективно діяти у складних і невизначених умовах [10].

Підсумовуючи, можна зазначити, що зростання потреби у фахівцях із захисту критичної інфраструктури є об'єктивною відповіддю на сучасні виклики, пов'язані зі зростанням складності загроз, динамікою технологічного розвитку та підвищенням вимог до безпеки суспільства. Ефективна підготовка таких фахівців є ключовою умовою забезпечення стійкості та безпеки держави, а також розвитку конкурентоспроможної економіки у глобалізованому світі [10].

Метою цього підрозділу монографії є обґрунтування потреби у впровадженні цілісної, багаторівневої моделі підготовки фахівців у сфері цивільного захисту з акцентом на захист критичної інфраструктури (КІ). У сучасних умовах зростання складності ризиків – від воєнних загроз до гібридних і кібернетичних атак – виникає нагальна потреба у створенні системи підготовки, яка буде здатна оперативно реагувати на виклики сьогодення. Ключовим завданням такої системи є не лише формування теоретичних знань, а й розвиток практичних компетентностей для роботи в реальному полі ризику.

У межах цього підрозділу **об'єктом дослідження** виступає система професійної підготовки фахівців у галузі цивільного захисту з особливим акцентом на підготовку до виконання завдань, пов'язаних із забезпеченням сталого функціонування об'єктів критичної інфраструктури. Це система включає як базову вищу освіту, так і форми післядипломного навчання та підвищення кваліфікації, спрямовані на адаптацію кадрів до нових викликів безпеки.

Предметом дослідження є освітні підходи, принципи та інструменти формування ключових компетентностей у майбутніх та діючих фахівців у сфері цивільного захисту. Зокрема, аналізується, яким чином зміст навчальних програм, методи викладання, практичне навчання та інтеграція міждисциплінарних знань сприяють формуванню професійної готовності до роботи в умовах надзвичайних ситуацій, ризиків техногенного, природного, соціального та воєнного характеру.

Сучасний стан безпеки вимагає від освітніх програм не лише забезпечення базових знань (наприклад, у сфері нормативно-правового регулювання або організації евакуаційних заходів), а й розвитку системного мислення, здатності до моделювання сценаріїв загроз, управління стійкістю об'єктів інфраструктури, комунікації в умовах кризи, використання цифрових та геоінформаційних технологій. Тому ключовими компетентностями, що вивчаються у межах дослідження, є:

– аналітичні та прогностичні навички;
– знання сучасних систем моніторингу та реагування;
– розуміння концепцій ризик-менеджменту та управління безперервністю діяльності;
– готовність до взаємодії з суб'єктами безпекового сектору (ДСНС України, поліція, технічні служби, кіберзахист).

Також у межах предмету дослідження розглядаються міжнародні підходи до підготовки фахівців (наприклад, стандарти ЄС з цивільного захисту, ініціативи NATO щодо захисту КІ), щоб порівняти їх з українською освітньою практикою та запропонувати інтеграційні механізми.

Таким чином, дослідження зосереджене на тому, як і за допомогою яких педагогічних моделей, технологій та інституційних механізмів можна забезпечити ефективну, адаптивну та актуальну підготовку кадрів, здатних реагувати на складні та багатоаспектні загрози критичній інфраструктурі у XXI столітті.

Зважаючи на окреслені об'єкт і предмет дослідження, особливу увагу варто приділити порівняльному аналізу існуючих освітніх практик у сфері цивільного захисту, що застосовуються в Україні та країнах Європейського Союзу. Такий аналіз дозволяє виявити як структурні відмінності, так і потенційні точки інтеграції, які можуть підвищити ефективність національної моделі підготовки фахівців.

Враховуючи актуальність і багатовимірність викликів, постає питання: як забезпечити підготовку фахівців, здатних діяти ефективно в умовах високої невизначеності та взаємопов'язаних загроз? Відповідь на це запитання вимагає аналізу як національних, так і міжнародних освітніх практик, особливо тих, що успішно застосовуються в ЄС та НАТО у сфері захисту критичної інфраструктури.

Це дає підстави для формулювання наукової гіпотези, яка далі лягає в основу аналітичного розділу цієї роботи.

Наукова гіпотеза: інтеграція європейських освітніх підходів – зокрема, компетентнісної моделі, міждисциплінарного змісту навчання та модульної післядипломної підготовки – у національну систему освіти в галузі цивільного захисту дозволить суттєво підвищити ефективність підготовки фахівців для захисту критичної інфраструктури в Україні в умовах сучасних гібридних загроз.

Результати

1. Теоретичні засади захисту критичної інфраструктури

1.1. Поняття критичної інфраструктури та її вразливості. Термін "критична інфраструктура" (КІ) у міжнародній практиці охоплює системи, об'єкти, мережі та послуги, що є життєво необхідними для забезпечення національної безпеки, економічної стабільності, здоров'я населення та суспільного добробуту. Наприклад, у Директиві Ради Європейського Союзу 2008/114/ЕС "Про визначення та призначення європейської критичної інфраструктури та оцінку необхідності підвищення її захисту" зазначено, що критична інфраструктура – це об'єкти, системи чи їх частини, які є життєво важливими для підтримки основних функцій суспільства, здоров'я, безпеки, економічного чи соціального добробуту людей, і руйнування чи порушення функціонування яких може мати серйозні наслідки для держав-членів ЄС. У США під КІ розуміють системи та об'єкти, які є настільки важливими, що їх вихід з ладу або руйнування матиме руйнівний вплив на безпеку, національну економіку, громадське здоров'я чи безпеку [12].

В Україні поняття критичної інфраструктури закріплене у Законі України від 05.10.2021 № 2223-IX "Про критичну інфраструктуру", який визначає КІ як сукупність об'єктів, систем, мереж, послуг, що мають стратегічне значення для забезпечення безпеки, оборони, економічної стабільності, здоров'я населення та функціонування держави. Закон встановлює правові, організаційні та технічні засади захисту критичної інфраструктури, а також визначає відповідальність за її порушення [13].

КІ охоплює низку ключових секторів, безперервне функціонування яких є основою для стабільності держави. До них належать: енергетика, транспорт, зв'язок, телекомунікації,

водопостачання, охорона здоров'я, фінансові послуги, державне управління та оборона. З розвитком цифрових технологій до КІ дедалі частіше відносять інформаційно-комунікаційні системи, зокрема центри обробки даних, мережі Інтернету речей (IoT), автоматизовані системи управління технологічними процесами (SCADA).

Енергетика є фундаментом для функціонування інших секторів, оскільки забезпечує електропостачання, теплопостачання та паливо. Транспортна інфраструктура забезпечує логістику, мобільність населення та вантажів, що є критично важливим для економіки та безпеки. Сектор зв'язку та телекомунікацій забезпечує передачу інформації, координацію дій у надзвичайних ситуаціях, а також підтримку інших інфраструктурних систем. Водопостачання необхідне для життєдіяльності населення, роботи промисловості та сільського господарства. Охорона здоров'я забезпечує медичне обслуговування та реагування на надзвичайні ситуації, такі як пандемії чи масові травми [14]. Взаємозалежність між секторами створює ризик каскадних ефектів – наприклад, відключення електроенергії може паралізувати водопостачання, медичні послуги, транспорт тощо.

1.2. Системна відповідь і освітні засади забезпечення захисту КІ. Захист критичної інфраструктури 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 акцентують увагу на необхідності системного підходу до захисту КІ, який включає комплексну оцінку вразливостей, ідентифікацію критичних функцій та планування заходів із забезпечення стійкості в умовах багаторівневих загроз [15].

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 [16]. 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.

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 на рівні бакалаврату, магістратури та підвищення кваліфікації, такі як реалізована у Львівському державному університеті безпеки життєдіяльності, є не лише педагогічною інновацією, а й елементом національної стратегії зміцнення обороноздатності держави.

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.

З огляду на складність і динаміку сучасних загроз, захист КІ вимагає впровадження багаторівневих систем безпеки, регулярного моніторингу, оцінки ризиків, підвищення кваліфікації персоналу та розвитку міжнародної співпраці. Особливої ваги набуває впровадження кращих практик, міжнародних стандартів (NIST, ISO, IEC) і використання

сучасних технологій для забезпечення стійкості та безперервності функціонування критичних систем [17].

У підсумку, теоретичні засади захисту КІ поєднують концепції системності, проактивності, освітньої трансформації та інституційної інтеграції. Це – основа для формування стійкої, адаптивної і ефективної системи захисту життєво важливої інфраструктури в умовах гібридних загроз XXI століття.

Модель, яка обґрунтовується у підрозділі, передбачає три основні рівні освітнього впливу: підготовка бакалаврів, магістрів, а також систему підвищення кваліфікації для фахівців з інших технічних спеціальностей. Такий підхід дозволяє забезпечити безперервність навчального процесу, враховуючи як формальну вищу освіту, так і потребу у швидкому перенавчанні та перепідготовці кадрів у зв'язку зі зміною технологій, стандартів безпеки або структури ризиків.

На бакалаврському рівні акцент робиться на закладенні фундаментальних знань у сфері інженерного захисту, нормативного регулювання, основ кризового управління та реагування на надзвичайні ситуації. Цей етап є критично важливим для формування базової компетентності, яка дозволяє молодим фахівцям включатися у процеси аналізу ризиків, підтримки стабільного функціонування об'єктів КІ та участі у системі національної безпеки.

Магістерський рівень орієнтований на розвиток аналітичного мислення, здатності до стратегічного планування, моделювання сценаріїв загроз і управління системами захисту в умовах нестабільності. У фокусі підготовки – інтердисциплінарний підхід: поєднання знань у галузях управління, кіберзахисту, інженерії. Це забезпечує високу адаптивність випускників до змінних викликів і робить їх здатними працювати на стику кількох критичних сфер.

Особливу увагу в статті приділено системі підвищення кваліфікації для фахівців, які вже працюють у суміжних технічних галузях, але не мають спеціалізованих знань у сфері цивільного захисту та КІ. Завдяки модульним програмам, короткостроковим курсам, дистанційним платформам та практико-орієнтованому навчанню можливе швидке перенавчання кадрів із високим потенціалом. Таким чином, створюється механізм гнучкого кадрового резерву, здатного закривати "вузькі місця" на стратегічно важливих об'єктах у кризові моменти.

У сукупності запропонована багаторівнева модель є відповіддю на вимогу часу – сформувати висококваліфікованих, стійких, аналітично мислячих та міждисциплінарно підготовлених фахівців, здатних захищати критичну інфраструктуру країни в умовах гібридних викликів XXI століття (рис. 1).

Рисунок 1 – Багаторівнева модель підготовки фахівців із захисту критичної інфраструктури

2. Підготовка фахівців на рівні бакалавра у сфері захисту критичної інфраструктури

Підготовка бакалаврів за освітньою програмою "Захист критичної інфраструктури" у межах спеціальності 263 "Цивільна безпека" орієнтована на формування висококваліфікованих фахівців, здатних здійснювати оцінку вразливостей, підтримку інженерного захисту, реагування на надзвичайні ситуації та забезпечення стійкості критично важливих об'єктів. Ця програма спрямована на комплексне поєднання фундаментальної теоретичної підготовки з практико-орієнтованим навчанням у сфері цивільного захисту, що є ключовим для ефективної діяльності у цій галузі.

Основна мета освітньої програми – забезпечити здобувачів знаннями, уміннями та навичками для виявлення та аналізу ризиків для об'єктів КІ; прогнозування надзвичайних ситуацій; розробки та впровадження заходів з інженерного захисту; організації реагування і ліквідації наслідків НС. Таким чином, програма формує у здобувачів комплексне розуміння процесів управління ризиками та практичні навички їх мінімізації.

Програма відповідає стандартам EQF (6 рівень) та FQ-EHEA (перший цикл) і є частиною національної системи реалізації концепції стійкості. Відповідність цим стандартам гарантує якість освіти та її інтеграцію у європейський освітній простір.

Освітня програма підготовки бакалаврів за спеціальністю "Захист критичної інфраструктури" передбачає загальний обсяг 240 кредитів ECTS та триває 3 роки і 10 місяців. Структура програми охоплює чотири основні компоненти: загальну, професійну, вибіркову підготовку та атестаційний блок. Кожен із цих компонентів спрямований на формування комплексних знань і навичок, необхідних для професійної діяльності.

Загальна підготовка обсягом 57,5 кредитів включає фундаментальні дисципліни, зокрема математику, фізику, хімію та інформатику, а також гуманітарні предмети, як-от українська мова, філософія та психологія, і природничий компонент, який містить основи теорії горіння та вибуху. Професійна підготовка, що становить 116,5 кредитів, зосереджена на вивченні фахових дисциплін – моніторингу, рятувальної справи, категоризації об'єктів критичної інфраструктури, техногенної безпеки – та спеціалізованих курсів, серед яких застосування безпілотних літальних апаратів, вивчення SCADA-систем і автоматизованих систем управління. У рамках цієї частини передбачено проходження трьох видів практик: навчальної, фахової та переддипломної. Атестаційний блок включає виконання курсової роботи, складання комплексного кваліфікаційного іспиту та захист кваліфікаційної роботи. Вибірковий компонент програми, що охоплює 60 кредитів, орієнтований на формування індивідуальної освітньої траєкторії кожного здобувача, забезпечуючи гнучкість навчального процесу та можливість його персоналізації відповідно до професійних інтересів і запитів ринку праці.

Освітня програма передбачає набуття загальних та фахових компетентностей. Особливо важливо підкреслити ті фахові компетентності, які безпосередньо пов'язані з профілем програми та орієнтовані на реальні професійні завдання в умовах загроз техногенного, природного та соціального походження. Центральною спеціальною компетентністю є здатність до усвідомлення функцій держави у сфері цивільного захисту, правових засад його реалізації, а також знання принципів організації захисту на об'єктах критичної інфраструктури. Важливою складовою є здатність визначати рівень захисту таких об'єктів у межах посадових обов'язків, а також планувати комплекс заходів, спрямованих на забезпечення безпеки інфраструктури. До критичних умінь належить також ідентифікація загроз, що можуть спричинити надзвичайні ситуації, та оцінювання ймовірних ризиків їх виникнення.

Фахівець повинен бути здатним не лише здійснювати прогнозування загроз, а й брати участь у виконанні аварійно-рятувальних робіт та ліквідації наслідків надзвичайних ситуацій на об'єктах критичної інфраструктури. Особлива увага у компетентнісному переліку приділяється здатності забезпечення енергетичної безпеки держави в умовах збройного конфлікту, зокрема під час широкомасштабної агресії. Така компетентність вимагає не тільки технічних знань, а й розуміння стратегічного значення енергетичних об'єктів.

Таким чином, фахові компетентності формують фундамент професійної готовності бакалавра до роботи в умовах високої відповідальності, складної міжгалузевої взаємодії та необхідності оперативного прийняття рішень у кризових ситуаціях. Це забезпечує не лише здатність до реагування на надзвичайні події, а й до системного управління ризиками у контексті захисту критичних об'єктів інфраструктури держави.

Випускники бакалаврської програми з підготовки фахівців у сфері захисту критичної інфраструктури мають широкий спектр можливостей для працевлаштування у державному, муніципальному та приватному секторах, зокрема в органах влади, службах цивільного захисту, інфраструктурних підприємствах та аналітичних центрах. Зокрема, вони можуть працювати експертами та аналітиками із захисту критичної інфраструктури – це фахівці, які здійснюють комплексний аналіз загроз, розробляють профілі вразливості об'єктів КІ, проводять аудит безпеки та формують рекомендації щодо посилення стійкості інфраструктурних систем. Актуальність цієї спеціалізації особливо висока в умовах гібридної війни та кібератак, коли стратегічні об'єкти перебувають під постійним тиском фізичних і цифрових загроз. Інша ключова група – фахівці з оцінки загроз та ризиків, які спеціалізуються на моделюванні сценаріїв надзвичайних ситуацій, здійсненні превентивного аналізу потенційних небезпек, розробці карт ризиків та впровадженні систем раннього попередження. Вони затребувані у державних антикризових структурах, у великих корпораціях та на підприємствах енергетичного, транспортного і телекомунікаційного секторів. Інженери критичної інфраструктури з техногенно-екологічної безпеки забезпечують проектування, обстеження та експлуатацію об'єктів з урахуванням норм безпеки, екологічних стандартів та ризик-орієнтованого підходу; ця позиція є актуальною в умовах екологічних катастроф, зношеної інфраструктури та необхідності модернізації систем життєзабезпечення. До сфери безпосереднього реагування належать фахівці цивільного захисту та державні інспектори з нагляду – вони працюють у Державній службі з надзвичайних ситуацій, виконуючи завдання з моніторингу, контролю, ліцензування об'єктів підвищеної небезпеки, а також беруть участь у плануванні евакуацій, навчаннях та ліквідації наслідків надзвичайних подій. Найбільш прикладний напрям – керівники рятувальних підрозділів оперативного реагування, які координують дії під час надзвичайних ситуацій, організовують взаємодію між службами, забезпечують оперативне управління рятувальними операціями на місцях аварій, атак чи катастроф. Ця група посад потребує не лише технічної компетентності, а й лідерських якостей, уміння швидко приймати рішення в умовах стресу та невизначеності. Загалом, кожна із зазначених спеціальностей відображає сучасні запити безпекового сектору, пов'язані зі зростанням складності загроз, технологічною інтеграцією КІ та потребою у висококваліфікованих кадрах, здатних діяти у багатовимірному ризиковому середовищі.

Таким чином, освітня програма бакалаврського рівня з підготовки фахівців у сфері захисту критичної інфраструктури забезпечує формування міждисциплінарних, практично орієнтованих і стійких до криз знань та навичок. Її реалізація сприяє розбудові кадрового потенціалу системи цивільного захисту, формує професіоналів, готових діяти в умовах гібридних загроз та багаторівневих ризиків.

3. Підготовка фахівців на магістерському рівні у сфері захисту критичної інфраструктури

Магістерська програма "Безпека та захист критичної інфраструктури" реалізується у межах спеціальності 263 "Цивільна безпека" й орієнтована на формування у здобувачів глибоких знань і навичок для практичної, управлінської та дослідницької діяльності в умовах підвищеної загрозливості об'єктам критичної інфраструктури. Її мета полягає у підготовці фахівців, здатних вирішувати задачі дослідницького та інноваційного характеру, застосовувати сучасні методи управління ризиками та забезпечувати стійкість КІ як у мирний час, так і в умовах надзвичайних ситуацій. Особливістю програми є активне залучення експертів-практиків, представників органів державної влади, ДСНС України та управлінських структур, що забезпечує високу практичну орієнтацію підготовки та сприяє працевлаштуванню випускників у профільних установах.

Навчання триває 1 рік 6 місяців, має обсяг 90 ECTS і охоплює загальну, фахову, практичну та вибіркову підготовку. До обов'язкових освітніх компонентів належать вивчення

професійної іноземної мови, системного аналізу, методології досліджень, політики та структури КІ, комп'ютерного моделювання небезпечних процесів, моніторингу, управління ризиками, функціонування енергетичної та транспортної інфраструктури. Також передбачено навчальні практики та атестацію у вигляді комплексного кваліфікаційного екзамену. Вибірковий блок дозволяє адаптувати навчальний трек під індивідуальні потреби здобувача, зосередившись на специфічних технологічних або правових аспектах КІ.

Програма спрямована на розвиток цілісного комплексу компетентностей. Серед загальних – здатність до критичного мислення, комунікації іноземною мовою, ухвалення рішень в умовах невизначеності, інноваційність та соціальна відповідальність. Фахові компетентності включають управління ризиками і безпекою, техніко-економічне обґрунтування рішень, моніторинг об'єктів КІ, впровадження ІТ-технологій у безпекову діяльність, розуміння міжнародного контексту та здатність до міжгалузевої координації. Окремо виділяються спеціальні компетентності програми: оцінка вразливостей об'єктів КІ, моделювання загроз та планування заходів безпеки – навички, критично важливі для керівників підрозділів, експертів з оцінки ризиків, інженерів з техногенної безпеки та аналітиків кризових ситуацій.

Таким чином, освітня програма є відповіддю на потребу в підготовці нової генерації фахівців, здатних інтегрувати технічні, організаційні та наукові рішення для захисту критичної інфраструктури в умовах гібридних загроз. Вона не лише формує високий рівень професійної підготовки, а й забезпечує основу для подальшого навчання на третьому рівні освіти або в програмах професійного розвитку.

Випускники магістерської освітньої програми "Безпека та захист критичної інфраструктури" зі спеціальності "Цивільна безпека" суттєво відрізняються від фахівців бакалаврського рівня як за рівнем підготовки, так і за спектром професійних можливостей. Основна відмінність полягає у глибшій аналітичній, стратегічній та управлінській компетентності, що дозволяє їм обіймати не лише технічні, а й керівні або експертно-аналітичні посади у сфері захисту критичної інфраструктури.

Магістри здатні виконувати комплексні завдання з оцінки ризиків, розроблення політик безпеки, моделювання загроз і кризових сценаріїв, а також організовувати системи управління безперервністю функціонування КІ. Вони можуть обіймати посади керівників відділів із безпеки в державних структурах (ДСНС України, Міноборони, СБУ, Мінінфраструктури), аналітиків у кризових центрах та службах стратегічного планування, фахівців у міжнародних проєктах із безпеки, а також експертів у приватних компаніях, що обслуговують енергетичну, транспортну або інформаційну інфраструктуру. Їх також залучають до роботи у дослідницьких інститутах, аналітичних центрах та ІТ-компаніях, які спеціалізуються на інструментах моніторингу, SCADA-системах або кіберзахисті.

На відміну від бакалаврів, які зазвичай займають початкові технічні або виконавчі посади – інженерів, операторів, інспекторів, спеціалістів із моніторингу – магістри здатні здійснювати міжвідомчу координацію, очолювати безпекові підрозділи або виступати радниками з безпеки в урядових або корпоративних структурах. Їх підготовка включає стратегічне мислення, роботу з нормативно-правовими рамками ЄС і НАТО, антикризове управління та комунікацію зі стейкхолдерами різного рівня. Це робить їх надзвичайно актуальними в умовах зростання загроз для КІ, необхідності адаптації до євроатлантичних стандартів безпеки та розвитку системи цивільного захисту на новому рівні інтеграції.

Отже, працевлаштування магістрів можливе як у державному, так і в комерційному та міжнародному секторах, де необхідна аналітична експертиза, системне бачення та лідерські якості у сфері захисту КІ. Їх компетентності дозволяють діяти не лише в межах оперативного реагування, а й у сфері політик безпеки, стратегічного розвитку та міжнародної координації безпекових заходів.

4. Підвищення кваліфікації фахівців

Основною метою підвищення кваліфікації осіб, які залучаються до здійснення заходів захисту об'єктів критичної інфраструктури (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 [13, 15, 16, 18-23])

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 ОКІ.

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 КІ, нових знань, умінь та навичок, спрямованих на створення і організацію безпеки КІ, зокрема:

– забезпечення функціональності, безперервності роботи, цілісність і стійкість КІ;

– набуття теоретичних основ та поглиблення набутих теоретичних знань щодо законодавчої бази у сфері захисту КІ;

– 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. 2).

Змістовий модуль № 1 "Загальні положення щодо організації захисту, безпеки та стійкості критичної інфраструктури" зосереджений на організаційних та правових аспектах захисту КІ, основних засадах державної політики у сфері захисту КІ, стійкості КІ, ознайомленні з міжнародним досвідом захисту ОКІ.

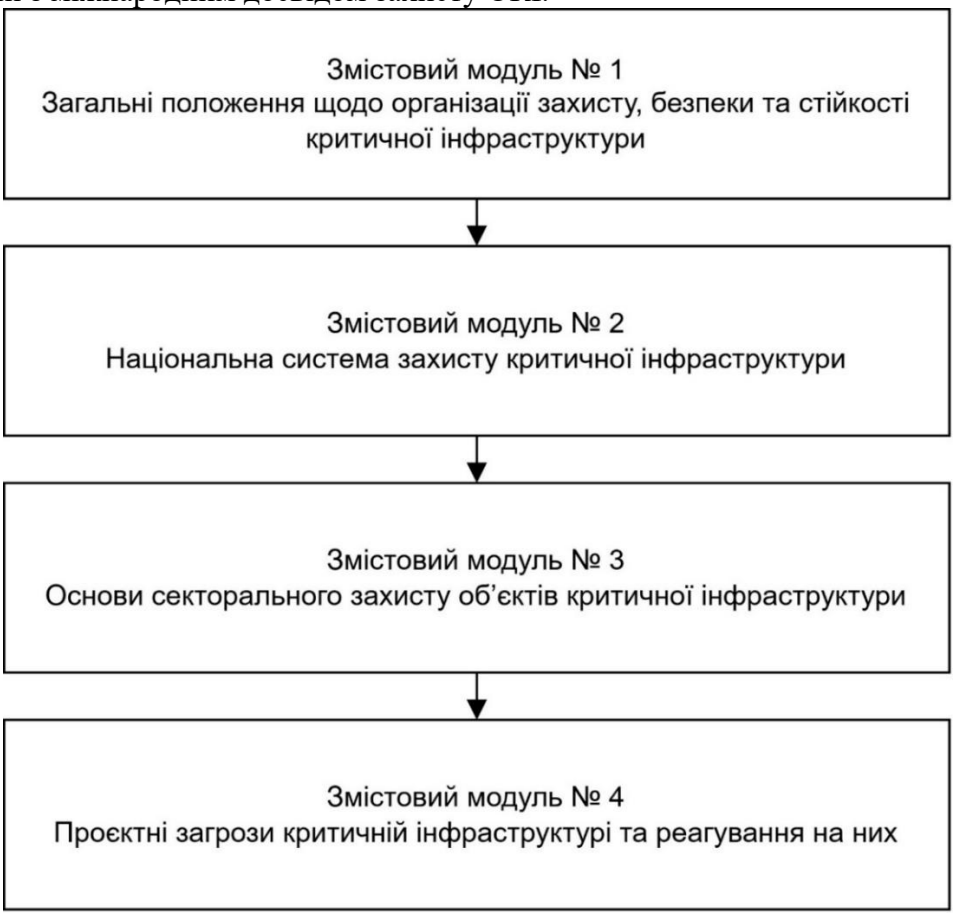

Рисунок 1 – Схема змістових модулів освітньої програми підвищення кваліфікації "Захист об'єктів критичної інфраструктури" у Львівському державному університеті безпеки життєдіяльності

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 КІ, порядок взаємодії між суб'єктами захисту КІ.

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 КІ, 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 КІ 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 КІ, 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 КІ;

– визначати критичні елементи ОКІ;

– визначати можливі загрози для КІ;

– 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 КІ, 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.

5. Очікувані результати та суспільний ефект

Створення системи підготовки фахівців нового покоління у сфері захисту КІ є одним із ключових завдань національної безпеки та сталого розвитку держави. У сучасних умовах, коли загрози стають дедалі комплекснішими і багатовимірними, потреба у висококваліфікованих кадрах, які здатні ефективно протистояти різноманітним викликам, зростає в рази. Така система підготовки має ґрунтуватися на інтеграції теоретичних знань, практичних навичок і сучасних технологій, а також на міждисциплінарному підході, що охоплює технічні, управлінські, правові та соціальні аспекти захисту КІ.

Перш за все, створення такої системи дозволить забезпечити формування фахівців, які володітимуть не лише глибокими технічними знаннями, а й стратегічним мисленням, здатністю до комплексного аналізу ризиків, прийняття ефективних управлінських рішень та організації взаємодії між різними структурами. Вони будуть підготовлені до роботи в умовах високої невизначеності, багаторівневих загроз та швидких змін у технологічному та безпековому середовищі. Важливо, що така підготовка сприятиме розвитку інноваційного потенціалу, що особливо актуально для впровадження новітніх технологій у сфері захисту КІ.

Підвищення рівня безпеки ОКІ є безпосереднім і найважливішим результатом реалізації системи підготовки фахівців. Компетентні спеціалісти здатні проводити детальний аналіз вразливостей, прогнозувати можливі загрози та розробляти ефективні заходи для їх нейтралізації. Це, в свою чергу, сприяє зниженню ризику виникнення надзвичайних ситуацій, таких як техногенні аварії, кібернетичні атаки, диверсії чи природні катастрофи. Підвищення стійкості критично важливих об'єктів дозволяє забезпечити безперервність функціонування життєво важливих систем, що є фундаментом для соціальної стабільності та економічного розвитку країни.

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

колективна монографія
за загальною редакцією
БОНДАРЯ Дмитра Володимировича

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