Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 006.86+641.841
DOI: 10.32447/20784643.29.2024.13

Т. З. Бубела[1], М. Я. Мельник[2], О. Б. Назаровець[2], Ю. І. Рудик[1,2]
[1]Національний університет "Львівська політехніка", м. Львів, Україна
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/ 0000-0002-2525-9735 – Т. З. Бубела
https://orcid.org/0009-0007-2557-0877 – М. Я. Мельник
https://orcid.org/0000-0003-4532-9259 – О. Б. Назаровець
https://orcid.org/0000-0002-7372-5876 – Ю. І. Рудик
rudyk@ldubgd.edu.ua

АНАЛІЗ ВИЗНАЧЕНЬ ТА НОРМАТИВНИХ ВИМОГ СИСТЕМИ ЗАХИСТУ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ. Зважаючи на умови постійних прогресивних змін проєктного середовища, враховуючи чинники воєнного стану та постійну невизначеність і нестабільність, стає очевидним збільшення ризику небезпеки для життєдіяльності територій та населення. В першу чергу це відображається через масовані обстріли об'єктів критичної інфраструктури підступним ворогом. Варто зазначити, що під час російської повномасштабної агресії на сході України, за останні роки було завдано значних пошкоджень і втрат в інфраструктурі. Дані про економічні збитки підсумовуються та оновлюються і можуть повідомлятися у вигляді офіційних звітів урядових органів, міжнародних організацій, таких як Міжнародний валютний фонд або Світовий банк.

Мета. Метою є аналіз стану урегульованості профілактики та реагування щодо можливих основних загроз та потенційних негативних наслідків для об'єктів критичної інфраструктури (ОКІ), визначення їх показників для запобігання таким загрозам для критичної інфраструктури.

Методи дослідження. Дослідження об'єктів критичної інфраструктури України можуть проводитися за допомогою різноманітних методів і підходів залежно від конкретної потреби та мети дослідження. Технічне обстеження, моделювання та симуляція, соціально-економічні дослідження, методи системного аналізу – все це інструменти для подальшої нашої роботи.

Результати. Результати дослідження показників систем захисту в області, що стосується об'єктів критичної інфраструктури, їх технічного стану та стандартів безпеки, полягають у виявленні вразливостей та потенційних загроз, оцінці можливих ризиків і встановленні пріоритетів для захисту, оскільки в певних аспектах наші оборонні спроможності таких об'єктів є обмеженими. Ідентифіковані та опрацьовані вразливості і ризики дають змогу визначити та відповідно здійснити категоризацію та пріоритезацію найбільш критичних об'єктів, які потребують негайного вдосконалення відповідних заходів захисту. Відповідно до результатів цього аналізу розробляються конкретні рекомендації із заходів захисту та планів реагування на потенційні надзвичайні ситуації. Крім того, важливо постійно відстежувати зміни у загрозах, які в нинішніх умовах відбуваються ледь не щодня, та оновлювати заходи захисту з урахуванням змін. Ці результати дослідження є основою для розроблення стратегій захисту критичної інфраструктури та забезпечення національних інтересів.

Висновки. Сформовані дані дослідження об'єктів критичної інфраструктури, включаючи паспортизацію, а також впровадження показників систем захисту на базі системи LIDAR, показали майбутню перспективу та великі можливості для розвитку та заохочення впровадження нових технологій. Існує висока ймовірність, що саме ці нововведення стануть дуже корисними та необхідними для забезпечення безпеки та ефективного функціонування інфраструктури.

Ключові слова: об'єкти критичної інфраструктури, система LIDAR, воєнний стан, індекс захисту, гідротехнічні споруди, інженерно-технічні заходи цивільного захисту.

***T. Z. Bubela*[1] *, M. Y. Melnyk*[2]*, O. B. Nazarovets*[2]*, Y. I. Rudyk*[1, 2]**
[1]Lviv Polytechnic National University
[2]Lviv State University of Life Safet

ANALYSIS OF DEFINITIONS AND REGULATORY REQUIREMENTS OF THE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

Introduction. Taking into account the conditions of constant progressive changes in the project environment, taking into account the factors of the state of war and constant uncertainty and instability, it becomes obvious that the risk to life safety of the territories and the population is increasing. First of all, this is reflected in the massive shelling of critical infrastructure facilities by an insidious enemy. It is worth noting that during the conflict in the east of Ukraine and Russia's full-scale aggression, significant damage and losses in infrastructure were caused in recent years. Data on economic losses are summarised and updated and can be reported in the form of official reports of government bodies, and international organisations such as the International Monetary Fund or the World Bank.

Goal. The goal is to analyse possible main threats and potential negative consequences for critical infrastructure objects, to prevent and prevent the occurrence of such threats to critical infrastructure.

Research methods. Research of critical infrastructure objects of Ukraine can be carried out using various methods and approaches modelling and simulation, socio-economic research, and methods of system analysis – all these are tools for our further work.

The results. The results of the study of the area concerning the objects of critical infrastructure, their technical condition and standards consist in identifying vulnerabilities and potential threats, assessing possible risks and establishing priorities for protection, since in certain aspects our defence capabilities of such objects are limited. Identified and processed vulnerabilities and risks make it possible to identify and, accordingly, carry out the categorisation and prioritisation of the most critical objects that require immediate improvement of relevant protection measures. Based on the processing of this analysis, specific recommendations for protective measures and response plans for potential emergencies are developed. In addition, it is important to constantly monitor changes in threats, which in current conditions appear almost daily, and to update protection measures taking into account the changes. These research results are the basis for developing strategies to protect critical infrastructure and ensure the security of national interests.

Conclusions. The generated data from the study of critical infrastructure facilities (CIF), including certification, as well as the implementation of the LIDAR system, showed a future perspective and great opportunities for the development and promotion of new technologies. There is a high probability that these innovations will become very useful and necessary to ensure the safety and efficient functioning of the infrastructure.

Keywords: critical infrastructure facilities, passporting, LIDAR system, martial law, progressive changes, hydraulic facilities, civil defence facilities.

Вступ. Головним критерієм віднесення підприємств, установ чи організацій до об'єктів критичної інфраструктури (ОКІ) є визнання того, що наслідки порушення сталого функціонування одного або низки їхніх підрозділів, можуть спричинити надзвичайні ситуації або мати негативний вплив на стан різних галузей соціального розвитку. Оскільки енергосистема України тісно взаємопов'язана, то багато ОКІ є в енергетичній галузі. Тому передусім необхідно визначити важливість інфраструктурних об'єктів для надання основних послуг у всіх секторах економіки та сферах діяльності для впровадження низки заходів із захисту таких об'єктів від можливості виникнення кризових ситуацій. У розгляді цього дискурсу нам допоможе Постанова КМУ №1109, в якій визначаються механізм і критерії віднесення об'єктів до критичної інфраструктури. Цю постанову розроблено з урахуванням вимог законодавства ЄС. Визначений порядок встановлює механізм віднесення об'єктів до критичної інфраструктури та їх категоризації. Методичні рекомендації цієї Постанови можуть бути використані секторальними органами, а також центральним органом виконавчої влади з питань цивільного захисту, у сфері захисту критичної інфраструктури та операторами критичної інфраструктури для проведення категоризації об'єктів критичної інфраструктури. У секторальному органі у сфері захисту критичної інфраструктури створюється постійно діюча робоча група з ідентифікації та категоризації об'єктів критичної інфраструктури [1-2].

Акцентуючи увагу на активізацію загроз природного та техногенного походження, підвищення ризиків терористичних актів, збільшення кількості кібератак на енергетичні об'єкти, руйнування та пошкодження об'єктів інфраструктури в зоні військового конфлікту на сході України, ми підтверджуємо важливість та обумовлюємо нагальність питання розбудови державної системи захисту об'єктів критичної інфраструктури в Україні. Розглянемо питання щодо існуючого порядку їх паспортизації та категоризації. Нині в Україні існують декілька функціональних систем забезпечення галузевих об'єктів. Так, у сфері цивільного захисту відповідно до Закону України «Про об'єкти підвищеної небезпеки», до вересня 2022 року

найбільш пристосованим до вирішення завдань захисту критичної інфраструктури було передбачено декларування безпеки об'єкта підвищеної небезпеки шляхом підготовки документа, в якому наводяться результати аналізу ступеня небезпеки та оцінки рівня ризику цього об'єкта. Цей документ передбачав комплекс заходів, що вживаються суб'єктом господарської діяльності з метою запобігання аваріям, а також забезпечення готовності до дій за призначенням служб цивільного захисту [3-5], включаючи *гідротехнічні об'єкти,* що є предметом зацікавлення в опрацюванні авторами цієї статті. Це, насамперед, загальна інформація про об'єкт, дані про небезпечні природні умови та технологічні процеси, дані щодо основних джерел небезпеки та об'єктів впливу надзвичайних ситуацій, аварійно-рятувальна документація тощо. Враховуючи сучасні умови варто визначати рівень захищеності ОКІ. Треба відмітити, що в рамках Державної системи фізичного захисту, яка однак функціонує щодо ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання, за результатами оцінки вразливості формуються документи, які є значно ширшими з точки зору оцінки загроз. Відповідно до концепції створення державної системи захисту критичної інфраструктури в Україні, ця система спрямована на забезпечення стійкості критичної інфраструктури до всіх типів загроз, включаючи загрози природного і техногенного характеру, кіберзагрози, а в умовах воєнного стану також розробляються заходи інженерного захисту від комбінованих атак з повітря. Метою оцінювання безпеки ОКІ є встановлення можливих ризиків та негативних наслідків їх прояву для ОКІ. При проведенні оцінки негативних наслідків надзвичайних ситуацій на об'єктах критичної інфраструктури має враховуватися шкода для життя і здоров'я людей, виражена через кількість постраждалих, травмованих, загиблих, евакуйованих. У цілому це є складовим етапом створення державної системи захисту критичної інфраструктури, що потребує дієвої взаємодії різних структур, секторальних органів виконавчої влади і спецслужб, що мають погоджувати заходи безпеки, а також пряме залучення фахівців цивільного захисту. Забезпечення такої взаємодії та її захист можливо врегулювати через ухвалення відповідних змін до Закону від 16.11.2021 № 1882-IX «Про критичну інфраструктуру», що перебувають на етапі узгодження і надання пропозицій [6].

Методи дослідження. Дослідження об'єктів критичної інфраструктури України можуть проводитися за допомогою таких різноманітних методів і підходів залежно від конкретної потреби та мети дослідження: технічне обстеження, моделювання та симуляція, соціально-економічні дослідження, методи системного аналізу. У зв'язку з розвитком законодавства у сфері забезпечення захисту критичної інфраструктури постає необхідність вирішення комплексу питань, серед яких важливе значення має визначення та наповнення показників системи захисту ОКІ. Розрахунок узагальненої нормованої оцінки рівня критичності здійснюється за такою формулою:

$$РК_{ОКІ} = \frac{\sum РК_і}{\sum РК_{max}},$$

де: $РК_{окі}$ – узагальнена нормована оцінка рівня критичності об'єкта критичної інфраструктури; $РК_i$ – сума балів, які отримав об'єкт критичної інфраструктури за всіма критеріями критичності; $РК_{max}$ – максимальна можлива сума балів (розраховується, виходячи з того, що об'єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу).

Рішення щодо категорії критичності об'єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об'єкта критичної інфраструктури відповідно до такої таблиці з такими вихідними даними:

Таблиця 1

Категорії нормованої оцінки рівня критичності ОКІ [17]

I категорія критичності	$0,8 < РК_{ОКІ} \leq 1$
II категорія критичності	$0,63 < РК_{ОКІ} \leq 0,8$
III категорія критичності	$0,37 < РК_{ОКІ} \leq 0,63$
IV категорія критичності	$0,2 < РК_{ОКІ} \leq 0,37$

Об’єкт не є критичним	$РК_{ОКІ} \leq 0,2$

Аналіз останніх досліджень і публікацій. Однією з важливих умов є визначення рівня негативного впливу на життєдіяльність населення у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури [7, 8].

Суб’єкти господарювання, інші юридичні особи, у користуванні яких є об’єкти підвищеної небезпеки, зобов’язані укладати договори страхування відповідальності за шкоду, яка може бути заподіяна внаслідок НС, у тому числі пожеж та аварій на об’єктах підвищеної небезпеки, екологічно небезпечних аварій та надзвичайних ситуацій техногенного та природного характеру, аварій, що становлять загрозу санітарному чи епідемічному здоров’ю населення [9, 10]. Вищенаведена інформація свідчить про беззаперечну важливість елементів, що забезпечують безпеку та стабільність усіх сфер життєдіяльності, національної економіки та соціальної сфери, а саме об’єктів критичної інфраструктури. Проте не варто забувати, що як і будь-який інший об’єкт, ці об’єкти можуть бути піддані ризикам, які можуть призвести до серйозних наслідків для безпечної та нормальної життєдіяльності. Управління ризиками на об'єктах критичної інфраструктури є складним завданням, що потребує комплексного підходу. Один з ключових аспектів цього управління – це управління проєктними ризиками. Це означає врахування можливих проблем, які можуть виникнути на будь-якому етапі реалізації спеціальних проєктів – від планування до введення в експлуатацію і подальшого функціонування. Для успішного управління проєктними ризиками на гідротехнічній споруді об'єкта критичної інфраструктури необхідно розробити концепцію, яка визначатиме підходи до ідентифікації, оцінки та управління цими ризиками, що представлено у вигляді компонентів нижче:

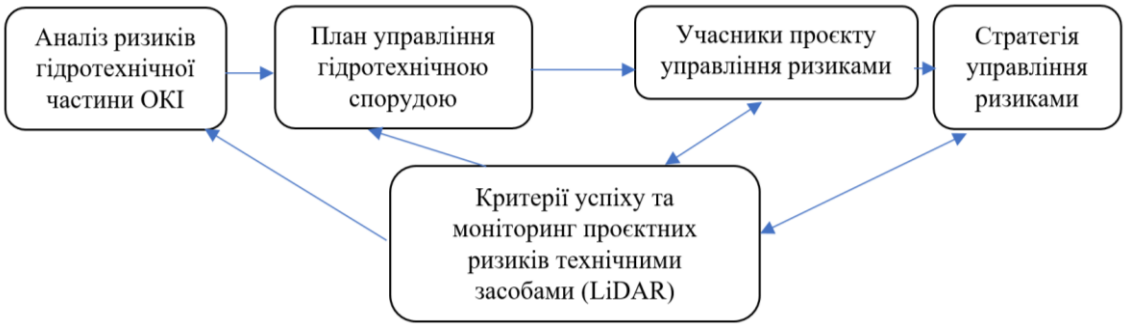

Рисунок 1 – Схема ризик-орієнтованого аналізу управління проєктними ризикам

Формування концепції управління ризиками передбачає розробку плану управління та аварійних заходів, визначення ролей та відповідальності, а також систему моніторингу та оцінки ризиків. Ефективне управління дозволяє забезпечити стабільність функціонування, що важливо для національної безпеки та економічного розвитку [11].

Зважаючи на аналіз наслідків військових дій на території України, стає очевидним, що противник, крім звичайної стратегічної мети досягнення перемоги на полі бою, також спрямовує свої дії на завдання значної шкоди інфраструктурі, яка забезпечує життєво важливі функції суспільства. Це має на меті не лише фізичне підкорення території, а й створення психологічного тиску на населення через руйнування та паралізацію систем, що забезпечують безпеку та комфорт життя. Такий підхід є типовим для військової стратегії, спрямованої на деморалізацію та знищення ворожих ресурсів [12]. У контексті захисту національної безпеки, важливою стає організація ефективного захисту критичної інфраструктури. Це включає в себе всі сфери, які необхідні для нормального функціонування суспільства: енергетику, транспорт, комунікації, водопостачання та інші [13, 14]. ОКІ є основою життя і безпеки країни, тому їх захист стає пріоритетним завданням у разі воєнного конфлікту чи надзвичайної ситуації. Законодавство України чітко визначає відповідальність та вимоги до безпеки ОКІ [15, 16]. Державна служба спеціального зв'язку та захисту інформації України виконує важливу роль у цьому процесі, розробляючи стратегії та рекомендації для захисту секторів ОКІ. Одним з головних завдань цієї служби є підготовка рекомендацій щодо визначення вимог до забезпечення стійкості критичних секторів інфраструктури в умовах загрози військового конфлікту або інших надзвичайних обставин [17]. Важливо також зазначити, що запобігання

надзвичайним ситуаціям є ключовим аспектом безпеки. Тому заходи фізичного захисту від зовнішніх та внутрішніх загроз, а також інженерно-технічні заходи цивільного захисту, відіграють важливу роль у забезпеченні безпеки населення та територій. Умови воєнного конфлікту чи надзвичайної ситуації вимагають розробки та впровадження нових технічних рішень для захисту ОКІ. Наукові дослідження у цій галузі стають актуальними і сприяють досягненню оптимальних стратегій захисту [18]. Результати цих досліджень можуть впливати на зміни у законодавстві, що регулює питання цивільного захисту, як це сталося, наприклад, з Законом України від 24 серпня 2022 р. №2486-IX "Про внесення змін до деяких законодавчих актів України щодо забезпечення вимог цивільного захисту під час планування та забудови територій" [19].

Результати. Для подальшого прогресу та впровадження новітніх технологій у такому секторі цивільної безпеки, як гідротехнічні споруди (ГТС), важливо провести аналіз існуючих методів їх захисту. Розробка нових методів та оптимізація параметрів, які вже існують є кроком у напрямку поліпшення ефективності та надійності захисних систем гідротехнічних споруд, які забезпечують захист від повеней, зсувів ґрунту та інших природних катастроф. Одним із перспективних напрямків в цьому процесі є впровадження LiDAR-сканування, що має низку переваг порівняно з традиційними методами збору гідротехнічних даних [20]. Ця технологія базується на використанні лазерних променів для сканування поверхні землі та отримання точної і деталізованої інформації про рельєф території, що є критично важливим для проектування та будівництва гідротехнічних споруд.

Однією з важливих переваг є можливість створення тривимірних моделей з високою деталізацією, що дає змогу точніше розраховувати параметри для проектування гідротехнічних споруд і ефективніше використовувати ресурси. Серед основних визначальних ознак, якими характеризується така система сканування є:

1. Точність: LiDAR-системи надають дані з точністю до кількох сантиметрів.
2. Швидкість сканування: LiDAR-системи можуть швидко сканувати великі області.
3. Широкий кут огляду: LiDAR-системи можуть охоплювати великі кути огляду, що дає можливість збирати дані з різних кутів та перспектив, що робить LiDAR сканування більш універсальним.
4. Безпечність: В першу чергу це стосується безпеки особового складу та фахівців, присутніх на ГТС. Це дасть змогу проводити всі необхідні розрахунки та вимірювання у відносно безпечних місцях або безпосередньо з укриттів. Також LiDAR-системи можуть працювати безпечно на висоті.

ГТС є надзвичайно перспективною галуззю для впровадження LiDAR-технології, враховуючи всі теперішні умови воєнного стану. Вагомою є допомога західних партнерів в технологічному аспекті. В подальшому це дозволить інженерам цивільного захисту приймати інноваційні рішення в досить короткий проміжок часу. Сфера є цікавою для обговорення, пропонування тем для конкурентних дискусій та напрацювання нових методів використання даної технології. Визначення класу точності потребує великої кількості знань та застосування значного матеріального ресурсу. Проте за допомогою наявних технологій ми зможемо розробити теоретичну план-схему, щодо встановлення дистанційного спостереження за гідротехнічними спорудами.

Для початку визначимо точки вимірювань на гідротехнічних спорудах, де буде проводитися зондування. Вибір точок повинен враховувати особливості структури та мету вимірювань. Наступним кроком буде обрання правильних інструментів. Виберемо відповідні інструменти для зондування. Це може включати геодезичні інструменти, ехолоти, гідроакустичні пристрої та інші.

Важливим є обрання правильної методики. Визначати методику вимірювань потрібно для кожної точки. Це може включати вимірювання глибини води, рельєфу дна, товщини шару осаду тощо. В процесі потрібно розробити систему класифікації точності завдяки відповідним класам для необхідних вимірювань. Класи можуть визначати допустимі відхилення вимірювань від реальних значень.

Протягом наступного етапу потрібно перевірити точність наших вимірювань через валідацію. Порівняємо результати з референтними даними, якщо такі будуть наявні. Забезпечимо систему контролю за точністю вимірювань та врахуємо різні фактори, які можуть впливати на точність вимірювань, такі як атмосферні умови, вологість, течія води тощо [21].

Результати дослідження показників систем захисту в області, що стосується об'єктів критичної інфраструктури, їх технічного стану та стандартів безпеки, полягають у виявленні вразливостей та потенційних загроз, оцінці можливих ризиків і встановленні пріоритетів для захисту, оскільки в певних аспектах наші оборонні спроможності таких об’єктів є обмеженими. Ідентифіковані та опрацьовані

вразливості і ризики дають змогу визначити та відповідно здійснити категоризацію та пріоритезацію найбільш критичних об'єктів, які потребують негайного удосконалення відповідних заходів захисту [22-25]. Відповідно до результатів цього аналізу розробляються конкретні рекомендації із заходів захисту та планів реагування на потенційні надзвичайні ситуації. Крім того, важливо постійно відстежувати зміни у загрозах, які в теперішніх умовах відбуваються ледь не щодня, та оновлювати заходи захисту з урахуванням змін. У вибраному напрямку дослідження для подальшого розвитку та впровадження нових технологій потрібно проводити аналіз існуючих методів гідротехнічного захисту. Вивчення різних видів гідротехнічних захисних споруд та їх параметрів допоможе нам в майбутньому з розробкою кращих систем та інновацій Також це стосується і аналізу існуючих методів визначення ефективності та безпеки таких споруд. Розробка нового методу доповнення параметрів – наступний етап покращення систем функціонування ГТС. Варто визначити ключові критерії ефективності та безпеки для гідротехнічних споруд. Не потрібно забувати і про розробку алгоритмів для визначення оптимальних параметрів споруд з урахуванням встановлених критеріїв.

Напрями подальших досліджень. Одним з найважливіших та водночас важким кроком є проведення заходів щодо інтеграції в систему цивільного захисту. Інженери цивільного захисту постійно розробляють різні методи для впровадження нових параметрів в існуючі гідротехнічні споруди [26, 27]. Оскільки функціонал ДСНС є доволі різноманітним, потрібно забезпечити взаємодію з іншими компонентами системи цивільного захисту. Перед кожним практичним застосуванням слід проводити експерименти та тестування новорозроблених заходів. Проведення експериментів з кожного розробленого методу є запорукою мінімізації впливу небезпечних факторів на співробітників ДСНС у майбутньому. Після тестувань систем функціонування ГТС варто аналізувати отримані результати та порівнювати їх з існуючими рішеннями.

Звичайно важливим є також підвищення на безпеки співробітників ДСНС. Акцентувати увагу потрібно і на дослідженнях взаємодії нових параметрів з природними силами та визначення їхнього впливу на безпеку. Впровадження системи, яка б постійно функціонувала та збирала інформацію про виникнення різних ризиків та визначала заходи для зменшення можливих загроз, а пізніше проводила аналіз, забезпечить нашій структурі велику економію часу та надасть змогу залучати людей до праці в інших, не менш важливих напрямах [28]. Переведення документації та звітності, як необхідний процес бюрократії, у цифрову форму скоротить матеріальні ресурси та час обробки інформації. Варто провести попередню підготовку технічної документації та звітів, які включатимуть в себе результати дослідження та рекомендації для подальшого використання.

Варто відзначити, що новий Закон «Про критичну інфраструктуру» регламентує захист критичної інфраструктури як складову частину забезпечення національної безпеки України.

Цілком погоджуємось із цим формулюванням, мотивуючись ще одним аргументом, закріпленим Стратегією внутрішньої безпеки США [29], якою визначено шість основних напрямів забезпечення національної безпеки, серед яких є і захист критичної інфраструктури.

Варто враховувати вплив різноманітних чинників, починаючи від військово-політичних і закінчуючи погіршенням екологічної ситуації, на управління системою цивільного захисту. Ці виклики вимагають від нас якісну підготовку працівників цивільного захисту для цієї галузі.

Підготовка такого рівня потребує впровадження нових та сучасних методик, включаючи мінливу обстановку, пов’язану з військовими діями. Слід поєднувати різноманітні концепції науково-методичних засад для комплексної підготовки. Потрібно постійно працювати над створенням необхідних умов для подальшого забезпечення такої підготовки на рівні бакалавра та здобутті вищих наукових ступенів.

Пропонуємо звернути увагу на застосування програмно-моделюючих комплексів, які в свою чергу передбачають прогнозування та надання оцінки окремим видам надзвичайних ситуацій. Включаючи вагомий чинник воєнного стану та досвід, отриманий за більше ніж два роки ведення війни з жорстоким ворогом, можемо спрогнозувати низку його задумів та працювати над мінімізацією наслідків таких дій.

Висновки. Захист ОКІ залишається актуальним і необхідним протягом усього періоду існування української держави. З огляду на численні наукові доробки слід зазначити, що ефективність інженерно-технічних заходів цивільного захисту (ІТЗ ЦЗ) ОКІ все ще не є досконалою. Таким чином, у статті здійснено наукову розвідку щодо причин, які негативно впливають на надійність цивільного захисту об’єктів критичної інфраструктури в умовах воєнного стану та

прямого впливу бойових дій, та недоліків, які виникають під час розроблення розділу ІТЗ ЦЗ із захисту ОКІ. У дослідженні обґрунтовані пропозиції змін до нормативно-правових актів, а також окремі інженерно-технічні рішення, які спрямовані на запобігання виникненню НС, забезпечення захисту ОКІ, населення і територій.

Подяка. Автори висловлюють подяку Національному фонду досліджень України, проект № 0123U103529 (2022.01/0009) «Оцінка та прогнозування загроз відновленню та сталому функціонуванню об'єктів критичної інфраструктури» з конкурсу «Наука для відновлення України у воєнний та післявоєнний періоди» за підтримку в проведенні дослідження.

Список літератури:

1. Іванюта С. П. Пріоритети формування реєстру об’єктів критичної інфраструктури та порядку їх обліку. *Стратегічні пріоритети : науково-аналітичний щоквартальний збірник № 3-4 (48)* Національний інститут стратегічних досліджень. Київ : Видавництво НІСД, 2018. С. 26-35.

2. Деякі питання об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України; Порядок, Перелік, Методика від 09.10.2020 № 1109.

3. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. Наказ № 23 від 15 січня 2021 року Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури' (із змінами).

4. Закон України Про страхування . 2019. 1909-IX, чинний. Редакція від 19.04.2024.

5. Про внесення змін до деяких законодавчих актів України щодо уточнення повноважень суб’єктів забезпечення цивільного захисту та імплементації норм міжнародного гуманітарного права у сфері цивільного захисту. Закон України, № 2394-IX, набрав чинності 3 серп. 2022 р.

6. Про внесення змін до деяких законодавчих актів України щодо уточнення повноважень суб'єктів забезпечення цивільного захисту, вдосконалення законодавства з питань [...] Закон України від 08.11.2023 № 3441-IX .

7. Шведов В., Рудик Ю., Куць В. Урахування воєнних ризиків втрат якості електропостачання об’єктів критичної інфраструктури. Управління якістю в освіті та промисловості: досвід, проблеми та перспективи: тези доповідей VI Міжнар. наук.-практ. конф., (16–17 листопада) 2023 року. Режим доступу: https://science.lpnu.ua/qm-2023/proceedings (англ.); https://science.lpnu.ua/uk/qm-2023/tezy-dopovidey (укр.), С.296-298.

8. Павук І. В., Кобилкін, Д. С. Особливості формування концепції управління проєктними ризиками на об’єктах критичної інфраструктури. Інновінг сучасних трендів в менеджменті безпеки: тези доповідей Всеукр. наук.-практ. конф. (м. Львів, 26 травня 2023 року.). Львів : Астропринт, 2023. С. 47-49.

9. Зачко О. Б. Управління безпекою складних інфраструктурних проектів в системі цивільного захисту. *Управління проектами : стан та перспективи* : матер. 10 Міжнар. наук.-практ. конф. Миколаїв: НУК. 2014. С. 91-92.

10. Кобилкін Д.С. Антикризове управління проектами захисту об’єктів критичних інфраструктур *Управління проектами: стан та перспективи*: матер. XII Міжнар. наук.-практ. конф. Миколаїв: МНУК, 2016. С. 75-76.

11. Rudyk, Y., Starodub, A., Kuts, V., Karpenko, V., Zdeb V. Comparative assessment of renewable sources for critical facilities of decentralized supply. ISTCMTM. 2023; Number 84(4). Pp. 10-16. https://doi.org/10.23939/istcmtm2023.04.010.

12. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. 389-VIII Офіційний вісник України. 2015. 98. С. URL : https://zakon.rada.gov.ua/laws/ show/389-19#Text (дата звернення : 09.01.2023).

13. Про правовий режим надзвичайного стану. Закон України від 16.03.2000 р. 1550-III. Офіційний вісник України. URL https://zakon.rada.gov.ua/laws/show/1550-14 (дата звернення : 10.01.2023).

14. Про функціонування єдиної транспортної системи України в особливий період: Закон України від 20.10.1998 р. 194-XIV. Офіційний вісник України. 1998. . URL : https://zakon.rada.gov.ua/laws/show/194-14#Text (дата звернення: 11.01.2023).

15. Про основи національного спротиву : Закон України від 16.07.2021 р. 1702-IX. Офіційний вісник України. 2021. 62. С. 201. URL: https://zakon.rada.gov.ua/laws /show/1702-20#Text (дата звернення : 06.02.2023)

16. Про критичну інфраструктуру. Закон України від 16.11.2021 р. 1882-IX. Офіційний вісник України. 2021. 98. С. 23. URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення : 06.02.2023).

17. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього. Постанова Кабінету Міністрів України від 28.04.2023 № 415.

18. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави.

Державне управління: удосконалення та розвиток. 2022. № 1. URL: http://www.dy.nayka.com.ua.

19. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матер. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С.І. Конд ратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2015. 176 с.

20. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83-93.

21. Мельник М. Я., Рудик Ю. І. Опис моделювання сходження селевого потоку за рельєфом цифрової картографічної основи. *Інформаційна безпека та інформаційні технології*: Збірник тез доповідей VI Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів, Львів, 30 листоп. 2023 р. Львів: ЛДУ БЖД, 2023. С. 350-352.

22. Хоменко М. І. До питання пожежної безпеки об'єктів критичної інфраструктури в умовах воєнного часу. Проблеми пожежної безпеки 2022 (Fire Safety Issues 2022) : матеріали Міжнар. наук.-практ. конф. Харків.: НУЦЗ України, 2022. С. 50-52

23. Department of Homeland Security (2013), Presidential Policy Directive. Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov.

24. Rudyk Y., Bubela T., & Maciuk K. (2023). Russia-Ukraine war: transport and logistics support for grain supply chain in regional food safety. Scientific Journal of Silesian University of Technology.Series Transport, 119, 223-233. doi:10.20858/sjsutst. 2023.119.13

25. Скороход Я. Аналіз проблемних питань захисту критичної інфраструктури держави. *Наука про цивільний захист як шлях становлення молодих вчених*. Харків, 2018.

26 Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

27. Тарасюк О., Павлюк Ю., Бабаджанова, О. (2023). Безпека функціонування об'єктів критичної інфраструктури. матеріали Всеукр. наук.-практ. конф. курсантів, студентів, ад'юнктів (аспірантів) 12 травня 2023 року. ЧІПБ, Черкаси.

28 Menshykova O., Rak T., Rudyk Y. Expanding of Compliance Assessment for Preventive Measures of Fire Safety as a Local Facilities with High Risk Level in Ukraine Przedsiębiorczość I Zarządzanie Tom XIX, Zeszyt 1, Część 3, ss. 181–194 Wydawnictwo SAN 2018.

29. Теленик С. С. Досвід правового регулювання системи захисту критичної інфраструктури в США. Науковий вісник НАВС. 2018. № 2 (107). С. 358-370.

References:

1. Ivaniuta, S. P. (2018). Priorities of Formation of the Register of Critical Infrastructure Objects and the Procedure for Their Accounting. *Strategic priorities: scientific and analytical quarterly collection № 3-4 (48)* National Institute for Strategic Studies. Kyiv : NISS Publishing House. 26-35 [in Ukrainian].

2. Some issues of critical infrastructure facilities. Resolution of the Cabinet of Ministers of Ukraine; Procedure, List, Methodology of 09.10.2020 No. 1109 [in Ukrainian].

3. Administration of the State Service for Special Communications and Information Protection of Ukraine. Order No. 23 of January 15, 2021 On Approval of Methodological Recommendations for Categorization of Critical Infrastructure Objects (as amended) [in Ukrainian].

4. Law of Ukraine On Insurance. 2019. 1909-IX, current. Edition of 19.04.2024 [in Ukrainian].

5. On Amendments to Certain Legislative Acts of Ukraine on Clarifying the Powers of Civil Protection Entities and Implementation of International Humanitarian Law in the Field of Civil Protection. Law of Ukraine, No. 2394-IX, entered into force on August 3. 2022 [in Ukrainian].

6. On Amendments to Certain Legislative Acts of Ukraine to Clarify the Powers of Civil Protection Actors, Improve Legislation on [...] Law of Ukraine of 08.11.2023, No. 3441-IX [in Ukrainian].

7. Shvedov, V., Rudyk, Y., Kuts, V. (2023). Taking into account the military risks of losses in the quality of power supply to critical infrastructure facilities. Quality management in education and industry: experience, problems and prospects: abstracts of the VI International Scientific and Practical Conference, November 16-17, 2023. Access mode: https://science.lpnu.ua/qm-2023/proceedings (in Ukrainian); https://science.lpnu.ua/uk/qm-2023/tezy-dopovidey (in English), pp. 296-298.

8. Pavuk, I.V., Kobylkin, D.S. (2023). Features of the formation of the concept of project risk management at critical infrastructure facilities. Innovating modern trends in security management: abstracts of the All-Ukrainian scientific and practical conference (Lviv, May 26, 2023). Lviv: Astroprint, C. 47-49 [in Ukrainian].

9. Zachko, O.B. (2014). Security management of complex infrastructure projects in the civil protection system. Project management: state and prospects: materials. 10 International scientific and practical conference - Mykolaiv: NUK . 91-92 [in Ukrainian].

10. Kobylkin, D. S. (2016). Anti-crisis project management for the protection of critical infrastructure facilities Project management: state and

prospects: materials. XII International Scientific and Practical Conference Mykolaiv: MNUK, 75-76 [in Ukrainian].

11. Rudyk, Y., Starodub, A., Kuts, V., Karpenko, V., Zdeb V. (2023). Comparative assessment of renewable sources for critical facilities of decentralized supply. *ISTCMTM.* 84(4) 10-16. https://doi.org/10.23939/istcmtm2023.04.010.

12. On the legal regime of martial law: Law of Ukraine of 12.05.2015 389-VIII Official Gazette of Ukraine. 2015. 98. [in Ukrainian]. URL: https://zakon.rada.gov.ua/laws/ show/389-19#Text (accessed on January 09, 2023).

13. On the Legal Regime of the State of Emergency. Law of Ukraine of 16.03.2000, 1550-III. Official Gazette of Ukraine [in Ukrainian]. URL https://zakon.rada.gov.ua/laws/show/1550-14 (accessed on January 10, 2023).

14. On the Functioning of the Unified Transport System of Ukraine in a Special Period: Law of Ukraine of 20.10.1998, 194-XIV. Official Gazette of Ukraine. 1998. [in Ukrainian]. URL : https://zakon.rada.gov.ua/laws/show/194-14#Text (accessed on January 11, 2023).

15. On the basis of national resistance: Law of Ukraine dated 16.07.2021, 1702-IX. Official Gazette of Ukraine. 2021. 62 [in Ukrainian]. 201. URL: https://zakon.rada.gov.ua/laws /show/1702-20#Text (accessed 06.02.2023).

16. On critical infrastructure. Law of Ukraine of 16.11.2021, 1882-IX. Official Gazette of Ukraine. 2021. 98. C. 23 [in Ukrainian]. URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed February 06, 2023).

17. On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Objects, Inclusion of Such Objects in the Register, Access and Provision of Information from it. Resolution of the Cabinet of Ministers of Ukraine of 28.04.2023. No. 415 [in Ukrainian].

18. Yaremenko, O.I., Strakhnytskyi, Y. A. (2022). Theoretical and methodological foundations of ensuring the system of protection of the critical infrastructure of the state. Public administration: improvement and development. N1. [in Ukrainian] URL: http://www.dy.nayka.com.ua.

19. Green Book on the Protection of Critical Infrastructure in Ukraine: a collection of materials of international expert meetings / ed. D.S. Biriukov, S.I. Kondratov; edited by O.M. Sukhodola. Kyiv: NISS, 2015. 176 [in Ukrainian].

20. Bobro, D.G. (2015). Determination of criteria for assessing and threats to critical infrastructure. Strategic priorities. Series: Economics. № 4. C. 83-93 [in Ukrainian].

21. Melnyk, M.Y., Rudyk, Y.I. (2023). Description of modeling of mudflow descent on the relief of a digital mapping base. *Information security and information technology*: Collection of abstracts of the VI All-Ukrainian scientific and practical conference of young scientists, students and cadets, Lviv, November 30. 2023 Lviv, 350-352 [in Ukrainian].

22. Khomenko, M. I. (2022). On the issue of fire safety of critical infrastructure facilities in wartime. Fire Safety Issues 2022: Proceedings of the International Scientific and Practical Conference, Kharkiv: NUCZ of Ukraine, 50-52 [in Ukrainian].

23. Department of Homeland Security (2013), Presidential Policy Directive. Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov.

24. Rudyk, Y., Bubela, T., & Maciuk, K. (2023). Russia-Ukraine war: transport and logistics support for grain supply chain in regional food safety. Scientific Journal of Silesian University of Technology.Series Transport, 119, 223-233 [in Ukrainian]. doi:10.20858/sjsutst.2023.119.13

25. Skorokhod, Y. (2018). Analysis of problematic issues of protection of critical infrastructure of the state. Science of civil defense as a way of formation of young scientists. Kharkiv, [in Ukrainian].

26 Yermenchuk, O.P. (2018). Main approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine: monograph. Dnipro: Dnipro State University of Internal Affairs, 180 [in Ukrainian].

27. Tarasiuk, O., Pavliuk, Y., Babadzhanova, O. (2023). Materials of the All-Ukrainian scientific and practical conference of cadets, students, adjuncts (graduate students) on May 12, 2023. ChIPB, Cherkasy [in Ukrainian].

28 Menshykova, O., Rak, T., Rudyk, Y. (2018). Expanding of Compliance Assessment for Preventive Measures of Fire Safety as a Local Facilities with High Risk Level in Ukraine Przedsiębiorczość I Zarządzanie Tom XIX, Zeszyt 1, Część 3, ss. 181-194 Wydawnictwo SAN.

29. Telenyk, S.S. (2018). Experience of legal regulation of the critical infrastructure protection system in the United States. *Scientific Bulletin of the National Academy of Internal Affairs*. № 2 (107). C. 358-370. [in Ukrainian].

Оглядова стаття.
Надійшла до редакції 31.05.2024.
Прийнято до публікації 12.06.2024.