УДК 504.064
DOI https://doi.org/10.32846/2306-9716/2025.eco.6-63.10

ЕКОЛОГІЧНА МОДЕРНІЗАЦІЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПАЛИВНО-ЕНЕРГЕТИЧНОГО СЕКТОРУ

Бойко В. М., Пронь О. В.
Державний університет «Київський авіаційний інститут»
пр. Любомира Гузара, 1, 03680, м. Київ
3998111@stud.kai.edu.ua, 8390733@stud.kai.edu.ua

У статті представлено інтегрований підхід до екологічної модернізації об'єктів критичної інфраструктури паливно-енергетичного сектору, спрямований на підвищення їхньої стійкості, енергоефективності та екологічної безпеки в умовах загострення техногенних, кліматичних і воєнних ризиків. Запропонована методика поєднує аналіз життєвого циклу, екологічний та техногенний ризик-аналіз, багатокритеріальну оцінку альтернатив модернізації, цифровий моніторинг і елементи кіберстійкості. Це дозволяє сформувати комплексну модель вибору найкращих доступних технологій з урахуванням повних витрат життєвого циклу, вартості вуглецевих викидів, потенційних збитків від інцидентів та впливу кіберзагроз на достовірність екологічної телеметрії.

Особливу увагу приділено інтеграції технічних, управлінських та цифрових рішень: впровадженню очисних і енергоефективних технологій, систем безперервного моніторингу параметрів довкілля і технологічного обладнання, застосуванню цифрових двійників для моделювання аварійних сценаріїв, а також створенню системи показників, що поєднує екологічні, технічні та кібернетичні індикатори. Практичним результатом дослідження є дорожня карта екологічної модернізації, регламент екологічного й цифрового моніторингу та уніфікована система оцінювання ефективності заходів.

Апробація методики на об'єктах паливно-енергетичної інфраструктури продемонструвала зниження екологічних ризиків, скорочення вуглецевого сліду, підвищення надійності технологічних процесів, зменшення операційних витрат і поліпшення керованості виробничих систем. Запропонований підхід має високу практичну цінність для планування модернізаційних проєктів у воєнних та післявоєнних умовах, забезпечуючи стійкий, безпечний і екологічно відповідальний розвиток паливно-енергетичного сектору. *Ключові слова:* екологічна модернізація, паливно-енергетичний сектор, критична інфраструктура, найкращі доступні технології, аналіз життєвого циклу, управління екологічними ризиками, цифровий моніторинг, кіберстійкість, енергоефективність, вуглецевий слід.

Environmental modernization of critical infrastructure facilities in the fuel and energy sector. Boiko V., Pron O.

The article presents an integrated approach to the environmental modernization of critical infrastructure facilities in the fuel and energy sector, aimed at enhancing their resilience, energy efficiency, and environmental safety under increasing technological, climate-related, and war-induced risks. The proposed methodology combines life-cycle assessment, environmental and technogenic risk analysis, multi-criteria evaluation of modernization options, digital monitoring, and elements of cyber resilience. This enables the development of a comprehensive model for selecting the best available technologies, taking into account full life-cycle costs, the economic value of carbon emissions, potential losses from incidents, and the impact of cyber threats on the reliability of environmental telemetry.

Particular attention is given to integrating technical, managerial, and digital solutions: deployment of advanced pollution-control and energy-efficient technologies, real-time environmental and process monitoring systems, the use of digital twins for simulating emergency scenarios, and the formation of a unified system of indicators combining environmental, technical, and cybersecurity metrics. The practical outcome includes a modernization roadmap, a regulatory framework for environmental and digital monitoring, and a system for evaluating the effectiveness of modernization measures.

Approbation of the methodology on fuel-energy infrastructure facilities demonstrated reduced environmental risks, a lower carbon footprint, improved reliability of technological processes, decreased operational costs, and enhanced manageability of production systems. The proposed approach shows high practical relevance for planning modernization projects in wartime and post-war recovery conditions, ensuring sustainable, safe, and environmentally responsible development of the fuel and energy sector. *Key words:* environmental modernization, fuel and energy sector, critical infrastructure, best available technologies, life-cycle assessment, environmental risk management, digital monitoring, cyber resilience, energy efficiency, carbon footprint.

Постановка проблеми. Екологічна модернізація об'єктів критичної інфраструктури паливно-енергетичного сектору постає як відповідь на комбінацію викликів – від зношеності виробничих фондів і накопичених екологічних ризиків до нових загроз безпеці, включно з кібернетичними, що впливають на надійність технологічних процесів і систем моніторингу. В українському контексті особливої ваги набуває чіткість понятійного апарату та методології ідентифікації критичної інфраструктури, адже саме

правова й управлінська визначеність створює рамку для інвестиційних рішень щодо модернізації та дає змогу вибудувати ієрархію пріоритетів: від вузлів високої аварійної небезпеки й викидів до підсистем, де першочерговий ефект очікується від цифровізації та підвищення кіберстійкості [3; 9].

Актуальність дослідження зумовлена тим, що паливно-енергетичний сектор України функціонує в умовах підвищених екологічних, технічних та кліматичних викликів. Значний ступінь фізичного зношення інфраструктури, накопичення техногенного навантаження та посилення впливів глобальних кліматичних змін потребують оновлення підходів до забезпечення екологічної безпеки та довгострокової стійкості енергетичних об'єктів.

У таких умовах екологічна модернізація критичної інфраструктури набуває стратегічного значення, оскільки передбачає впровадження сучасних технологій, систем екологічного моніторингу, енергоефективних рішень та інноваційних методів управління ризиками. Використання найкращих доступних технологій, зменшення негативного природоохоронного впливу та оптимізація ресурсоспоживання є необхідними для підвищення надійності, безпеки та конкурентоспроможності підприємств паливно-енергетичного комплексу. Отже, дослідження напрямів і механізмів екологічної модернізації є актуальним та своєчасним, адже воно спрямоване на підвищення ефективності функціонування критично важливих енергетичних об'єктів, мінімізацію екологічних ризиків та формування основ сталого розвитку галузі.

Зв'язок авторського доробку із важливими науковими та практичними завданнями. Дослідження екологічної модернізації об'єктів критичної інфраструктури паливно-енергетичного сектору безпосередньо пов'язане з актуальними завданнями підвищення стійкості та безпеки енергетичної системи України в умовах війни та післявоєнного відновлення. У роботі здійснюється акцент на уточненні методології оцінювання екологічної стійкості, інтеграції ризик-орієнтованого управління, підходів сталого розвитку та інструментів «зеленої» модернізації, що дозволяє формувати життєвий цикл рішень, орієнтований на зниження екологічних та техногенних ризиків [1; 4; 6]. Практичне значення авторського доробку проявляється у можливості застосування запропонованих критеріїв, моделей і рекомендацій органами влади, операторами критичної інфраструктури та енергетичними компаніями для планування інвестицій, удосконалення моніторингу та зменшення вразливості стратегічно важливих об'єктів [2; 7]. Це безпосередньо відповідає державним пріоритетам підвищення екологічної, технологічної та кібернетичної стійкості сектору.

Аналіз останніх досліджень і публікацій. Проблематика розвитку, класифікації та захисту критичної інфраструктури активно висвітлюється у сучасних наукових працях. Зокрема, у дослідженнях Т. Болвановської розглянуто підходи до системного аналізу критичних об'єктів та їхніх функцій у структурі національної інфраструктури [1], тоді як І. Ботнаренко уточнює понятійно-правові засади та законодавче визначення критичної інфраструктури в Україні [3]. Ю. Борсук досліджує функціонування об'єктів західного регіону в умовах війни, зокрема просторові та логістичні аспекти вразливості [2]. Значну увагу приділено кібербезпеці: О. Корченко пропонує методи оцінювання рівня кіберзахисту об'єктів критичної інфраструктури [4], Н. Трушкіна аналізує розвиток критичної інформаційної інфраструктури [8], а В. Шиповський систематизує показники кіберстійкості інформаційних систем [10]. Важливі економічні й макросистемні аспекти взаємодії інфраструктурних елементів розглядає В. Кулик у моделях міжгалузевого розвитку в умовах війни та відновлення [5].

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на наявність значної кількості досліджень, низка аспектів залишається недостатньо опрацьованою. Зокрема, питання екологічної модернізації паливно-енергетичних об'єктів розглядається фрагментарно, а інтеграція екологічних, техногенних та кібернетичних ризиків у єдину модель управління досі не сформована належним чином [4; 6; 10]. Бракує системних підходів, які враховують просторову диференціацію екологічних ризиків у воєнний час, взаємозалежність інфраструктурних елементів, а також вплив кіберзагроз на достовірність екологічного моніторингу [2; 5]. Практично відсутні комплексні методики, що поєднують життєвий цикл технологічних рішень, аналіз екологічних наслідків, багатокритеріальну оцінку інвестицій та цифрову підтримку процесів управління. Саме на вирішення цих науково-практичних прогалин і спрямована дана стаття.

Новизна роботи. Новизна полягає в узагальненні та уточненні підходів до екологічної модернізації об'єктів критичної інфраструктури паливно-енергетичного сектору з урахуванням воєнних ризиків. Запропоновано акценти на оцінюванні екологічної стійкості, управлінні екологічними ризиками та інтеграції «зелених» технологій у систему управління такими об'єктами.

Методологічне та загальнонаукове значення. Робота ґрунтується на системному, ризик-орієнтованому та міждисциплінарному підходах до аналізу критичної інфраструктури. Її результати поглиблюють теоретичні засади екологічної модернізації та можуть бути використані як методична база для подальших досліджень у сфері екобезпеки та стійкості паливно-енергетичних систем.

Виклад основного матеріалу. Екологічна модернізація об'єктів критичної інфраструктури паливно-енергетичного сектору потребує ґрунтовного аналізу умов, у яких функціонують такі об'єкти, а також чинників, що впливають на їхню екологічну та техногенну

безпеку. Оскільки ці об'єкти мають стратегічне значення для енергетичної стабільності держави, важливо враховувати комплекс ризиків, що виникають у процесі експлуатації, технічного обслуговування та взаємодії з навколишнім середовищем. Саме виявлення й систематизація таких ризиків є відправною точкою для формування ефективних рішень з модернізації.

Для забезпечення ефективної екологічної модернізації об'єктів критичної інфраструктури паливно-енергетичного сектору необхідно враховувати комплекс зовнішніх і внутрішніх факторів, що формують ризики та перешкоди для впровадження сучасних природоохоронних технологій. У процесі аналізу встановлено, що виклики мають багатовимірний характер і охоплюють техногенні, екологічні, організаційні, кібернетичні, воєнно-географічні та фінансові аспекти. Узагальнені групи цих викликів та їх ключові прояви подано в таблиці 1.

Концептуальна рамка екологічної модернізації для об'єктів паливно-енергетичного сектору повинна поєднувати оцінювання впливів на довкілля за підходом життєвого циклу, аналіз технологічних та організаційних ризиків, багатокритеріальну пріоритизацію інвестицій, а також цифрові компоненти, що забезпечують безперервний моніторинг і керування в режимі, наближеному до реального часу. На рівні технічних рішень базовим є перехід до найкращих доступних технологій, що зменшують викиди летких органічних сполук під час зберігання та перекачування пального, мінімізують ризики витоків завдяки подвійним стінкам резервуарів і вторинним контейнментним бар'єрам, скорочують водоспоживання та навантаження на очисні споруди за рахунок замкнених контурів водовикористання, а також інтегрують відновлювані джерела енергії і високоефективні приводи для технологічного обладнання.

Таблиця 1

Основні виклики для екологічної модернізації об'єктів критичної інфраструктури ПЕС

№	Група викликів	Зміст / прояви
1	Техногенні	Зношеність обладнання, високий ризик аварій, витоки нафтопродуктів, значні обсяги викидів
2	Екологічні	Накопичені забруднення ґрунтів і вод, значні викиди ЛОС, водоспоживання та відходи
3	Організаційні	Недостатня стандартизація процедур, слабкий внутрішній аудит, низька культура екологічної безпеки
4	Кібернетичні	Вразливість систем моніторингу, ризик компрометації телеметрії, загрози керуючим системам
5	Воєнно-географічні	Руйнування логістики, підвищена небезпека зберігання пального, регіональна диференціація ризиків
6	Фінансові	Обмеженість інвестиційних ресурсів, висока капіталомісткість модернізації

Однак технічна модернізація матиме стійкий ефект лише за умови зміни управлінської логіки: ключовим стає введення прозорих екологічних показників у систему виробничого контролінгу, ув'язування їх з операційними та фінансовими індикаторами, а також інституціалізація механізмів внутрішнього аудиту, інспекцій і навчання персоналу щодо екологічної безпеки. Важливим елементом є цифрова підтримка – впровадження систем збору даних з датчиків рівня, тиску, температури, концентрацій парів і якості стоків, використання цифрових двійників резервуарних парків та насосних станцій для симуляції сценаріїв «що-якщо», а також застосування аналітики для раннього виявлення відхилень у поведінці об'єктів, що може свідчити про зародження інциденту або про кібервтручання [4; 6; 8; 10].

Власне, взаємопов'язаність екологічної безпеки та кіберстійкості стає очевидною: коректність екологічної звітності та своєчасність реакції на витік залежить від достовірності телеметрії та безперервності роботи інформаційно-керуючих систем, тому методики оцінювання рівня підвищення кіберзахисту і системи показників кіберстійкості потрібно включати до проєктів екологічної модернізації як обов'язковий компонент, що захищає сам інструмент моніторингу від компрометації [4; 10].

З погляду макро- та мезорівневого планування, екологічна модернізація критичної інфраструктури паливно-енергетичного сектору має узгоджуватися зі сценаріями відновлення та трансформації економіки, у яких паливна логістика, електро- і теплоенергетика, а також нафтогазова інфраструктура формують взаємозалежну мережу. Моделі міжгалузевої взаємодії дозволяють оцінити непрямі ефекти екологічних інвестицій – від підвищення енергоефективності технологічних процесів до зменшення втрат у транспорті та зберіганні, що відгукується на вартісних параметрах у суміжних галузях і регіонах; ці моделі є підставою для вибору черговості модернізаційних проєктів і визначення «вузьких місць», де кожна гривня екологічної інвестиції приносить максимальний системний ефект [5].

У воєнних умовах і на етапі післявоєнного відновлення сценарний підхід допомагає поєднати екологічні цілі з вимогами стійкості постачань, безпеки розміщення складів пального та диверсифікації транспортних маршрутів, що зменшує ризики техногенних і екологічних інцидентів у разі порушення роботи окремих ланок [2; 5; 7].

З огляду на те, що інформаційні системи об'єктів критичної інфраструктури є одночасно операційним ресурсом і джерелом ризику, державний аудит кіберзахисту, стандарти перевірок і стратегічні орієнтири підвищення кіберстійкості мають бути інтегровані

до екологічних програм модернізації, аби забезпечити цілісність даних і здатність організацій адаптуватися до змін загрозового середовища [6; 8].

Практична реалізація екологічної модернізації потребує узгодженого алгоритму, що починається з багатошарового екологічного аудиту: інвентаризації джерел викидів і потенційних витоків, аналізу водокористування та утворення відходів, оцінки стану ґрунтів і підземних вод у зонах можливого забруднення, перевірки технічного стану резервуарів, трубопроводів та арматури, а також ревізії процедур технічного обслуговування.

Наступний шар – ризик-орієнтована діагностика з виділенням сценаріїв, що мають найбільшу ймовірність і тяжкість наслідків, із використанням статистичних даних, експертних оцінок і результатів моделювання. На цій основі формується портфель заходів: від негайних низьковитратних дій до капіталомістких інвестицій. Паралельно має бути розгорнута цифрова інфраструктура збору, зберігання та аналізу даних, включно з мережевою сегментацією, контролем доступу, журналюванням подій і засобами аномалієвого виявлення, що підсилює довіру до екологічних показників і створює основу для автоматизованого реагування на інциденти [4; 6; 10].

Важливим практичним кроком є інтеграція екологічних і кібернетичних регламентів у єдині процедури підприємства: навчання персоналу має одночасно охоплювати дії при розгерметизації та протидію соціальній інженерії, а внутрішні аудити – перевіряти як справність запірної арматури й стан бонових загороджень, так і налаштування резервного копіювання й контроль цілісності конфігурацій технологічних контролерів [7; 8; 10].

Щоб екологічна модернізація не зводилася до разової кампанії, потрібна система вимірюваних показників, вмонтована у регулярний цикл планування та звітності. До ключових індикаторів доцільно віднести інтенсивність викидів за категоріями забруднювачів, питомі витрати енергії та води, частку рекуперованих парів, частоту та масштаб інцидентів, час виявлення й усунення витоків, обсяг утилізації небезпечних відходів, а також інтегральні показники стійкості, що враховують здатність системи відновлюватися після збоїв і інцидентів.

Водночас для інформаційних систем, які підтримують моніторинг і керування технологічними процесами, має бути визначено набір показників кіберстійкості: середній час відновлення, частота критичних вразливостей у периметрі, частка систем із актуальними оновленнями, рівень сегментації мережі, інтенсивність реєстрації аномальних подій, наявність і тестованість планів реагування; обґрунтування такої системи показників представлене в спеціалізованих дослідженнях і може бути адаптоване до паливно-енергетичного профілю [10].

На рівні державної політики методичні підходи до оцінювання рівня підвищення кіберзахисту мають бути узгоджені з екологічними стандартами звітності, що дозволяє одномоментно оцінювати прогрес за двома взаємозалежними осями – екологічною та кібернетичною – і коригувати пріоритети у фінансуванні [4; 6].

Враховуючи регіональний вимір функціонування критичної інфраструктури, корисно запроваджувати просторову аналітику, яка відображає екологічні навантаження та ризики в розрізі громад і агломерацій, що допомагає визначати локації для резервування потужностей, оптимізації логістики та розміщення екологічних постів спостереження [2].

Інституційна спроможність відіграє не меншу роль, ніж технології. Організація безпеки та захисту об'єктів критичної інфраструктури має включати чіткий розподіл відповідальності, регулярні тренування, взаємодію з місцевими службами, механізми публічного інформування й участі громад у нагляді за екологічними показниками, а також незалежні аудити, що перевіряють не лише формальну відповідність, а й фактичну ефективність процедур реагування [7].

Державний аудит і нагляд у сфері кіберзахисту мають синхронізуватися з екологічними перевірками, аби уникнути ситуації, коли окремі підсистеми модернізуються розрізнено й створюють «ефект ковдри», що не покриває всі критичні ризики [6; 8].

Вдосконалення правового поля і методичних документів щодо критичної інфраструктури, зокрема запровадження уніфікованих критеріїв важливості, прозорих процедур ідентифікації, категоризації та обов'язків власників і операторів, створює передумови для масштабування екологічної модернізації та стабільного фінансування з боку держави, міжнародних партнерів і приватних інвесторів [3; 9].

Науково-методичні результати, накопичені українськими дослідниками з питань структури критичної інфраструктури, регіональних особливостей її функціонування та підходів до оцінювання стійкості, формують базу знань, яку можна безпосередньо використовувати при проектуванні модернізаційних програм для паливно-енергетичних об'єктів [1; 2; 5; 9].

Зрештою, екологічна модернізація в паливно-енергетичному секторі – це не лише про захист довкілля, а й про операційну надійність, конкурентоспроможність і соціальну ліцензію на діяльність. Поєднання технічних рішень із управлінськими реформами та цифровими інструментами, підкріплене правовою визначеністю і належним контролем, дозволяє одночасно знизити ймовірність та наслідки інцидентів, скоротити вуглецевий слід і витрати життєвого циклу, підвищити прозорість і довіру з боку суспільства. Український досвід останніх років демонструє, що інфраструктурні системи мають бути стійкими не лише до природних і техногенних факторів, але й до кіберзагроз і воєнних ризиків; тому екологічна модернізація має спиратися на міждисциплінарні методики, які інтегрують просторовий, економічний, екологічний і кібернетичний

Таблиця 2

Етапи екологічної модернізації об'єктів ПЕС

Етап	Зміст робіт	Результат
1. Екологічний аудит	Інвентаризація джерел викидів, витоків, водокористування	Карта екологічних проблем
2. Ризик-діагностика	Ідентифікація сценаріїв аварій та витоків	Пріоритети антикризових заходів
3. Технічний аналіз	Оцінка стану обладнання, трубопроводів, резервуарів	Визначення обсягів модернізації
4. Вибір технологій	MCDA, LCA, оцінка витрат циклу	Найкращі доступні технології
5. Цифровізація	IoT, SCADA, аналітика, кіберзахист	Раннє виявлення відхилень
6. Впровадження	Будівельно-монтажні роботи, навчання	Запуск оновлених систем
7. Моніторинг і аудит	Оцінка KPIs, екологічні й кіберперевірки	Підтримка ефекту модернізації

аналіз, а також на сценарне планування, що враховує невизначеність майбутнього [2; 5; 6; 8; 10].

Саме така інтегральна логіка – від чіткої ідентифікації об'єктів критичної інфраструктури й належної організації їх захисту до впровадження найкращих доступних технологій і цифрових систем моніторингу – створює умови для стійкого, безпечного та екологічно відповідального розвитку паливно-енергетичного сектору в Україні [1; 3; 7; 9; 10].

Головні висновки. Екологічна модернізація паливно-енергетичної критичної інфраструктури має бути інтегрованою: правова ідентифікація об'єктів і пріоритезація інвестицій, впровадження найкращих доступних технологій, а також безперервний цифровий моніторинг із захистом даних, що забезпечує раннє виявлення відхилень і керованість процесів. Ефективність вимірюється системою показників: інтенсивність викидів, питомі витрати енергії та води, частка рекуперації, частота інцидентів і час реагування, узгоджених із повними витратами життєвого циклу.

На рівні політики та просторового планування заходи мають узгоджуватися зі сценаріями міжгалузевої взаємодії та умовами воєнних ризиків і відновлення, аби підсилити системний ефект інвестицій і стійкість ланцюгів постачання. Поєднання екологічних і кібернетичних стандартів контролю та аудиту гарантує достовірність телеметрії, прозорість звітності й зниження екологічних та операційних ризиків, формуючи конкурентоспроможний і безпечний розвиток сектору.

Література

1. Болвановська Т. В. Аналіз об'єктів критичної інфраструктури. Дніпровський національний університет залізничного транспорту. *Збірник наукових праць ДНУЗТ ім. акад. В. Лазаряна. Вип. 16*. 2018. С. 151–152.
2. Борсук Ю. Критична інфраструктура західного регіону україни в умовах війни: суспільно-географічне дослідження. *XXIV-а Всеукраїнська студентсько-аспірантська наукова конференція «Реалії, проблеми та перспективи розвитку географії, екології, туризму та сфери»*. 2023. С. 52. URL:https://geography.lnu.edu.ua/wpcontent/uploads/2023/10/Zbirnyk_studkonf_2023.pdf#page=52 (дата звернення: 20.11.2025).
3. Ботнаренко І. А. Критична інфраструктура в україні та її складові: поняття, зміст та законодавче визначення. *Юридичний науковий електронний журнал*. 2024. С. 17.
4. Корченко О. Метод оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури держави. *Вісн. НАН України*. 2024. 61.1. С. 3–20. 14.
5. Кулик В. В. Моделювання міжгалузевої економіки як критичної інфраструктури: розроблення сценаріїв розвитку економіки україни в умовах війни та післявоєнного відновлення. *Кібернетика та системний аналіз*. 2023. Т. 59, № 6. С. 116–136. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001442971 (дата звернення: 20.11.2025).
6. Кучма О. Критична інфраструктура та кіберзагрози: досягнення стратегічних цілей державного аудиту щодо кіберзахисту критичної інфраструктури. *Наукові перспективи*. 2023. 10 (40). URL: https://perspectives.pp.ua/index.php/np/article/view/7060 (дата звернення: 20.11.2025).
7. Пригунов П. Я., Мельник С. І., Франчук В. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії*. 2021. Вип. 3 (13). С. 142–148.
8. Трушкіна Н. В. Розвиток критичної інформаційної інфраструктури з позицій кібербезпеки: теоретичні аспекти. *Українська інженерно-педагогічна академія*. 2023. 5. С. 206. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22200/1/32-38.pdf (дата звернення: 20.11.2025).
9. Трушкіна, НВ. Сутність методології ідентифікації об'єктів критичної інфраструктури: досвід франції та великобританії. *Збірник тез доповідей VМіжнародної науково-практичної конференції (м. Мукачево, 11–12 квітня 2023 р.).* Мукачево: МДУ, 2023 С. 46. URL: https://dntb.gov.ua/wp-content/ (дата звернення: 20.11.2025).
10. Шиповський В. Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури. *Ukrainian Information Security Research Journal*. 2023. 25.1. С. 37–45.

Дата першого надходження рукопису до видання: 26.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 31.12.2025