Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2026. № 3.
ISSN 2307-2105

DOI: http://doi.org/10.32702/2307-2105.2026.3.43
УДК 338.2:351.86:004.056

М. М. Медвідь,
д. е. н., професор, заступник начальника Київського інституту Національної гвардії України з навчально-методичної роботи,
Київський інститут Національної гвардії України
ORCID ID: https://orcid.org/0000-0002-4506-8020
Ю. І. Медвідь,
к. пед. н., ст. досл. провідний науковий співробітник відділу організації наукової діяльності та інновацій,
Київський інститут Національної гвардії України
ORCID ID: https://orcid.org/0000-0001-9520-787X
Л. М. Сокол,
к. е. н., заступниця голови з управління земельними ресурсами,
СФГ «Сокіл»,
ORCID ID: https://orcid.org/0000-0002-0189-6334
Р. В. Суслов,
викладач кафедри тактики факультету службово-бойової діяльності,
Київський інститут Національної гвардії України
ORCID ID: https://orcid.org/0009-0006-6437-197X

СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ЧИННИК ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ: РИЗИКИ, РЕГУЛЮВАННЯ ТА КАДРОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ

M. Medvid,
Doctor of Economic Sciences, Professor, Deputy Head of Kyiv Institute of the National Guard of Ukraine for Academic and Methodological Work, Kyiv Institute of the National Guard of Ukraine
Yu. Medvid,
PhD in Pedagogical Sciences, Senior Researcher, Leading Research Fellow of the Department for Organization of Scientific Activity and Innovation, Kyiv Institute of the National Guard of Ukraine
L. Sokol,
PhD in Economics, Deputy Head for Land Resources Management, Farm Enterprise «Sokil»
R. Suslov,
Lecturer, Department of Tactics, Faculty of Service and Combat Activity, Kyiv Institute of the National Guard of Ukraine

RESILIENCE OF CRITICAL INFRASTRUCTURE AS A FACTOR OF STATE ECONOMIC SECURITY: RISKS, REGULATION, AND PERSONNEL SUPPORT MECHANISMS

У статті обґрунтовано роль стійкості критичної інфраструктури як системоутворюючого чинника економічної безпеки держави в умовах зростання багатовекторних ризиків та інфраструктурної вразливості. Доведено, що порушення функціонування енергетичних, транспортних, інформаційно-комунікаційних, фінансових і логістичних систем формує каскадні негативні ефекти для макроекономічної стабільності, виробничої безперервності та інвестиційної привабливості. Узагальнено наукові підходи до трактування стійкості критичної інфраструктури та систематизовано основні групи ризиків – фізичні, техногенні, кібернетичні, організаційні, воєнні та гібридні – з визначенням каналів їх впливу на економічні показники. Розроблено модель інтеграції індикаторів стійкості критичної

інфраструктури до системи показників економічної безпеки держави. Обґрунтовано включення коефіцієнта кадрової спроможності та результативності підготовки персоналу як коригуючого чинника зниження інфраструктурних ризиків. Запропоновано концептуальну модель забезпечення інфраструктурної стійкості, що поєднує ризик-орієнтоване регулювання, аналітичний індикаторний інструментарій та кадрові механізми. Практичне значення результатів полягає у можливості використання запропонованих підходів у системі державного регулювання економічної безпеки та плануванні розвитку кадрових спроможностей сектору безпеки і оборони.

The resilience of critical infrastructure is increasingly recognized as a key determinant of the economic security of the state, especially under conditions of growing geopolitical instability, technological risks, and hybrid threats. Modern economies depend on the stable functioning of infrastructure sectors such as energy, transport, financial systems, logistics, and information and communication networks. Disruptions in these systems can cause cascading effects that lead to production interruptions, supply chain failures, financial instability, and reduced investment attractiveness. Therefore, the resilience of critical infrastructure should be considered a systemic component of national economic security rather than only a sectoral or technical issue.

The purpose of this study is to substantiate the role of critical infrastructure resilience as a system-forming factor of economic security and to develop an integrated approach to its assessment based on risk-oriented regulation, indicator analysis, and personnel capacity mechanisms. The research is based on the synthesis of economic security theory, risk management principles, and approaches to infrastructure resilience within the framework of state regulation.

The study proposes an analytical model for assessing the resilience of critical infrastructure through a system of indicators reflecting major groups of risks, including physical, technological, cyber, organizational, military, and hybrid

threats. The methodology involves the normalization of indicators, their weighting according to relative significance, and the calculation of an integrated infrastructure risk index. In addition, the model incorporates a personnel capacity coefficient reflecting the availability of trained specialists capable of applying protection technologies and response mechanisms, including electronic warfare and technical protection tools.

The results demonstrate that the growth of qualified personnel capable of protecting infrastructure facilities significantly reduces the integrated infrastructure risk index and increases the macroeconomic resilience of the state. The relationship between infrastructure disruptions and economic stability is described through a macroeconomic resilience index reflecting the sensitivity of economic processes to infrastructure failures.

The study concludes that integrating infrastructure resilience indicators into the system of economic security assessment enhances the analytical capacity of strategic planning and state regulation. Personnel training and the development of professional competencies in the protection of critical infrastructure should therefore be considered an important investment factor in strengthening national economic security and ensuring the sustainable functioning of economic systems.

Ключові слова: *критична інфраструктура, економічна безпека держави, інфраструктурна стійкість, ризики, державне регулювання, індикатори, кадрові механізми, спроможність.*

Keywords: *critical infrastructure, economic security, resilience, risks, public regulation, indicators, personnel mechanisms, capacity.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Економічна безпека держави у сучасних умовах формується не лише під впливом фінансово-економічних чинників, а й від стійкості функціонування критичної інфраструктури, яка включає енергетичні, транспортні, інформаційно-

комунікаційні, фінансові та логістичні системи життєзабезпечення. Порушення роботи таких систем призводить до каскадних ефектів, що проявляються у зниженні виробничої активності, розриві ланцюгів постачання, зростанні бюджетного навантаження, втраті інвестиційної привабливості та погіршенні соціально-економічної стабільності. У масштабі держави питання стійкості критичної інфраструктури виходить за рамки окремих галузей і набуває стратегічного значення для формування ефективної економічної політики.

Суперечність полягає у тому, що існуючі методики оцінювання економічної безпеки здебільшого базуються на макрофінансових, виробничих, інвестиційних та соціальних показниках, тоді як інфраструктурний компонент розглядається фрагментарно. Відсутність формалізованих порогових значень, узгоджених індикаторів ризику та моделей впливу інфраструктурних порушень на економічні результати знижує аналітичну придатність наявних методик і ускладнює прийняття обґрунтованих управлінських рішень, особливо в умовах підвищеної турбулентності та багатовекторних загроз.

Практична складова проблеми пов’язана з необхідністю вдосконалення державного регулювання у сфері захисту критичної інфраструктури, розвитку системи моніторингу ризиків та формування кадрових спроможностей сил безпеки і оборони для запобігання, протидії та швидкого відновлення функціонування критичних об’єктів. Зокрема, виникає потреба у спеціалізованій підготовці командного складу та використанні сучасних технологічних засобів протидії загрозам, що безпосередньо впливає на рівень інфраструктурної та економічної стійкості держави.

Аналіз останніх досліджень і публікацій. Проблематика стійкості критичної інфраструктури як складової національної та економічної безпеки останніми роками набула системного висвітлення у вітчизняних наукових дослідженнях, що охоплюють концептуально-теоретичні, правові, управлінські, кібербезпекові, техніко-захисні та кадрові аспекти.

Теоретико-методологічні засади розуміння критичної інфраструктури та її місця в архітектурі безпеки держави розкрито у працях М. Кизима,

В. Хаустової, Н. Трушкіної, де обґрунтовано сутність поняття «критична інфраструктура» з позицій національної безпеки, визначено її системні ознаки, функціональні критерії та міжсекторальні зв'язки [9]. Економіко-безпековий вимір критичної інфраструктури та її вплив на стійкість держави й економічних процесів комплексно проаналізовано у дослідженнях О. Барановського та Д. Затонацького, які розглядають критичну інфраструктуру як структуроутворюючий елемент економічної безпеки та фактор макроекономічної стабільності [4; 8].

Нормативно-правові та інституційні засади функціонування системи захисту критичної інфраструктури розкрито в роботах А. Ковальчука, К. Шевченка, В. Крикуна, де досліджено механізми державного регулювання, форми та методи захисту об'єктів критичної інфраструктури, а також напрями удосконалення правового забезпечення в умовах воєнних та гібридних загроз [10; 11; 21]. Базові положення правового режиму та організації національної системи захисту критичної інфраструктури закріплено у профільному законодавстві України [14].

Окремий напрям становлять дослідження кіберстійкості та захисту інформаційної складової критичної інфраструктури. У працях С. Демедюка та В. Василенка розглянуто питання розбудови національної кіберстійкості, ролі правоохоронних органів та сектору безпеки у протидії кіберзагрозам в умовах цифровізації [5; 6]. Порівняльний та інституційний аналіз зарубіжних моделей кіберзахисту критичної інфраструктури подано у роботі Г. Санжарової, О. Сіренка, В. Санжарова, де узагальнено технічні, правові та організаційні новації європейських підходів [15].

Суттєвий масив досліджень присвячено ризикоорієнтованим і техніко-методичним підходам до оцінювання та підвищення захищеності об'єктів критичної інфраструктури. У роботах С. Чумаченка, О. Кутового, О. Гуйди, В. Попеля, Н. Заїки, Р. Мурасова розроблено методичні підходи до інтегрального оцінювання рівня безпеки об'єктів енергетичної та іншої інфраструктури, зокрема з урахуванням загроз повітряного нападу та безпілотних систем [18–20]. Технічні рішення щодо захисту телекомунікаційної складової інфраструктури, зокрема мереж 5G,

запропоновано у дослідженні С. Цяпи [17]. Зазначені праці формують інструментальну базу оцінювання ризиків і ефективності захисних систем.

Важливим напрямом є дослідження ролі сектору безпеки і оборони у забезпеченні стійкості критичної інфраструктури та економічної безпеки. У попередніх наших дослідженнях проаналізовано трансформацію ролі Національної гвардії України (НГУ) у системі державного регулювання національної та економічної безпеки [12], що безпосередньо пов'язано із завданнями захисту критичних об'єктів. Також висвітлено питання професійної підготовки персоналу сектору безпеки, зокрема майбутніх офіцерів, та ефективності організаційно-педагогічних умов формування спеціальних компетентностей, зокрема застосування засобів радіоелектронної боротьби (РЕБ) [13].

Окремий кластер становлять наукові праці, присвячені кадровим механізмам забезпечення стійкості критичної інфраструктури. У серії робіт Л. Арсенович та О. Суходолі обґрунтовано принципи, завдання, класифікацію та організаційні моделі підготовки фахівців для національної системи захисту критичної інфраструктури, визначено компетентнісні профілі, напрями розвитку професійної майстерності та зміст освітніх програм [1–3; 16]. Доповнює цей напрям дослідження В. Євсєєва щодо інструментів інформальної освіти у сфері захисту критичної інфраструктури [7].

Водночас, попри наявність значного наукового доробку, у дослідженнях переважає або правовий та організаційно-управлінський, або техніко-захисний, або освітньо-кадровий вимір проблеми. Недостатньо інтегрованими залишаються підходи, що поєднують оцінювання стійкості критичної інфраструктури з параметрами економічної безпеки держави, ризик-орієнтованим регулюванням та системними кадровими механізмами забезпечення. Це зумовлює необхідність комплексного міждисциплінарного аналізу, що і визначає напрям даного дослідження.

Формулювання цілей статті (постановка завдання). Метою статті є наукове обґрунтування ролі стійкості критичної інфраструктури як системоутворюючого чинника економічної безпеки держави та розроблення комплексного підходу до її оцінювання і забезпечення на основі поєднання

ризик-орієнтованого регулювання, індикаторного аналізу та кадрових механізмів спроможності.

Виклад основного матеріалу дослідження. Стійкість критичної інфраструктури – це інтегральна властивість систем і об'єктів життєзабезпечення держави зберігати працездатність, керованість і функціональну цілісність під впливом загроз, порушень і дестабілізуючих чинників, а також здатність до швидкого відновлення після збоїв із мінімальними соціально-економічними втратами. У науково-аналітичному та управлінському вимірі (на рівні держави, зокрема в практиці регулювання в Україні) стійкість критичної інфраструктури охоплює такі складові:

превентивна спроможність – здатність запобігати або знижувати ймовірність порушень (захищеність, резервування, диверсифікація);

поглинальна спроможність – здатність витримувати вплив загроз без втрати ключових функцій;

адаптивна спроможність – здатність перебудовувати режими роботи в умовах змін та обмежень;

відновлювальна спроможність – швидкість і повнота відновлення функціонування після ушкоджень;

кадрово-операційна спроможність – наявність підготовленого персоналу, здатного застосовувати спеціальні засоби захисту (зокрема радіоелектронної протидії), аварійного реагування та відновлення.

У прикладних дослідженнях стійкість доцільно вимірювати через систему індикаторів: рівень відмовостійкості, час простою, коефіцієнт резервування, інцидентність, відновлювальний час, кадрову укомплектованість і підготовленість. Це дозволяє безпосередньо пов'язувати параметри інфраструктурної стійкості з показниками економічної безпеки держави.

Економічна безпека держави формується під впливом як макроекономічних та фінансових чинників, так і стійкості функціонування критичної інфраструктури, що включає енергетичні, транспортні, фінансові, інформаційно-комунікаційні та логістичні системи. Порушення роботи таких об'єктів призводить до каскадних ефектів, що відображаються на ВВП, інвестиційній привабливості та соціально-економічній стабільності.

Відповідно, інтеграція індикаторів стійкості критичної інфраструктури у систему показників економічної безпеки дозволяє оцінювати реальні ризики та прогнозувати їх наслідки для державної економіки (табл. 1).

Таблиця 1. Групи ризиків для критичної інфраструктури та канали їх впливу на макроекономіку

Група ризиків	Типові джерела / події	Уражені підсистеми інфраструктури	Канали впливу на макроекономічні показники	Вплив на стійкість економічних процесів	Ключові індикатори впливу
Фізичні	природні явища, руйнування об'єктів, пошкодження мереж	енергетика, транспорт, водопостачання, логістика	переривання постачань → зупинка виробництва → падіння випуску	зниження безперервності виробничих циклів	ВВП (–), промисловий випуск (–), індекс безперервності послуг
Техногенні	аварії, відмови обладнання, зношеність фондів	енергосистеми, хімічні об'єкти, мережі зв'язку	технологічні збої → простої → зростання витрат	зниження операційної надійності галузей	коеф. простою, втрати продуктивності, операційні витрати (+)
Кібернетичні	кібератаки, зломи, блокування систем керування	IT-інфраструктура, фінансові системи, диспетчеризація	порушення керування → фінансові затримки → ринкова нестабільність	втрата керованості та прогнозованості процесів	фінансові транзакційні затримки, волатильність ринків (+)
Організаційні	помилки управління, дефіцит кадрів, слабка координація	оператори КІ, служби реагування, регуляторні ланки	неузгоджені рішення → повільне реагування → мультиплікація збитків	зниження адаптивності та швидкості відновлення	час реагування, коеф. укомплектованості, втрати від затримок
Воєнні	цілеспрямований вплив на інфраструктурні об'єкти	енергетика, транспортні вузли, зв'язок	пряме ураження → руйнування потужностей → структурні втрати	різке зниження системної стійкості	капітальні втрати, інфраструктурна доступність (–)
Гібридні	комбіновані впливи: інформаційні, кібер, економічні	багатосекторно (енерго + IT + фінанси + логістика)	каскадні ефекти → ланцюгові збої → довгий економічний шок	порушення міжгалузевих зв'язків	індекс системного ризику, міжгалузеві втрати, шоки пропозиції

Оцінювання стійкості критичної інфраструктури доцільно здійснювати за такими етапами.

На першому етапі формується система індикаторів за основними групами ризиків: фізичними, техногенними, кібернетичними, організаційними, воєнними та гібридними. Для кожної групи визначаються вимірювані показники, зокрема: частка втрати потужностей, тривалість простою, частота технічних відмов, кількість кіберінцидентів, рівень

кадрової неукомплектованості, частка уражених або недоступних об’єктів, каскадність порушень міжгалузевих зв’язків. Відібрані індикатори мають відповідати критеріям вимірюваності, порівнюваності та чутливості до змін стану систем.

На другому етапі здійснюється нормування первинних даних шляхом переведення абсолютних значень у рейтингову шкалу (наприклад, від 0 до 4 балів), де нуль відповідає відсутності негативного впливу, а максимальне значення – критичному рівню порушень. Нормування виконується за заздалегідь визначеними інтервальними шкалами для кожного індикатора, що забезпечує уніфікацію різнорозмірних показників.

На третьому етапі вводяться вагові коефіцієнти індикаторів, які відображають їх відносну значущість у формуванні загального ризиконавантаження. Ваги можуть визначатися експертним методом, методом аналізу ієрархій або статистичним калібруванням на основі ретроспективних даних. Нормована сума ваг дорівнює одиниці.

Інтегральний індекс ризиконавантаження критичної інфраструктури визначається як зважена сума рейтингових оцінок:

$$R_{CI} = \sum_{i=1}^{n} (I_i \cdot w_i) \tag{1}$$

де I_i – рейтинговий бал і-го індикатора,

w_i – його ваговий коефіцієнт.

Отримане значення інтерпретується за рівнями стійкості (висока, прийнятна, напружена, критична) та може використовуватися для міжсекторного порівняння або моніторингу в динаміці.

З метою врахування впливу підготовленості спеціалізованого персоналу, що застосовує засоби радіоелектронної боротьби та технічного захисту, до моделі вводиться коефіцієнт кадрової спроможності. Він

визначається як відношення чисельності підготовленого особового складу до нормативної потреби:

$$K_{staff} = \frac{N_{trained}}{N_{required}} \quad \text{.....} \quad \text{.....(2)}$$

де $N_{trained}$ – фактична чисельність підготовлених фахівців,

$N_{required}$ – розрахункова потреба системи.

З урахуванням ефективності підготовки вводиться коригуючий множник зниження ризику:

$$K_{corr} = \frac{1}{1 + \gamma K_{staff}} \quad (3)$$

де γ – коефіцієнт результативності підготовки та застосування персоналу.

Скоригований індекс ризику визначається як:

$$R_{adj} = R_{CI} \cdot K_{corr} \quad (4)$$

Така залежність формалізує компенсуючий ефект підготовки кадрів – зі зростанням частки підготовленого персоналу зменшується інтегральний ризик порушення функціонування об’єктів критичної інфраструктури.

Зв’язок зі стійкістю економічних процесів доцільно описувати через індекс макроекономічної стійкості:

$$S_{econ} = S_0 - \alpha R_{CI}(1 - K_{staff}) \quad (5)$$

де S_{econ} – інтегральний показник економічної стійкості,

S_0 – базовий рівень за відсутності порушень,

α – коефіцієнт чутливості макроекономічних показників до інфраструктурних збоїв (визначають експертно).

Запропонована модель дозволяє аналітично довести, що зростання чисельності підготовленого особового складу, здатного застосовувати засоби радіоелектронної боротьби та технічного захисту, прямо знижує інтегральний інфраструктурний ризик, скорочує масштаб і тривалість порушень функціонування та, відповідно, підвищує стійкість економічних процесів у національному масштабі. Це обґрунтовує пріоритетність інвестицій у підготовку профільних кадрів як складову забезпечення економічної безпеки держави.

Висновки. У результаті проведеного дослідження обґрунтовано, що стійкість критичної інфраструктури є не похідним, а системоутворюючим чинником економічної безпеки держави, оскільки безпосередньо визначає безперервність виробничих процесів, стабільність ринкових зв'язків, бюджетну рівновагу та інвестиційну привабливість. Для України в умовах підвищених безпекових загроз інфраструктурний компонент економічної безпеки набуває стратегічного значення і потребує формалізованого включення до системи державного моніторингу.

Встановлено, що існуючі підходи до оцінювання економічної безпеки переважно зосереджені на макрофінансових та соціально-економічних індикаторах і недостатньо враховують параметри інфраструктурної стійкості. Це знижує прогностичну цінність аналітичних моделей у кризових і турбулентних умовах.

Систематизація основних груп ризиків (фізичних, техногенних, кібернетичних, організаційних, воєнних, гібридних) та визначення каналів їх впливу на макроекономічні показники дозволили встановити закономірність каскадного поширення інфраструктурних порушень на виробництво, логістику, фінансові потоки та бюджетні параметри. Доведено, що міжсекторні залежності формують мультиплікативний ефект втрат, який має враховуватися в моделях державного регулювання та стратегічного планування.

Розроблено формалізовану модель урахування кадрової спроможності у сфері захисту критичної інфраструктури, яка відображає залежність між чисельністю підготовленого персоналу та інтегральним індексом інфраструктурного ризику і макроекономічної стійкості. Показано, що зростання частки підготовленого особового складу, здатного застосовувати засоби радіоелектронної боротьби та технічного захисту, знижує скоригований індекс ризику та підвищує узагальнений показник економічної стійкості.

Доведено, що кадрові механізми забезпечення стійкості, включаючи спеціалізовану та післядипломну підготовку персоналу сектору безпеки і оборони (зокрема підрозділів НГУ), мають розглядатися як інвестиційний фактор економічної безпеки, а не лише як елемент функціонального забезпечення. Розвиток компетентностей у сфері застосування засобів РЕБ і технічного захисту формує вимірюваний ефект зниження інфраструктурних ризиків і підвищення відновлювальної спроможності систем.

Література

1. Арсенович Л. Класифікація та методи організації системи підготовки кадрів для сфери захисту критичної інфраструктури. *Державне управління: удосконалення та розвиток*. 2024. No 11. DOI: https://doi.org/10.32702/2307-2156.2024.11.11

2. Арсенович Л. Напрями поліпшення майстерності та фахової підготовки фахівців суб’єктів національної системи захисту критичної інфраструктури у контексті забезпечення кібербезпеки та кіберзахисту об’єктів критичної інфраструктури. *Державне управління: удосконалення та розвиток*. 2025. No 1. DOI: https://doi.org/10.32702/2307-2156.2025.1.15

3. Арсенович Л. Основні принципи, завдання та напрями реалізації професійної підготовки фахівців національної системи захисту критичної інфраструктури. *Державне управління: удосконалення та розвиток*. 2024. No 10. DOI: https://doi.org/10.32702/2307-2156.2024.10.7

4. Барановський О. Критична інфраструктура: безпековий вимір. *Acta Academiae Beregsasiensis. Economics / Економіка та менеджмент*. 2025. No 8. С. 13–37. DOI: https://doi.org/10.58423/2786-6742/2025-8-13-37

5. Василенко В. Національна кібербезпека в умовах диджиталізації суспільства: роль поліції в захисті критичної інфраструктури. *Вісник Харківського національного університету внутрішніх справ*. 2025. No 2. С. 392–405. DOI: https://doi.org/10.32631/v.2025.2.33

6. Демедюк С. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона*. 2023. No 2. С. 78–85. DOI: https://doi.org/10.36486/np.2023.2(60)

7. Євсєєв В. Інструменти інформальної освіти у сфері захисту критичної інфраструктури: сучасний стан та перспективи розвитку. *Суспільство та національні інтереси*. 2025. No 1(9). С. 405–414. DOI: https://doi.org/10.52058/3041-1572-2025-1(9)-405-414

8. Затонацький Д. Критична інфраструктура в структурі економічної безпеки держави. *Фінанси України*. 2025. No 6. С. 83–100. DOI: https://doi.org/10.33763/finukr2025.06.083

9. Кизим М., Хаустова В., Трушкіна Н. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. *Бізнес Інформ*. 2022. No 12. С. 58–78. DOI: https://doi.org/10.32983/2222-4459-2022-12-58-78

10. Ковальчук А. Система правового регулювання захисту об’єктів критичної інфраструктури в Україні: сучасний стан та напрями удосконалення. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2025. No 90(5). С. 172–184. DOI: https://doi.org/10.24144/2307-3322.2025.90.5.21

11. Крикун В. Форми та методи захисту об’єктів критичної інфраструктури в Україні. *Juris Europensis Scientia*. 2020. No 3. С. 99–103. DOI: https://doi.org/10.32837/chern.v0i3.107

12. Медвідь М. М., Медвідь Ю. І., Сокол Л. М. Трансформація ролі Національної гвардії України у системі державного регулювання

національної та економічної безпеки. *Економіка та суспільство.* 2025. No 82. URL: https://economyandsociety.in.ua/index.php/journal/issue/view/82 (дата звернення 12.02.2026).

13. Медвідь М., Суслов Р. Результати експериментальної перевірки ефективності організаційно-педагогічних умов формування здатності застосовувати засоби радіоелектронної боротьби майбутніми офіцерами НГУ. *Вісник Черкаського національного університету імені Богдана Хмельницького. Серія «Педагогічні науки».* 2025. No 4. С. 5-16. DOI: https://doi.org/10.31651/2524-2660-2025-4-5-16

14. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради (ВВР)*. 2023. № 5. Ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення 12.02.2026).

15. Санжарова Г., Сіренко О., Санжаров В. Італійська кібербезпекова архітектура: захист критичної інфраструктури, технічні, правові та інституційні нововведення. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2025. No 90(1). С. 124–129. DOI: https://doi.org/10.24144/2307-3322.2025.90.1.17

16. Суходоля О. Формування системи підготовки фахівців у сфері захисту критичної інфраструктури: компетенції випускників та зміст навчальних дисциплін. *Вісник Київського національного університету імені Тараса Шевченка. Серія «Державне управління»*. 2024. No 1. С. 122–131. DOI: https://doi.org/10.17721/2616-9193.2024/19-20/22

17. Цяпа С. Комплексна методика захисту інфраструктури мережі мобільного зв'язку 5G. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія «Технічні науки»*. 2023. Т. 34(73), No 2(1). С. 116–124. DOI: https://doi.org/10.32782/2663-5941/2023.2.1/19

18. Чумаченко С., Кутовий О., Гуйда О., Попель В., Заїка Н. Комплексний підхід до визначення рівня безпеки критичної енергетичної інфраструктури на основі інтегральної системи захисту її об'єктів від БПЛА

та крилатих і балістичних ракет. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія «Технічні науки»*. 2023. Т. 34(73), No 2(1). С. 261–267. DOI: https://doi.org/10.32782/2663-5941/2023.2.1/41

19. Чумаченко С., Кутовий О., Попель В., Гуйда О., Заїка Н., Мурасов Р. Науково-методичний підхід щодо оцінювання безпеки критичної інфраструктури на основі комплексу засобів захисту її об'єктів від БПЛА і крилатих ракет. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія «Технічні науки»*. 2023. Т. 34(73), No 1. С. 144–154. DOI: https://doi.org/10.32782/2663-5941/2023.1/22

20. Чумаченко С., Самойленко О., Невзгляденко Ю. Системний підхід до оцінювання ефективності системи захисту об’єктів критичної інфраструктури в умовах протидії ураженню їх засобами повітряного нападу. *Збірник наукових праць Державного науково-дослідного інституту авіації*. 2024. No 20. С. 32–36. DOI: https://doi.org/10.54858/dndia.2024-20-4

21. Шевченко К. Механізми державного управління при захисті об’єктів критичної інфраструктури в умовах воєнної агресії. *Вісник Національного університету цивільного захисту України. Серія «Державне управління»*. 2025. No 1. С. 304–312. DOI: https://doi.org/10.52363/2414-5866-2025-1-33

References

1. Arsenovych, L. (2024), “Classification and methods of organizing the personnel training system for the sphere of critical infrastructure protection”, *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, vol. 11. https://doi.org/10.32702/2307-2156.2024.11.11

2. Arsenovych, L. (2025), “Directions for improving professional skills and training of specialists of the national critical infrastructure protection system in the context of ensuring cybersecurity and cyber protection of critical infrastructure

facilities", *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, vol. 1. https://doi.org/10.32702/2307-2156.2025.1.15

3. Arsenovych, L. (2024), "Basic principles, tasks and directions for implementing professional training of specialists of the national critical infrastructure protection system", *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, vol. 10. https://doi.org/10.32702/2307-2156.2024.10.7

4. Baranovskyi, O. (2025), "Critical infrastructure: security dimension", *Acta Academiae Beregsasiensis. Economics*, vol. 8, pp. 13–37. https://doi.org/10.58423/2786-6742/2025-8-13-37

5. Vasylenko, V. (2025), "National cybersecurity in the conditions of digitalization of society: the role of police in protecting critical infrastructure", *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav*, vol. 2, pp. 392–405. https://doi.org/10.32631/v.2025.2.33

6. Demediuk, S. (2023), "Development of national cyber resilience and protection of critical information infrastructure", *Nauka i pravookhorona*, vol. 2, pp. 78–85. https://doi.org/10.36486/np.2023.2(60)

7. Yevsieiev, V. (2025), "Informal education tools in the field of critical infrastructure protection: current state and prospects for development", *Suspilstvo ta natsionalni interesy*, vol. 1(9), pp. 405–414. https://doi.org/10.52058/3041-1572-2025-1(9)-405-414

8. Zatonatskyi, D. (2025), "Critical infrastructure in the structure of economic security of the state", *Finansy Ukrainy*, vol. 6, pp. 83–100. https://doi.org/10.33763/finukr2025.06.083

9. Kyzym, M., Khaustova, V. and Trushkina, N. (2022), "The essence of the concept of 'critical infrastructure' from the perspective of national security of Ukraine", *Biznes Inform*, vol. 12, pp. 58–78. https://doi.org/10.32983/2222-4459-2022-12-58-78

10. Kovalchuk, A. (2025), "The system of legal regulation for the protection of critical infrastructure facilities in Ukraine: current state and directions for

improvement", *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia 'Pravo'*, vol. 90(5), pp. 172–184. https://doi.org/10.24144/2307-3322.2025.90.5.21

11. Krykun, V. (2020), "Forms and methods of protecting critical infrastructure facilities in Ukraine", *Juris Europensis Scientia*, vol. 3, pp. 99–103. https://doi.org/10.32837/chern.v0i3.107

12. Medvid, M.M., Medvid, Yu.I. and Sokol, L.M. (2025), "Transformation of the role of the National Guard of Ukraine in the system of state regulation of national and economic security", *Ekonomika ta suspilstvo*, vol. 82, available at: https://economyandsociety.in.ua/index.php/journal/issue/view/82 (Accessed 12 February 2026).

13. Medvid, M. and Suslov, R. (2025), "Results of experimental verification of the effectiveness of organizational and pedagogical conditions for developing the ability to use electronic warfare means by future officers of the National Guard of Ukraine", *Visnyk Cherkaskoho natsionalnoho universytetu imeni Bohdana Khmelnytskoho. Seriia 'Pedahohichni nauky'*, vol. 4, pp. 5–16. https://doi.org/10.31651/2524-2660-2025-4-5-16

14. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine "On Critical Infrastructure", available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Accessed 12 February 2026).

15. Sanzharova, H., Sirenko, O. and Sanzharov, V. (2025), "Italian cybersecurity architecture: protection of critical infrastructure, technical, legal and institutional innovations", *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia 'Pravo'*, vol. 90(1), pp. 124–129. https://doi.org/10.24144/2307-3322.2025.90.1.17

16. Sukhodolia, O. (2024), "Formation of a training system for specialists in the field of critical infrastructure protection: competencies of graduates and the content of academic disciplines", *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Seriia 'Derzhavne upravlinnia'*, vol. 1, pp. 122–131. https://doi.org/10.17721/2616-9193.2024/19-20/22

17. Tsiapa, S. (2023), “Comprehensive methodology for protecting the infrastructure of 5G mobile communication networks”, *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho. Seriia ‘Tekhnichni nauky’*, vol. 34(73), no. 2(1), pp. 116–124. https://doi.org/10.32782/2663-5941/2023.2.1/19

18. Chumachenko, S., Kutovyi, O., Huida, O., Popel, V. and Zaika, N. (2023), “Integrated approach to determining the level of security of critical energy infrastructure based on an integrated system for protecting its facilities from UAVs and cruise and ballistic missiles”, *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho. Seriia ‘Tekhnichni nauky’*, vol. 34(73), no. 2(1), pp. 261–267. https://doi.org/10.32782/2663-5941/2023.2.1/41

19. Chumachenko, S., Kutovyi, O., Popel, V., Huida, O., Zaika, N. and Murasov, R. (2023), “Scientific and methodological approach to assessing critical infrastructure security based on a complex of means for protecting its facilities from UAVs and cruise missiles”, *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho. Seriia ‘Tekhnichni nauky’*, vol. 34(73), no. 1, pp. 144–154. https://doi.org/10.32782/2663-5941/2023.1/22

20. Chumachenko, S., Samoilenko, O. and Nevzhliadenko, Yu. (2024), “System approach to evaluating the effectiveness of the protection system of critical infrastructure facilities under conditions of counteracting air attack weapons”, *Zbirnyk naukovykh prats Derzhavnoho naukovo-doslidnoho instytutu aviatsii*, vol. 20, pp. 32–36. https://doi.org/10.54858/dndia.2024-20-4

21. Shevchenko, K. (2025), “Mechanisms of public administration in protecting critical infrastructure facilities under conditions of military aggression”, *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriia ‘Derzhavne upravlinnia’*, vol. 1, pp. 304–312. https://doi.org/10.52363/2414-5866-2025-1-33

Отримано редакцією журналу / Received: 14.03.26

Прорецензовано / Revised: 17.03.26

Схвалено до друку / Accepted: 20.03.26