РОЗДІЛ 1.
ЕКОНОМІКА ТА МЕНЕДЖМЕНТ

1. FEJEZET.
GAZDÁLKODÁS ÉS MENEDZSMENT

CHAPTER 1.
ECONOMICS AND MANAGEMENT

DOI 10.58423/2786-6742/2025-8-13-37
УДК 351.862.4:340.13+338.583(477)

Олександр БАРАНОВСЬКИЙ
доктор економічних наук, професор, Заслужений економіст України,
професор ДННУ «Академія фінансового управління»,
м. Київ, Україна
ORCID ID: 0000-0002-5505-5098
Scopus Author ID: 56896045000
e-mail: bai.professor@gmail.com

КРИТИЧНА ІНФРАСТРУКТУРА: БЕЗПЕКОВИЙ ВИМІР

Анотація. *Розглянуто значущість забезпечення безпеки критичної інфраструктури (КІ), її об'єктів. Проаналізовано ступінь висвітлення цієї проблематики у вітчизняній і зарубіжній економічній літературі. Визначено характер унормування досліджуваного питання в чинному українському законодавстві і підзаконних актах, а також нормативно-правових актах, стратегічних і програмних документах зарубіжних країн і економічних союзів. Представлено еволюцію поглядів на забезпечення критичних елементів інфраструктури. Відображено вітчизняні й зарубіжні підходи до тлумачення сутності понять «критична інфраструктура» (КІ), «об'єкт критичної інфраструктури» (ОКІ), «захист критичної інфраструктури», «безпека критичної інфраструктури». Наведено авторське бачення безпеки КІ, її економічної безпеки. Визначені вимоги до організації фінансової безпеки КІ. Наголошено на взаємозв'язку безпеки КІ з енергетичною, промисловою, сировинно-ресурсною, продовольчою, екологічною, техногенною, соціальною, фінансовою, банківською, майновою, транспортною, інформаційною, науково-технологічною, оборонною, військовою, демографічною, радіаційною, біологічною, хімічною видами безпеки, безпекою активів, безпекою в сфері охорони здоров'я. Охарактеризовано національні пріоритети розвитку КІ та забезпечення її безпеки. З'ясовано безпекові аспекти функціонування КІ загалом і ОКІ зокрема, визначено співвідношення між їхнім захистом і забезпеченням безпеки й стійкості, з'ясовано виклики і загрози у цій сфері і підходи до оцінки рівня та методи аналізу такої безпеки. Наведено перелік індикаторів безпеки КІ. Виявлено взаємозв'язок стану КІ і різновидів безпеки в окремих країнах. Наголошено на необхідності формування державної системи захисту, безпеки та стійкості КІ в Україні. Зроблено висновок про перспективні напрями й організацію досліджень у цій сфері.*

Ключові слова: *критична інфраструктура (КІ), об'єкти критичної інфраструктури (ОКІ), економічна безпека, енергетична безпека, фінансова безпека, інфраструктурна безпека, кібербезпека, безпека критичної інфраструктури та її об'єктів.*

JEL Classification: E65, F63, H12, H54, H56

Abstract. *Vizsgálatra kerültek a kritikus infrastruktúra és objektumai biztonságának biztosításának jelentősége. Elemzésre került, hogy a hazai és a külföldi gazdasági szakirodalom milyen mértékben foglalkozik ezzel a kérdéssel. Meg lett határozva a vizsgált téma szabályozási megközelítéseinek jellege a hatályos ukrán jogszabályokban, az alárendelt jogszabályokban, valamint a külföldi országok és gazdasági szövetségek normatív jogi aktusaiban, stratégiai és programadó dokumentumaiban. Bemutatásra került a kritikus infrastruktúra elemeinek biztosításával kapcsolatos perspektívák alakulása. Kiemelésre kerültek a "kritikus infrastruktúra", "kritikus infrastruktúra-objektumok", "kritikus infrastruktúra védelme" és "kritikus infrastruktúra biztonsága" fogalmak lényegének értelmezésére vonatkozó hazai és külföldi megközelítések. A szerző elképzelése a kritikus infrastruktúra biztonságáról és annak gazdasági biztonságáról. A kritikus infrastruktúrák pénzügyi biztonságának megszervezésére vonatkozó követelmények kerültek felvázolásra. Kiemelésre került a létfontosságú infrastruktúrák biztonságának összefüggése az energetikai, ipari, erőforrás-, élelmiszer-, környezetvédelmi, technogén, szociális, pénzügyi, banki, vagyon-, közlekedési, információs, tudományos-technológiai, védelmi, katonai, demográfiai, sugárvédelmi, biológiai, kémiai biztonsággal és a vagyonbiztonsággal, valamint az egészségügyi ágazat biztonságával. A kritikus infrastruktúra fejlesztésének és biztonságának biztosításával kapcsolatos nemzeti prioritásokat jellemzésre kerültek. Tisztázásra kerültek a létfontosságú infrastruktúrák működésének biztonsági szempontjai általában és a létfontosságú infrastruktúra-objektumok különösen, valamint a védelmük és a biztonság és ellenálló képesség biztosítása közötti kapcsolat. Meg lettek határozva az e területet érintő kihívások és veszélyek, valamint a biztonsági szintek értékelésének megközelítései és az ilyen biztonság elemzésére szolgáló módszerekek. A kritikus infrastruktúrák biztonságára vonatkozó mutatók listája is rendelkezésre áll. Feltárásra került a létfontosságú infrastruktúrák állapota és az egyes országok biztonságának különböző típusai közötti összefüggés. A szerző kiemelte a létfontosságú infrastruktúrák védelmét, biztonságát és ellenálló képességét szolgáló állami rendszer kialakításának szükségességét Ukrajnában. A következtetésekben szó esik az ígéretes irányokról és a kutatás megszervezésére vonatkozó feltételekről ezen a területen.*

Kulcsszavak: *létfontosságú infrastruktúra, létfontosságú infrastruktúra-objektumok, gazdasági biztonság, energiabiztonság, pénzügyi biztonság, infrastruktúra biztonsága, kiberbiztonság, létfontosságú infrastruktúra és annak objektumai biztonsága.*

Abstract. *The significance of ensuring the security of critical infrastructure and its elements has been examined. The degree of coverage of this issue in domestic and foreign economic literature has been analyzed. The nature of regulatory approaches to the investigated topic in the current Ukrainian legislation, subordinate acts, as well as normative legal acts, strategic and programmatic documents of foreign countries and economic unions has been determined. The evolution of perspectives on ensuring critical infrastructure elements has been presented. Domestic and foreign approaches to interpreting the essence of the concepts "critical infrastructure", "critical infrastructure objects", "critical infrastructure protection" and "critical infrastructure security" have been highlighted. The author's vision of critical infrastructure security and its economic security has been provided. Requirements for organizing the financial security of critical infrastructure have been outlined. The interconnection of critical infrastructure security with energy, industrial, resource, food, environmental, technogenic, social, financial, banking, property, transport, informational, scientific-technological, defense, military, demographic, radiation, biological, chemical security, and asset security, as well as security in the healthcare sector, has been emphasized. National priorities for the development of critical infrastructure and ensuring its security have been characterized. Security aspects of critical infrastructure functioning in general and critical infrastructure objects (CIOs) in particular have been*

clarified, along with the relationship between their protection and ensuring safety and resilience. Challenges and threats in this area have been identified, as well as approaches to assessing security levels and methods for analyzing such security. A list of critical infrastructure security indicators has been provided. The interconnection between the state of critical infrastructure and various types of security in individual countries has been revealed. The necessity of forming a state system for the protection, security, and resilience of critical infrastructure in Ukraine has been highlighted. Conclusions regarding promising directions and the organization of research in this area have been made.

Keywords: *critical infrastructure, critical infrastructure objects, economic security, energy security, financial security, infrastructure security, cybersecurity, critical infrastructure security and its objects.*

Постановка проблеми. Безпека національних КІ сьогодні вважається першочерговим завданням всіх країн світу. Пріоритетна увага при цьому приділяється захисту енергетичних, транспортних, інформаційних, комунікаційних структур. Вже накопичений досвід розробки відповідних національних планів і програм, координації дій державних і приватних органів, реалізації завдань і функцій державної і місцевої влад [1, с.132].

Тоді як безпечне функціонування критичної інфраструктури (КІ), її належне фінансування є чинником *національної безпеки* / сталого функціонування економіки / добробуту та захисту населення країни, незадовільний технічний стан / рівень захисту об'єктів КІ / нестача інвестицій для її оновлення й розвитку є потенційною загрозою несанкціонованих втручань фізичного й кіберхарактеру в її функціонування є головними викликами і загрозами у сфері *виробничої* / *фінансової* безпек будь-якої країни [2, с.60, 78-79].

Крім того, КІ піддається значним щорічним пошкодженням унаслідок катастроф / змін клімату, які лише в Європі на 2021 р. обчислювалися у €9,3 млрд, з кратним збільшенням до 2050 р. до €19,3 млрд, а до 2080 р. – €37 млрд. За експертними оцінками, найбільш уразливими в цьому плані є енергетика (з річними втратами до 2080 р. у €8,2 млрд) й транспорт (€0,8 млрд)[3, с. 68].

Стратегія національної безпеки України[4] визнала посилення загроз КІ, пов'язаних з погіршенням її технічного стану / відсутністю інвестицій в її оновлення та розвиток / несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України. Водночас в цьому документі було наголошено, що держава створить *ефективну систему безпеки та стійкості КІ*, засновану на чіткому розподілі відповідальності її суб'єктів та державно-приватному партнерстві.

А Стратегія забезпечення *державної безпеки* проголошує, що *об'єктами забезпечення державної безпеки* є[5]: державний суверенітет, конституційний лад, територіальна цілісність України, оборонний, економічний і науково-технічний потенціал, кібербезпека, інформаційна безпека, *об'єкти критичної інфраструктури*, державна таємниця та службова інформація.

Аналіз останніх досліджень і публікацій. Проблематикою забезпечення безпеки елементів КІ загалом та об'єктів критичної інфраструктури (ОКІ) зокрема займалися такі вітчизняні і зарубіжні дослідники, як: Д. Бірюков [6, 7] , Д. Бобро [10-12], Є. Брежнєв [13-18], О. Верголяс[19], Д. Гріцаліс (D. Gritzalis) [30], Р. Даркін (R.Darken) [54], , С. Домбровська [20], О. Єрменчук [21,22,39], В. Заплатинський[23], Л. Кверцоні (L. Querzoni)[29], К. Клименко[2, 41], С. Кондратов [6], П. Котцніколау (P. Kotzanikolaou) [30], В. Кудряшов [24-26], А. Лазарі (A. Lazari) [27], Т. Льюїс (T. Lewis) [28, 54], І. Манжул [1], С. Мельник [31], Л. Монтарані (L. Montanari)[29], К. Павлюк [2], П. Пригунов [31], А. М. Савостьяненко [2, 41], Дж. Стергіопулос (G. Stergiopoulos) [30], О. Суходоля [51, 52], М. Теохаріду (M. Theocharidou) [30], В. Франчук [31], В. Харченко [18], В. Шведун [20].

Утім, досі відсутнє усталене бачення сутності безпек КІ й ОКІ, їхніх різновидів, їхнього співвідношення з національною безпекою й економічною безпекою держави в усіх проявах, підходів до формування системи їхнього забезпечення.

Формулювання цілей статті (постановка завдання). Мета статті полягає у з'ясуванні безпекових аспектів функціонування КІ загалом і ОКІ зокрема, визначенні співвідношення між їхнім захистом і забезпеченням безпеки й стійкості, з'ясуванні викликів і загроз у цій сфері, підходів до оцінки рівня такої безпеки та індикаторів безпеки, перспектив подальших досліджень у цій сфері.

Виклад основного матеріалу. Дослідження КІ – відносно нове явище, прискіплива увага до якого започаткована наприкінці минулого століття. Скажімо, в червні 1996 р. указом президента США № 13010 «Про роботу з дослідження уразливості захисту КІ від кібернетичних і фізичних загроз» була утворена Комісія з захисту критичної інфраструктури при президенті США (President's Commission on Critical Infrastructure Protection – PCCIP). Нині ж дослідження КІ з розвитком інформаційних технологій і можливостями сучасних комплексів імітаційного моделювання набули пріоритетності в багатьох країнах. Дослідження КІ базуються на теорії центрів тяжіння К. Клаузевіца [32], підході Дж. Вардена[33], теорії мереж, що самоорганізуються (scale-free network) Р. Альберта й А. Барабаші [34].

Термін «критична інфраструктура» (КІ) усе частіше використовується в різних сферах життєдіяльності суспільства. Ним послуговуються експерти, науковці у своїх публікаціях і коментарях, під час наукових конференцій, семінарів, міжнародних форумів, присвячених питанням розвитку та захисту КІ, цей термін вживають журналісти в ЗМІ. У багатьох країнах світу цей безпековий напрям визнано пріоритетним у політиці національної безпеки. Відтак у цих країнах активно розбудовуються національні системи із забезпечення захисту (безпеки) та стійкості КІ, ухвалюються законодавчі документи для регламентації діяльності учасників системи, готуються відповідні кадри, налагоджуються партнерські відносини з приватним сектором, здійснюються освітні заходи серед населення [9, с.7].

Важливість дослідження розвитку та захисту КІ зумовлюється зростанням потреби в розв'язанні практичних завдань зі створення її системи, яка забезпечує протидію різким потрясінням (через внутрішні / зовнішні чинники), упровадження належних заходів недопущення загострення ризиків у економічній / соціальній / інших сферах, застосування механізмів відновлення та стабілізації після подолання кризових явищ, а також фінансування КІ з дотриманням принципів фінансової стабільності. Розроблення парадигми (рамок) дослідження розвитку та захисту КІ в Україні передбачає взяття за основу (в державному регулюванні) чіткого визначення змісту понять з її формування та розвитку [25, с.8,11].

Проте, ще до того як вирішувати питання, як захищати, необхідно визначитися з тим, що саме слід захищати, від чого і якою мірою. Саме в такій послідовності вирішуються завдання побудови систем безпеки ОКІ. При цьому забезпечення безпеки ОКІ ускладнюється такими чинниками: безперешкодність пересування населення і транспорту всередині та/або поблизу таких найважливіших об'єктів; різні форми власності таких об'єктів; потреба ними різних рівнів безпеки; наявність на ОКІ власної системи (служби) безпеки; відсутність узгодженості між діями останньої і спеціалізованих органів з ліквідації надзвичайних ситуацій; розподіл функцій забезпечення безпеки в межах одного населеного пункту між позавідомчими, відомчими і приватними охоронними структурами; єдині для всіх об'єктів і територій системи життєзабезпечення (електропостачання, теплопостачання, водопостачання і каналізація, громадський транспорт, міська телефонна мережа, вуличне освітлення), порушення функціонування яких може спричинити виникнення на ОКІ надзвичайних ситуацій [20, с.26, 29].

При цьому питання про *формування політологічної концепції захисту КІ* розглядається як *спосіб розуміння / пояснення / дослідження процесів перетворень в системах забезпечення національної безпеки сучасних держав.* За розгляду цієї концепції як *конструктивної ідеї в теорії національної безпеки*, вбачається низка можливостей для практичного застосування. Зокрема, така концепція уможливлює постановку й дослідження таких питань, як *операціоналізація національних інтересів, залучення всіх стейкхолдерів (в т.ч. недержавних акторів забезпечення безпеки), врахування «м'яких» (нетрадиційних) загроз, децентралізація / приватизація безпекових функцій, пріоритизація дій та розподіл ресурсів* [35, с.231-232]. Причому *захист КІ* в свою чергу є відображенням *трансформації безпеки: від безпеки держав до безпеки груп / окремих індивідуумів; від безпеки окремої держави до міжнародної безпеки; з виключно воєнної в економічну / енергетичну / екологічну безпеки за підвищення політичної відповідальності за забезпечення безпеки як для держави, так і інших акторів, включно з громадськими / міжнародними організаціями* [36].

Коли йдеться про захист КІ, постає питання *не лише «від чого захищатись», але й «що захищати»: об'єкт чи функцію?* Слід зазначити, що захист цих елементів КІ має відмінності, оскільки щодо *об'єктів* він спрямований передусім на *зниження рівня загроз та вразливості об'єктів*, *мінімізацію наслідків*, а щодо

функцій – на *безперервність їх надання та швидше відновлення у разі переривання* [11, с.78].

Крім того, з огляду на міждисциплінарний характер *забезпечення безпеки й стійкості КІ* опрацьовується в економічному, технологічному, правовому, *безпековому* аспектах [37, с.201]. Для недопущення погіршення стану інфраструктури, її навмисного пошкодження та руйнування шляхом внутрішніх і зовнішніх диверсійних впливів та терористичних атак важливе місце відводиться також ***її захисту***, що проявляється в розробленні й реалізації відповідних державних програм, які спрямовують органи влади, приватний сектор на підтримку формування такої інфраструктури, її розбудови та збереження [24, с.8-9].

Термін *«критична»* застосовується для характеристики рівня інфраструктури, за відсутності якого (внаслідок недостатності / погіршення її стану / руйнування) економічній / соціальній / політичній / іншим сферам життєдіяльності країни завдається така шкода, що призводить до неможливості виконання (частково чи повністю) необхідних функцій та загрожує *національній безпеці* [25, с.9].

Аналіз міжнародного досвіду показує, що в основі забезпечення захищеності і безпеки КІ лежить вирішення низки питань, серед яких ключовими є [6, с.6]:

координація та взаємодія силових відомств та обмін інформацією про загрози;

організація державно-приватного партнерства в сфері безпеки;

використання ризик-орієнтованого підходу при попередженні загроз КІ.

Вперше про ***вимогу забезпечення безпеки критичних елементів інфраструктури*** було зазначено в директиві PDD-63 *(Presidential Decision Directive)*, підписаній президентом США Б. Клінтоном у 1996 році. Згодом питанням ***КІ*** та її ***безпеки*** почали приділяти увагу в інших країнах, зокрема: Німеччині, Великій Британії, Нідерландах, Чеській Республіці, Словаччині, Польщі, Угорщині[31, с.143-144].

У Директиві президента США 2013 р. (PPD-21) «Безпека та стійкість критичної інфраструктури» [38] зазначено, що *стійкість КІ* відображає *її здатність протидіяти викликам (зокрема, навмисним атакам, аваріям і природним катаклізмам), а також швидко відновлюватися після їх подолання*. Терміни *«безпечність»* та *«безпека»* відображають зниження ризиків розвитку КІ з використанням засобів фізичного впливу або у сфері протидії кібервторгненням, атакам чи наслідкам стихійних лих і техногенних катастроф. А під ***забезпеченням безпеки КІ*** розуміється *зменшення ризику КІ від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, за рахунок реалізації заходів із фізичного захисту або кіберзахисту*, а під ***стійкістю КІ*** – *спроможність підготуватись та адаптуватися до змінних умов, а також протистояти загрозам порушень функціонування та швидко відновлюватися від порушень. Стійкість включає спроможність протистояти загрозам та відновлюватися від цілеспрямованих атак, аварій, природних загроз та інцидентів*.

Директива була спрямована на об'єднання зусиль для зміцнення / підтримки безпечного функціонування КІ; встановлювала засади національної політики в цій сфері / спільну відповідальність всіх державних і приватних структур за стан КІ; вимагала підвищення координації їхніх дій; встановлювала три стратегічні імперативи для зміцнення безпеки КІ (пошук / уточнення функціональних взаємозв'язків, ефективний обмін інформацією, здійснення інтеграції та аналізу планування та операцій захисту КІ), роль та обов'язки міністра внутрішньої безпеки, секретаря ради національної безпеки; кожного сектора КІ; міністерств і відомств; уточнення Національного плану захисту інфраструктури [1, с.134].

Захист КІ розглядається в країнах ЄС як необхідна передумова розвитку масштабних інфраструктурних проектів / залучення інвестицій для їхнього здійснення. І хоча, як правило, одні органи державної влади реалізують економічну політику, а інші – відповідають за *забезпечення безпеки* і *стійкості КІ*, на рівні національних планів розвитку КІ *питання безпеки* враховуються. Загалом *стійкість КІ та її об'єктів* у деяких державах розглядається не окремо, а як одна із складових *забезпечення безпеки регіону або держави*. Крім того, забезпечення стійкості також включає не лише спеціально вжиті заходи, а розглядається як інтегрований елемент поведінки людей та соціально-економічних відносин у суспільстві. Тобто регулюється не лише нормами права, а і нормами моралі у суспільстві. *Забезпечення стійкості об'єктів КІ* досягається не тільки спеціальними заходами, а включає також підвищення інформованості персоналу об'єктів КІ та населення про можливі загрози та наслідки від них, навчання персоналу об'єктів КІ та постійного його тренування, розробки рекомендацій, процедур та правил поведінки працівників об'єкта КІ при впливі загроз для мінімізації можливих збитків, а також координацію дій уповноважених працівників державних органів влади та спеціальних служб і порядок їхньої взаємодії. Важливе значення приділяється заходам з підвищення інформованості населення про захист об'єктів КІ, залучення його до участі з попередження та ліквідації наслідків ураження об'єктів КІ за встановленими правилами. Такі заходи розглядаються як важливий інструмент з формування поведінки окремих груп людей та суспільства загалом при виникненні загроз КІ держави та є запорукою формування ефективних соціально-економічних відносин. У ряді європейських держав обов'язком ОКІ є *вжиття належних заходів для виявлення на ранній стадії загроз, недопущення ризиків від їхньої дії та подальшого постійного контролю за ними для забезпечення сталого функціонування об'єктів КІ, надання відповідних послуг та сприяння стабільності в регіоні та загалом у державі*. До таких несприятливих чинників, поряд із *ризиковими операціями, порушеннями вимог законодавчих актів у сфері фінансово-господарської діяльності та вчинення правопорушень, передбачених адміністративним чи кримінальним законодавством* (охоплюються ризик-менеджментом), також включають *загрози стихійних явищ, терактів, кіберінцидентів, шпигунства, конкурентної розвідки*, котрі можуть значно впливати на подальшу діяльність та навіть існування об'єкта[39, с.41-42, 45].

ЄК прийнято *Європейську програму захисту КІ*[40] для поліпшення захисту критично важливих інфраструктур в ЄС, де наведені *загрози КІ, принципи захисту (субсидіарність, взаємодоповнюваність, конфіденційність інформації, співпраця зі стейкхолдерами, відповідність заходів загрозам, секторальний підхід), межі захисту (національна КІ держав-членів ЄС), підходи до складання плану дій* та документ *«Захист критичної енергетичної й транспортної інфраструктури Європи»*, що містить критерії їхнього захисту, характеристику потенційних наслідків їхнього руйнування[1, с.135].

Для України імплементація загальноєвропейських положень про захист КІ є важливим питанням, поряд із зобов'язаннями з раннього попередження надзвичайних ситуацій, пов'язаних із зупинками постачання енергоносіїв / кібератаками / стихійними лихами, які наша держава вже взяла на себе в рамках Угоди про асоціацію з ЄС.

Зазвичай уряди визначають *національні пріоритети розвитку КІ* для поліпшення державної політики управління нею на рівні країни / регіонів, беручи до уваги наявні ризики, а також доступність ресурсу, що залучається для забезпечення її функціонування. До першочергових питань відносять *оцінку викликів і загроз розбудові КІ / її стійкості, запровадження програм управління ризиками, створення належної інформаційної бази динаміки її показників*.

У *захисті КІ* представники урядів багатьох країн бачать інструмент, за допомогою якого можна істотно впливати на *стан національної безпеки, в розрізі таких її складників, як кібербезпека, фінансова й енергетична безпеки*, говорять про важливе прикладне значення здійснення захисту КІ, зазначають, що вона дозволяє *операціоналізувати національні інтереси, тобто відстежувати вплив зміни стану такої інфраструктури на ступінь досягнення цілей, що визначаються національними інтересами, а також створювати необхідні резерви фінансових / матеріальних ресурсів для реагування на кризові ситуації / ліквідації їхніх наслідків*.

Відтак, *захист КІ життєдіяльності суспільства* стає одним з найважливіших пріоритетів держави. Важливість *безпечного функціонування КІ / її фінансування* є чинниками *забезпечення національної безпеки* / сталого функціонування економіки / добробуту / захисту населення країни. Проблему впровадження цілісної концепції / формування дієвої системи захисту КІ потрібно вирішувати з огляду на загальні процеси модернізації *системи забезпечення національної безпеки держави* / перспективної системи адміністративного й політичного устрою держави [41].

При цьому слід зазначити, що в різних країнах при визначенні взаємозв'язку стану *КІ* й *різновидів безпеки* застосовуються різні безпекові рівні. Так, у США, Австралії – це *національна / внутрішня (homeland security) безпеки*, у Великій Британії, Чехії, Нідерландах, Туреччині – *державна безпека,* Німеччині – *публічна безпека* (*public security*), в Польщі – *безпека держави та її громадян*, в Україні – *національна й державна безпеки*.

Зазначається, що *захист КІ* включає *систему скоординованих організаційних / нормативно-правових / адміністративних / пошукових / охоронних / режимних*

інженерно-технічних / наукових та інших заходів, матеріальних / нематеріальних засобів, спрямованих на забезпечення стійкості та безпеки КІ [21]; *заходи із забезпечення безпеки взаємозалежних систем, мереж і активів, що покладені в основу діяльності служб, життєво необхідних для функціонування суспільства* [2, с.70]; *комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості КІ* [8, с. 11].

За Законом «Про критичну інфраструктуру» *захист КІ* являє собою *усі види діяльності, що виконуються перед / під час створення / функціонування / відновлення / реорганізації ОКІ, спрямовані на своєчасне виявлення / запобігання / нейтралізацію загроз безпеці ОКІ, а також мінімізацію / ліквідацію наслідків у разі їх реалізації.*

Запровадження системи захисту КІ передбачає цілий ряд необхідних заходів, обов'язкових для кожного ОКІ, за таким алгоритмом[39, с.45]: *визначення виду притаманних загроз (стихійні явища, технічні поломки і недбалість персоналу, теракти, злочини) та їх можливої інтенсивності; оцінка уразливих місць; аналіз стійкості; визначення ризиків; визначення категорії об'єкта, його рівня захисту (від наявних на потенційних загроз); прогнозування розвитку ситуації залежно від наслідків та загроз; формування мети захисту та визначення заходів, необхідних для її досягнення; реалізація спільних заходів держави та приватних партнерів; на основі аналізу та з урахуванням розвитку ситуації постійне внесення коректривів у спільні дії та регулятивні нормативно-правові акти.*

Загалом ***безпека КІ*** розглядається як *її стан, за якого ризик завдання шкоди людині / суспільству / довкіллю скорочується до прийнятного рівня завдяки постійному моніторингу / управлінню ризиками; емерджентна властивість КІ, пов'язана з цілковитою відсутністю ризиків / наявністю прийнятних ризиків її небезпечних відмов / аварій внаслідок відмов окремих систем* [18, с.25]. О. Єрменчук під ***безпекою КІ*** розуміє стан її захищеності від дії зовнішніх / внутрішніх чинників, що забезпечує її стабільне функціонування [22, с.117], дослідники НІСД – стан КІ, за якого дія зовнішніх / внутрішніх чинників не спричиняє аварії / інші порушення її функціонування [9, с.201], В. Франчук, П. Пригунов і С. Мельник – стан, за якого забезпечується його функціонування / цілісність / самодостатність / стійкість та діяльність з попередження / виявлення / ліквідація загроз / небезпек, а за реалізації останніх, – відновлення / відшкодування збитків [31, с.146].

Причому безпека КІ / ризики, пов'язані з її недотриманням, не є статичними, а відтак, під впливом розмаїття як стохастичних, так і нестохастичних чинників, величина ризиків є мінливою, що зумовлює необхідність аналізу такої безпеки протягом всього життєвого циклу (ЖЦ) КІ[15, с.258]. Водночас неминучим чинником, що впливає на безпеку КІ протягом всього її життєвого циклу, є невизначеність, що вимірюється невідповідністю знань, уявлень суб'єкта аналізу / дослідника про реальні процеси / поведінку / структуру КІ[18, с.27].

Крім того, наголошується, що цілком очевидним і зрозумілим є, що *кожен ОКІ, процес виробництва / надання ним послуг* ***можуть зазнавати дестабілізуючої дії від впливу тих чи інших загроз, або можуть самі бути джерелом загрози***, у зв'язку з чим, з одного боку, він має бути ***об'єктом безпеки***, а з іншого – й ***суб'єктом безпеки***, тобто мати за обов'язок і право самостійно ***здійснювати безпекову діяльність та нести відповідальність за власну бездіяльність щодо протидії тим чи іншим загрозам у межах законодавства***. А стосовно КІ у базовому законі застосовуються три *безпекових поняття*: ***безпека КІ*** – стан захищеності КІ, за якого забезпечується функціональність, безперервність роботи, відновлюваність, цілісність і стійкість КІ; ***захист критичної інфраструктури*** – всі види діяльності, що виконуються перед або під час створення, функціонування / відновлення / реорганізації ОКІ, спрямовані на своєчасне виявлення / запобігання / нейтралізацію загроз їхній безпеці, а також мінімізацію та ліквідацію наслідків у разі їх реалізації; ***національна система захисту КІ*** – сукупність органів управління / сил / засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення) / органів місцевого самоврядування / операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту КІ. Крім того, на наш погляд, національна система захисту КІ, поряд з державною політикою у сфері захисту КІ, має включати також регіональну / місцеву / корпоративну політику у цій сфері.

Утім, аналізуючи зміст наведених термінів, можна зробити висновок про те, що **під час його формулювання законотворці не використовували сучасні надбання такої науки, як безпекознавство, яка стрімко розвивається в Україні. Зокрема, складно зрозуміти, чому безпеку КІ пропонується розглядати лише з пасивного боку як стан захищеності, як результат вжитих дій, а активну складову, тобто діяльнісну, пропонується закласти в іншому терміні «захист»** [31, с.144-145].

Вітчизняними фахівцями стійкість КІ трактується як *спроможність надійно функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після реалізації загроз будь-якого виду* [8]. Утім, на наш погляд, ***безпека КІ не зводиться лише до*** *стану її захищеності й спроможності надійного функціонування / адаптації до умов, протистояння й відновлення,* а має й інші сутнісні / змістовні характеристики.

Стратегія національної безпеки України (2015 р.)[42], в якій КІ держави була приділена значна увага, визначила такі ***пріоритети забезпечення її безпеки***: комплексне вдосконалення правової основи захисту КІ, створення системи державного управління її безпекою; посилення охорони ОКІ, зокрема, енергетичної / транспортної; налагодження співробітництва між суб'єктами захисту КІ, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них; розробка та запровадження механізмів обміну інформацією між державними органами / приватним сектором / населенням про загрози КІ / захист інформації у цій сфері; профілактика техногенних аварій / оперативне й адекватне реагування на них, локалізація /

мінімізація їхніх наслідків; розвиток міжнародного співробітництва у цій сфері. Безумовно, все перелічене має відношення до можливих пріоритетів забезпечення безпеки КІ. Однак, на наш погляд, ***вони мають визначатися не лише комплексним вдосконаленням правової основи захисту КІ, а й формуванням і реалізацією обґрунтованих промислової, енергетичної, транспортної, екологічної, інформаційної, фінансової, інвестиційної, інноваційної, боргової, соціальної політики стосовно КІ загалом та ОКІ зокрема.***

Відтак, на наше переконання, ***безпека КІ*** – це:

важлива складова національної безпеки, яка базується на незалежності, конкурентоспроможності і ефективності КІ, що характеризують збалансованість її функціонування, потенціал розвитку, наявність виробничих і фінансових резервів;

рівень забезпеченості економічних агентів і суспільства достатніми за обсягом і раціональними за структурою ресурсами, послугами і продуктами КІ та ОКІ;

стан захищеності, за якого виклики, загрози і ризики завдання шкоди від деструктивного розвитку, нештатних ситуацій, природних катастроф, навмисних дій третіх осіб, терористичних проявів КІ як такій, ОКІ, економічним агентам і довкіллю попереджаються, усуваються, нейтралізуються, мінімізуються, скорочуються до прийнятного рівня і забезпечує їхні цілісність, функціональність, безперервність, відновлюваність, стійке і стабільне функціонування та подальший поступальний розвиток;

комплекс заходів органів державної влади і управління, органів місцевого самоврядування, власників і операторів КІ та ОКІ, інститутів громадянського суспільства з убезпечення її загалом та ОКІ;

гарантоване дотримання життєво важливих національних інтересів, інтересів населення, суб'єктів господарювання, ОКІ, секторів національної економіки і фінансових ринків, суспільства і держави в політичній, економічній, фінансовій, соціальній, оборонній, військовій, техногенні, екологічній, інформаційній сферах в частині функціонування й розвитку КІ та її об'єктів.

Унаслідок міждисциплінарного характеру *забезпечення стійкості / безпеки КІ* досліджується в правовому / економічному / технологічному / суто безпековому (забезпечення правопорядку / оборона / цивільний захист) аспектах [37, с.201].

При цьому важливе значення має *економічна безпека КІ (ЕБКІ) / фінансова безпека КІ (ФБКІ) / її об'єктів як таких*. *ЕБКІ* асоціюється з її стійким і стабільним функціонуванням, оновленням основних фондів. Для оцінки її рівня можуть застосовуватися показники рентабельності послуг / частки збиткових об'єктів КІ; коефіцієнт оновлення основних фондів. А оскільки КІ виробляє не кінцевий, а проміжний продукт, її безпека пов'язана не з максимізацією реалізованих послуг, а з їхньою оптимізацією. При цьому викликом для ЕБКІ під

впливом зовнішніх і внутрішніх загроз є вимушені витрати / понесений збиток / утрачена вигода внаслідок призупинення функціонування об'єктів КІ.

Безпека КІ безпосередньо пов'язана з *енергетичною / промисловою / сировинно-ресурсною / продовольчою / екологічною / техногенною / соціальною / фінансовою / банківською / майновою / транспортною / інформаційною / науково-технологічною / оборонною / військовою / демографічною / радіаційною / біологічною / хімічною безпеками / безпекою активів / безпекою в сфері охорони здоров'я*.

Так, *промислова безпека* визначається як *стан захищеності життєво важливих інтересів особи та суспільства від аварій на небезпечних виробничих об'єктах та їх наслідків*[43].

При цьому під *енергетичною безпекою* здебільшого розуміють *здатність держави в особі її органів управління забезпечити кінцевих споживачів енергією в необхідному обсязі та належної якості у звичайних умовах, а також під час дії дестабілізуючих чинників (надзвичайних ситуацій) внутрішнього і зовнішнього характеру у межах гарантованого покриття мінімального обсягу найважливіших потреб країни, окремих її районів, міст, селищ чи об'єктів у паливно-енергетичних ресурсах*[44, с.261-262]; *здатність ПЕК забезпечувати економічно обґрунтований внутрішній та експортний попит достатнім обсягом енергоносіїв відповідної якості, здатність споживчого сектору економіки раціонально використовувати енергоресурси, а також стійкість енергетичної системи до зовнішніх економічних, політичних, техногенних та природних загроз*[45].

Натомість *продовольчу безпеку* визначають, як: *стан економіки, забезпечений відповідними ресурсами, потенціалом і гарантіями, за якого, незалежно від внутрішніх і зовнішніх загроз, зберігається необмежена у часі здатність держави (суспільства) забезпечувати економічну та фізичну доступність для всього населення до життєво важливих продуктів харчування в обсягах, якості й асортименті, достатніх для розширеного відтворення кожної особи у звичних умовах і мінімально необхідних для підтримки здоров'я та працездатності в надзвичайних продовольчих ситуаціях*[46]; *соціально-економічне явище, яке характеризує рівень доступності продуктів харчування для основної частини населення країни з метою підтримки нормального способу життя, а не цифри виробництва продуктів харчування на 1 особу*[47]; *стан економіки, за якого населенню країни загалом і кожному громадянину окремо гарантується забезпечення доступу до продуктів харчування, питної води в якості, асортименті і обсягах, необхідних і достатніх для фізичного і соціального розвитку особистості, забезпечення здоров'я і розширеного відтворення населення країни* [48].

У забезпеченні *ЕБ* важливе місце належить *безпеці в інфраструктурній сфері / інфраструктурній безпеці*, під якою розуміють *стан інфраструктури, що забезпечує не лише загальний рівень конкурентоспроможності галузей національної економіки, але й безпеку особистості, господарюючих суб'єктів і держави загалом, має відповідати тому рівню порогової безпеки, який необхідний*

для виходу з кризи; стан безперебійного функціонування інфраструктури країни, що уможливлює забезпечення стабільного відтворення / збереження інфраструктури / безпеку господарюючих суб'єктів / поліпшення умов розвитку особистості. Забезпечення інфраструктурної безпеки передбачає комплексну взаємодію таких її функціональних складових, як: *фізична безпека інфраструктури / економічна, фінансова й інформаційна її безпеки*.

Дослідники зазначають, що рівень *інфраструктурної безпеки* зумовлюється *безпекою її систем / підсистем на всіх інфраструктурних рівнях*. Скажімо, *безпека АЕС* визначається не лише *функціональною безпекою самої станції / її систем / підсистем*, а й *рівнем безпеки всіх повязаних з АЕС підсистем енергосистеми*[14, с.261]. Це означає, що має бути забезпечений всеосяжний, швидкий і зрозумілий, за справедливими цінами доступ до інфраструктури, збережена її комплексність, необхідна для підтримання конкурентоспроможності економіки. *Стратегія інфраструктурної безпеки*, насамперед, має забезпечувати її фізичний захист, але жодним чином не може ним обмежуватись. Безпека забезпечується через розвиток, що означає достатність і надійність, навіть у пікових, надзвичайних ситуаціях, послуг і продукції інфраструктури.

Тобто, наведені визначення підкреслюють урахування в них елементів, притаманних сферам КІ / ОКІ, які виокремлюються в країнах світу.

Залежно від типу *безпекової архітектури* ***захист КІ*** є невід'ємною частиною політики внутрішньої безпеки країни (США)[28] / носить як наднаціональний характер, так і забезпечується окремими країнами (ЄС)[27]. При цьому у США захист КІ і ключових активів вимагає переходу до нової національної кооперативної парадигми. Традиційно *національна безпека США* визнавалася в основному відповідальністю федерального уряду, підтримувалася колективними зусиллями військових, зовнішньополітичних установ, розвідувального співтовариства в захисті повітряного простору та національних кордонів, а також операціями за кордоном для захисту національних інтересів. Безпека ж КІ та захист ключових активів є *спільною відповідальністю, яка не може бути забезпечена виключно федеральним урядом, що вимагає злагодженості дій федеральних, державних і місцевих органів влади; приватного сектора та небайдужих громадян*[49].

Стратегія національної безпеки України «Безпека людини – безпека країни»[4], наголосила на посиленні ***загроз для КІ***, зумовлених погіршенням її технічного стану / відсутністю інвестицій в її оновлення й розвиток / несанкціонованим втручанням у її функціонування, зокрема фізичним і кіберхарактеру / триваючими бойовими діями, а також тимчасовою окупацією частини території України й ***необхідності створення державою ефективної системи безпеки / стійкості КІ***, яка ґрунтується на чіткому розподілі відповідальності її суб'єктів і державно-приватному партнерстві. ***Проте, при цьому остання теза в зазначеній стратегії залишилася не розкритою***.

Цільова група ЄС та НАТО щодо стійкості КІ в 2023 р. представила звіт про *поточні виклики безпеці* і визначила рекомендації зі зміцнення *стійкості інфраструктури,* що, зокрема, стосуються *необхідності забезпечення стійкості і*

розвитку співпраці шляхом: посилення взаємодії при повному використанні синергії, наприклад, у разі виникнення серйозної загрози / значних змін у контексті безпеки; сприяння взаємодії між членами НАТО, державами-членами і приватним сектором, у т.ч. щодо безпеки критично важливої інфраструктури; проведення спеціальних дискусій на основі сценаріїв; посилення структурованого діалогу з питань стійкості / військової мобільності / розширення існуючих штабних переговорів з питань кібербезпеки, космосу, морських перевезень і енергетики; сприяння поширенню найкращих практик / оцінок / посиленню моніторингу впливу на безпеку та співпрацю, в т.ч. між цивільними і військовими суб'єктами; проведення регулярних паралельних і скоординованих оцінок загроз КІ[50].

Основою забезпечення захищеності й безпеки КІ є вирішення низки питань, з-поміж яких основними виділяються такі: *координація і взаємодія органів державної влади та обмін інформацією про загрози; організація державно-приватного партнерства у сфері безпеки; використання ризик-орієнтованого підходу при попередженні загроз КІ*[6, с. 5].

Безпекова діяльність у сфері КІ – це надто складний процес, який, окрім безпекових механізмів, міститиме ще й координаційні, а також як діяльність потребує ще й відповідного управління. Це потребує відповідних фахівців, підготовки, перепідготовки, які потрібно розпочинати у закладах вищої освіти, що мають навчально-безпекові технології, певний досвід із залученням практиків. Важливим і обов'язковим елементом в організуванні безпеки об'єктів критичної інфраструктури має бути сертифікація їхніх підрозділів безпеки та ведення реєстрів[31, с.147].

Більш того, США усвідомили необхідність не тільки забезпечення *безпеки та стійкості КІ*, але й *ланцюжків постачання критичних матеріалів, ресурсів, технологій та послуг, поширюючи опрацьований підхід і на інші складові забезпечення національної безпеки і стійкості.*

Інші розвинені країни світу широко використовують напрацьовані у США підходи, звичайно, враховуючи при цьому власну національну специфіку. На міжнародному рівні *проблематика захисту / безпеки КІ включена до порядку денного ряду структур і організацій, таких як НАТО і ЄС*, членства в яких Україна прагне набути, а також ОЕСР. Причому останніми роками у розвинених країнах посилюється тенденція розширення контексту заходів, пов'язаних із забезпеченням функціонування КІ: ***питання захисту / безпеки*** КІ розглядаються разом із питаннями її ***стійкості***. При цьому, питанням забезпечення *стійкості – готовності / адаптування до умов, що змінюються, а також протистояння змінам і швидкого відновлення після порушень функціонування* – приділяється дедалі більше уваги порівняно з питаннями *захисту,* що зумовлено тим, що *сучасне безпекове середовище характеризується появою нових загроз / небезпек на тлі швидких процесів еволюції / трансформації існуючих загроз, можливості їхніх різноманітних комбінацій*, оскільки за таких умов, ***жодна створена система захисту / безпеки не може повною мірою забезпечити захист від усіх***

загроз / небезпек, позаяк поки триває розбудова системи захисту, розрахованої на певні загрози, у світі з'являються нові загрози / небезпеки[51, с.5].

В ***організації забезпечення фінансової безпеки об'єктів КІ*** слід ураховувати:

їхню категорійність (життєво необхідні об'єкти КІ; життєво важливі об'єкти КІ; важливі об'єкти КІ; необхідні об'єкти[52, с.73]*);*

приналежність (об'єкти національної КІ (виключно у державній власності); об'єкти регіональної та локальної КІ (як у державній, так і комунальній/приватній власності));

наявність серед них потенційно небезпечних об'єктів й об'єктів підвищеної небезпеки;

ступінь вразливості об'єктів КІ до впливу небезпечних чинників (високий, середній, низький);

загальносистемні функції КІ загалом;

зовнішні чинники безпекового середовища і чинники функціонування конкретних ОКІ;

ідентифікацію усіх викликів, загроз фінансовій безпеці об'єктів КІ і ризиків у цій сфері;

розмір можливих збитків від наслідків надзвичайних ситуацій техногенного і природного характерів, зловмисних дій/людських помилок, тероризму, війни, завданих здоров'ю людей та об'єктам національної економіки;

умови функціонування (в мирний час, в умовах надзвичайного стану, воєнного стану та стану війни);

стимулювання інвестування/перспективу формування публічно-приватного партнерства у забезпеченні фінансової безпеки КІ;

інтеграцію України до європейського безпекового простору.

Головними викликами у забезпеченні безпеки КІ є[28]: *величезність кожного з її секторів та її як такої; управління безпекою за умов взаємозалежності діяльності урядових органів, державного / приватного секторів, регулюючих / економічних чинників; проблема обміну інформацією, позаяк державні органи здебільшого є вертикально-орієнтованими структурами, що здебільшого накопичують інформацію, тоді, як елементи КІ розпорошені між державою та великою кількістю приватних компаній; взаємозалежність елементів / секторів КІ внаслідок притаманним їм комплексних різнорівневих взаємодій / взаємозв'язків*. Крім того, існує *величезна кількість й значна неоднорідність об'єктів і систем, що належать до різних секторів КІ, необхідність враховувати різноманітні характеристики об'єктів та систем з огляду на всі типи загроз*[6, с.25].

Найбільш типовими загрозами безпеці КІ є: *природні*: повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії; б) *техногенні*: промислові / ядерні / радіологічні / транспортні аварії; б) *зловмисні*: кібер- і терористичні атаки, втрата елементів КІ.

До ***загроз КІ*** відносять: стихійні лиха, пандемії, виробничі аварії, злочину / терористичну діяльність, кібератаки[53]; .

Проблемами ж у захисті КІ є[54]: *розподіл повноважень у цій сфері між різними рівнями влади; відсутність єдиної методології визначення ризиків / вразливості ОКІ; забезпечення активної участі власників / операторів ОКІ у такому захисті*.

А ***за відсутності державної системи захисту (безпеки) та стійкості КІ відповідні об'єкти не можуть бути ефективно захищені існуючими в Україні системами безпеки та кризового реагування, особливо у випадках реалізації масштабних комплексних загроз і небезпек***. Відповідальність за безпеку ОКІ покладено на різні міністерства і відомства, які забезпечують функціонування відповідних систем. При цьому кожна система має «власні» набори загроз та ризиків, якими вона опікується, «власні» режими функціонування у різних безпекових умовах, «власні» плани і процедури реагування, викладені із застосуванням відомчої системи термінів і понять. До того ж визначені у положеннях і планах механізми і процедури взаємодії між існуючими національними системами безпеки і кризового реагування здебільшого є недостатньо відпрацьованими та апробованими для випадків масштабних кризових ситуацій, оскільки в країні до цього часу практика міжвідомчих навчань і тренувань на рівнях, вищих ніж об'єктовий, була розвинута слабко. Натомість ***головне призначення систем забезпечення захисту / безпеки та стійкості КІ полягає у запобіганні саме масштабним комплексним кризам та у реагуванні на них***, якщо вони все ж трапляються[51, с.21-22].

Оцінювання безпеки КІ / її об'єктів зумовлено важливістю завдань, що вирішуються ними. Так, скажімо, їхнє безпечне функціонування визначає стратегію індустріального розвитку будь-якої держави / зростання добробуту громадян[17, с.210].

У літературі виокремлюються три підходи до аналізу *ризиків, притаманних функціонуванню КІ*: *детермінований і ймовірнісний аналіз*, а також *аналіз, що базується на теорії можливостей, які можуть застосовуватися як апріорно, так і апостеріорно*. При цьому апріорний аналіз безпеки КІ передує виникненню несприятливої події, базується на сценарному аналізі, за якого використовуються / аналізуються безліч можливих сценаріїв, пов'язаних з подією / можливою поведінкою КІ як реакцією на її виникнення. Причому наслідки, характерні для різних сценаріїв, оцінюються з урахуванням шкоди, пов'язаної з ними. Кількісні / якісні характеристики сценаріїв визначаються з огляду на модель, прийняту для аналізу, що будується з урахуванням властивих їй припущень / обмежень.

Апріорний аналіз здійснюється в умовах епістомологічної (пов'язаної з відсутністю у суб'єкта аналізу повних знань про об'єкт досліджень) й алеаторної (що безпосередньо пов'язана з об'єктом аналізу, зумовлена еволюцією властивостей і поведінки об'єкта; є невід'ємною властивістю КІ, зумовленою дією випадкових чинників) невизначеності. Епістомологічна невизначеність є властивістю об'єкта аналізу безпеки й може бути знижена за рахунок одержання додаткових відомостей про характеристики КІ, її поведінку.

Апостеріорний аналіз здійснюється після небажаної події і спрямований на розробку рекомендацій з підвищення рівня безпеки КІ / зниження ризиків для

ідентичних систем у майбутньому. Цей аналіз пов'язаний з дослідженням одного із передбачуваних реалізованих сценаріїв. При цьому невизначеність, властива такому аналізу, може спричинити реалізацію послідовності подій, нехарактерних вихідній безлічі сценаріїв. Відтак, один вид аналізу доповнює інший, а їхній вибір визначається складністю системи / відомістю параметрів КІ з прийнятною точністю[15, с.258-259].

Безпека КІ забезпечується аналізом процесів її функціонування / моніторингом стану / моделюванням і оцінкою ризиків відмови / оцінкою шкоди / розробкою дієвих безпекових стратегій. Утім, це ускладнюється відсутністю єдиного комплексного підходу до оцінки безпеки КІ, позаяк кожна сфера людської діяльності оперує своїм інструментарієм / понятійним апаратом аналізу безпеки, що спричиняє розмаїття методів оцінки безпеки КІ, частина яких застаріла і не відповідає рівню розвитку КІ і вимогам до її безпеки, не забезпечуючи прийнятний рівень достовірності результатів.

Оцінка безпеки КІ – складна й неоднозначна проблема, зумовлена: нечіткістю визначення меж останньої; складністю поведінки КІ, емерджентністю її властивостей; неергодичністю (властивістю динамічних систем) КІ; неможливістю визначення всіх її станів і переходів між ними; відсутністю статистичних даних, пов'язаних з великими аваріями / збоями; немонотонністю проблеми, коли збільшення знань не спричиняє її глибше розуміння.

Отже, розробка точної / повної моделі оцінки безпеки КІ – складне завдання, пов'язане з нестачею знань про можливі відмови / поведінку КІ, наявністю вихідних даних у різних кваліметричних вимірах[13, с.277].

Основні характеристики методів аналізу безпеки КІ виглядають таким чином (табл. 1).

Оцінювання безпеки КІ здійснюється *якісними* й *кількісними* методами. Останні відіграють важливу роль для оцінювання ризиків, проте їхня точність, особливо на початкових етапах життєвого циклу КІ, коли її функціонування характеризується високим рівнем невизначеності, може бути недостатньою. В разі достатньо повного оцінювання функціонування КІ статистичними даними для оцінок безпеки доцільне застосування методів / підходів, що базуються на теорії ймовірності. Утім, основним питанням залишається валідність статистики / її повнота, що істотно обмежує застосування цих методів за недостатнього обсягу статистичних даних / обмеженнях на час одержання оцінок безпеки. Водночас, частина безпекових параметрів, незалежно від етапу ЖЦ КІ, не можуть оцінюватися кількісно, з використанням статистичних методів [16, с.118].

Для аналізу безпеки КІ застосовують *спеціальні методи / і технології оцінки і контролю небезпек протягом її ЖЦ*. Відтак, ідентифікація / класифікація / оцінка / управління ризиками / контроль залишкового ризику є основними етапами ризик-аналізу КІ. А для цього *необхідна інтеграція різних методів оцінки безпеки, що базуються на різній вхідній інформації, однак уможливлюють визначення ідентичного вихідного показника безпеки, як-от величину ризику / ймовірність аварій*.

Таблиця 1.

Основні характеристики методів аналізу безпеки КІ

	DSA	PSA	SC
Вхідні дані	Детерміновані вхідні дані. Точкова оцінка (верхня, нижня, середня)	Імовірнісний розподіл вхідних параметрів	Нечіткі вхідні змінні, чіткі, нечіткі випадкові величини
Множинність подій, що розглядаються	Лише з найгіршими наслідками	Всі прогнозні події	Всі прогнозні події
Частота	Достовірні події (P=1)	Імовірність оцінюється згідно з прийнятими законами розподілу	Лінгвістичні оцінки, нечіткі числа
Тяжкість наслідків	Передбачається відомою	Передбачається відомою	Лінгвістичні змінні, нечіткі змінні
Ризик оцінка	Якісний аналіз	Якісний аналіз	Нечіткий аналіз
Урахування невизначеності	Невизначеність не розглядається	Стохастична невизначе-ність (випадкові перемінні з відомим розподілом) Невизначеність першого роду	Нестохастична невизначе-ність. Невизначеність дру-гого роду

Джерело: [13, с.281]

Нині для оцінки безпеки КІ застосовуються аналітичні / експериментальні, що базуються на статистичному моделюванні / логіко-графічні / нечіткі / якісні / експертні методи, кожні з яких мають як індивідуальні переваги, так і недоліки, і можуть застосовуватися незалежно одні від одних.

Позаяк КІ відзначається невизначеністю поведінки / нелінійністю зміни гетерогенних параметрів / наявністю великих масивів даних у різних кваліметричних шкалах, то це спричиняє недоцільність застосування лише однієї групи методів ризик-аналізу, що не забезпечує потрібний рівень достовірності оцінок безпеки КІ. Крім того, використання лише однієї групи методів на основі уподобань експерта, спричиняє втрату частини інформації, обробка якої унеможливлюється внаслідок обмежень застосовуваних методів [16, с.116].

За оцінювання безпеки КІ можуть використовуватися два способи інтеграції методів: послідовний і паралельний. Послідовна інтеграція для отримання одного параметра безпеки передбачає застосування безлічі методів, причому вихідні параметри одного метода є вхідними параметрами для іншого. Головною вимогою є їхня сумісність, а основною перевагою – зниження обсягу необхідних вхідних даних. Натомість паралельна інтеграція передбачає паралельні обчислень одного і того ж самого параметра двома / трьома групами методів, дозволяє уточнити оцінки безпеки, одержані різними методами.

Аналіз безпеки КІ має базуватися на *принципах інтеграції / диверсифікації методів ризик-аналізу* з огляду на застосування методів з вихідними даними різної (диверсної) кваліметричної природи для одержання параметрів безпеки. Скажімо,

величина ризику аварії може одержуватися як на основі традиційних імовірнісних підходів, так і нечітких продукційних систем, коли кількісні й якісні методи є диверсними, що використовують різні вхідні дані. Вихідним параметром є ймовірнісна оцінка безпеки КІ.

Оцінювання безпеки КІ з використанням якісних методів застосовуються: *номінальна* (шкала *найменувань*, *класифікаційна* шкала), в якій значення визначаються з точністю до взаємооднозначних перетворень; *нечітка* (*лінгвістична*), де значення визначаються з точністю до еквівалентних лінгвістичних перетворень; *порядкова* (*рангова*) шкали, які використовуються для порівняльної оцінки об'єктів, коли визначається лише порядок їхньої переваги (ранжирування), і де числові значення визначаються з точністю до монотонних перетворень.

Вихідними даними для кількісних методів є параметри КІ, вимірювані з використанням: інтервальної шкали з визначенням чисельних значень з точністю до лінійних перетворень[16, с.117].

Серед ***індикаторів безпеки КІ***, на наш погляд, мають бути:

імовірна шкода «еталонних об'єктів» / шкала чинників їхньої ризикованості / небезпечності;

ступінь забезпеченості економічних агентів публічними послугами, енергоресурсами, транспортними і медичними, інформаційними й комунікаційними, поштовими і фінансовими / банківськими послугами, послугами водопостачання й водовідведення в необхідних обсягах / якості;

високий рівень обороноздатності і безпеки держави, цивільного захисту населення, космічних технологій, дослідницької діяльності;

економічна динаміка;

економічні збитки;

стійкість енергетичного й оборонно-промислового комплексів, хімічної, фармацевтичної та харчової промисловості, сільськогосподарської та наукової сфер, урядових структур, правоохоронних органів;

покращення / погіршення стану довкілля та зростання / зменшення викидів парникових газів;

підвищення / зниження рівня життя населення;

поліпшення / погіршення стану здоров'я й активності населення.

Утім, як наголошують В. Франчук, П. Пригунов і С. Мельник, в **Україні відсутня система забезпечення безпеки КІ, що базується на засадах, впроваджених в країнах-членах ЄС та НАТО**. Відтак, ***вітчизняні механізми забезпечення безпеки КІ мають бути наближені до загальноєвропейського й стати одним із пріоритетів державної політики. Для цього необхідне адекватне науково-методичне забезпечення, включно з розробленням системного підходу до формування змістовної / організаційної складових вітчизняної системи забезпечення безпеки КІ*** [31, с.145].

Висновки та перспективи подальших наукових досліджень. Отже, формування системи забезпечення безпеки КІ – складне й багатогранне завдання, без вирішення якого неможливо забезпечити нормальну життєдіяльність держави

й убезпечити всіх економічних агентів. *Перспективні дослідження з забезпечення безпеки КІ* мають включати: визначення наявного стану об'єктів КІ; виявлення критично важливих об'єктів інфраструктури (КВОІ); урахування взаємозв'язку / взаємозумовленості об'єктів КІ, мережевої складової кожного сектора КІ (економічного / фінансового / енергетичного та інших); прогнозування умов функціонування / розвитку об'єктів КІ з огляду на ймовірні позаштатні (критичні / надзвичайні) ситуації; з'ясування напрямів / заходів / засобів подолання / локалізації / зниження негативного впливу позаштатних (критичних / надзвичайних) ситуацій, а також резервів забезпечення безпеки об'єктів КІ. Доцільним убачається впровадження досвіду США з формування кластера НДІ, що переймаються розробкою сучасних математичних моделей для дослідження КІ. Крім того, на порядку денному необхідність інтеграції / конвергенції досліджень КІ, якості життя (як одного із чинників, який слід ураховувати при визначенні КВОІ як об'єктів життєзабезпечення) і безпеки.

Список використаних джерел

1. Манжул І. Поняття та захист критичної інфраструктури в США, ЄС, Україні. *European political and law discourse*. 2016. Volume 3. Issue 2. С.132-138.
2. Клименко К. В., Павлюк К. В., Савостьяненко М. В. Світова практика фінансування захисту критичної інфраструктури. *Наукові праці НДФІ.* 2021. № 3. С.58-82.
3. UN Office for Disaster Risk Reduction. Making Critical Infrastructure Resilient. Ensuring Continuity of Service Police and Regulations in Europe and Central Asia. 2020. URL: https://www.google.com/search?q=mechanisms+and+tools+for+financial+support+of+critical+infrastructure+development&rlz=2C1BLWB_enUA0537UA0557&oq=mechanisms
4. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/ show/392/2020#Text.
5. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» Введено в дію Указом Президента України від 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text
6. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. Київ : НІСД, 2012. 57 с.
7. Бірюков Д. С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки.* 2015. № 3-4. С. 155-170.
8. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. мат. Міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2016. 176 с.
9. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналітична доповідь. Київ : НІСД, 2019.224 с.
10. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Серія: Економіка*. 2015. № 4. С.83–93.
11. Бобро Д. Г. Методологія оцінки рівня критичності об'єктів інфраструктури. *Стратегічні пріоритети*. 2016. № 3. С. 77–86.
12. Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналітична записка. URL: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf
13. Брежнєв Є. В. Аналіз підходів до оцінки безпеки критичних інфраструктур в умовах невизначеності. *Системи обробки інформації*. 2011. Випуск 2. С.277-281.

14. Брежнєв Є. В. Ризик-аналіз множинних відмов в інстраструктурах. *Системи обробки інформації.* 2011. Випуск 5. С.261-264.
15. Брежнєв Є. В. Метод інтеграції результатів апріорного і апостеріорного аналізу безпеки критичних інфраструктур. *Системи обробки інформації.* 2012. Випуск 9. С.258-262.
16. Брежнєв Є. В. Метод диверсифікації оцінок безпеки критичних інфраструктур в умовах невизначеності. *Системи озброєння і військова техніка.* 2012. № 3. С.116-120.
17. Брежнєв Є. В. Розробка гібридного методу оцінки безпеки інфраструктур і об'єктів критичного застосування в умовах невизначеності. *Збірник наукових праць Харківського університету Повітряних Сил.* 2013. Випуск 3.
18. Брежнєв Є. В., Харченко В. С. Методологія забезпечення безпеки критичних інфраструктур в умовах невизначеності: концепція та принципи. *Радіоелектронні і комп'ютерні системи.* 2015. № 1. С25-32.
19. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. URL: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennyastiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html
20. Домбровська С. М., Шведун В. О. Безпека критичної інфраструктури в Україні: теоретико-прикладні засади державного управління: монографія Харків: НУЦЗУ. 2024. 227 с.
21. Єрменчук О. П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. *Науковий вісник ДДУВС*. 2017. № 3. С. 135-140.
22. 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.
23. Zaplatynskyi V., Uriadnikova I. Аналіз окремих елементів критичної інфраструктури на прикладі України. *Bezpieczenstwo w administracji i biznesie jako czynnik Europejskiej integracji i rozwoju* / Wyzsza Szkola Administracji i Biznesuim Eugeniusza Kwiatkowskiego w Gdyni, 2015. S. 414-438.
24. Кудряшов В. П. Критична інфраструктура та фінансова безпека. *Фінанси України*. 2021. № 2. С.7-25.
25. Кудряшов В. П. Формування критичної інфраструктури в Україні. *Фінанси України*. 2022. № 2. С.7-25.
26. Кудряшов В. П. Фінансування інфраструктури в період подолання наслідків війни. *Фінанси України*. 2022. № 4. С.46-66.
27. Lazari A. European Critical Infrastructure Protection. Springer, 2014. 154 p.
28. Lewis T. G. Critical infrastructure protection in homeland security: defending a networked nation. Willey and Sons, 2006. 486 p.
29. Montanari L., Querzoni L. Critical infrastructure protection: Threats, attacks and countermeasures. 2014. URL: http://wpage.unina.it/roberto.pietrantuono/deliverables/Tenace-Deliverable1.pdf
30. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D. Risk mitigation strategies for critical infrastructures based on graph centrality analysis. URL: https://www.sciencedirect.com/science/article/pii/ S1874548215000414
31. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії*. 2021. Випуск 3. С. 142-148.
32. Clausewitz C. On War. Princeton university press princeton, New Jersey. 1976. 30 p.
33. Warden J. Centers of gravity in military operations. Preliminary draft. Royal Swedish Defence College, 2004. 185 p.
34. Albert R., Barabasi A.-L. Statistical mechanics of complex networks. *Reviews of Modern Physics*. 2002. Vol. 74. P.47-97.
35. Бірюков Д. С. Концептуалізація захисту критичної інфраструктури в сучасних безпекових дослідженнях. *Гілея: науковий вісник»*. 2016. Випуск 108. С.231-234.

36. Rothschild E. What is Security? *Daedalus*. 1995. 124 (3). P.53–98.
37. Business and Security: Public–Private Sector Relationships in a New Security Environment / Edt. A. Bailes, I. Frommelt. Oxford University Press, 2004. 328 p.
38. Presidential Policy Directive – Critical Infrastructure Security and Resilience (2013). URL: https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf
39. Єрменчук О.П. Європейський досвід захисту критичної інфраструктури: правовий аналіз та перспективи впровадження в Україні. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2018. № 2. С.40-46.
40. Communication from the Commission on a European programme for critical infrastructure protection (2006), 1-10. URL: http://ccpic.mai.gov.ro/docs/COM2006%20786final.pdf
41. Клименко К. В., Савостьяненко М. В. Інноваційні інструменти фінансового захисту критичної інфраструктури. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/12/134-1.pdf
42. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року №287/2015. *Офіційний вісник України*. 2015. № 43. Ст. 1353.
43. Загорняк В.Б. Економіко-організаційне забезпечення управління промисловою безпекою праці на нафтогазовидобувних підприємствах: автореф. дис. на здобуття наукового ступеня канд. екон. наук: спец.: 08.00.04 – економіка та управління підприємствами (нафтова і газова промисловість). Івано-Франківськ, 2010. 23 с.
44. Мітюшкіна Х. С. Сучасні системи енергетичної безпеки в країнах світу. *Вісник Донецького національного університету. Сер.: економіка і право*. 2008. № 2. С.261-262.
45. Юспін О. В. Напрями оптимізації структури енергетичної галузі України в контексті економічної безпеки: автореф. дис. на здобуття наукового ступеня канд. екон. наук: спец.: 21.04.01 – економічна безпека держави. К., 2007. 20 с.
46. Шкаберін В.М. Державне регулювання забезпечення продовольчої безпеки в Україні: автореф. дис. на здобуття наукового ступеня кандидата наук з державного управління: спец.: 25.00.02 – механізми державного управління. Запоріжжя, 2006. 22 с.
47. Мішина І.Г. Економічна безпека в умовах ринкових трансформацій: автореф. дис. на здобуття наукового ступеня кандидата економічних наук: спец.: 08.00.01 – економічна теорія та історія економічної думки. Донецьк, 2007. 17 с.
48. Римська декларація з всесвітньої продовольчої безпеки. 1996. URL: https://www. fao. org/4/y1889r/ y1889r.htm
49. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. 2003. URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf
50. ЄС і НАТО представили рекомендації для захисту критичної інфраструктури. URL: https://www.eurointegration.com.ua/news/2023/06/29/7164693/
51. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. К.: НІСД, 2020. 28 с.
52. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики. *Стратегічні пріоритети.* 2016. Вип. 3. С. 62–75.
53. Critical infrastructure resilience strategy – Australian Government. URL: http://www.tisn.gov.au/
54. Lewis T., Darken R. Potholes and Detours in the Road to Critical Infrastructure Protection Policy. *Homeland security affairs*. 2005. Vol.1, Issue 2. URL: https://www.hsaj.org/articles/177

References

1. Manzhul, I. (2016) Concept and protection of critical infrastructure in the US, EU, Ukraine. *European political and law discourse*. Volume 3, Issue 2. P.132-138 [in Ukrainian].
2. Klymenko, K., Pavliuk, K., Savostianenko, M. World practice of financing the protection of critical infrastructure. *RFI Scientifi c Papers*. 3. P.58–82 [in Ukrainian].
3. UN Office for Disaster Risk Reduction (2020). Making Critical Infrastructure Resilient. Ensuring Continuity of Service Police and Regulations in Europe and Central Asia. URL:

https://www.google.com/search?q=mechanisms+and+tools+for+financial+support+of+critical+infrastructure+development&rlz=2C1BLWB_enUA0537UA0557&oq=mechanisms.

4. On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 «On the National Security Strategy of Ukraine»: Decree of the President of Ukraine of September 14, 2020 No. 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Tex
5. On the decision of the National Security and Defense Council of Ukraine dated December 30, 2021 «On the Strategy for Ensuring State Security» Entered into force by Decree of the President of Ukraine dated February 16, 2022 No. 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text
6. Biryukov, D., Kondratov, S. (2012). Critical Infrastructure Protection: Problems and Prospects for Implementation in Ukraine. Analytical Report. K.: NISS. 57 p. [in Ukrainian]
7. Biryukov, D. (2015). Protection of critical infrastructure in Ukraine: from scientific understanding to development of policy principles, Naukovo-informatsiinyi visnyk Akademii natsionalnoi bezpeky, vol. 3-4. P.155–170[in Ukrainian].
8. Green paper on critical infrastructure protection in Ukraine. Proceedings of International Expert Meetings (2016). K.: NISS. 176 p.[in Ukrainian]
9. Organizational and legal aspects of ensuring security and resilience of critical infrastructure of Ukraine (2019). Analytical report. K.: NISS. 224 p.[in Ukrainian].
10. Bobro, D. (2015). Definition of evaluation criteria and threats to critical infrastructure. *Strategic priorities. Series: Economics*. 4. P.83-93[in Ukrainian].
11. Bobro, D. (2016) Methodology of estimation of infrastructure objects criticality level. *Strategic priorities. Series: Economics*. 3. P.77–86[in Ukrainian].
12. Bobro, D. (2016). Improvement of the methodology of ranking critical infrastructure objects and their assignment to critical infrastructure: analytical note. URL: http://www.niss.gov.ua/ content/articles/files/krutuchna_infra-a7636.pdf[in Ukrainian].
13. Brezhnev, E. (2011). Analysis of approaches to assessing the safety of critical infrastructures under conditions of uncertainty. *Information Processing Systems*. Issue 2. P.277-281[in Ukrainian].
14. Brezhnev, E. (2011). Risk analysis of multiple failures in infrastructures. *Information processing systems*. Issue 5. P.261-264[in Ukrainian].
15. Brezhnev, E. (2012). Method of integrating the results of a priori and a posteriori analysis of the security of critical infrastructures. *Information processing systems*. Issue 9. P.258-262[in Ukrainian].
16. Brezhnev, E. (2012). Method of diversification of critical infrastructure safety assessments under conditions of uncertainty. *Weapons systems and military equipment*. 3. P.116-120[in Ukrainian].
17. Brezhnev, E. (2013). Development of a hybrid method for assessing the safety of infrastructures and critical applications under conditions of uncertainty. *Collection of scientific papers of the Kharkiv Air Force University*. Issue 3[in Ukrainian].
18. Brezhnev, E. Kharchenko, V. (2015). Methodology for ensuring the security of critical infrastructures in conditions of uncertainty: concept and principles. *Radioelectronic and computer systems*. 1. P.25-32[in Ukrainian].
19. Vergolyas O. Reforming the protection system and increasing the resilience of Ukraine's critical infrastructure in the context of current threats. URL: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennyastiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html
20. Dombrovska, S., Shvedun, V. (2024). Critical Infrastructure Security in Ukraine: Theoretical and Applied Principles of Public Administration: Monograph Kharkiv, NUCZU. 227 p.[in Ukrainian]
21. Yermenchuk, O. (2017). Normative legal regulation of activity in the protection of national critical infrastructure: analysis and coordination of US normative practice. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. vol 3. P.135-140[in Ukrainian].
22. Yermenchuk, O. (2018). Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine. Dniprop. derzh. un-t vnutr. sprav, Dnipro. 180 p.[in Ukrainian]

23. Zaplatynskyi, V., Uriadnikova, I. (2015). Analysis of individual elements of critical infrastructure on the example of Ukraine. *Bezpieczenstwo w administracji i biznesie jako czynnik Europejskiej integracji i rozwoju* / Wyzsza Szkola Administracji i Biznesuim Eugeniusza Kwiatkowskiego w Gdyni. P.414-438[in Ukrainian].
24. Kudrjashov, V. (2021). Critical infrastructure and financial security. *Finance of Ukraine*. 2. P. 7-25.[in Ukrainian].
25. Kudrjashov, V. (2022). Formation of critical infrastructure in Ukraine. *Finance of Ukraine*. 2. P.7-25.[in Ukrainian].
26. Kudrjashov, V. (2022). Financing of infrastructure during the period of overcoming the consequences of the war. Finances of Ukraine. 4. P.46-66[in Ukrainian].
27. Lazari, A. (2014). European Critical Infrastructure Protection. Springer. 154 p.
28. Lewis, T. (2006). Critical infrastructure protection in homeland security: defending a networked nation. Willey and Sons. 486 p.
29. Montanari, L., Querzoni, L. (2014). Critical infrastructure protection: Threats, attacks and countermeasures. URL: http://wpage.unina.it/roberto.pietrantuono/deliverables/Tenace-Deliverable1.pdf
30. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Gritzalis, D. (2015). Risk mitigation strategies for critical infrastructures based on graph centrality analysis. URL: https://www.sciencedirect.com/science/ article/pii/S1874548215000414
31. Franchuk, V., Pryhunov, P., Melnyk, S. (2021). Security of critical infrastructure facilities in Ukraine: organizational and regulatory problems and approaches. Social & Legal Studios. Issue 3. P.142-148
32. Clausewitz, C. (1976). On War. Princeton university press princeton, New Jersey. 30 p.
33. Warden, J. (2004). Centers of gravity in military operations. Preliminary draft. Royal Swedish Defence College. 185 p.
34. Albert, R., Barabasi, A.-L. (2002)/ Statistical mechanics of complex networks. *Reviews of Modern Physics*. Vol. 74. P.47-97.
35. Biryukov, D. (2016). Conceptualisation of the critical infrastructure protection within contemporary security studies. Collection of scientific works «Gilea: Scientific Bulletin». Vol.108. P. 231-234[in Ukrainian].
36. Rothschild, E. (1995). What is Security? *Daedalus*. 124. P.53–98.
37. Business and Security: Public–Private Sector Relationships in a New Security Environment (2004) / Edt. A. Bailes, I. Frommelt. Oxford University Press. 328 p.
38. Presidential Policy Directive – Critical Infrastructure Security and Resilience (2013). URL: https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf
39. Yermenchuk, O. (2018). European experience in critical infrastructure protection: legal analysis and prospects for implementation in Ukraine. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2. P.40-46[in Ukrainian].
40. Communication from the Commission on a European programme for critical infrastructure protection (2006). 1-10. URL: http://ccpic.mai.gov.ro/docs/COM2006%20786final.pdf
41. Klymenko, K., Savostyanenko, M. (2021). Innovative instruments of financial protection of critical infrastructure. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/12/134-1.pdf [in Ukrainian].
42. On the decision of the National Security and Defense Council of Ukraine of May 6, 2015 «On the National Security Strategy of Ukraine»: Decree of the President of Ukraine of May 26, 2015 No. 287/2015. Official Gazette of Ukraine. 2015. No. 43. Art. 1353. [in Ukrainian].
43. Zagornyak, V. (2010). Economic and organizational support for industrial safety management at oil and gas production enterprises: author's abstract of dissertation for the degree of candidate of economic sciences: specialty: 08.00.04 - economics and management of enterprises (oil and gas industry). Ivano-Frankivsk, 23 p. [in Ukrainian].
44. Mityushkina, Kh. Modern energy security systems in countries around the world. *Bulletin of Donetsk National University. Ser.: Economics and Law*. 2008. No.2. P.261-262[in Ukrainian].

45. Yuspin, O. (2007). Directions for optimizing the structure of the energy industry of Ukraine in the context of economic security: author's abstract. dissertation for the degree of candidate of economic sciences: special: 21.04.01 – economic security of the state. Kyiv, 2007. 20 p. [in Ukrainian].
46. Shkaberin, V. (2006). State regulation of food security in Ukraine: author's abstract of the dissertation for the degree of candidate of sciences in public administration: speciality: 25.00.02 – mechanisms of public administration. Zaporizhzhia. 22 p. [in Ukrainian].
47. Mishina, I. (2007) Economic security in the context of market transformations: author's abstract. dissertation for the degree of candidate of economic sciences: speciality: 08.00.01 – economic theory and history of economic thought. Donetsk, 17 p. [in Ukrainian].
48. The Rome Declaration on World Food Security. 1996. URL: https://www. fao org/4/y1889r/y1889r.htm
49. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (2003). URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf
50. EU and NATO presented recommendations for the protection of critical infrastructure (2023). URL: https://www.eurointegration.com.ua/news/2023/06/29/7164693/[in Ukrainian].
51. The State Critical Infrastructure Protection System in the National Security System: Analytical Supplement (2020) / edited by O. M. Sukhodoli. Kyiv: NISD. 28 p. [in Ukrainian].
52. Sukhodolia, O. (2016). Protection of critical infrastructure in conditions of hybrid warfare: problems and priorities of the state policy of Ukraine. *Strategic priorities*. 3. 62-76[in Ukrainian].
53. Critical infrastructure resilience strategy – Australian Government (2023). URL: http://www.tisn.gov.au/
54. Lewis, T., Darken, R. (2005). Potholes and Detours in the Road to Critical Infrastructure Protection Policy. *Homeland security affairs*. Vol.1, Issue 2. URL: https://www.hsaj.org/articles/177

Отримано:	*23.12.2024*	*Beérkezett:*	*2024.12.23*	*Received:*	*23.12.2024*
Прийнято до друку:	*01.03.2025*	*Elfogadva:*	*2025.03.01*	*Accepted:*	*01.03.2025*
Опубліковано:	*12.05.2025*	*Megjelent:*	*2025.05.12*	*Published:*	*12.05.2025*