УДК 300.332

Лойко В. В.
доктор економічних наук, доцент,
Київський університет імені Бориса Грінченка, Україна;
e-mail: v.loiko@kubg.edu.ua; ORCID ID: 0000-0003-3248-1585
Храпкіна В. В.
доктор економічних наук, професор,
Національний університет «Києво-Могилянська академія», Україна;
e-mail: valentina_31@i.ua; ORCID ID: 0000-0003-3431-4369
Маляр С. А.
аспірант кафедри фінансів та економіки,
Київський університет імені Бориса Грінченка, Україна;
e-mail: st.malyar@gmail.com; ORCID ID: 0000-0003-3136-853X
Руденко М. В.
аспірант кафедри менеджменту,
Чернігівський національний технологічний університет, Україна;
e-mail: mvrudenko@i.ua; ORCID ID: 0000-0003-3134-5354

ЕКОНОМІКО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. В умовах активного реформування сфери економіки України питання ідентифікації та економіко-правового забезпечення захисту критичної інфраструктури в національній економіці є актуальним і потребує додаткового дослідження. Узагальнено наявні підходи до визначення термінів «критична інфраструктура» та «об'єкти критичної інфраструктури» у наукових працях вітчизняних і зарубіжних учених та у вітчизняних і зарубіжних нормативно-правових актах. Виявлено прогалини у законах і підзаконних нормативно-правових актах України щодо ідентифікації та захисту критичної інфраструктури. Запропоновано класифікацію об'єктів критичної інфраструктури за певними класифікаційними ознаками. Проаналізовано динаміку виникнення надзвичайних ситуацій на території України за період 2015—2019 рр. та їхні наслідки для функціонування критичної інфраструктури. Виявлено тенденцію до зростання кількості надзвичайних ситуацій за рахунок природних явищ і зростання збитків, спричинених цими надзвичайними ситуаціями. Виявлено, що найбільші збитки за останні 10 років нанесено 2020 року медико-біологічною надзвичайною ситуацією, а саме пандемією, спричиненою корона вірусом COVID-19. Запропоновано авторське бачення концептуальних положень щодо захисту критичної інфраструктури. Обґрунтовано основні напрями вдосконалення державної політики щодо захисту критичної інфраструктури, серед яких виділено найбільш пріоритетні: комплексне вдосконалення нормативно-правової бази з питань забезпечення безпеки критичної інфраструктури; створення системи державного управління безпекою об'єктів критичної інфраструктури; розроблення критеріїв ідентифікації об'єктів критичної інфраструктури і складання кадастру цих об'єктів; налагодження партнерства між урядом та операторами інфраструктури на принципах співробітництва, довіри та розділеної відповідальності; розвиток державно-приватного партнерства у сфері забезпечення безпеки критичної інфраструктури та запобігання виникненню надзвичайних ситуацій; розвиток міжнародного співробітництва у сфері захисту критичної інфраструктури.

***Ключові слова*:** критична інфраструктура, життєдіяльність людини, потреби, захист, безпека, кібербезпека, надзвичайна ситуація, нормативно-правове забезпечення, економічні чинники, державна власність, приватна власність, державно-приватне партнерство, пандемія, COVID-19, моніторинг.

Формул: 0; рис.: 0; табл.: 4; бібл.: 20:

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

Loiko V.
Doctor of Economics, Associate Professor;
Boris Grinchenko Kyiv University, Ukraine;
e-mail: v.loiko@kubg.edu.ua; ORCID ID: 0000-0003-3248-1585
Khrapkina V.
Doctor of Economics, Professor,
NationalUniversity «Kiev-Mohyla Academy», Ukraine;
e-mail: valentina_31@i.ua; ORCID ID: 0000-0003-3431-4369
Maliar S.
Ph. D. student of the Department of Finance and Economics,
Boris Grinchenko Kyiv University, Ukraine;
e-mail: st.malyar@gmail.com; ORCID ID: 0000-0003-3136-853X
Rudenko M.
Ph. D. student of the Department of Management,
Chernihiv National Technological University, Ukraine;
e-mail: mvrudenko@i.ua; ORCID ID: 0000-0003-3134-5354

ECONOMIC AND LEGAL PRINCIPLES FOR PROTECTING CRITICAL INFRASTRUCTURE PROTECTION

Abstract. In the context of active reform of the economy of Ukraine, the issue of identification and economic and legal support for the protection of critical infrastructure in the national economy is relevant and needs further study. The existing approaches to the definition of the terms «critical infrastructure» and «critical infrastructure objects» in the scientific works of foreign and domestic scientists and in the regulatory documents of Ukraine and other countries are summarized. Gaps in the laws and bylaws of Ukraine on the identification and protection of critical infrastructure have been identified. The classification of critical infrastructure objects according to certain classification features is offered. The dynamics of emergencies on the territory of Ukraine for the period 2015—2019 and their consequences for the functioning of critical infrastructure are analyzed. There is a tendency to increase the number of emergencies due to natural phenomena and increase the damage caused by these emergencies. It was found that the greatest damage in the last 10 years was caused in 2020 by a medical and biological emergency, namely the pandemic caused by the coronavirus COVID-19. The author's vision of conceptual provisions on critical infrastructure protection is offered. The main directions of improvement of the state policy on protection of critical infrastructure are substantiated, among which the most priority ones are singled out: complex improvement of the normative-legal base on the issues of ensuring the safety of critical infrastructure; creation of a system of state management of critical infrastructure safety; development of criteria for identification of critical infrastructure objects and compilation of inventory of these objects; establishing a partnership between the government and infrastructure operators on the principles of cooperation, trust and shared responsibility; development of public-private partnership in the field of security of critical infrastructure and prevention of emergencies; development of international cooperation in the field of critical infrastructure protection.

***Keywords*:** critical infrastructure, human life, needs, protection, security, cybersecurity, emergency, regulatory support, economic factors, state property, private property, public-private partnership, pandemic, COVID-19, monitoring.

Formulas: 0; fig.: 0; tabl.: 4; bibl.: 20.

Вступ. Дієвий механізм функціонування і захисту критичної інфраструктури є одним із ключових елементів системи забезпечення національної безпеки в усіх країнах світу. Саме тому останнім часом зросла увага науковців до питань визначення, розвитку, розроблення і вдосконалення нормативно-правової бази щодо функціонування та захисту критичної інфраструктури. Підходи до віднесення тих чи інших об'єктів до числа критичної інфраструктури в різних країнах світу відрізняються. Здебільшого під цим поняттям

розуміють системи життєзабезпечення населення, до яких, зокрема, належать тепло- і водопостачання, утилізація відходів, екстрена допомога, електромережі, телекомунікації, мережа «Інтернет», транспорт, фінансова система, служби реагування на надзвичайні ситуації. Захист критичної інфраструктури стає дедалі пріоритетнішим у забезпеченні національної безпеки ще і тому, що збільшуються загрози через кліматичні зміни, терористичні акти і кібератаки. Поширення пандемії коронавірусної хвороби COVID-19, яка не оминула практично жодну країну світу, також сприяло приверненню уваги науковців багатьох розвинутих країн і усього суспільства загалом до проблеми захисту та ефективного управління критичною інфраструктурою. В Україні питанню захисту критичної інфраструктури тільки починають приділяти увагу. Верховна рада України, на жаль, до цього часу не ухвалила профільне законодавство про захист критичної інфраструктури. На законодавчому рівні практично не закріплено, які об'єкти є складовими елементами критичної інфраструктури, порядок їх ідентифікації, особливості управління ними, обмеження при їх використанні, у чиїй власності ці об'єкти можуть перебувати, який рівень втручання держави у ці правовідносини має відбуватися тощо. Саме тому доцільно провести дослідження щодо повноти формування нормативно-правової бази з метою забезпечення сталого і ефективного функціонування критичної інфраструктури, без чого не можна досягти економічної безпеки у країні.

Аналіз досліджень і постановка завдання. Питанню забезпечення безпеки окремих елементів критичної інфраструктури приділялася увага у працях таких українських і зарубіжних учених: Д. С. Бірюков і С. І. Кондратов («Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні») [1]; Д. С. Бірюков («Захист критичної інфраструктури в Україні: наукового осмислення до розробки засад політики») [2]; Д. С. Бірюков і С. І. Кондратов («Зелена книга з питань захисту критичної інфраструктури в Україні») [3], В. Заплатинський, І. Урядникова («Анализ отдельных элементов критической инфраструктуры на примере Украины») [4]; Д. Г. Бобра, С. П. Іванюти, С. І. Кондратова і Суходолі О. М. («Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України») [5]; G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis («Risk mitigation strategies for critical infrastructures based on graph centrality analysis») [6] та інших.

Метою статті є узагальнення економіко-правових засад забезпечення захисту критичної інфраструктури в Україні та представлення авторського бачення концептуальних положень щодо захисту критичної інфраструктури. Досягнення цієї мети здійснено шляхом вирішення **завдань** щодо аналізу понять «критична інфраструктура» та «об'єкти критичної інфраструктури» у наукових працях учених і нормативно-правових актах України й інших країн світу, проведення комплексного аналізу динаміки виникнення надзвичайних ситуацій на території України за період 2015—2019 рр. і розроблення авторських концептуальних положень щодо надання захисту критичної інфраструктури в сучасних умовах господарювання.

Результати дослідження. Україна перебуває на початковому етапі формування системи захисту критичної інфраструктури. Уряди і науковці США, Австралії, країн Європейського Союзу провели дослідження і напрацювали певний досвід щодо критичної інфраструктури, її сталості та захисту. У США, Австралії та країнах ЄС ухвалено окремі закони, які стосуються ідентифікації об'єктів критичної інфраструктури і забезпечення їхнього захисту. В Україні немає закону, який би визначав порядок віднесення тих чи інших об'єктів до числа критичної інфраструктури і регулював би правила поводження з нею. У різних законодавчих актах України трапляються окремі положення щодо критичної інфраструктури, проте відсутній системний підхід на національному рівні до врегулювання питань управління захистом об'єктів критичної інфраструктури та взаємодії держави і власників або операторів цих об'єктів. Так, у Законі України «Про основні засади здійснення кібербезпеки України» наведено визначення критичної інформаційної інфраструктури, критично важливих об'єктів інфраструктури та об'єктів критичної

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

інформаційної інфраструктури [7]. Визначено, що критична інфраструктура є об'єктом кіберзахисту і коло осіб, відповідальних за безпечне функціонування. У статті 6 цього закону перелічено групи підприємств, установ та організацій, які можуть бути віднесені до числа критичної інфраструктури. Водночас відповідний закон визначає правові та організаційні основи забезпечення захисту інтересів держави і суспільства саме в кіберпросторі, чим і обмежується сфера його застосування.

Зважаючи на те, що захист критичної інфраструктури належить до національної безпеки, не можна механічно застосовувати методи ідентифікації і засоби захисту критичної інфраструктури інших країн. При формуванні національної системи захисту критичної інфраструктури доцільно розробити власну систему і критерії ідентифікації об'єктів критичної інфраструктури, цілі, механізми та інструменти системи захисту критичної інфраструктури з урахуванням реалій розвитку української економіки.

В офіційних нормативно-правових актах України термін «критична інформаційна інфраструктура» уперше використано в тексті «Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства» [8]. У Стратегії національної безпеки «Україна у світі, що змінюється» використано термін «критична інфраструктура паливно-енергетичного комплексу» у пропозиції створення дієвого захисту від еколого-техногенних впливів та зловмисних дій [9]. У новій Стратегії національної безпеки України (2015) термін «критична інфраструктура» (пункт 3.8) присвячено «загрозам безпеці критичної інфраструктури», вказано на «недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій», проте немає визначення, що саме віднесено до критичної інфраструктури [10].

Узагальнення наявних підходів до визначення терміна «критична інфраструктура» у наукових працях вітчизняних науковців (*табл. 1*) дозволило зробити такі висновки.

Таблиця 1

Результати узагальнення наявних підходів до визначення термінів «критична інфраструктура» та «об'єкти критичної інфраструктури» вітчизняними авторами

Автор (джерело)	Визначення
Бірюков Д. С., Кондратов С. І. [1, с. 3]	До критичної інфраструктури зазвичай належать транспортні й енергетичні мережі, системи міжбанківських розрахунків і телекомунікації, а також об'єкти, необхідні для функціонування органів державної влади, служби реагування на надзвичайні ситуації та екстреної допомоги населенню, системи життєзабезпечення мегаполісів.
Бірюков Д. С. [2, с. 155-156]	Терміном «критична інфраструктура», зазвичай, охоплюються ті об'єкти, порушення функціонування або руйнування яких призведе до найсерйозніших наслідків для соціальної та економічної сфер держави, негативно вплине на рівень її обороноздатності та національної безпеки, а також підтримування життєво важливих функцій у суспільстві. Як правило, до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади.
Зелена книга з питань захисту критичної інфраструктури в Україні [3, с. 15]	Критична інфраструктура України — це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.
В. Заплатинський, І. Урядникова [4]	Фізичні та віртуальні системи, об'єкти і ресурси — руйнування, знищення або зниження дієздатності яких призведе до суттєвих загроз країні (регіону або місту), національній безпеці держави, безпеці і здоров'ю населення.
Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. [5, с. 220]	Критична інфраструктура — системи, мережі, об'єкти, ресурси (як фізичні, так і віртуальні чи інформаційні), які забезпечують реалізацію життєво важливих функцій та послуг і мають настільки велике значення, що їх знищення, пошкодження або виведення з ладу призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку країни, обороноздатності держави та забезпечення національної безпеки.

Закінчення табл. 1

Автор (джерело)	Визначення
Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M. and Gritzalis, D. [6]	Інфраструктури, які викликають каскадні відмови (наприклад, енергетична та інформаційна та комунікаційна інфраструктури). Вплив кожної залежності слід розглядати разом з положенням кожної критичної інфраструктури в мережі взаємозалежних критичних інфраструктур.
Щодо створення державної системи захисту критичної інфраструктури [11]	Критична інфраструктура – об'єкти, системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку, обороноздатності держави та забезпечення національної безпеки.
Закон України «Про основні засади здійснення кібербезпеки України» [7]	До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які: 1) провадять діяльність і надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; 2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; 3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; 4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; 5) є об'єктами потенційно небезпечних технологій і виробництв.

Примітка. Складено авторами.

До критичної інфраструктури як матеріальні об'єкти автори відносять:

— транспортні й енергетичні мережі, системи міжбанківських розрахунків і телекомунікації, а також об'єкти, потрібні для функціонування органів державної влади [1];

— енергетичні та транспортні магістральні мережі, нафто- і газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізації відходів, підприємства військово-промислового комплексу, центральні органи влади [2];

— системи, мережі, об'єкти, ресурсифізичні чи віртуальні [4; 5; 10];

— інфраструктури, які викликають каскадні відмови [6];

— підприємства, установи та організації [11].

Попри, що підходи до питання віднесення матеріальних об'єктів до числа критичної інфраструктури в різних авторів різняться, усі вони зазначають, що основною ознакою, за якою вказані матеріальні об'єкти потрібно віднести саме до критичної інфраструктури, є те, що їхнє пошкодження, виведення із роботи або знищення буде мати негативні або катастрофічні наслідки для забезпечення національної безпеки та обороноздатності країни, життєдіяльності населення, соціально-економічного розвитку. Доцільно проаналізувати визначення поняття «критична інфраструктура», які наведено в офіційних нормативно-правових актах інших країн (*табл. 2*).

Таблиця 2

Сучасні підходи до визначення сутності поняття «критична інфраструктура» у нормативних документах інших країн

Автор (джерело), країна	Визначення
Закон США (USA PATRIOT ACT, 2001), США [12]	Критична інфраструктура означає системи та ресурси, фізичні або віртуальні, що є надзвичайно важливими для Сполучених Штатів, а недієздатність або знищення таких систем та активів матиме катастрофічний регіональний чи національний вплив на здоров'я населення або безпеку, економічну безпеку або національну безпеку, в т. ч. бази даних для реєстрації виборців, машини для голосування та інші системи зв'язку, які керують виборчим процесом, а також представляють і публікують результати від імені державних та місцевих органів влади.
Defending American Security from Kremlin Aggression Act of 2018. США [13]	Критична інфраструктура — системи та засоби, фізичні чи віртуальні, настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів підривало би національну безпеку, національну економіку, загрожувало би здоров'ю чи безпеці населення, чи мало би результатом будь-яку комбінацію із переліченого.

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

Закінчення табл. 2

Автор (джерело), країна	Визначення
Директива Ради ЄС [14]	Актив, система або її частина, які мають важливе значення для підтримки життєво важливих функцій суспільства, здоров'я, безпеки. Пошкодження критичної інфраструктури, її руйнування або порушення в результаті стихійних лих, тероризму, злочинної діяльності або зловмисного поведінки може істотно негативно вплинути на безпеку ЄС і добробут громадян.
National Strategy for Critical Infrastructure Protection. Німеччина [15]	До критичної інфраструктури належать організаційні та фізичні структури і об'єкти настільки життєво важливі для суспільства та економіки країни, що їх вихід з ладу або погіршення функціонування будуть мати своїм результатом стійкі зриви постачання, значний підрив державної безпеки або інші драматичні наслідки.
Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.Велика Британія [16]	Елементами критичної інфраструктури є ті установки, системи, об'єкти й мережі, необхідні для функціонування країни та надання важливих послуг, від яких залежить повсякденне життя Великої Британії.
Zakon o privatnoj zaštiti: zakon HR. Хорватія [17]	Критична інфраструктура — діяльність, мережі, послуги, матеріальні блага й інформаційні технології, вихід з ладу або знищення яких значно вплинуло б на здоров'я та безпеку громадян або на діяльність державної влади.
Critical Infrastructure Reliance Strategy: Policy Австралія [18]	Критична інфраструктура лежить в основі надання основних послуг, таких як енергетика, вода, охорона здоров'я, комунікаційні системи та банківська справа.

Примітка. Складено авторами.

У нормативно-правових документах інших країн також підкреслюється важливість критичної інфраструктури саме в тому, що до об'єктів критичної інфраструктури віднесено матеріальні і віртуальні системи, об'єкти, мережі, установки, організаційні і фізичні структури, навіть послуги, руйнування, пошкодження або знищення яких може мати важкі наслідки для життєзабезпечення населення країни, безпеки громадян і держави, діяльності державної влади.

На основі проведеного аналізу наявних визначень поняття «критична інфраструктура» і з позиції захисту національних інтересів пропонуємо таке визначення. Критична інфраструктура — це сукупність об'єктів, систем, мереж, послуг, які є стратегічно важливими для економіки та безпеки країни, суспільства, населення і пошкодження, знищення або порушення діяльності яких може завдати шкоди життєво важливим інтересам України.

Проаналізувавши закони та підзаконні нормативно-правові акти України щодо захисту критичної інфраструктури виявлено таке:

- відсутність державного профільного закону про критичну інфраструктуру, забезпечення її стійкості та захисту, який би визначив правові та організаційні основи забезпечення захисту критичної інфраструктури, основні цілі, напрями та принципи державної політики у сфері захисту критичної інфраструктури України, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності;
- відсутність критеріїв і процедур віднесення об'єктів до критичної інфраструктури та порядку їх ідентифікації і паспортизації;
- відсутність реєстру об'єктів критичної інфраструктури та їхніх паспортів;
- відсутність державного органу, який на національному рівні відповідав би за захист критичної інфраструктури і розподіл обов'язків між державою та її власниками чи операторами;
- невизначеність функцій органів державної влади та місцевого самоврядування, прав і обов'язків власників та операторів критичної інфраструктури щодо її захисту;

- відсутність механізму попередження виникненню кризових ситуацій, які пов'язані з функціонуванням критичної інфраструктури;
- відсутність єдиної методології оцінки ризиків і загроз економічній безпеці критичній інфраструктурі;
- неналагоджений збір та обробка інформації щодо стану критичної інфраструктури;
- неналагодженість активного міжнародного співробітництва щодо захисту критичної інфраструктури

Останні події в Україні та світі показують, що все частіше саме надзвичайні ситуації негативно впливають на стале функціонування критичної інфраструктури. Серед актуальних прикладів варто виділити медико-біологічну надзвичайну ситуацією — пандемію коронавірусної хвороби (COVID-19), спричинену SARS-CoV-2, повені на Закарпатті, пожежі в Чорнобильській зоні відчудження, масові пожежі в Австралії, вибух і пожежу в м. Бейруті, лісові пожежі в заповіднику Анджелес у США тощо.

Саме тому процес ідентифікації об'єктів критичної інфраструктури або їхніх окремих елементів має включати аналіз за певними класифікаційними ознаками (*табл. 3*) та оцінку наслідків можливого припинення їх функціонування в разі виникнення аварії або надзвичайної ситуації.

Таблиця 3

Класифікація об'єктів критичної інфраструктури за виділеними класифікаційними ознаками

Класифікаційна ознака	Види
За ієрархічним рівнем управління (для окремої країни)	Національна, регіональна, локальна, об'єктна
За формою власності	Об'єкти національної критичної інфраструктури (тільки державна власність); об'єкти регіональної та локальної критичної інфраструктури (державна, комунальна, приватна власність)
За масштабом (географічне охоплення території внаслідок аварії або втрати елементу критичної інфраструктури)	Глобальний, міжнародний, національний, регіональний, локальний, об'єктний
За тяжкістю можливих наслідків за показниками	Економічні наслідки: розмір прямих і непрямих економічних втрат (частини ВВП, частки ринку, кількості робочих місць, податкових надходжень у бюджет, значні витрати на підсилення роботи аварійно-рятувальних служб та екстреної допомоги населенню). Соціальні втрати: порушення безпеки життєдіяльності та здоров'я населення (кількість загиблих і постраждалих, кількість евакуйованого і переселеного населення, кількість населення, яке потерпає від порушення умов життєзабезпечення). Безпека держави: втрата авторитету держави, порушення управління державою, зниження обороноздатності. Екологічні наслідки: екологічні аварії та катастрофи, які чинять негативний вплив на навколишнє природне середовище
За тривалістю відновлення після негативного впливу на об'єкти критичної інфраструктури	Довготривале, середньотривале і швидкотривале відновлення об'єктів критичної інфраструктури від наслідків негативного впливу на об'єкти критичної інфраструктури
За вразливістю об'єкта до впливу небезпечних чинників	Висока, середня і низька ступінь вразливості об'єкта критичної інфраструктури до впливу небезпечних чинників
За термінами відновлення роботи	Для національної критичної інфраструктури: до шести годин. Для регіональної критичної інфраструктури: до 12 годин. Для локальної та об'єктної критичної інфраструктури: до 24-х годин.

Примітка. Запропоновано авторами.

Через те, що для об'єктів критичної інфраструктури важлива стабільність їхнього фізичного існування і надійне функціонування, доцільно виділити такі види ризиків і загроз, вплив яких може нанести значні збитки на різних ієрархічних рівнях і на які потрібно звертати увагу при розробленні заходів захисту об'єктів критичної інфраструктури.

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

До першої групи загроз доцільно віднести загрози і ризики, пов'язані з небезпечними природними явищами (повені, урагани, пожежі, землетруси, зсуви, цунамі, космічні явища, пандемії та епідемії).

До другої групи загроз віднесено загрози і ризики, які можуть викликати аварії техногенного характеру (різного роду аварії та відмови обладнання і систем, аварії в системах енергозабезпечення, водо- і теплопостачання тощо).

До третьої групи загроз доцільно віднести загрози та ризики, пов'язані з соціальними діями (терористична та злочинна діяльність, кібератаки, політичні події тощо).

Реалізація ризиків і загроз може призвести до виникнення надзвичайних ситуацій, унаслідок яких відбувається загибель або травмування людей і завдаються матеріальні збитки об'єктам інфраструктури. Аналіз динаміки надзвичайних ситуацій в Україні (*табл. 4*), проведений на підставі статистичних даних Державної служби України з надзвичайних ситуацій [19], дозволив зробити такі висновки.

Таблиця 4

Динаміка виникнення надзвичайних ситуацій (НС) на території України за період 2015—2019 рр.

Назва показника	Роки					Відхилення даних 2019 від даних 2015, %
	2015	2016	2017	2018	2019	
Загальна кількість надзвичайних ситуацій	148	149	166	128	146	- 1,35
У тому числі: - техногенного характеру	63	56	50	48	60	- 4,76
питома вага НС техногенного характеру у загальній кількості НС, %	42,57	37,58	30,12	37,50	41,10	- 3,45
- природного характеру	77	89	107	77	81	5,19
питома вага НС природного характеру в загальній кількості НС, %	52,03	59,73	64,46	60,16	55,48	6,63
- соціального характеру	8	4	9	3	5	- 37,5
питома вага НС соціального характеру в загальній кількості НС, %	5,40	2,69	5,42	2,34	3,42	- 36,67
У тому числі: - державного рівня	2	1	2	2	2	-
- регіонального рівня	9	9	8	6	7	- 22,22
- місцевого рівня	62	64	69	64	63	1,61
- об'єктового рівня	75	75	87	56	74	- 1,33
питома вага НС об'єктового рівня в загальній кількості НС, %	50,68	50,34	52,41	43,75	50,68	-
Загинуло людей унаслідок надзвичайної ситуації, осіб	243	183	172	168	199	- 18,11
Постраждало людей унаслідок надзвичайної ситуації, осіб	962	1856	892	839	1492	55,09
Прямі матеріальні збитки внаслідок виникнення надзвичайної ситуації, тис. грн	5 632 723	265 306	896 804	496 965	685 269	28,64
Втрати ВВП від матеріальних збитків унаслідок виникнення НС, %	0,35	0,01	0,04	0,01	0,02	- 94,29

Примітка. Складено авторами.

Загальна кількість надзвичайних ситуацій на території України за період 2015—2019 років зменшилась на 1,35 % і 2019 року становила 146 випадків. Динаміка у структурі надзвичайних ситуацій за досліджуваний період є такою: НС техногенного характеру зменшилось на 4,76 %, НС природного характеру зросло на 5,19 %, НС соціального характеру зменшилось на 37,5%. Найбільшу питому вагу у структурі надзвичайних ситуацій мають ситуації природного характеру, зокрема 2019 року їхня питома вага становила 55,48 % у загальній кількості НС. Динаміка виникнення надзвичайних ситуацій за ієрархічними

рівнями є такою: кількість НС державного рівня не змінилась за досліджуваний період і становила тільки два НС за рік, кількість НС регіонального рівня зменшилась на 22,22%, кількість НС місцевого рівня зросла на 1,61 %, кількість НС об'єктового рівня зменшилась на 1,31 %. Найбільшу питому вагу мають надзвичайні ситуації об'єктового рівня (2019 р. – 50,68 %). Динаміка кількості людей, які загинули внаслідок виникнення надзвичайної ситуації, за досліджуваний період має позитивний характер до зниження на 18,11 %. Проте кількість людей, що постраждали внаслідок виникнення надзвичайної ситуації, за період 2015—2019 рр. зросла на 55,09 %. Сума прямих матеріальних збитків унаслідок виникнення надзвичайної ситуації зросла на 28,64 %. Динаміка втрат ВВП від виникнення надзвичайної ситуації за досліджуваний період поліппшилась, а саме зменшилась на 94,29 %. Втрати ВВП від виникнення НС у 2019 року становили 0,01 % (і це з урахуванням тільки прямих матеріальних збитків). Реальні втрати ВВП від виникнення надзвичайної ситуації значно більші через синергетичний ефект виникнення втрат у різних суміжних сферах економіки.

Проведений аналіз виникнення надзвичайних ситуацій показав, що значного коливання їхньої кількості протягом п'яти останніх років не спостерігалося. У кількісному вимірі аналогічна тенденція виникнення надзвичайних ситуацій в Україні спостерігається й у тривалішому періоді аналізу — 10 років. Проте рівень ризиків і втрат від виникнення надзвичайних ситуацій в Україні не зменшується. За статистичними даними Державної служби України з надзвичайних ситуацій, станом на 01.07.2020 в Україні внаслідок виникнення надзвичайних ситуацій загинуло 1 241 людина і постраждало 43 873 особи, що відповідно, в 11,78 раза та 52,5 рази перевищує показник попереднього року за той самий період часу. Погіршення стану викликано медико-біологічною надзвичайною ситуацією, а саме пандемієюкоронавірусної хвороби (COVID-19).

Пріоритетним завданням національної безпеки із забезпечення захисту критичної інфраструктури є запобігання або попередження виникнення ризиків і загроз, які можуть викликати значні ушкодження різних видів інфраструктури та завдати значних збитків. Проблемою у виконанні цього завдання є складність у визначенні, які саме активи в національній і регіональній економіці, на рівні кожного окремого підприємства або навіть на рівні житлово-комунальної інфраструктури визнавати критичними. Перевіреного методу для ідентифікації критичних ресурсів інфраструктури, на жаль, не існує до сьогодні. Законом США щодо протидії тероризму [13] визначено, що для забезпечення національної безпеки пріоритетними є дії щодо попередження терористичних актів на об'єктах інфраструктури, зриви в роботі яких можуть мати виснажливий вплив на національну економічну безпеку, національну охорону здоров'я і безпеку навколишнього середовища або будь-яка їхня комбінація. Наслідки руйнівних впливів на критичну інфраструктуру можуть виникати далеко за межами її географічно-територіального розміщення і відчуватися протягом тривалого часу [20]. Беручи до уваги актуальні соціально-політичні події на території України, зростання небезпеки від терористичних загроз та збройну агресію на Сході, доцільно розглядати досвід та нормативно правові акти США як такі, що можуть частково бути використані для врегулювання відповідних питань в Україні.

Для запобігання виникненню надзвичайних ситуацій та аварій на об'єктах критичної інфраструктури доцільно запропонувати такі заходи:

– паспортизацію об'єктів критичної інфраструктури;

– моніторинг фізичного стану об'єктів критичної інфраструктури;

– діагностику ризиків і загроз;

– розроблення і постійне вдосконалення плану реагування на загрози;

– розроблення заходів щодо швидкого ремонту і відновлення функціонування об'єктів критичної інфраструктури в разі надзвичайних ситуацій, яким не можна запобігти.

За результатами проведених досліджень економіко-правової бази щодо захисту критичної інфраструктури в Україні доцільно запропонувати удосконалення державної політики за такими напрямами:

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

– комплексне вдосконалення нормативно-правової бази з питань забезпечення безпеки критичної інфраструктури;

– створення системи державного управління безпекою об'єктів критичної інфраструктури;

– розроблення та впровадження механізмів збору, накопичення та обробки інформації щодо стану об'єктів критичної інфраструктури;

– розроблення критеріїв ідентифікації об'єктів критичної інфраструктури та складання кадастру цих об'єктів;

– профілактика виникнення техногенних аварій на об'єктах критичної інфраструктури та мінімізація їх наслідків;

– розроблення заходів щодо підвищення рівня самозахисту, самопомочі, власних можливостей громадян та організацій, уразливих до погіршення або припинення послуг, які надає критична інфраструктура;

– посилення охорони об'єктів критичної інфраструктури, особливо енергетичної і транспортної галузей;

– налагодження партнерства між урядом та операторами інфраструктури на принципах співробітництва, довіри та розділеної відповідальності;

– розвиток державно-приватного партнерства у сфері забезпечення безпеки критичної інфраструктури і запобігання виникненню надзвичайних ситуацій;

– розвиток міжнародного співробітництва у сфері захисту критичної інфраструктури.

Україна перебуває в суворих фінансово-економічних і безпекових умовах, що зумовлює потребу виокремити більш пріоритетні об'єкти критичної інфраструктури для невідкладного забезпечення їхнього захисту, спираючись на наявні ресурси і потреби захисту національних інтересів, розвитку економіки та підтримання умов безпечного існування населення.

Висновки. Ураховуючи гіперзв'язок основних ресурсів критичної інфраструктури, що ускладнюється цифровою системою трансформації, потрібна всебічна державна політика для посилення стійкості критичної інфраструктури. Для забезпечення безпеки критичної інфраструктури доцільно розробляти і впроваджувати заходи щодо обмеження ризиків збоїв у роботі основних служб і збільшення здатності швидкого відновлення після аварій. Потрібне коригування державної політики щодо посилення стійкості критичної інфраструктури. Аналіз законів і підзаконних нормативно-правових актів, що регулюють правила поводження з критичною інфраструктурою, і сучасний стан її захищеності в Україні та інших країнах світу, свідчить про те, що для ефективного подолання складностей і взаємозалежностей в критичній інфраструктурі, найкращим є узгоджений системний підхід. Для більшого обміну інформацією та ефективного спрямування інвестицій доцільно налагодити партнерство міжурядом та власниками і операторами інфраструктури на принципах співробітництва, довіри та розподілу відповідальності. Ураховуючи унікальність системи забезпечення національної безпеки для кожної країни, для забезпечення безпеки критичної інфраструктури України недостатньо механічно копіювати зарубіжний досвід щодо захисту критичної інфраструктури, потрібно розробляти і впроваджувати власні заходи.

Література

1. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні : аналітична доповідь. Київ : НІСД, 2012. 57 с.
2. 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.
3. 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, 2015. 176 с.
4. Zaplatynskyi V., Uriadnikova I. Анализ отдельных элементов критической инфраструктуры на примере Украины. *Bezpieczenstwo w administracji i biznesie jako czynnik Europejskiej integracji i rozwoju* / Wyzsza Szkola Administracji i Biznesuim Eugeniusza Kwiatkowskiego w Gdyni, 2015. S. 414—438.
5. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналітична доповідь / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] ; за заг. ред. О. М. Суходолі. Київ : НІСД, 2019. 224 с.

6. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Gritzalis, D. Risk mitigation strategies for critical infrastructures based on graph centrality analysis. *International Journal of Critical Infrastructure Protection.* 2015. Vol. 10. P. 34—44.
7. Про основні засади забезпечення кібербезпеки України : Закон України № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.
8. Рекомендації парламентських слухань з питання розвитку інформаційного суспільства : Постанова Верховної Ради України № 3175-IV. *Відомості Верховної Ради України*. 2006. № 15. Ст. 131. URL : https://zakon.rada.gov.ua/laws/show/3175-15#Text.
9. Про Стратегію національної безпеки України «У світі, що змінюється» : Указ Президента України № 389 від 08.06.2012. Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/105/2007#Text.
10. Про стратегію національної безпеки : Указ Президента України № 287/2015 від 26.05.2015. Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/287/2015#Text.
11. Щодо створення державної системи захисту критичної інфраструктури : аналітична записка. 2017. URL : https://niss.gov.ua/sites/default/files/2017-02/infrastrukt-86de2.pdf.
12. U.S. Government. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT). Act of 2001. Public Law 107-56. Washington, DC, 2001.
13. Defending American Security from Kremlin Aggression Act of 2018. *CONGRESS.GOV*. URL: https://www.congress.gov/bill/115th-congress/senate-bill/3336/text?q=%7B%22search%22%3A%5B% 22S.3336%22%5D%7D&r=1.
14. European Commission. Commission Staff Working Document on the Reviewof the European Programme for Critical Infrastructure Protection (EPCIP), SWD (2012) 190 Final. Brussels, Belgium, 2012.
15. National Strategy for Critical Infrastructure Protection. Federal Ministry of Interior. Germany. Berlin, 2009. June 17. URL : http://www.bmi.bund. de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf.
16. Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. UK Cabinet Office. 2010. March. URL : https://www.gov.uk.
17. Zakon o privatnoj zaštiti : zakon HR № 16/30. Republike Hrvatske. 2020. 22.02. URL: http://www.zakon.hr/z/291/Zakon-o-privatnoj-za%20titi.
18. Australian Government. Critical Infrastructure Reliance Strategy: Policy Statement. Barton, Australia, 2015. URL : http://www.tisn.gov.au.
19. Офіційний сайт Державної служби України з надзвичайних ситуацій. Інформаційно-аналітична довідка про виникнення надзвичайних ситуацій в Україні упродовж 2019 року. URL : https://www.dsns.gov.ua/ua/Dovidka-za-kvartal/103179.html.
20. OECD. Good Governance for Critical Infrastructure Resilience. *OECD Reviews of Risk Management Policies.* Paris, 2019. URL : https://www.oecd.org/science/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm.

Статтю рекомендовано до друку 02.12.2020.

References

1. Biriukov, D. S., & Kondratov, S. I. (2012). *Zakhyst krytychnoi infrastruktury: problemy ta perspektyvy vprovadzhennia v Ukraini [Protection of critical infrastructure: problems and prospects for implementation in Ukraine]*. Kyiv: NISD [in Ukrainian].
2. Biriukov, D. S. (2015). Zakhyst krytychnoi infrastruktury v Ukraini: vid naukovoho osmyslennia do rozrobky zasad polityky [Protection of critical infrastructure in Ukraine: from scientific understanding to the development of policy principles]. *Naukovo-informatsiinyi visnyk Akademii natsionalnoi bezpeky — Scientific and information bulletin of the Academy of National Security, 3—4*, 155—170 [in Ukrainian].
3. Sukhodolia, O. M. (Ed.). (2015). *Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini: zbirnyk materialiv Mizhnarodnykh ekspertnykh narad [Green Paper on Critical Infrastructure Protection in Ukraine: a collection of materials of International Expert Meetings]*. Compilers D. S. Biriukov, S. I. Kondratov. Kyiv: NISD [in Ukrainian].
4. Zaplatynskyi, V., & Uriadnikova, I. (2015). Analiz otdel'nyh elementov kriticheskoj infrastruktury na primere Ukrainy [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 Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni. S. 414—438 [in Russian].
5. Bobro, D. H., Ivaniuta, S. P., Kondratov, S. I., & Sukhodolia, O. M. (Eds.) (2019). *Orhanizatsiini ta pravovi aspekty zabezpechennia bezpeky i stiikosti krytychnoi infrastruktury Ukrainy [Organizational and legal aspects of security and stability of critical infrastructure of Ukraine]*. Kyiv: NISD [in Ukrainian].
6. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., & Gritzalis, D. (2015). Risk mitigation strategies for critical infrastructures based on graph centralityanalysis. *International Journal of Critical Infrastructure Protection*, *Vol. 10*, 34—44.
7. Verkhovna Rada Ukrainy. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy № 2163-VIII [On the basic principles of cybersecurity of Ukraine: Law of Ukraine № 2163-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 45*. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].
8. Verkhovna Rada Ukrainy. (2006). Rekomendatsii parlamentskykh slukhan z pytannia rozvytku informatsiinoho suspilstva: Postanova № 3175-IV [Recommendations of parliamentary hearings on the development of the information society: Resolution № 3175-IV]. *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 15*. Retrieved from https://zakon.rada.gov.ua/laws/show/3175-15#Text [in Ukrainian].
9. Verkhovna Rada Ukrainy. (2012). *Pro Stratehiiu natsionalnoi bezpeky Ukrainy «U sviti, shcho zminiuietsia» : Ukaz Prezydenta Ukrainy № 389 vid 08.06.2012 [On the National Security Strategy of Ukraine «In a Changing World»: Decree of the President of Ukraine № 389 of 08.06.2012]*. Retrieved from https://zakon.rada.gov.ua/laws/show/105/2007#Text [in Ukrainian].
10. Verkhovna Rada Ukrainy. (2015). *Pro stratehiiu natsionalnoi bezpeky: Ukaz Prezydenta Ukrainy № 287/2015 vid 26.05.2015 [On the national security strategy: Decree of the President of Ukraine № 287/2015 of 26.05.2015]*. Retrieved from https://zakon.rada.gov.ua/laws/show/287/2015#Text [in Ukrainian].
11. *Shchodo stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury [On the creation of a state system for critical infrastructure protection]*. (2017). Retrieved from https://niss.gov.ua/sites/default/files/2017-02/infrastrukt-86de2.pdf [in Ukrainian].
12. U. S. Government. (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT). Act of 2001, Public Law 107-56, Washington, DC.

 ISSN 2306-4994 (print); ISSN 2310-8770 (online)

13. Defending American Security from Kremlin Aggression Act of 2018. (2018). *CONGRESS.GOV*. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/3336/text?q=%7B%22search%22%3A%5B% 22S.3336%22%5D%7D&r=1.
14. European Commission. (2012). Commission Staff Working Document on the Reviewof the European Programme for Critical Infrastructure Protection (EPCIP), SWD 190 Final. Brussels, Belgium.
15. Federal Ministry of Interior, Germany. (2009, June 17). National Strategy for Critical Infrastructure Protection. Berlin. Retrieved from http://www.bmi.bund. de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf.
16. UK Cabinet Office. (2010, March). Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. Retrieved from https://www.gov.uk.
17. Zakon o privatnoj zaštiti: zakon HR. (2020, 22.02). Republike Hrvatske. Retrieved from http://www.zakon.hr/z/291/Zakon-o-privatnoj-za%20titi [in Croatian].
18. Australian Government. (2015). Critical Infrastructure Reliance Strategy: Policy Statement. Barton, Australia. Retrieved from http://www.tisn.gov.au.
19. Derzhavna sluzhba Ukrainy z nadzvychainykh sytuatsii. (2019). *Informatsiino-analitychna dovidka pro vynyknennia nadzvychainykh sytuatsii v Ukraini uprodovzh 2019 roku [Information and analytical information on the origin emergencies in Ukraine during 2019]*. Retrieved from https://www.dsns.gov.ua/ua/Dovidka-za-kvartal/103179.html [in Ukrainian].
20. OECD. (2019). Good Governance for Critical Infrastructure Resilience. *OECD Reviews of Risk Management Policies*. Paris. Retrieved from https://www.oecd.org/science/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm.

The article is recommended for printing 02.12.2020.

ISSN 2306-4994 (print); ISSN 2310-8770 (online)