УДК: 351.862.4:338.49-021.412.1(477)"364"

О. В. Батюк, С. В. Писаревський, О. В. Тітов

ОСНОВОПОЛОЖНІ ПРИНЦИПИ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Досліджено нормативно-правові акти України, країн Європейського Союзу, а також Великої Британії щодо забезпечення безпеки об'єктів критичної інфраструктури. Вивчено погляди вітчизняних і іноземних науковців стосовно розуміння сутності принципів безпеки об'єктів критичної інфраструктури і шляхів їх реалізації.

Визначено і проаналізовано такі основоположні принципи безпеки об'єктів критичної інфраструктури в Україні у період воєнного стану, як-от: принцип єдності методологічних засад; принцип координованості; принцип безпеки, захисту й охорони інформації з обмеженим доступом; принцип державно-приватного партнерства; принцип координації зусиль; принцип компліментарного розвитку; принцип побудови комплексного захисту; принцип міжнародного співробітництва.

Зроблено висновки, що дотримання основоположних принципів безпеки об'єктів критичної інфраструктури в Україні у період воєнного стану дасть змогу забезпечити готовність до дій у надзвичайних ситуаціях, запобігти загрозам у майбутньому та ефективно реагувати на надзвичайні події, пов'язані з функціонуванням критичної інфраструктури. Це уможливить створення умов для відновлення її об'єктів, а також мінімізації й ліквідації наслідків надзвичайних ситуацій на цих об'єктах або на об'єктах, що взаємодіють з її функціонуванням.

Ключові слова: *безпека, воєнний стан, держава, загрози, заходи, енергетика, інфраструктура, об'єкти, принципи.*

Постановка проблеми. Актуальність теми забезпечення безпеки об'єктів критичної інфраструктури вважається особливо важливим елементом національної безпеки України, що охоплює комплекс заходів із захисту, охорони, оборони та підтримання безперервної роботи таких об'єктів в умовах воєнного стану, в якому Україна перебуває з 5 години 30 хвилин 24 лютого 2022 р. терміном на 30 діб згідно з Указом Президента України № 64/2022 від 24 лютого 2022 р. [1]. Варто зауважити, що сьогодні Україна постає перед наймасштабнішими безпековими загрозами за весь період своєї незалежності. Глибока соціально-політична криза, яка розгортається в умовах зовнішнього військового втручання у внутрішні справи держави, супроводжується посиленням екстремістських і терористичних проявів, зростанням рівня злочинності, зокрема із застосуванням вогнепальної зброї, суттєвим падінням економічних показників і поглибленням гуманітарної кризи у східних регіонах. Руйнування та пошкодження значної кількості підприємств і об'єктів інфраструктури формують нову безпекову реальність, у межах якої має забезпечуватися захист громадян, суспільства та інститутів державної влади.

Вочевидь, така ситуація актуалізує нагальну потребу у глибокому реформуванні національного сектору безпеки з урахуванням міжнародного досвіду та стратегічного курсу на європейську інтеграцію. У цьому контексті особливого значення набуває впровадження в Україні концепції захисту критичної інфраструктури, що як ключовий інструмент сучасної безпекової політики широко застосовується у країнах Європейського Союзу, НАТО та інших провідних державах.

Зауважимо, що в Україні, як і в інших державах, функціонують системи, об'єкти та ресурси, знищення або пошкодження яких може спричинити значні негативні наслідки для громадян, суспільства й державних інституцій. Водночас некоректно стверджувати, що питання їх захисту та безпеки залишаються поза увагою. Навпаки, в сучасних умовах діє комплекс законодавчих і нормативно-правових актів, які регламентують повноваження й компетенцію відповідних державних органів, а також визначають особливості організації охорони і забезпечення безперебійного функціонування цих об'єктів і систем. Однак констатуємо, що в Україні наразі бракує цілісного й системного підходу на національному рівні до управління захистом та безпекою комплексу систем, об'єктів і ресурсів, які належать до критичної інфраструктури. Це призводить до домінування відомчих методів управління, недостатньої взаємодії та координації між суб'єктами, а також неефективного розподілу ресурсів, особливо в умовах надзвичайних ситуацій державного масштабу та в умовах воєнного стану.

Аналіз останніх досліджень і публікацій. Науковим дослідженням окремих аспектів забезпечення безпеки критичної інфраструктури приділяли увагу чимало науковців, зокрема С. І. Азаров [7], С. В. Бєлай [9], Д. С. Бірюков [10], С. Г. Братель [11], В. Гармаш [8], І. В. Гора [12], В. П. Кудряшов [13]. Тематика їхніх досліджень стосувалася правових, економічних, управлінських, службово-бойових питань захисту об'єктів критичної інфраструктури в Україні. Це свідчить про недостатній рівень наукових досліджень, спрямованих на визначення основоположних принципів безпеки об'єктів критичної інфраструктури в Україні в умовах воєнного стану.

Мета статті – дослідження національних і міжнародних нормативно-правових документів, вивчення поглядів вітчизняних та іноземних науковців задля визначення основоположних принципів безпеки об'єктів критичної інфраструктури в Україні в умовах воєнного стану.

Виклад основного матеріалу. За офіційними даними Звіту про прямі збитки інфраструктури від руйнувань унаслідок військової агресії росії проти України станом на листопад 2024 р. від початку вторгнення загальна сума прямих збитків нерухомості, іншій інфраструктурі, транспортним засобам і запасам становила майже 170 млрд дол. США. Порівняно з попередньою оцінкою (станом на початок 2024 р.) сума збільшилася на 12,6 млрд дол. (8 %) [6].

Загальні прямі втрати у секторі енергетики оцінюються на рівні 14,6 млрд дол. США. Сумарна вартість зруйнованих або пошкоджених активів у промисловості, сфері послуг та будівництві становить 14,4 млрд дол. США. Прямі втрати аграрного сектору та земельних ресурсів унаслідок бойових дій сягають 10,3 млрд дол. США. Сукупний обсяг прямих збитків, завданих об'єктам громадського сектору – зокрема соціальній інфраструктурі, закладам освіти, науки, охорони здоров'я, об'єктам культури, спорту та адміністративним будівлям, – орієнтовно становить 16,3 млрд дол. США (таблиця 1, рисунок 1) [6].

Таблиця 1. Загальна оцінка прямих збитків інфраструктури станом на листопад 2024 р.

Тип майна	Оцінка прямих втрат, млрд дол. США	Частка, %	Попередня оцінка, млрд дол. США	Динаміка, %
Житлові будівлі	60,0	35,3	58,9	1,9
Інфраструктура	38,5	22,7	36,8	4,6
Енергетика *	14,6	8,6	10,0	46,0
Активи підприємств, промисловість	14,4	8,5	14,2	1,4
АПК та земельні ресурси	10,3	6,1	10,3	0,0
Освіта	7,3	4,3	7,4	– 0,8
Лісовий фонд	4,5	2,7	4,3	4,7
Охорона здоров'я	3,2	1,9	3,2	0,0
Культура, туризм, спорт	2,5	1,5	2,1	20,0
ЖКГ *	2,4	1,4	3,4	-29,4
Транспортні засоби	2,0	1,2	1,6	25,0
Торгівля	1,2	0,7	1,2	0,0
Цифрова інфраструктура	0,8	0,5	0,2	140,0
Адміністративні будівлі	0,8	0,4	0,5	60,0
Соціальна сфера	0,2	0,1	0,2	0,0
Фінансовий сектор	0,0	0,0	0,0	0,0
Усього	169,8	100	157,2	8,0

Примітка. KSE: показники тепла було перенесено із ЖКГ до показників енергетики, оскільки ТЕЦ виробляють одночасно електричну й теплову енергію. З метою порівняння перенесення зроблено і для попередньої оцінки.

Доцільно зазначити, що в абсолютному вимірі найбільший приріст обсягів завданих збитків зафіксовано у сфері енергетики (понад 4,6 млрд дол. США), що зумовлено цілеспрямованими атаками противника на об'єкти електрогенерації та розподілу електроенергії. Значні нові втрати також спостерігались у транспортній інфраструктурі, соціальній сфері та серед виробничих активів підприємств. У відносному вимірі найвищі темпи приросту збитків зареєстровано щодо адміністративних будівель (+60 %), об'єктів енергетичної інфраструктури (+46 %), закладів охорони здоров'я (+32 %), а також у сферах культури, туризму та спорту (+29 %). Зростання збитків у сегменті цифрової інфраструктури мало ще більш виражений характер, проте такі показники не є повноцінно репрезентативними через відсутність оновлених оцінок у попередньому звіті внаслідок браку відповідних даних [6].

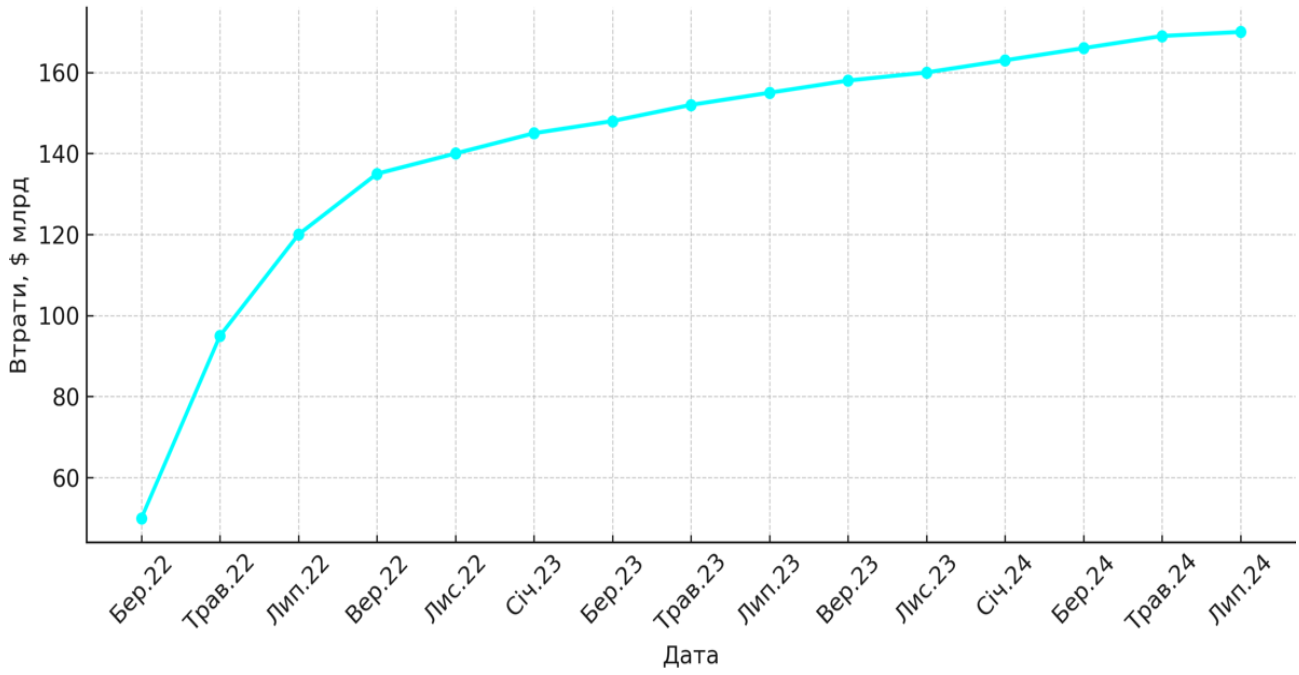

Рисунок 1 – Динаміка сукупної оцінки прямих витрат економіки України (у млрд дол. США)

У географічному вимірі найбільших втрат зазнали регіони, розташовані у безпосередній близькості до зони бойових дій (рисунок 2). Зокрема, на десять областей, що були тимчасово окуповані, межують із російською федерацією або мають вихід до морського узбережжя, припадає понад 90 % сукупного обсягу прямих збитків. Зважаючи на систематичне завдання ударів противником по інфраструктурних об'єктах у відносно віддалених від фронту регіонах, до числа найбільш уражених територій також входить Дніпропетровська область [6].

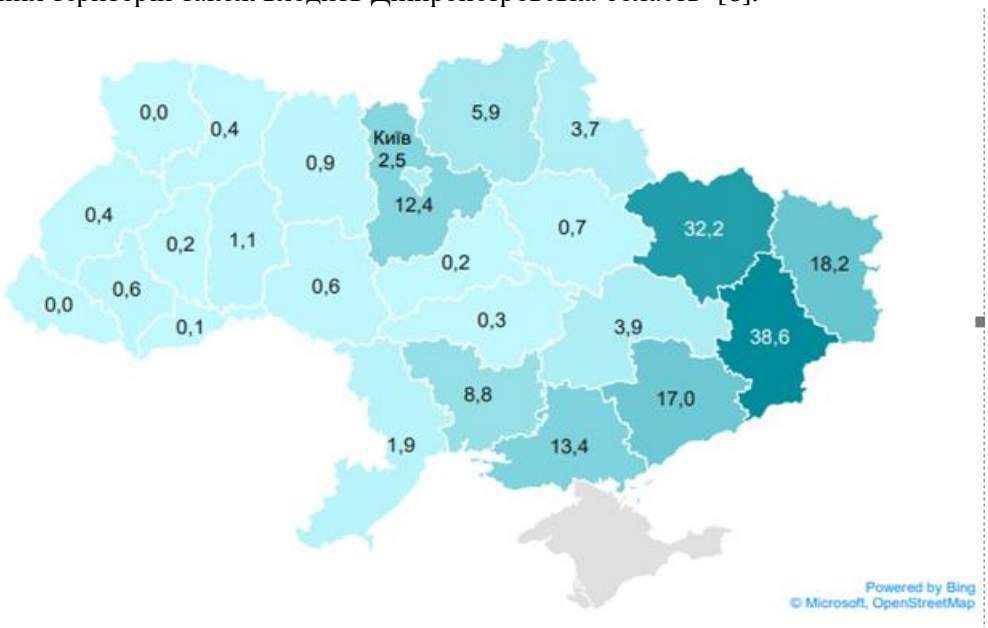

Рисунок 2 – Розподіл прямих втрат за областями (у млрд дол. США)

Зазначені вище дані свідчать про актуальність і необхідність дослідження проблематики захисту об'єктів критичної інфраструктури у період дії воєнного стану загалом і дослідження основоположних принципів безпеки об'єктів критичної інфраструктури в Україні в умовах воєнного стану зокрема.

Розкриваючи тему основоположних принципів безпеки об'єктів критичної інфраструктури в Україні в умовах воєнного стану, вважаємо за доцільне насамперед провести аналіз норм чинного законодавства України. Згідно із Законом України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII (ст. 3) основними принципами, що визначають порядок формування державної політики у сферах національної безпеки і оборони, є: верховенство права, підзвітність, законність, прозорість та дотримання засад демократичного цивільного контролю за функціонуванням сектору безпеки і оборони та застосуванням сили; дотримання норм міжнародного права, участь в інтересах України у міжнародних зусиллях з підтримання миру і безпеки, міждержавних системах та механізмах міжнародної колективної безпеки; розвиток сектору безпеки і оборони як основного інструменту реалізації державної політики у сферах національної безпеки і оборони» [2].

Закон України «Про критичну інфраструктуру» (ст. 6) до основних принципів функціонування національної системи захисту критичної інфраструктури відносить:

1) єдність методологічних засад;

2) координованість;

3) державно-приватне партнерство;

4) безпека, захист та охорона інформації з обмеженим доступом;

5) міжнародне співробітництво [3].

Статтею 25 Закону України «Про національну безпеку України» визначено мету, принципи й види планування у сфері національної безпеки і оборони. Планування у сферах національної безпеки і оборони здійснюється відповідно до таких принципів:

1) дотримання національного законодавства і міжнародних зобов'язань України;

2) демократичний цивільний контроль за сектором безпеки і оборони, відкритість інформації про державну політику, стратегічні документи, цілі, пріоритети і завдання планування, прозорість та підзвітність використання ресурсів;

3) цілісність, узгодженість, системність планування у секторі безпеки і оборони, врахування пріоритетів і обмежень, установлених державними програмами, планами та прогнозними документами;

4) своєчасність і відповідність прийнятим рішенням щодо захисту національних інтересів України [2].

Доцільно зазначити, що під захистом критичної інфраструктури слід розуміти сукупність заходів, реалізованих через нормативно-правові, організаційні та техніко-технологічні механізми і спрямованих на запобігання загрозам, зниження рівня ризиків, усунення вразливостей, мінімізацію негативних наслідків та забезпечення відновлення функціонування об'єктів критичної інфраструктури у разі виникнення надзвичайних ситуацій (збоїв, аварій тощо). У мирний період наведені заходи мають на меті гарантування захищеності, безпеки і стабільного функціонування всіх компонентів критичної інфраструктури: об'єктів, систем і мереж (об'єктів).

Основоположні принципи формування системи захисту критичної інфраструктури обґрунтовано відповідно до значущості забезпечення національної безпеки в сучасній державі Україна. Вважаємо, що принципи, на яких має ґрунтуватися захист критичної інфраструктури, слід розглядати в контексті стратегічних безпекових завдань.

На нашу думку, до основоположних принципів формування системи безпеки об'єктів критичної інфраструктури в Україні у період воєнного стану слід віднести такі.

Принцип єдності методологічних засад у сфері безпеки об'єктів критичної інфраструктури передбачає застосування уніфікованої, системної та послідовної методології для аналізу, планування, упровадження та оцінювання заходів із забезпечення захисту критично важливих об'єктів. Цей принцип забезпечує гармонізацію підходів до ідентифікації загроз, оцінювання ризиків, розроблення стратегій безпеки та контролю за їх реалізацією, що сприяє підвищенню ефективності системи захисту.

Реалізація принципу передбачає:

– використання єдиної понятійної і методологічної бази для комплексного аналізу загроз та уразливостей об'єктів критичної інфраструктури, що охоплює техногенні, природні, соціально-політичні та воєнні чинники;

– інтеграцію ризик-орієнтованих методів аналізу і прогнозування для визначення пріоритетів заходів із запобігання та реагування на загрози;

– урахування особливостей функціонування системи захисту як у мирний час, так і в умовах

надзвичайних ситуацій і режиму надзвичайного стану;

– координацію нормативно-правових, організаційних та технічних інструментів, що забезпечують реалізацію заходів безпеки у взаємозв'язку між державними і приватними суб'єктами;

– застосування стандартизованих процедур оцінювання загроз, ведення паспортизації об'єктів критичної інфраструктури та моніторингу їх стану;

– забезпечення єдності підходів у плануванні кадрового, технічного й науково-технічного забезпечення безпеки.

Дотримання принципу єдності методологічних засад забезпечує цілісність, скоординованість і адаптивність системи безпеки критичної інфраструктури, що є необхідною умовою її ефективного функціонування в умовах сучасних викликів.

Принцип координованості у сфері безпеки об'єктів критичної інфраструктури передбачає скоординовану, узгоджену діяльність усіх зацікавлених суб'єктів – державних органів, приватного сектору, громадськості та експертного середовища – з метою ефективного формування, реалізації та контролю заходів із захисту об'єктів критичної інфраструктури щодо єдності дій у стратегічному й оперативному управлінні безпекою, мінімізацію дублювання функцій, зменшення ризиків фрагментації відповідальності та посилення ефективності використання наявних і потенційних ресурсів.

Принцип координованості на практиці реалізується через:

– узгоджений розвиток нормативно-правових, організаційних і науково-технологічних інструментів, необхідних для підтримання цілісної системи захисту критичної інфраструктури;

– планування заходів безпеки на загальнонаціональному рівні з урахуванням стратегічних пріоритетів захисту національних інтересів;

– інтеграцію питань безпеки критичної інфраструктури у загальнодержавні програми соціально-економічного розвитку та оцінювання їх ефективності;

– створення і функціонування єдиного координаційного центру або платформи, відповідальної за оцінювання стану захищеності, прогнозування загроз і управління ризиками;

– централізоване управління державними і приватними ресурсами для забезпечення їх раціонального й ефективного використання в умовах загроз;

– установлення механізмів горизонтальної (між органами виконавчої влади) та вертикальної (між центральним, регіональним і місцевим рівнями) координації дій;

– забезпечення прозорості, обміну інформацією та участі громадськості через консультаційно-дорадчі структури.

Дотримання принципу координованості сприяє створенню стійкої, адаптивної та взаємозалежної системи безпеки, що здатна ефективно реагувати на сучасні комплексні загрози критичній інфраструктурі.

Принцип безпеки, захисту й охорони інформації з обмеженим доступом у сфері безпеки об'єктів критичної інфраструктури полягає у комплексному захисті від зловмисних дій та охороні інформації про вразливості, технічні характеристики та особливості систем фізичного захисту об'єктів критичної інфраструктури від несанкціонованого доступу, за винятком випадків, передбачених чинним законодавством.

Реалізація принципу безпеки, захисту й охорона інформації з обмеженим доступом у практичній діяльності передбачає:

– установлення чітких правил і процедур щодо обмеження доступу до інформації про вразливості й характеристики систем фізичного захисту критичної інфраструктури на основі прийнятих нормативних документів;

– застосування механізмів контролю доступу, таких, як розмежування прав користувачів, багатофакторна автентифікація та шифрування даних;

– проведення навчань і підвищення рівня обізнаності персоналу щодо важливості конфіденційності та відповідальності за розголошення службової інформації;

– використання технічних засобів захисту інформації, зокрема й систем інформаційної безпеки, аби запобігти несанкціонованому доступу, витоку чи втраті даних;

– забезпечення законодавчого і нормативного регулювання порядку роботи з конфіденційною інформацією, а також контроль за дотриманням цих норм;

– визначення виключних випадків розголошення інформації відповідно до чинного законодавства та забезпечення суворого контролю у таких випадках.

Принцип державно-приватного партнерства у сфері безпеки об'єктів критичної інфраструктури передбачає інтеграцію всіх зацікавлених сторін, залучених до функціонування об'єктів критичної інфраструктури, з одночасним чітким розмежуванням зон відповідальності між ними (зокрема, держава як власник, органи влади – представники суспільства, регулятор – наглядовий орган,

оператор як виконавець).

Реалізація цього принципу має ґрунтуватися на таких ключових положеннях:

– раціональне й комплексне використання ресурсів державного і приватного секторів з метою забезпечення ефективного захисту критичної інфраструктури;

– запровадження практики офіційного декларування рівня безпеки об'єкта його власником (оператором), а також здійснення паспортизації об'єктів критичної інфраструктури;

– забезпечення участі громадянського суспільства і представників експертного середовища у процесах формування вимог до безпеки об'єктів критичної інфраструктури, зокрема через створення і функціонування консультативно-дорадчих органів.

Принцип координації зусиль у сфері безпеки об'єктів критичної інфраструктури передбачає системну узгодженість дій усіх суб'єктів національної безпеки з метою досягнення цілісної, ефективної та раціональної системи захисту.

Зміст цього принципу охоплює:

– гармонійний розвиток нормативно-правової, організаційної та науково-технологічної баз, що забезпечують реалізацію завдань у сфері захисту критичної інфраструктури;

– стратегічне планування безпеки на державному рівні відповідно до національних інтересів і через формування механізмів впливу на рівень захищеності критичних об'єктів;

– інтеграцію питань безпеки критичної інфраструктури у процеси соціально-економічного планування, визначення державних пріоритетів та здійснення оцінювання розвитку країни;

– створення і функціонування централізованої системи оцінювання стану захищеності, прогнозування загроз і ризик-аналізу для об'єктів критичної інфраструктури;

– централізоване управління наявними державними ресурсами з метою їх оптимального й цільового використання у сфері безпеки;

– визначення і впровадження національного сценарію (проєктної загрози) для критичної інфраструктури на основі комплексного оцінювання загроз національній безпеці.

Принцип компліментарного розвитку у сфері безпеки об'єктів критичної інфраструктури полягає у послідовному, взаємодоповнюючому впровадженні комплексних заходів, що забезпечують поступове вдосконалення системи захисту й безпеки. Застосування цього принципу передбачає:

– поетапне впровадження нормативно-правових, організаційних та науково-технологічних інструментів, які становлять основу для вдосконалення засобів і заходів захисту критичної інфраструктури;

– розроблення методологічних підходів до ідентифікації та класифікації об'єктів критичної інфраструктури на основі аналізу наявних даних;

– регулярне оцінювання загроз, ризиків і вразливостей об'єктів критичної інфраструктури із застосуванням кращих практик, зокрема з урахуванням досвіду ядерної галузі та банківського сектору;

– упровадження результатів науково-прикладних досліджень і перспективного планування у сфері безпеки, а також використання інноваційних високотехнологічних рішень;

– стратегічне планування розвитку кадрового потенціалу з урахуванням ресурсів і можливостей спеціалізованих навчальних закладів.

Принцип побудови комплексного захисту у сфері безпеки об'єктів критичної інфраструктури полягає у формуванні системи захисту критичної інфраструктури, що ґрунтується на єдиній методологічній і понятійній основі для аналізу загроз з огляду на комплексний вплив чинників техногенного, природного, соціально-політичного та воєнного характеру.

Цей принцип передбачає врахування особливостей функціонування захисту як у мирний час, так і в умовах надзвичайних ситуацій і режиму надзвичайного стану. Крім того, він надає пріоритет заходам із превенції загроз, застосовуючи ризик-орієнтовані методи аналізу і прогнозування, що забезпечує ефективне запобігання надзвичайним ситуаціям та мінімізацію їх наслідків.

Принцип міжнародного співробітництва у сфері безпеки об'єктів критичної інфраструктури передбачає системну й активну взаємодію України з міжнародними організаціями, платформами та державами-партнерами з метою забезпечення ефективного захисту національних інтересів і підвищення рівня безпеки. Цей принцип ґрунтується на інтеграції міжнародних стандартів, норм і угод у національне законодавство, а також практичні заходи, що сприяють гармонізації політик і процедур у сфері цивільного захисту, кібербезпеки та протидії тероризму.

Реалізація принципу міжнародного співробітництва передбачає:

– активну участь України у міжнародних організаціях і платформах, що регулюють питання цивільного захисту, кібербезпеки та протидії тероризму;

– імплементацію міжнародних стандартів, норм і угод у національне законодавство та практичну діяльність із метою гармонізації заходів захисту критичної інфраструктури;

– обмін інформацією та координацію дій з іншими державами щодо виявлення, оцінювання та реагування на трансграничні загрози й ризики;

– спільне проведення навчань, тренінгів та операцій із партнерами для підвищення рівня готовності і взаємодії у надзвичайних ситуаціях;

– розвиток міждержавних механізмів оперативного реагування і підтримки у випадках кризових подій, що можуть мати трансграничний характер;

– забезпечення участі національних фахівців у міжнародних дослідницьких проєктах та обміні досвідом у сфері захисту критичної інфраструктури.

Міжнародні нормативно-правові акти так само визначають принципи безпеки об'єктів критичної інфраструктури.

Європейська комісія 17 листопада 2005 р. ухвалила Зелену книгу щодо Європейської програми захисту критичної інфраструктури, яка передбачала розроблення варіантів політики, спрямованих на формування цілісної програми та створення мережі попередження про загрози критичній інфраструктурі. У відповідях, отриманих на положення Зеленої книги, було зазначено про додаткову цінність рамкової програми Європейського Союзу щодо захисту критичної інфраструктури. Наголошувалося на необхідності посилення потенціалу захисту критично важливих об'єктів у межах Європейського Союзу, а також на важливості зменшення їхньої вразливості до можливих загроз. Особливу увагу приділено дотриманню ключових принципів: субсидіарності, пропорційності, взаємодоповнюваності, а також забезпеченню ефективної взаємодії між усіма зацікавленими сторонами [5].

Зауважимо, що у Директиві Ради ЄС від 8 грудня 2008 р. № 2008/114/ЄС здійснено ідентифікацію та визначення європейських об'єктів критичної інфраструктури та оцінювання потреби у підвищенні рівня їхнього захисту [4].

Варто погодитися з науковцями, які вважають, що у процесі розвитку національної нормативно-правової бази у сфері захисту критичної інфраструктури особливу увагу слід приділити документам, які максимально наближають вимоги національного законодавства до вимог щодо функціонування й захисту критичної інфраструктури в галузі енергетики і транспорту, визначених у директивах ЄС і вказаних в Угоді про асоціацію між Україною та ЄС. Зокрема йдеться про таке:

– Директива № 2005/89/ЄС щодо заходів з забезпечення безпеки постачання електроенергії та інвестицій в інфраструктуру;

– Директива № 2004/67/ЄС стосовно заходів щодо забезпечення безперервного постачання природного газу;

– Директива № 2005/65/ЄС Європейського Парламенту та Ради від 26 жовтня 2005 р. про посилення безпеки портів;

– Регламент (ЄС) № 725/2004 Європейського Парламенту та Ради від 31 березня 2004 р. про посилення безпеки суден та портових споруд;

– Директива № 2004/49/ЄС Європейського Парламенту та Ради від 29 квітня 2004 р. про безпеку залізниць у Співтоваристві, яка вносить зміни до Директиви Ради № 96/18/ЄС про ліцензування підприємств залізничного транспорту та до Директиви № 2001/14/ЄС про розділення пропускної здатності залізничних інфраструктур та стягнення платежів за використання залізничної інфраструктури та про сертифікацію безпеки (Директива про безпеку на залізницях);

– Регламент (ЄС) № 336/2006 Європейського Парламенту та Ради від 15 лютого 2006 р. про імплементацію Міжнародного кодексу з управління» [5].

Висновки

Проаналізувавши положення чинного законодавства України, деяких країн ЄС і Великої Британії, вивчивши позиції провідних вітчизняних та іноземних науковців, доходимо таких висновків.

1. До основоположних принципів безпеки об'єктів критичної інфраструктури в Україні у період воєнного стану доцільно віднести такі принципи: єдності методологічних засад; координованості; безпеки, захисту й охорони інформації з обмеженим доступом; державно-приватного партнерства; координації зусиль; компліментарного розвитку; побудови комплексного захисту; міжнародного співробітництва.

2. Дотримання основоположних принципів безпеки об'єктів критичної інфраструктури в Україні у період воєнного стану дасть змогу мінімізувати ризики для функціонування критичної інфраструктури, зокрема йдеться про локалізацію та нейтралізацію загроз на ранніх етапах їх виникнення.

3. У разі надзвичайних ситуацій на об'єктах критичної інфраструктури насамперед слід забезпечити безпеку населення і територій від найнебезпечніших радіологічних, хімічних і

бактеріологічних чинників, що можуть виникнути.

4. Доцільно розробляти і впроваджувати інженерно-технічні заходи цивільного захисту задля організації фізичного захисту об'єктів критичної інфраструктури, запобігання несанкціонованим діям (зокрема й терористичним актам), пом'якшення негативних наслідків таких дій і відновлення функціонування об'єктів у разі їх реалізації.

5. Забезпечити захист об'єктів критичної інформаційної інфраструктури від кібератак, а також захист даних і технічної інформації, що міститься в системах управління технологічними процесами на об'єктах критичної інфраструктури, від несанкціонованого блокування та модифікації.

6. Із метою забезпечення стабільного функціонування критичної інфраструктури в умовах надзвичайних ситуацій та воєнного стану доцільно сформувати матеріальні резерви, чому мають передувати оцінювання та інвентаризація ресурсів на об'єктах критичної інфраструктури.

Подальші наукові пошуки будуть спрямовані на дослідження практичного застосування силами безпеки й оборони основоположних принципів безпеки об'єктів критичної інфраструктури в Україні в умовах воєнного стану.

Перелік джерел посилання

1. Про введення воєнного стану в Україні : Указ Президента України № 64/2022 від 24.02.2022 р. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення: 01.05.2025).
2. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.05.2025).
3. Про критичну інфраструктуру : Закон України від 16.11.2021 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.05.2025).
4. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). URL: https://www.legislation.gov.uk/eudr/2008/114/introduction (дата звернення: 01.05.2025).
5. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ : Національний інститут стратегічних досліджень, 2014. 31 с. URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf (дата звернення: 01.05.2025).
6. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії росії проти України станом на листопад 2024 року / Д. Андрієнко та ін. Київ : Міністерство розвитку громад та територій, 2025. URL: https://surl.li/hroeqr (дата звернення: 01.05.2025).
7. Захист критичної інфраструктури в умовах надзвичайних ситуацій : монографія / С. І. Азаров та ін.; за заг. ред. П. Б. Волянського. Київ, 2021. 375 с.
8. Бєлай С., Лавров І. Теоретичні основи формування системи захисту об'єктів критичної інфраструктури України. *Честь і закон*. 2023. № 2 (85). С. 5–11. DOI: https://doi.org/10.33405/2078-7480/2023/2/85/282518 (дата звернення: 01.05.2025).
9. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні : аналітична доповідь. Київ : ФЕНІКС, 2012. 92 с.
10. Братель С. Г. Досвід зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури. *Південноукраїнський правничий часопис*. 2023. № 3. С. 261–265. DOI: https://doi.org/10.32850/sulj.2023.3.41.
11. Гора І. В., Батюк О. В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії.* 2021. Вип. 1 (11). С. 132–139.
12. Кудряшов В. П. Державне регулювання критичної інфраструктури. *Фінанси України*. 2021. № 7. С.72–92.

Стаття надійшла до редакції 20.05.2025 р.

UDC: 351.862.4:338.49-021.412.1(477)"364"

O. Batiuk, S. Pysarevskyi, O. Titov

BASIC PRINCIPLES OF SECURITY FOR CRITICAL INFRASTRUCTURE FACILITIES IN UKRAINE UNDER MARTIAL LAW

In the provisions of the scientific article, the authors examine the regulatory legal acts of Ukraine and the countries of the European Union, Great Britain, the views of scientists in Ukraine and foreign countries regarding the understanding of the essence of the principles and ways of their implementation to secure

critical infrastructure facilities. The authors of the scientific article determine: the expediency of assessing threats to critical infrastructure at the national level, taking into account the interrelationships between individual objects and infrastructure sectors, the impact of external factors of a natural, socio-political and technogenic nature, as well as the assessment of risks at the level of individual objects, regions and the state as a whole; the importance of developing and implementing a national programme for the protection of critical infrastructure; the further need to ensure the functioning of a network of emergency centres, the formation and maintenance of the database of critical infrastructure; the provision of ongoing support and coordination of the work of expert and advisory councils at various levels in the development and implementation of regulatory, organisational and technological measures for the protection of critical infrastructure; the expediency of developing emergency response plans and forming a comprehensive research programme in the field of critical infrastructure protection with a view to organising and further implementing cooperation with European Union structures and state bodies of EU member states.

The authors of the article conclude that compliance with the fundamental principles of critical infrastructure security in Ukraine during martial law will ensure readiness for action in emergency situations, prevent future threats, and enable effective response to emergencies related to the functioning of critical infrastructure, which will create conditions for the restoration of its facilities, as well as the minimisation and elimination of the consequences of emergencies at these facilities or at facilities that interact with its functioning.

Keywords: *security, martial law, state, threats, measures, power engineering, infrastructure, facilities, principles.*

Батюк Олег Володимирович – доктор юридичних наук, професор, професор кафедри національної безпеки, Волинський національний університет імені Лесі Українки
https://orcid.org/0000-0002-2291-4247

Писаревський Сергій Васильович – кандидат наук з державного управління, доцент, заступник начальника центру перепідготовки та підвищення кваліфікації, Національна академія Національної гвардії України
https://orcid.org/0000-0002-2537-0767

Тітов Олег Валерійович – начальник відділу підготовки органів управління, Головне управління Національної гвардії України
https://orcid.org/0009-0004-4416-6843