

УДК 35.088.6:[004:007:351.86](477)
DOI <https://doi.org/10.32782/tnv-pub.2024.3.1>

ВПРОВАДЖЕННЯ МЕХАНІЗМУ РЕАЛІЗАЦІЇ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Арсенович Л. А. – доктор філософії з публічного управління та адміністрування,
заступник начальника управління – начальник відділу
Департаменту кадрової роботи та управління персоналом
Адміністрації Держспеццв'язку
ORCID: 0000-0001-7081-2838

Глобалізація та швидкі зміни навколишнього середовища вимагають пошуку нових методів і механізмів партнерства не лише між національними економіками на макрорівні, а й між учасниками ринкових відносин всередині держави – на мікрорівні. Одним із таких механізмів співпраці є розвиток державно-приватного партнерства.

В умовах розбудови цифрового світу та розвитку інформаційних технологій особливою значення набувають проблеми професійної підготовки спеціалістів ІТ-сфери, у тому числі фахівців сфери захисту критичної інфраструктури.

Зовнішні та внутрішні загрози у безпековому середовищі України актуалізують потребу підвищення рівня професійної компетенції фахівців, які в умовах протидії збройній агресії російської федерації опікуються питаннями виявлення, запобігання і нейтралізації загроз безпеці об'єктів критичної інфраструктури, а також мінімізації та ліквідації наслідків у разі їх реалізації.

У контексті проведення освітніх реформ у всіх сферах діяльності українського суспільства, співробітництво між державою та приватним сектором шляхом створення дієвої та ефективної системи підготовки кадрів та підвищення компетентності фахівців сфери захисту критичної інфраструктури набуває особливої актуальності та потребує окремої уваги.

У статті розглянуто методологічні засади формування державно-приватного партнерства у сфері захисту критичної інфраструктури, здійснено аналіз нормативно-правового підґрунтя щодо формування державно-приватного партнерства у зазначеній сфері, наведено приклади зарубіжного досвіду розбудови державно-приватного партнерства, запропоновано механізм реалізації державно-приватного партнерства у сфері захисту критичної інфраструктури, який спрямований на подальшу розбудову державно-приватного партнерства, впровадження нових інформаційних та освітніх технологій, застосування прогресивних форм організації освітнього процесу та активних методів навчання, а також сучасних навчально-методичних матеріалів, які в сукупності є основою для всебічного розвитку людини та добробуту населення в цілому.

Ключові слова: державно-приватне партнерство, критична інфраструктура, підвищення кваліфікації, система підготовка кадрів, сфера захисту критичної інфраструктури.

Arsenovych L. A. Introducing a way of public-private partnership implementation in critical infrastructure protection

Globalization and rapid changes in the environment require to seek new methods and ways of partnership not only between national economies at the macro level, but also between participants in market relations within the state – at the micro level. One of such ways of cooperation is the development of public-private partnership.

In the context of digital world and information technology development, special focus is made on issues related to professional training of IT specialists, including critical infrastructure protection specialists.

External and internal threats in the security environment of Ukraine make it relevant to increase the level of professional competence of specialists who, under the conditions of countering the armed aggression of the Russian Federation, are involved in identifying, preventing and neutralizing critical infrastructure security threats, as well as minimizing and eliminating the consequences if such threats materialize.

In the context of educational reforms in all spheres of activity of Ukrainian society, cooperation between the state and the private sector by way of developing an effective system of personnel training and increasing the competence of critical infrastructure protection specialists is getting especially relevant and requires particular attention.

The article studies the methodological principles of how public-private partnership evolves in the area of critical infrastructure protection, analyzes the regulatory basis for evolving of public-private partnership in the specified area, provides examples of foreign experience of how to develop public-private partnership, and proposes a way of implementing public-private partnership in critical infrastructure protection, which is aimed at further development of public-private partnership, introduction of new information and educational technologies, use of forward-looking ways of education and active teaching methods, as well as modern teaching and methodical materials, which in aggregate form the basis for comprehensive human development and well-being of the population as a whole.

Key words: *Public-private partnership, critical infrastructure, advanced professional training, personnel training system, critical infrastructure protection.*

Постановка проблеми. Розвиток партнерських відносин між державою та бізнесом на теперішній час відіграє вагомую роль у підвищенні не тільки ефективного функціонування підприємств, закладів та установ, а й соціально-економічного розвитку країни в цілому. Завдяки такому розвитку з'являється можливість залучення в державний сектор економіки додаткових ресурсів, іншими словами – інвестицій. Такі відносини сприяють підняттю ефективності використання наявних ресурсів, розподілу ризиків між державним і приватним сектором та їх мінімізації завдяки об'єднанню ресурсів та потенціалів держави та бізнесу [1, с. 23].

Система підготовки кадрів у будь-якій сфері діяльності завжди буде унікальною. На конфігурацію та функціонування такої системи впливає цілий комплекс чинників: від особливостей законодавства до розподілу повноважень між державними органами або підрозділами всередині органу, від менталітету та рівня освіти співробітників (населення) до їх комп'ютерної грамотності, від соціальної відповідальності до розвитку державно-приватного партнерства у цій сфері тощо. При цьому комплексний характер завдань, пов'язаних зі створенням такої системи, вимагає забезпечення потреб у навчанні в широкому діапазоні цільових аудиторій, створення можливостей як для розповсюдження серед співробітників базових понять знань (підвищення інформованості), так і отримання додаткової вищої освіти [1, с. 23–24].

Аналіз останніх досліджень та публікацій. Необхідність подальшої розбудови системи підготовки кадрів у сфері захисту критичної інфраструктури шляхом удосконалення державно-приватного партнерства підкреслюють як іноземні так і сучасні науковці, які з моменту прийняття Закону України «Про критичну інфраструктуру» [2] сигналізують і нагадують про це у наукових статтях і доповідях.

Так, старший викладач Національної академії Служби безпеки України Жевелева І.С. у своїй статті доводить, що державно-приватне партнерство є ключовим елементом захисту критичної інфраструктури, та визначає основні напрями його розвитку у сфері забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Науковиця зазначає, що зважаючи на процес реформування Служби безпеки України у частині переходу від боротьби з економічною злочинністю до зосередження уваги на захисті об'єктів критичної інфраструктури, державно-приватне партнерство у сфері забезпечення, у тому числі, інформаційної безпеки об'єктів критичної інфраструктури доцільно здійснювати через Службу безпеки України [3, с. 26].

Інший науковець, Лук'яненко І.Г., доктор економічних наук, професорка, завідувачка кафедри фінансів Національного університету «Києво-Могилянська

академія» у своїй науковій роботі визначає основні джерела фінансування проєктів розвитку критичної інфраструктури в Україні, аналізує досвід країн Європи, Канади та США щодо реалізації проєктів державно-приватного партнерства та обґрунтовує необхідність застосування механізму реалізації проєктів розвитку інфраструктури на засадах державно-приватного партнерства. Крім цього, авторка зазначає, що, незважаючи на можливості щодо залучення фінансових ресурсів для модернізації інфраструктури, наявні механізми потребують удосконалення в частині стимулювання залучення бізнесу на умовах державно-приватного партнерства для реалізації проєктів розбудови критичної інфраструктури для досягнення цілей сталого розвитку в Україні. Також Лук'яненко І.Г. пропонує подальші кроки щодо розвитку критичної інфраструктури в Україні на умовах державно-приватного партнерства з огляду на досягнення цілей сталого розвитку [4, с. 291].

Питання подальшого впровадження державно-приватного партнерства у сфері захисту критичної інфраструктури розглядають також у своїй науковій статті офіцери кафедри Інституту Управління державної охорони України Київського національного університету імені Тараса Шевченка Павлов Д.М. та Микитюк М.А. вивчаючи вплив підвищення ефективності державно-приватного партнерства на рівень безпеки та стійкості критичної інфраструктури. Зазначені науковці підкреслюють, що під час розроблення системи захисту критичної інфраструктури в Україні, враховуючи євроінтеграційний курс нашої держави, необхідно спрямувати зусилля на досягнення узгодженості національного законодавства з нормативними актами ЄС та впровадження чинних в ЄС стандартів захисту критичної інфраструктури, включаючи державно-приватне партнерство [5, с. 72].

Крім цього, Суходоля О.М., доктор наук з державного управління, професор, у своїй роботі приходить до висновку про необхідність суттєвого перегляду державної політики у сфері критичної інфраструктури. Суходоля О.М. зазначає, що незважаючи на важливі зміни на рівні стратегічного цілепокладання, практична діяльність органів державної влади, принципи взаємодії цивільного сектору та сектору безпеки і оборони, механізми залучення приватного сектору до діяльності із захисту критичної інфраструктури потребують уточнення. Як наголошує вчений, такий підхід вимагає прийняття відповідного законодавства, яке б відобразило нові принципи державної політики щодо захисту критичної інфраструктури, врегулювало питання державно-приватного партнерства (розподіл відповідальності між державою та приватним сектором), забезпечило координацію дій відомчих систем захисту та реагування на окремі типи загроз у єдиній, скоординованій системі захисту критичної інфраструктури [6, с. 74–75].

Зазначені наукові роботи ще раз підкреслюють, що питання державно-приватного партнерства у сфері захисту критичної інфраструктури в контексті реалізації Закону України «Про критичну інфраструктуру» та інших нормативно-правових актів залишилося поза увагою комплексних наукових досліджень, що потребує окремої уваги та подальшої розвідки.

Метою статті є вивчення питання щодо подальшого удосконалення державно-приватного партнерства у сфері захисту критичної інфраструктури.

Виклад основного матеріалу. Державно-приватне партнерство є важливою ланкою взаємодії між державою та бізнесом, що пов'язує їх інтереси і дозволяє ефективно та дієво реалізовувати пріоритетні, соціально значущі проєкти. Державно-приватне партнерство стимулює залучення інвестицій у реальний сектор

економіки та сприяє розвитку ринків капіталу, товарів та послуг, інноваційних галузей промисловості. Механізми державно-приватного партнерства використовують практично у всіх галузях економіки.

Поняття державно-приватного партнерства можна тлумачити як в широкому так і у вузькому значеннях. У широкому розумінні державно-приватне партнерство – це система відносин держави (уряду) та приватної (комерційної) сфери, яка широко використовується як інструмент національного, міжнародного, регіонального (міського), економічного або соціального розвитку. У вузькому розумінні державно-приватне партнерство – це відповідні проекти, що запроваджуються державними органами спільно із приватними компаніями на об'єктах національної (державної) та муніципальної (приватної) власності.

До ознак державно-приватного партнерства відносять: забезпечення вищих техніко-економічних показників ефективності діяльності; довготривалість відносин (від 5 до 50 років); передачу приватному партнеру частини ризиків; внесення приватним партнером інвестицій в об'єкти партнерства із легальних джерел. Крім того, до ключових ознак державно-приватного партнерства прийнято відносити конкурентний спосіб відбору та фільтрації партнерів, а успіх реалізації проекту за технологіями державно-приватного партнерства залежить від прозорості проведеного конкурсу, оскільки тільки такий спосіб забезпечує вибір найбільш економічно вигідного проекту та надійного партнера [7, с. 221].

Передбачається, що взаємодія між державою і приватним сектором повинна будуватися на принципах: законності, «здорової» конкуренції, прозорості, підзвітності, зрозумілості і передбачуваності, економічної а також фінансової сталості, врахування відповідної специфіки, гнучкості та рівності [1, с. 25].

Формування державно-приватного партнерства має відповідати умовам нестабільної економіки та ґрунтуватися на таких методологічних засадах:

- партнерство має відповідати цілям розвитку економіки країни та її суб'єктів;
- партнерство має бути підпорядковане вирішенню не лише поточних, а й стратегічних завдань розвитку відповідної сфери економіки країни загалом та її суб'єктів окремо;

- дотримання рівності інтересів сторін та свободи вибору дій;

- невтручання держави у сферу відповідальності приватного партнера;

- конкурентність та відповідальність за виконання умов контракту [8, с. 107–108].

Відповідно до законодавчих актів, нормативно-правових актів Президента України та Уряду України державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури, визначення суб'єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, а також умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури. І однією із таких засад, яка є стрижневою у всій сфері захисту критичної інфраструктури, є застосування державно-приватного партнерства, яке реалізовується, у тому числі, шляхом розбудови системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури.

Так, відповідно до статті 25 Закону України «Про критичну інфраструктуру» державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом обміну інформацією щодо загроз критичній інфраструктурі та

реагування на кризові ситуації, визначення повноважень та відповідальності державних органів і операторів критичної інфраструктури у сфері забезпечення безпеки та стійкості критичної інфраструктури, визначення порядку взаємодії між державними органами та операторами критичної інфраструктури у різних режимах функціонування об'єктів критичної інфраструктури, а також шляхом створення системи підготовки кадрів для сфери захисту критичної інфраструктури та підвищення комплексних знань, навичок і умінь персоналу та керівного складу операторів критичної інфраструктури, персоналу суб'єктів господарювання, які провадять діяльність, пов'язану із забезпеченням безпеки об'єктів критичної інфраструктури, з питань реагування на кризові ситуації на таких об'єктах.

Згідно Указу Президента України від 26 серпня 2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [9] Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить посилення національної кіберготовності та кіберзахисту шляхом:

запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановлення обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;

впровадження системи аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначення механізмів та базових методик проведення аудитів, встановлення вимог до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов'язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки;

проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів.

Крім цього, відповідно до Концепції створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р [10], протягом 2017–2027 років на загальнодержавному рівні передбачається забезпечити:

формування засад державно-приватного партнерства у сфері захисту критичної інфраструктури на основі взаємної довіри, обміну інформацією, створення стимулів для інвестування у здійснення заходів, спрямованих на захист критичної інфраструктури, запровадження уніфікованих підходів щодо вимог до підвищення рівня захисту;

організацію взаємодії суб'єктів державної системи захисту критичної інфраструктури, обміну інформацією між ними про загрози критичній інфраструктурі, створення мережі ситуаційних центрів;

створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури;

розроблення і затвердження єдиної методології проведення оцінки загроз критичній інфраструктурі;

встановлення вимог до планування заходів щодо захисту критичної інфраструктури, включаючи аварійні плани, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань (тренувань);

розроблення та затвердження Національного плану захисту та забезпечення стійкості критичної інфраструктури.

Зазначені акти ще раз підкреслюють необхідність подальшого вдосконалення освіти у сфері захисту критичної інфраструктури у тісній співпраці з державними органами, місцевими органами виконавчої влади (військово-цивільними адміністраціями), органами місцевого самоврядування, операторами критичної інфраструктури, громадськими об'єднаннями, організаціями роботодавців, що надасть змогу забезпечувати підготовку, перепідготовку та підвищення кваліфікації в обсязі, необхідному для задоволення потреб держави, у тому числі в умовах воєнного стану.

Державно-приватне партнерство є досить важливим і дієвим механізмом щодо залучення довгострокових інвестиційних ресурсів для модернізації критичної інфраструктури у світі. Залучення приватного партнера дозволяє державі відновити та розбудувати критичну інфраструктуру, не витрачаючи на це бюджетні кошти, більше того, отримати додаткові надходження до бюджету (наприклад, такі як плата за землю, сплата концесійного платежу, надходження у формі пайового внеску та інші) та створити нові робочі місця [4, с. 293].

Варто зазначити, що у провідних країнах світу ефективна взаємодія систем реагування на загрози, небезпеки і ризики є важливим елементом забезпечення національної безпеки. Наприклад, у США для характеристики здатності систем взаємодіяти широко використовують спеціальний термін “interoperability”, а забезпечення оптимальної здатності систем, персоналу й обладнання отримувати і надавати функціональну підтримку, дані, інформацію та послуги визначено як найбільш важливу вимогу для Міністерства внутрішньої безпеки США під час реагування на інциденти [5, с. 73].

За даними Європейського інвестиційного банку у 2022–2024 роках фінансового закриття досягли 39 проєктів державно-приватного партнерства у сфері захисту критичної інфраструктури на загальну суму 16,6 млрд євро. Проте найбільша кількість таких проєктів, що досягли фінансового закриття, припала на сектор «Освіта». У 2022 році Франція та Велика Британія запустили найбільшу кількість проєктів державно-приватного партнерства, 15 і 8 відповідно. Загалом з 2018 по 2022 роки Велика Британія стала лідером за кількістю укладених договорів державно-приватного партнерства, яка складає понад 80 договорів, у той час як Туреччина стала лідером за вартістю укладених договорів державно-приватного партнерства – на суму 22,76 млрд євро.

З огляду на успішний західний досвід, державно-приватне партнерство поступово розвивається і в Україні. І зміни, які було внесено протягом останніх років до Закону України «Про державно-приватне партнерство» [11], значно покращили стан правового регулювання щодо залучення бізнесу до розбудови інфраструктури в Україні, у тому числі у сфері освіти. Так, відповідно до закону державно-приватне партнерство застосовується в сферах машинобудування, збору, очищення та розподілення води, охорони здоров'я, туризму, відпочинку, рекреації, культури та спорту, управління відходами, здоров'я, а також у сфері надання освітніх послуг.

Серед механізмів системи освіти України сучасні науковці виділяють механізми удосконалення розвитку освіти (нормативно-правовий, організаційно-функціональний, кадрово-мотиваційний) та інтегровані механізми розвитку освіти (стратегічного фінансування, міжнародного співробітництва, науково-освітньої локалізації), які при комплексному застосуванні формують державну освітню політику. Інструментами реалізації вищезазначених механізмів визнано засоби,

прямі і непрямі форми, методи та прийоми, використовуючи які держава послідовно і систематично впливає на кон'юнктуру ринку освітніх послуг і діяльність закладів вищої освіти з метою підтримки оптимальних організаційних, соціальних, педагогічних, правових, кадрових, матеріально-фінансових та інших умов їх розвитку, забезпечення високоякісних освітніх послуг, рівного доступу до освіти, інтеграції української освітньої сфери у європейський простір [12].

Враховуючи наявність деякої нормативно-правової бази, яка хоча і перебуває на етапі становлення, мережу державних і приватних закладів освіти сфери захисту критичної інфраструктури, які у зв'язку із впровадженням цифрових технологій мають тенденцію до збільшення, суттєве розширення кола учасників освітньої діяльності у сфері захисту критичної інфраструктури, а також те, що механізми та інструменти системи освіти України, які мають як теоретичне, так і практичне значення, можуть так само застосовуватися і в системі підготовки кадрів у сфері захисту критичної інфраструктури, слід констатувати, що система, яка досліджується, заснована відповідно до чинного законодавства та перебуває на початковому шляху її розбудови.

На сьогодні, враховуючи думки та дослідження сучасних науковців, можна констатувати проблему відсутності єдиної методології в системі підготовки кадрів у сфері захисту критичної інфраструктури для всіх фахівців – як на державному, так і на приватному рівнях. Відсутність єдиних керівних документів, методичного забезпечення навчання, розбіжність у поглядах на мету, завдання та зміст підготовки з питань захисту критичної інфраструктури знижує ефективність та якість підготовки фахівців для всієї країни в цілому. Крім того, освітній рівень сфери захисту критичної інфраструктури в Україні має ризики до стрімкого послаблення через відсутність відповідної галузі знань.

Ці тези підтверджують статистичні дані, які узагальнено за результатами вивчення освітньо-практичних аспектів, а також численні інформаційні та аналітичні документи сучасних аналітиків і експертів. Так, протягом останніх двох – трьох років державні та приватні заклади вищої освіти випускають відповідних фахівців для потреб сфери захисту критичної інфраструктури у дуже вузькому та роздрібленому напрямі, що є суттєвим освітнім дисбалансом у зазначеній сфері.

Враховуючи зазначене, з метою розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури, необхідним є удосконалення реалізації відповідного механізму, що можна зробити шляхом удосконалення законодавства, вивчення міжнародного досвіду та запозичення кращих практик (рис. 1).

Розроблений проєкт – це механізм створений для зацікавленості приватного сектору в розвитку освіти у сфері захисту критичної інфраструктури, стимулювання співпраці між науковим і освітнім секторами економіки, підтримки суб'єктів національної системи захисту критичної інфраструктури, надання допомоги у створенні державної політики та плануванні освітніх ініціатив, а також для спільного усвідомлення і визначення ключових понять та складових у процесі формування комплексу організаційних, нормативно-правових, інженерно-технічних, ресурсних, інформаційно-аналітичних та методологічних заходів, спрямованих на забезпечення безпеки критичної інфраструктури.

Зазначений механізм спрямований на розбудову державно-приватного партнерства у сфері захисту критичної інфраструктури для впровадження нових інформаційних та освітніх технологій, застосування прогресивних форм організації освітнього процесу та активних методів навчання, а також сучасних навчально-методичних матеріалів, які в сукупності є основою для всебічного розвитку людини та добробуту населення в цілому.

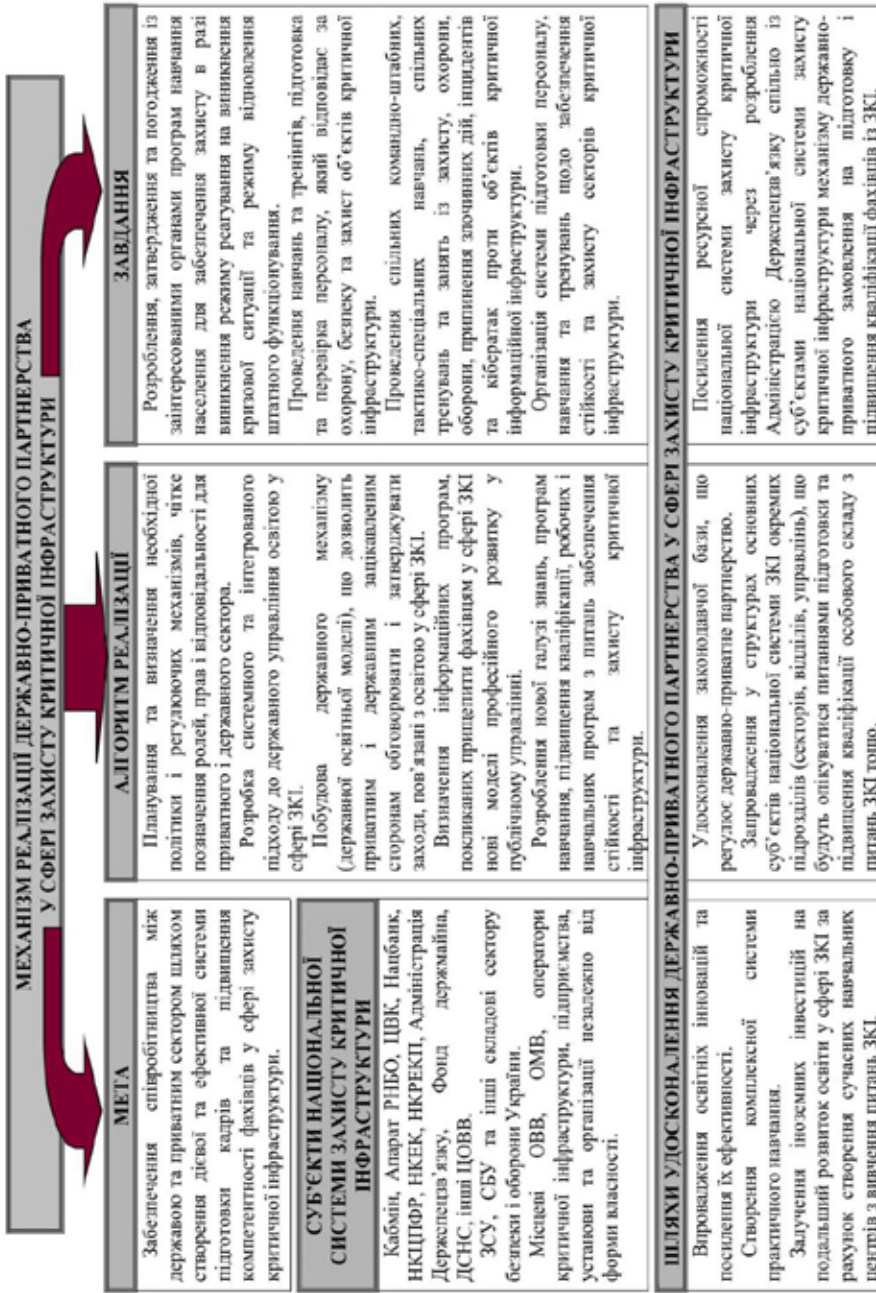


Рис. 1. Механізм реалізації державно-приватного партнерства у сфері захисту критичної інфраструктури

Джерело: розробка автора

Поле освіти у сфері захисту критичної інфраструктури України в тій чи іншій мірі формують Адміністрація Держспецзв'язку, яка забезпечує здійснення передбачених Законом України «Про критичну інфраструктуру України» повноважень уповноваженого органу у сфері захисту критичної інфраструктури під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування, секторальні органи у сфері захисту критичної інфраструктури, місцеві органи виконавчої влади та військово-цивільні адміністрації, оператори критичної інфраструктури, а також державні та приватні заклади вищої освіти.

Адміністрація Держспецзв'язку, відповідно до постанови Кабінету Міністрів України від 12 липня 2022 року № 787 «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України» [13], на теперішній час:

бере участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури;

забезпечує підготовку, перепідготовку, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури;

забезпечує в установленому порядку організацію підготовки, перепідготовки та підвищення кваліфікації державних службовців і працівників сфери захисту критичної інфраструктури.

Секторальні органи у сфері захисту критичної інфраструктури, а саме державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури, здійснюють організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури.

Місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення) у сфері захисту критичної інфраструктури забезпечують розроблення, затвердження та погодження із заінтересованими органами програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

Одними із основних завдань операторів критичної інфраструктури є проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури. При цьому оператори критичної інфраструктури забезпечують розроблення та затвердження у встановленому законодавством порядку проведення навчань та тренінгів, підготовку та перевірку персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури.

Процес освіти у сфері захисту критичної інфраструктури, створення в Україні дієвої та ефективної системи підготовки кадрів для сфери захисту критичної інфраструктури та підвищення компетентності фахівців різних сфер діяльності з питань захисту критичної інфраструктури необхідно розглядати, виходячи в першу чергу, з реалій та можливостей. Звісно, не можна не враховувати як позитивний, так і негативний досвід провідних країн світу, у яких вже впроваджені та функціонують аналогічні системи. Тому при аналізі алгоритму реалізації механізму державно-приватного партнерства необхідно робити особливий акцент, який вказує на необхідність:

розроблення відповідних змін до чинного законодавства, що у подальшому забезпечить єдність методологічно-освітніх засад діяльності суб'єктів державної системи захисту критичної інфраструктури;

правового регулювання з питань формування освітньої державної політики у сфері захисту критичної інфраструктури;

впровадження координації дій серед суб'єктів національної системи захисту критичної інфраструктури щодо підвищення компетентності фахівців у сфері захисту критичної інфраструктури;

підвищення рівня цифрових навичок та компетентностей в державі, а також рівня конкурентоспроможності країни щодо розвитку сфери захисту критичної інфраструктури;

створення певних індикаторів для контролю (моніторингу) стану розвитку цифрових навичок та компетентностей у сфері захисту критичної інфраструктури;

прискорення всіх освітніх процесів у сфері захисту критичної інфраструктури;

підвищення конкурентоспроможності співробітників сектору безпеки і оборони України, а також інших громадян шляхом оволодіння новими цифровими навичками та компетентностями у сфері захисту критичної інфраструктури.

Разом з тим виконання завдань, які визначені в рамках реалізації державно-приватного партнерства у сфері захисту критичної інфраструктури, надади би змогу:

забезпечити обмін інформацією між державними органами, місцевими органами виконавчої влади, органами місцевого самоврядування, операторами критичної інфраструктури, громадськими об'єднаннями, організаціями роботодавців, а також громадянами щодо загроз критичній інфраструктурі та реагування на кризові ситуації;

визначити повноваження та відповідальність державних органів і операторів критичної інфраструктури у сфері забезпечення безпеки та стійкості критичної інфраструктури;

визначити порядок взаємодії між державними органами та операторами критичної інфраструктури у різних режимах функціонування об'єктів критичної інфраструктури;

залучати експертний потенціал наукових установ, професійних та громадських об'єднань до підготовки галузевих проєктів та нормативно-правових актів у сфері захисту критичної інфраструктури;

залучати до виконання завдань із забезпечення сталого функціонування об'єктів критичної інфраструктури суб'єкти господарювання, які провадять діяльність, пов'язану із забезпеченням безпеки об'єктів критичної інфраструктури, громадських об'єднань та професійних організацій;

надавати державними органами консультативної та практичної допомоги операторам критичної інфраструктури з питань реагування на кризові ситуації на об'єктах критичної інфраструктури.

Наступною відправною точкою в удосконаленні державно-приватного партнерства у сфері захисту критичної інфраструктури є негайна потреба у розробленні освітньо-стратегічного бачення у зазначеній сфері, та затвердженні відповідних нормативно-правових документів урядового рівня, спрямованих на підвищення компетентності фахівців різних сфер діяльності з питань захисту критичної інфраструктури.

Впровадження освітніх інновацій та посилення їх ефективності, а також створення комплексної системи практичного навчання нададуть змогу:

створити сучасну цілісну та гнучку систему професійного розвитку;

забезпечити якість та безперервність набуття досвіду шляхом підвищення кваліфікації та самоосвіти;

створити належні умови для реалізації права на професійне зростання;

створити умови для конкуренції серед співробітників;
забезпечити розвиток професійної компетентності [1, с. 28–29].

Створення сучасних навчальних центрів з вивчення питань захисту критичної інфраструктури зможуть забезпечити:

гранти та стипендії для студентів, які опановують спеціальності тотожні сфері захисту критичної інфраструктури;

професійну сертифікацію та можливість тестування студентів на відповідність професійним стандартам сфери захисту критичної інфраструктури;

матеріальну підтримку та працевлаштування випускників.

Разом з тим, запровадження у структурах основних суб'єктів національної системи захисту критичної інфраструктури окремих підрозділів (секторів, відділів, управлінь), що будуть опікуватися питаннями підготовки та підвищення кваліфікації особового складу з питань захисту критичної інфраструктури, надасть можливість:

вдосконалити професійну підготовку шляхом поглиблення і розширення професійних знань, умінь і навичок;

набути фахівцями досвіду виконання додаткових завдань та обов'язків у межах отриманої спеціальності;

підвищувати рівень професійних знань, удосконалити свою майстерність;
закріпити й удосконалити особисті практичні уміння і навички, необхідні для якісного та ефективного виконання службових обов'язків;

оновити, розширити і формувати нові професійні знання;
вивчити сучасні методи управління, ознайомитись з досягненнями науки і техніки та перспективами їх розвитку;

розроблювати пропозиції щодо удосконалення і впровадження у практику найкращих досягнень науки і техніки.

У свою чергу посилення ресурсної спроможності національної системи захисту критичної інфраструктури через розроблення Адміністрацією Держспецзв'язку спільно із суб'єктами національної системи захисту критичної інфраструктури механізму державно-приватного замовлення на підготовку і підвищення кваліфікації фахівців із захисту критичної інфраструктури надав би змогу:

забезпечувати розвиток суб'єктів національної системи захисту критичної інфраструктури за рахунок впровадження освітніх інновацій та посилення їх ефективності;

підвищити загальну культуру відносин між державною і приватною сферою захисту критичної інфраструктури за допомогою створення комплексної системи практичного навчання;

вирішувати проблеми зайнятості населення та залучати іноземні інвестиції на подальший розвиток освіти у сфері захисту критичної інфраструктури за рахунок створення сучасних навчальних центрів з вивчення зазначених питань.

На сьогодні в Україні система підготовки кадрів у сфері захисту критичної інфраструктури перебуває у трансформаційному стані. Існують поодинокі стохастичні явища, але будь-яка комплексна системність практично відсутня. Закон України «Про критичну інфраструктуру» жодним чином не вирішує цієї проблеми, залишаючи осторонь ключові проблеми забезпечення і контролю якості та визнання освіти у сфері захисту критичної інфраструктури. Не існує офіційної статистики з цих питань, відсутні спеціальні концепції та освітні програми. Тому для України вкрай важливо найближчим часом вжити дієві заходи для подолання відставання у цій сфері.

Забезпеченню якісної підготовки фахівців у сфері захисту критичної інфраструктури має сприяти інтеграція закладів вищої освіти, академічних і галузевих секторів науки. У цьому контексті особливого значення має набути впровадження у діяльність закладів освіти інноваційних технологій на кшталт віртуальних лабораторій. Адже нині освіта у сфері захисту критичної інфраструктури характеризується недостатнім рівнем інноваційної активності. Цьому певною мірою сприяє і те, що, власне, в науці, яка нині поділяється на академічну, галузеву та вишівську, на жаль, існує незбалансованість її зусиль на розвиток та впровадження нових організаційних форм, які відповідають логіці ринкових відносин, у тому числі у сфері захисту критичної інфраструктури. Подолання цих недоліків сприятиме інтеграції освіти у сфері захисту критичної інфраструктури, залученню роботодавців до підготовки відповідних фахівців, прискоренню формування конкурентоспроможної головної продуктивної сили суспільства.

Висновки. Навчання протягом життя виходить на чільні позиції у світових освітніх процесах – це диктується базовими тенденціями сучасного розвитку людства. Такий підхід, на наш погляд, дозволить кардинально змінити систему підготовки кадрів у сфері захисту критичної інфраструктури. Адже до цього часу, на жаль, у переважній більшості вона зорієнтована на запити минулого. Сучасна ж економіка потребує кадрів, готових працювати в умовах конкуренції, тобто в інноваційній економіці [1, с. 29].

Слід відзначити, що на теперішній час вже здійснено перший крок у посиленні співпраці у сфері захисту критичної інфраструктури. На сьогодні, співробітництво України та міжнародних партнерів має стратегічне значення як для посилення захисту об'єктів критичної та критичної інформаційної інфраструктури України, так і для збільшення рівня стійкості систем наших партнерів. Тому Держспецзв'язку, розуміючи важливість зміцнення українських систем, які зазнають атак ворога як у кібер-, так і в фізичному просторі, постійно розширює співробітництво з іноземними партнерами. Так, у лютому 2024 року Держспецзв'язку розпочато співпрацю із Фондом цивільних досліджень та розвитку США CRDF, ключовими питаннями якої є захист українських інформаційних ресурсів у кіберпросторі та захист об'єктів критичної інфраструктури, які зазнають різноманітних загроз, пов'язаних передусім з російською агресією проти нашої держави [14].

Для посилення власного захисту в цих надзвичайно складних умовах наша держава потребує залучення допомоги у вигляді консультацій та навчань, а також сучасних технічних і технологічних засобів та інструментів. Україна має унікальний досвід протистояння численним спробам російських військових у різних доменах атакувати об'єкти критичної та критичної інформаційної інфраструктури, яким готова ділитися з партнерами. Передусім, цей досвід стосується комплексних ударів із застосуванням засобів, які раніше не використовувалися під час повномасштабних воєн: кібератак, масованих ракетних обстрілів, атак дронами.

Партнерами висловлено готовність не просто продовжувати всебічну підтримку України, а й посилювати співпрацю, яка є гарантією не лише захисту нашої держави під час війни, а й подальшого формування передових систем захисту, які стануть нормою для цивілізованого світу [14].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Арсенович Л. А. Деякі питання удосконалення державно-приватної взаємодії у сфері кіберосвіти. *Публічне управління і адміністрування в Україні*. Випуск № 31. 2022. С. 23–30.

2. Про критичну інфраструктуру : Закон України № 1882-IX від 16.11.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
3. Жевелєва І. С. Правові засади забезпечення інформаційної безпеки об'єктів критичної інфраструктури. *Міжнародний науковий журнал «Інтернаука». Серія : Юридичні науки*. 2020. № 5. С. 22–28.
4. Лук'яненко І. Г. Роль державно-приватного партнерства в розбудові критичної інфраструктури для досягнення цілей сталого розвитку в Україні / І. Г. Лук'яненко, М. Е. Мар'янович. *Економіка, фінанси, грошовий обіг і кредит*. 2020. № 1. С. 291–297.
5. Павлов Д. М. Правові та організаційні засади забезпечення захисту критичної інфраструктури у контексті формування нової безпекової парадигми України / Д. М. Павлов, М. А. Микитюк. *Честь і закон*. 2020. № 4 (75). С. 69–77.
6. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України / О. М. Суходоля. *Стратегічні пріоритети*. 2016. № 3. С. 62–76.
7. Губанова Т. Державно-приватне партнерство у сфері освіти і науки в Україні: нормативно-правова характеристика. *Підприємництво, господарство і право*. 2019. Вип. № 6. С. 220–224.
8. Шевчук О. А. Державно-приватне партнерство в сфері інноваційного розвитку : дис. ... доктора філософ. у галузі публ. управлін. та адмініструв. : 281 / Державний університет «Житом. політех». Житомир, 2021. 175 с.
9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України № 447/2021 від 26.08.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.
10. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України № 1009-р від 06.12.2017 р. URL: <https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text>.
11. Про державно-приватне партнерство : Закон України № 2404-VI від 01.07.2010 р. URL: <https://zakon.rada.gov.ua/laws/show/2404-17#Text>.
12. Якайтис І. Б. Механізми державного управління інноваційним розвитком вищої освіти в Україні : автореф. дис. ... канд. наук. з держ. упр. : 25.00.02. Івано-Франківськ, 2018. 22 с.
13. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : постанова Кабінету Міністрів України № 787 від 12.07.2022 р. URL: <https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text>.
14. Держспецзв'язку посилює співпрацю у сфері кіберзахисту та захисту критичної інфраструктури : веб-сайт. URL: <https://www.cip.gov.ua/ua/news/derzhspezczy-yazku-posilyuye-spivpracyu-u-sferi-kiberzakhistu-ta-zakhistu-kritichnoi-infrastrukturi>.

REFERENCES:

1. Arsenovych L. A. (2022) Deaki pytannia udoskonalennia derzhavno-pryvatnoi vzaiemodii u sferi kiberosvity [Some issues of improving public-private cooperation in the field of cyber education]. *Publichne upravlinnia i administruvannia v Ukraini*, Vyp. 31, 23–30.
2. The Verkhovna Rada of Ukraine (2021). Pro krytychnu infrastrukтуру [About critical infrastructure]. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
3. Zhevelieva I. S. (2020) Pravovi zasady zabezpechennia informatsiinoi bezpeky ob'ektiv krytychnoi infrastruktury [Legal principles of ensuring information security of critical infrastructure objects]. *Mizhnarodnyi naukovyi zhurnal "Internauka". Seriya : Yurydychni nauky*, Vyp. 5, 22–28.

4. Lukianenko I. H. (2020) Rol derzhavno-pryvatnoho partnerstva v rozbudovi krytychnoi infrastruktury dlia dosiahnennia tsilei staloho rozvytku v Ukraini [The role of public-private partnership in the development of critical infrastructure to achieve the goals of sustainable development in Ukraine]. *Ekonomika, finansy, hroshovy obih i kredyt*, Vup. 1, 291–297.

5. Pavlov D. M. (2020) Pravovi ta orhanizatsiini zasady zabezpechennia zakhystu krytychnoi infrastruktury u konteksti formuvannia novoi bezpekovoii paradyhmy Ukrainy [Legal and organizational principles of ensuring the protection of critical infrastructure in the context of the formation of a new security paradigm of Ukraine]. *Chest i zakon*, Vup. 4 (75), 69–77.

6. Cukhodolia O. M. (2016) Zakhyst krytychnoi infrastruktury v umovakh hibrydnoi viiny: problemy ta priorityety derzhavnoi polityky Ukrainy [Protection of critical infrastructure in conditions of hybrid warfare: problems and priorities of the state policy of Ukraine]. *Stratehichni priorityety*, Vup. 3, 62–76.

7. Hubanova T. (2019) Derzhavno-pryvatne partnerstvo u sferi osvity i nauky v Ukraini: normatyvno-pravova kharakterystyka [Public-private partnership in the field of education and science in Ukraine: regulatory and legal characteristics]. *Pidpriemnytstvo, hospodarstvo i pravo*, Vup. 6, 220–224.

8. Shevchuk O. A. (2021). Derzhavno-pryvatne partnerstvo v sferi innovatsiinoho rozvytku [Public-private partnership in the field of innovative development]. *Dissertation of the Doctor of Philosophy*. Zhytomyr [in Ukrainian].

9. Office of the President of Ukraine (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku “Pro Stratehiiu kiberbezpeky Ukrainy” [On the decision of the National Security and Defense Council of Ukraine from May 14, 2021 “About the Cyber Security Strategy of Ukraine”]. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.

10. The Cabinet of Ministers of Ukraine (2017). Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury [On the approval of the Concept of creation of a state system for the protection of critical infrastructure]. URL: <https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text>.

11. The Verkhovna Rada of Ukraine (2010). Pro derzhavno-pryvatne partnerstvo [About public-private partnership]. URL: <https://zakon.rada.gov.ua/laws/show/2404-17#Text>.

12. Yakaitis I. B. (2018). Mekhanizmy derzhavnoho upravlinnia innovatsiinym rozvytkom vyshchoi osvity v Ukraini [Mechanisms of state management of innovative development of higher education in Ukraine]. *Abstract for obtaining the scientific degree of candidate of sciences*. Ivano-Frankivsk [in Ukrainian].

13. The Cabinet of Ministers of Ukraine (2022). Pro utvorennia Derzhavnoi sluzhby zakhystu krytychnoi infrastruktury ta zabezpechennia natsionalnoi systemy stiiikosti Ukrainy [On the establishment of the State Service for the Protection of Critical Infrastructure and Ensuring the National System of Ukraine’s Stability]. URL: <https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text>.

14. Derzhspetsviazku posyliuie spivpratsiu u sferi kiberzakhystu ta zakhystu krytychnoi infrastruktury : veb-sait [The State Intelligence Service is strengthening cooperation in the field of cyber defense and critical infrastructure protection: website]. URL: <https://www.cip.gov.ua/news/derzhspetsv-yazku-posilyuye-spivpracyu-u-sferi-kiberzakhystu-ta-zakhystu-kritichnoyi-infrastrukturi>.