Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2024. № 11.

DOI: http://doi.org/10.32702/2307-2156.2024.11.11
УДК 35.088.6:[004:007:351.86] (477)

Л. А. Арсенович,

доктор філософії з публічного управління та адміністрування, заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом, Адміністрація Держспецзв'язку

ORCID ID: https://orcid.org/0000-0001-7081-2838

КЛАСИФІКАЦІЯ ТА МЕТОДИ ОРГАНІЗАЦІЇ СИСТЕМИ ПІДГОТОВКИ КАДРІВ ДЛЯ СФЕРИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

L. Arsenovych,

PhD in Public Management and Administration, Deputy Head – Head of Division at the HR Management Department of the Administration of the State Service for Special Communication and Information Protection of Ukraine, Derzhspetszviazok

CLASSIFICATION AND METHODS OF ORGANIZING A SYSTEM OF TRAINING CRITICAL INFRASTRUCTURE PROTECTION SPECIALISTS

Науково-технічний прогрес докорінно змінив сучасне суспільство: на теперішній день сфера захисту критичної інфраструктури відіграє важливу роль у розвитку країни та визначенні рівня життя населення. За останнє десятиліття сфера захисту критичної інфраструктури стала настільки потужним фактором розвитку суспільства, що привела до утворення нового технологічного укладу, який сприяє внутрішньодержавній і світовій інтеграції.

Україна на теперішній час впевнено стала на шлях впровадження сфери захисту критичної інфраструктури.

В умовах збройної агресії проти України, розвиток та впровадження сфери захисту критичної інфраструктури призвело до формування нового спектра ризиків і загроз у сфері національної безпеки. Загрози у сфері захисту критичної інфраструктури охоплюють усі базові сфери суспільної і громадської діяльності (політичну, безпекову, правову, економічну, соціальну тощо), погрозливо впливаючи на суб'єктів національної системи захисту критичної інфраструктури.

Забезпечення безпеки та безперебійного функціонування об'єктів критичної інфраструктури значною мірою залежить від так званого «людського фактору». Саме рівень підготовленості фахівців, їхні компетенції, розуміння специфіки діяльності об'єктів та механізмів здійснення взаємодії багато в чому зумовлюють успіх справи в цілому. Огляд і первинна систематизація наукових праць за обраною темою дозволив встановити, що попри значний інтерес дослідників до підготовки фахівців із захисту критичної інфраструктури поза увагою вчених залишаються суттєві аспекти даного питання.

Нові та небезпечні виклики регіональній і глобальній безпеці висувають на порядок денний завдання із побудови в Україні освітньої моделі захисту критичної інфраструктури та наукової розробки зазначеної проблематики. У таких умовах зазначені обставини спонукають до аналізу нормативно-правового забезпечення підготовки фахівців у сфері захисту критичної інфраструктури, розгляду апробованого досвіду з організації освітніх заходів у зазначеній сфері в провідних країнах світу, та побудови нової системи підготовки фахівців у сфері захисту критичної інфраструктури.

У статті автором розглянуто класифікацію та методи організації системи підготовки кадрів для сфери захисту критичної інфраструктури, яка в умовах воєнного стану повинна стати потужним важелем до створення, впровадження, розвитку та забезпечення функціонування національної

системи захисту критичної інфраструктури, а також забезпечення її безпеки та стійкості.

The science and technology progress has changed the modern society dramatically: today, the critical infrastructure protection plays an important role in the country development and in determining people's living standards. Over the past decade, the critical infrastructure protection has become so much a powerful society development driver that it was able to have resulted in a new technology structure that encourages the domestic and global integration. These days, Ukraine is strongly underway introducing the critical infrastructure protection functionality.

In the context of armed aggression against Ukraine, the development and implementation of critical infrastructure protection has given rise to a new range of national security risks and threats. Threats in the area of critical infrastructure protection involve all basic spheres of social and public activity (political, security, legal, economic, civic, etc.) dangerously affecting the entities of the national critical infrastructure protection system.

Safety and uninterrupted operation of critical infrastructure facilities largely depends on the so-called "human factor". It is the qualification of specialists, their competences, understanding of how the facilities operate and how the interaction occurs that largely determine the overall success in this area. The study and initial systematization of scientific works dedicated to the chosen topic helped us find out that despite significant interest of researchers in the training of critical infrastructure protection specialists, essential aspects of this issue still remain outside the attention of scientists.

New and dangerous challenges to regional and global security put the task on the agenda focused on building an educational model in Ukraine dedicated to the subject of critical infrastructure protection and on scientific development of the mentioned issues. In such conditions, these circumstances stimulate to analyze the regulatory support of the training of critical infrastructure protection specialists, to study the tried-and-tested practices of organizing critical infrastructure protection

education events in the world's major countries, and to build a new system of training critical infrastructure protection specialists.

In the article, the author analyzes the classification and methods of organizing a system of training critical infrastructure protection specialists, which, under martial law, should become a powerful leverage for creating, implementing, developing and ensuring the national system of critical infrastructure protection, as well as providing for its security and sustainability.

Ключові слова: *критична інфраструктура, національна система захисту критичної інфраструктури, освіта, професійна підготовка, сфера захисту критичної інфраструктури.*

Keywords: *critical infrastructure, national system of critical infrastructure protection, education, professional training, critical infrastructure protection.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Ефективність реформування публічного управління та децентралізації влади в Україні в умовах воєнного стану залежить певною мірою від рівня професіоналізму керівників органів державної і місцевої влади, у тому числі очільників суб'єктів національної системи захисту критичної інфраструктури, їх мотивації до впровадження відповідних змін, готовності розвивати особистий потенціал та сприяти розвитку органу, в якому вони працюють (проходять службу). Компетентність та обізнаність кадрів усіх рівнів управлінської ієрархії є критерієм дієвості та ефективності діяльності усіх органів влади, що в свою чергу впливає на характер сприйняття їхнього іміджу в державі та суспільстві в цілому.

Необхідною умовою для України щодо впровадження Болонського процесу та імплементації Угоди про асоціацію між Україною та ЄС в галузі освіти, створення єдиного європейського освітнього простору та забезпечення освіти упродовж життя є наближення професійної освіти до ринку праці на

засадах соціального партнерства відповідно до європейської і національної рамок кваліфікацій та вимог професійних стандартів [1, с. 18].

Разом з тим, професійна підготовка фахівців національної системи захисту критичної інфраструктури, а також відповідна система підготовки кадрів, яка на сьогодні перебуває в процесі становлення, не відповідають нинішнім вимогам та потребують модернізації. Для забезпечення впровадження відповідної системи підготовки кадрів для сфери захисту критичної інфраструктури недостатнім є закріплення відповідних положень у Законі України «Про критичну інфраструктуру» [2], Концепції створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 06 грудня 2017 року № 1009-р [3], а також у Національному плані захисту та забезпечення безпеки та стійкості критичної інфраструктури, затвердженим розпорядженням Кабінету Міністрів України від 19 вересня 2023 року № 825-р [4].

Аналіз останніх досліджень і публікацій. Впровадження системи підготовки кадрів для сфери захисту критичної інфраструктури можливе тільки через систему дієвих, ефективних та результативних механізмів державного регулювання. Адже науковими дослідженнями доведено, що нинішня система захисту критичної інфраструктури не відповідає сучасним загрозам, потребує як наукового (методичного) забезпечення, так і розроблення прикладних і практичних заходів адміністративно-правового та освітнього регулювання державної політики у цій сфері. Зазначене зумовлює актуальність окресленої проблематики.

Так, науковець С. Теленик досліджуючи пріоритети адміністративно-правового регулювання державної політики України у сфері захисту критичної інфраструктури у контексті прийняття нової стратегії Національної безпеки України зазначає, що для створення, розвитку і закріплення Державної системи захисту критичної інфраструктури, налагодження координації та посилення міжвідомчої взаємодії між усіма її суб’єктами в Україні необхідно організовувати й проводити низку ефективних заходів (навчання, тренінги,

семінари), внаслідок яких буде виявлятися актуальна потреба в адміністративно-правовому регулюванні діяльності суб'єктів захисту критичної інфраструктури, формуванні правових механізмів спільного захисту критично важливих для держави об'єктів життєдіяльності від усіх видів загроз і їх комбінацій («каскадних ефектів») [5, с. 257].

Крім цього, вчена Леоненко Н.А., співробітник Національного університету цивільного захисту України, вивчаючи державну політику забезпечення безпекового середовища функціонування критичної інфраструктури в Україні зазначає, що в умовах збройної агресії російської федерації проти України, серед невідкладних заходів, які необхідно вжити, є недопущення поширення інформації, розголошення якої може призвести до обізнаності противника про об'єкти критичної інфраструктури, у тому числі про критичну технологічну інформацію: запровадження навчальних програм, курсів підвищення кваліфікації з радіоелектронної розвідки та радіоелектронної боротьби для військовослужбовців підрозділів, залучених до забезпечення захисту і оборони об'єктів критичної інфраструктури [6, с. 168].

Вчена приходить до висновку, що в умовах існуючих реальних і потенційних загроз під час воєнного стану, пошук та розробка дієвих інструментів державної політики забезпечення безпекового середовища функціонування критичної інфраструктури в Україні – це необхідні кроки у напрямку стабілізації суспільного життя в умовах надзвичайних ситуацій, підтримки життєстійкості об'єктів критичної інфраструктури, узгодженості та координації діяльності суб'єктів національної системи захисту та ефективна протидія кризовим явищам в питаннях посилення обороноздатності і соціально-економічного розвитку держави [6, с. 168].

Разом з тим, співробітники Національного університету «Львівська політехніка» Дзяна Г.О. та Дзяний Р.Б. у своїй спільній статті зазначають, що система публічного управління відіграє основну роль у забезпеченні функціонування держави і суспільства та охоплює широкий спектр рішень і дій, від формування та реалізації державної політики до надання низки державних

послуг та прийняття управлінських рішень. Вчені приходять до висновку, що використання в державних структурах застарілих систем та програмного забезпечення, обмежені ресурси для їх оновлення, недостатня підготовка персоналу, брак знань та навичок у сфері кібербезпеки у державних службовців та відсутність чіткої політики і процедур реагування на кіберінциденти – є тими чинниками, що дозволяють розглядати систему публічного управління як об'єкт критичної інфраструктури [7, с. 372].

Враховуючи зазначені праці можемо зробити висновок, що використання усталених підходів до підготовки кадрів для сфери захисту критичної інфраструктури не забезпечить її інноваційний розвиток, а також професіоналізацію суб'єктів національної системи захисту критичної інфраструктури.

Формулювання цілей статті (постановка завдання). Метою статті є розгляд теоретичних підходів до впровадження професійної підготовки фахівців національної системи захисту критичної інфраструктури.

Виклад основного матеріалу дослідження. На сьогодні умови воєнного стану вимагають запровадити нові ефективні механізми державного регулювання системи підготовки кадрів для сфери захисту критичної інфраструктури, у тому числі в нормативно-правовому напрямі, забезпечити комплексність їх дії, а також створити умови для подальшого регулювання освітніх процесів.

У цьому аспекті серед актів Президента України слід виділити рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року, введеного в дію Указом Президента України від 17 жовтня 2023 року № 695/2023 «Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», відповідно до якого Міністерству оборони України передбачено запровадити навчальні програми, курси підвищення кваліфікації з радіоелектронної розвідки та радіоелектронної боротьби для

військовослужбовців підрозділів, залучених до забезпечення захисту і оборони об’єктів критичної інфраструктури [8].

Серед актів Уряду необхідно звернути увагу на Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19 червня 2019 року № 518 [9], які визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, а також повноваження власників/керівників об’єктів критичної інфраструктури, які передбачають впровадження програм підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечення щорічного контролю рівня обізнаності.

Крім цього план заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року, затверджений розпорядженням Кабінету Міністрів України від 10 листопада 2023 року № 1025-р [10], передбачає забезпечення розроблення та впровадження Нацдержслужбою, Міноборони та Адміністрацією Держспецзв’язку програм підвищення кваліфікації державних службовців, працівників державних органів, що входять до складу сектору безпеки та оборони, посадових осіб органів управління та органів місцевого самоврядування з питань кібербезпеки та захисту критичної інфраструктури.

Положення зазначених актів також наштовхують на думку, що для створення дієвої і ефективної системи підготовки кадрів для сфери захисту критичної інфраструктури, крім нормативно-правового врегулювання зазначеного питання, необхідно розкрити класифікацію такої системи, а також методи її організації.

У чинному Положенні про систему професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад, затвердженому постановою Кабінету Міністрів України від 6 лютого 2019 року № 106 [11], учасники професійного навчання можуть реалізовувати своє право на професійне навчання через підготовку, підвищення кваліфікації,

стажування та самоосвіту. Підвищення кваліфікації здійснюється за програмами, які за змістом навчання поділяються на загальні і спеціальні. Разом з тим, загальні та спеціальні програми підвищення кваліфікації за тривалістю та інтенсивністю поділяються на професійні (сертифікатні) програми та короткострокові програми. В свою чергу програми підвищення кваліфікації можуть передбачати очну (денну, вечірню), дистанційну та змішану (очну та дистанційну з використанням спеціальних інтернет-платформ, веб-сайтів тощо) форми навчання.

Відповідно до Концепції трансформації системи військової освіти, затвердженої постановою Кабінету Міністрів України від 15 грудня 1997 року № 1410 (в редакції постанови Кабінету Міністрів України від 30 грудня 2022 року № 1490) [12], система військової освіти включає:

– ступені та рівні освіти; рівні військової освіти; галузі знань і спеціальностей; стандарти освіти та професійні стандарти; освітні програми; кваліфікації;

– ліцензійні умови; заклади спеціалізованої освіти військового спрямування та інші суб'єкти освітньої діяльності;

– учасників освітнього процесу; органи управління у сфері військової освіти, а також нормативно-правові акти, що регулюють відносини між ними.

Разом з тим, структура військової освіти включає:

– підготовку ліцеїстів військових ліцеїв (ліцеїв з посиленою військово-фізичною підготовкою), а також учнів професійних коледжів з посиленою військовою та фізичною підготовкою;

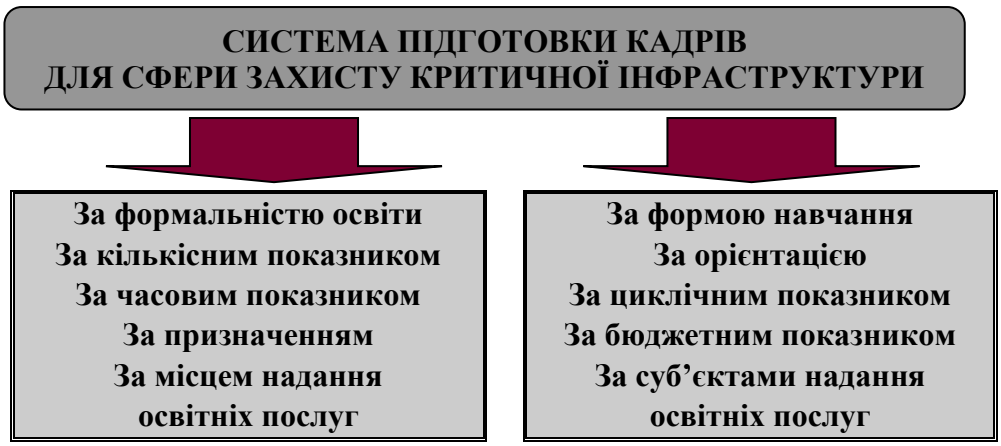
– підготовку військовослужбовців сержантського (старшинського) складу із одночасним здобуттям фахової передвищої військової освіти та вищої освіти;

– підготовку військовослужбовців офіцерського складу із одночасним здобуттям відповідних ступенів вищої освіти і рівнів військової освіти (тактичний, оперативний, стратегічний);

– підготовку військовослужбовців офіцерського складу на курсах професійної військової освіти для здобуття відповідних рівнів військової освіти (тактичний, оперативний, стратегічний);

– військову підготовку громадян України за програмою підготовки офіцерів запасу [12].

Аналіз цих переліків не забезпечує виявлення певної класифікаційної ознаки, за якою їх сформовано. Враховуючи індивідуальну освітню траєкторію фахівця сфери захисту критичної інфраструктури, що формується з урахуванням його здібностей, досвіду, мотивації, потреб, інтересів, можливостей, пропонуємо класифікувати систему підготовки кадрів для сфери захисту критичної інфраструктури з урахуванням необхідності її планування, організації, контролю й аналізу за такими ознаками (рис. 1):



Джерело: розробив автор

Рис. 1. Класифікація системи підготовки кадрів для сфери захисту критичної інфраструктури

Розкриємо зміст цієї класифікації.

За формальністю освіти система підготовки кадрів для сфери захисту критичної інфраструктури поділяється на формальну, неформальну та інформальну освіту. У рамках формальної освіти передбачено здобуття ступенів вищої освіти (бакалавр, магістр), наукових ступенів (доктор філософії та доктор наук), а також підвищення кваліфікації; у рамках неформальної освіти – здобуття ступеня вищої освіти за іншою спеціальністю (у тому числі тактичного, оперативного та стратегічного рівнів військової освіти – для осіб

офіцерського складу), навчання за програмами тематичних (фахових) постійно діючих і короткострокових семінарів (тренінгів, спеціалізованих короткострокових курсів), стажування, наставництво; у рамках інформальної освіти передбачено самоосвіту, що може здійснюватися у формі онлайн-навчання на освітніх веб-платформах, а також шляхом участі у конференціях (науково-практичних конференціях), майстер-класах, курсах з оволодіння практичними навичками тощо.

Перший (бакалаврський) рівень вищої освіти передбачає здатність до розв'язування спеціалізованих задач у сфері захисту критичної інфраструктури, які включають уміння запобігати проявам несанкціонованого втручання в її функціонування, прогнозувати та запобігати кризовим ситуаціям на об'єктах критичної інфраструктури, попереджувати кризові ситуації, що порушують безпеку критичної інфраструктури.

Другий (магістерський) рівень вищої освіти передбачає набуття здатності до розв'язування задач пов'язаних із створенням (впровадженням, розвитком) та забезпеченням функціонування національної системи захисту критичної інфраструктури.

Освітньо-науковий (науковий) рівень вищої освіти передбачає здобуття теоретичних знань (умінь, навичок) та інших компетентностей, достатніх для продукування нових ідей, розв'язання комплексних проблем у сфері захисту критичної інфраструктури, а також проведення власного наукового дослідження пов'язаного із розробленням та реалізацією державних цільових програм (нормативно-правової та нормативно-технічної бази) із захисту критичної інфраструктури та з питань забезпечення безпеки об'єктів критичної інфраструктури.

Підвищення кваліфікації фахівців суб'єктів національної системи захисту критичної інфраструктури – це набуття учасниками професійної підготовки нових та/або вдосконалення раніше набутих компетентностей пов'язаних із:

– визначенням вимог до забезпечення захисту та стійкості секторів критичної інфраструктури;

– здійсненням оцінки захищеності об’єктів критичної інфраструктури;

– проведенням оцінки загроз критичній інфраструктурі на національному рівні (оцінки загроз національній безпеці внаслідок реалізації загроз критичній інфраструктурі із залученням секторальних та функціональних органів у сфері захисту критичної інфраструктури) тощо.

Здобуття ступеня вищої освіти за іншою спеціальністю (у тому числі тактичного, оперативного та стратегічного рівнів військової освіти – для осіб офіцерського складу) – це організоване та цілеспрямоване навчання, що передбачає:

– задоволення потреб суб’єктів національної системи захисту критичної інфраструктури кваліфікованим особовим складом;

– набуття нових та/або вдосконалення раніше набутих знань, практичного досвіду виконання завдань та обов’язків у службовій діяльності;

– оновлення (розширення, формування) нових професійних знань у сфері захисту критичної інфраструктури;

– вивчення сучасних методів управління, ознайомлення з досягненнями науки і техніки та перспективами їх розвитку;

– створення умов щодо професійного та особистісного розвитку фахівців суб’єктів національної системи захисту критичної інфраструктури.

Навчання за програмами тематичних (фахових) постійно діючих і короткострокових семінарів (тренінгів, спеціалізованих короткострокових курсів) охоплює питання здійснення завдань, функцій та повноважень тим чи іншим суб’єктом національної системи захисту критичної інфраструктури, враховуючи особливості виконання учасниками професійної підготовки їх посадових (службових) обов’язків у сфері захисту критичної інфраструктури.

Стажування у сфері захисту критичної інфраструктури – набуття учасниками професійної підготовки практичного досвіду виконання завдань та обов’язків у професійній діяльності, застосування яких надасть змогу забезпечувати функціонування системи обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури, а також координацію

секторальних органів щодо забезпечення безпеки та стійкості сфери захисту критичної інфраструктури.

Наставництво є однією з форм навчання (виховання) та становлення прийнятих на службу військовослужбовців та осіб начальницького складу суб'єктів національної системи захисту критичної інфраструктури. Метою наставництва є забезпечення оптимальної адаптації військовослужбовців та осіб начальницького складу до умов проходження служби, а також цілеспрямоване формування та розвиток професійних якостей, необхідних для виконання завдань, визначених Законом України «Про критичну інфраструктуру». При цьому основними завданнями наставництва є:

– допомога військовослужбовцям та особам начальницького складу в оволодінні професійними знаннями і необхідними практичними навичками для самостійного виконання завдань в їх службовій діяльності;

– виховання у військовослужбовців та осіб начальницького складу професійних, психологічних, морально-етичних якостей і громадянської свідомості, необхідних для ефективного виконання службових завдань, зміцнення військової (службової) дисципліни та правопорядку.

Самоосвіта, що може здійснюватися у формі онлайн-навчання на освітніх веб-платформах, а також шляхом участі у конференціях (науково-практичних конференціях), майстер-класах, курсах з оволодіння практичними навичками – це самоорганізоване здобуття учасниками професійної підготовки певних компетентностей під час повсякденної діяльності, пов'язаної з професійною (громадською) або іншою діяльністю, у тому числі дозвіллям.

Самоосвіта може охоплювати загальні питання публічного управління та місцевого самоврядування (загальні аспекти щодо запобігання корупції, забезпечення прав і свобод людини, рівних прав та можливостей жінок і чоловіків тощо), європейської та євроатлантичної інтеграції, підвищення рівня володіння державною та іноземними мовами, цифрового розвитку та забезпечення кібербезпеки (кіберзахисту), забезпечення післявоєнного відновлення та розвитку України, а також інші питання, визначені

відповідними державними (регіональними, місцевими) програмами, стратегіями тощо.

За кількісним показником система підготовки кадрів для сфери захисту критичної інфраструктури поділяється на індивідуальне та групове навчання. Індивідуальне навчання – форма організації навчального процесу, за якої надається можливість опановувати теоретичні знання та практичні навички за індивідуальним графіком навчання шляхом реалізації індивідуально-орієнтованих освітніх технологій навчання. При цьому, індивідуально-орієнтовані освітні технології навчання – форми організації навчального процесу, спрямовані на забезпечення психологічних (педагогічних) умов для мотивації освітньої діяльності слухача на основі його саморозвитку та самоактуалізації під час оволодіння навчально-освітнім матеріалом.

Індивідуальне навчання реалізуються шляхом варіативності та альтернативності змісту і форм навчання, направлених на урахування індивідуальних особливостей слухача, його стану здоров'я, особливостей сприйняття навчальної інформації та життєвих цілей, що можуть забезпечити відповідні умови для активної пізнавальної діяльності, самоконтролю та створення ситуації успіху в навчальній діяльності.

Групове навчання організовується у малих групах слухачів, об'єднаних спільною навчальною метою. Таке навчання відкриває можливості співпраці зі своїми колегами, дозволяє реалізувати відповідне спілкування, сприяє досягненню високих результатів засвоєння знань та вмінь. Така освітня модель легко й ефективно поєднується з традиційними формами і методами навчання, може застосовуватися на різних його етапах, а також дозволяє реалізувати природне прагнення до спілкування, взаємодопомоги і співпраці.

За часовим показником система підготовки кадрів для сфери захисту критичної інфраструктури, зокрема підвищення кваліфікації, поділяється на довгострокове та короткострокове навчання. Так, відповідно до Положення про професійне навчання працівників на виробництві, затвердженого наказом Міністерства праці та соціальної політики України, Міністерства освіти і науки

України від 26 березня 2001 року № 127/151, зареєстрованого в Міністерстві юстиції України 06 квітня 2001 року за № 315/5506 [13]:

– довгострокове підвищення кваліфікації передбачає оволодіння фахівцями комплексом знань, умінь та навичок, що сприяють якісному виконанню ними своїх безпосередніх обов'язків, а також розширення зони компетенції за місцем роботи (служби) з тривалістю від 72 до 500 годин;

– короткострокове підвищення кваліфікації здійснюється з метою поглибленого вивчення певного напряму діяльності, зокрема в разі модернізації, перепрофілювання чи структурної перебудови органу (підрозділу), значних змін у нормативно-правовій базі, що регулює його діяльність, із тривалістю не більше 72 годин.

Разом з тим, часові показники здобуття ступенів вищої освіти, наукових ступенів, проходження стажування регулюються Законом України «Про вищу освіту» [14] та іншими нормативно-правовими актами.

Система підготовки кадрів для сфери захисту критичної інфраструктури за призначенням класифікується за такими показниками:

– з метою адаптації до нових умов роботи (служби) або посади – характеризує процес навчання особового складу з новими умовами і правилами роботи в органі (підрозділі) національної системи захисту критичної інфраструктури, а також освітню інтеграцію фахівця зазначеної системи в колектив. Зазначене навчання (підвищення кваліфікації) необхідне як для фахівців, які тільки прийшли працювати (проходити службу) в орган (підрозділ), так і для співробітників, які були підвищені на посаді;

– з метою реалізації змін у законодавстві – розкриває процес навчання фахівців суб'єктів національної системи захисту критичної інфраструктури новим компетентностям, необхідним для ефективного вирішення завдань професійної діяльності, здійснення (або впровадження) відповідних змін, та формування «управлінської» культури серед фахівців зазначеної системи;

– з метою впровадження інновацій – характеризує використання нових освітньо-навчальних технологій у службовій діяльності шляхом проведення

кібер майстер-класів, навчальних воркшопів, кібертренінгів, забезпечення освітніх вебінарів, індивідуальних та групових кіберпроєктів, організації кіберквестів, освітніх івентів та впровадження розвиваючих кіберхакатонів;

– з метою просування по службі – розкриває процес проходження навчання, яке організовується для формування управлінської еліти, залучення до системи управління молодих професійно підготовлених кадрів, а також соціального становлення молоді у сфері захисту критичної інфраструктури;

– з метою покращення результатів службової діяльності – проходження такого навчання направлене на покращення виконання фахівцями сфери захисту критичної інфраструктури поставлених завдань, а також з метою прийняття рішення щодо їх преміювання, планування їхньої кар'єри тощо;

– з метою підвищення рівня управлінської або професійної майстерності – проходження такого навчання передбачає підвищення управлінської компетентності керівників усіх рівнів, що обумовлено новими організаційними формами побудови того чи іншого підрозділу, формуванням його інформаційного середовища, встановленням взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури;

– з метою особистісного розвитку – проходження такого навчання характеризує процес психолого-педагогічної допомоги фахівцю національної системи захисту критичної інфраструктури в становленні його суб'єктивності, культурної ідентифікації, соціалізації, а також життєвого самовизначення;

– з метою обміном досвіду та формування професійних мереж – важливим елементом такого навчання є створення мережі для обміну досвідом, вдалими практиками, популяризації та поширення кращого досвіду. Навчання, яке організовується з метою обміном досвіду та формування професійних мереж, фокусується на: створенні, систематизації та оновленні навчальних продуктів та інформаційно-методичних матеріалів; проведенні навчальних та інформаційно-просвітницьких заходів для формування професійних знань, умінь та навичок фахівців національної системи захисту критичної

інфраструктури; формуванні професійної мережі зазначених фахівців шляхом створення середовища для їх комунікації.

Місцем надання освітніх послуг у системі підготовки кадрів для сфери захисту критичної інфраструктури може бути заклад освіти, місце проходження служби (роботи) або інше підприємство, установа, організація будь-якої форми власності, що провадить освітню діяльність (у тому числі міжнародні та іноземні установи, організації, зокрема ті, які реалізують відповідні проєкти (програми) міжнародної технічної допомоги).

За формою навчання система підготовки кадрів для сфери захисту критичної інфраструктури поділяється на інституційну (очну (денну, вечірню), заочну, дистанційну, мережеву) та дуальну.

Очна (денна, вечірня) форма здобуття вищої освіти – це спосіб організації та забезпечення навчання здобувачів вищої освіти для потреб національної системи захисту критичної інфраструктури, що передбачає проведення навчальних та практичних занять. Завершення навчання за даною формою здобуття вищої освіти надасть змогу:

– планувати безпеку на національному рівні, узгоджувати розвиток нормативно-правових (організаційних) та науково-технологічних інструментів, призначених для виконання завдань захисту критичної інфраструктури;

– забезпечувати захищеність критичної інфраструктури при плануванні, визначенні пріоритетів та оцінці соціально-економічного розвитку країни;

– створювати механізми впливу на стан захищеності критичної інфраструктури.

Заочна форма здобуття вищої освіти – це спосіб організації навчання для потреб національної системи захисту критичної інфраструктури шляхом поєднання навчальних занять і заходів під час короткочасних сесій та самостійного оволодіння освітньою програмою. Знання, уміння та навички, отриманні після завершення навчання за даною формою здобуття вищої освіти нададуть змогу:

– розробляти проєкти законів та інших нормативно-правових актів у сфері захисту критичної інфраструктури;

– формувати та вести Реєстр об’єктів критичної інфраструктури, а також узагальнювати пропозиції суб’єктів національної системи захисту критичної інфраструктури щодо удосконалення зазначеної системи;

– взаємодіяти з секторальними, функціональними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури з питань забезпечення захисту об’єктів критичної інфраструктури.

Дистанційна форма здобуття освіти характеризується індивідуалізованим процесом здобуття освіти та опосередкованою взаємодією учасників освітнього процесу в спеціалізованому середовищі, що функціонує на основі сучасних психолого-педагогічних (інформаційно-комунікаційних) технологій. Результати такого навчання нададуть змогу фахівцю сфери захисту критичної інфраструктури:

– організовувати проведення оцінки захищеності об’єктів критичної інфраструктури, аналізувати та оцінювати загальний стан їх захищеності;

– проводити оцінку загроз критичній інфраструктурі на національному рівні із залученням секторальних і функціональних органів у сфері захисту критичної інфраструктури;

– готувати щорічну оцінку ризиків і загроз критичній інфраструктурі національного рівня.

Мережева форма здобуття вищої освіти розкриває такий спосіб організації навчання, завдяки якому оволодіння знаннями відбувається за участю закладу освіти та інших суб’єктів освітньої діяльності (що взаємодіють між собою на договірних засадах). Здобуття відповідних умінь і навичок після завершення навчання за мережевою формою здобуття вищої освіти нададуть змогу фахівцю сфери захисту критичної інфраструктури погоджувати проєктні ризики і загрози критичній інфраструктурі секторального рівня, а також готувати рекомендації щодо визначення вимог до забезпечення захисту та

стійкості секторів критичної інфраструктури відповідно до категорій об’єктів критичної інфраструктури.

Дуальна форма здобуття вищої освіти передбачає навчання на робочому місці (на підприємствах, в установах та організаціях) на основі договору, що в свою чергу надасть змогу фахівцю сфери захисту критичної інфраструктури:

– розробляти комплекс заходів з контролю за ризиками безпеки, виявляти (запобігати, ліквідувати) наслідки інцидентів безпеки на об’єктах критичної інфраструктури;

– встановлювати обов’язкові вимоги із забезпечення безпеки об’єктів критичної інфраструктури, у тому числі під час їх створення (прийняття в експлуатацію, модернізації);

– оцінювати виклики та загрози, що впливають на стійкість критичної інфраструктури.

За орієнтацією система підготовки кадрів для сфери захисту критичної інфраструктури поділяється на особистісно-орієнтоване та ресурсно-орієнтоване навчання. Так, особистісно-орієнтоване навчання розкриває систему розвитку фахівця сфери захисту критичної інфраструктури з урахуванням його індивідуальних особливостей. В процесі такого навчання у зазначених фахівцях формується самостійність, відповідальність, ініціативність, критичне мислення та інші особистісні якості. Фахівець перестає бути об’єктом навчання, навпаки – створюються можливості для його самоосвіти, саморозвитку (самовиховання), самопізнання, а також для проявлення своєї індивідуальності та особливостей характеру.

Науковець Яценко С.Л. у своїй науковій роботі стверджує, що особистісна орієнтація освіти висуває найбільш інтегративний, найбільш важливий критерій прогресу людства – рівень гуманізації суспільства, тобто таке становище в ньому особистості, яке визначає рівень її економічної, політичної і соціальної свободи; рівень задоволення матеріальних і духовних потреб; стан її психофізичного і соціального здоров’я. Саме тому сучасна освіта, зокрема в контексті організації особистісно-орієнтованого навчання,

може і повинна закладати основи розуміння світу як динамічно змінного, в якому особистість перебуває в стані постійного творення цього світу і самої себе [15].

В контексті класифікації системи підготовки кадрів для сфери захисту критичної інфраструктури, застосування особистісно-орієнтованого навчання у практичній площині забезпечить:

– функціонування єдиного центру оцінки стану захищеності критичної інфраструктури, прогнозування загроз та оцінки ризиків для об’єктів критичної інфраструктури;

– створення механізмів координації зусиль всіх зацікавлених сторін – влади, бізнесу і суспільства щодо захисту критичної інфраструктури, включаючи горизонтальну координацію операторів взаємозалежних і однотипних об’єктів критичної інфраструктури.

Ресурсно-орієнтоване навчання – це комплекс форм (методів, засобів) навчання, націлених на цілісний підхід до організації навчального процесу, у тому числі у сфері захисту критичної інфраструктури, який зорієнтований на засвоєння знань, навичок, а також на тренінг здібностей самостійного й активного перетворення інформаційного середовища шляхом практичного застосування ІТ-ресурсів. Основною характеристикою ресурсно-орієнтованого навчання є те, що таке навчання здійснюється у тріаді «слухач – викладач – наставник» на основі сучасних інноваційно-освітніх технологій навчання, зорієнтованих на самостійну пошуково-дослідницьку роботу фахівця сфери захисту критичної інфраструктури у зазначеній сфері упродовж усього життя.

Принципами ресурсно-орієнтованого навчання у сфері захисту критичної інфраструктури є необхідність:

– розвитку у фахівців суб’єктів національної системи захисту критичної інфраструктури можливості заохочувати творче (авторське) розв’язання навчальних завдань, мотивувати їх до виходу за межі передвизначеності, формувати уміння обґрунтовувати власне рішення чи відповідь;

– активізувати загальну компетентність фахівців суб’єктів національної

системи захисту критичної інфраструктури характеризуючи й оцінюючи результат їх роботи, а також виділяти їх унікальні якості;

– сформулювати у фахівців суб'єктів національної системи захисту критичної інфраструктури уміння самоменеджменту застосовуючи прийоми самоорганізації для досягнення успіху та реалізації життєвих цілей;

– навчити фахівців суб'єктів національної системи захисту критичної інфраструктури аналізувати власний досвід успіхів і неуспіхів. Зазначений принцип охарактеризовує вплив та аксіологічне значення ідей науковців для розвитку науки та історії людства, а також сприяє формуванню моральної інтенції у слухачів;

– сформулювати у фахівців суб'єктів національної системи захисту критичної інфраструктури позиції співпраці у ставленні до інших. Сутність зазначеного принципу полягає у мотивуванні фахівців цінувати досвід спілкування з іншими, виділяючи унікальні, а не конкурентні якості інших фахівців;

– розвинути у фахівців суб'єктів національної системи захисту критичної інфраструктури прагнення до саморозвитку, спонукаючи зазначених фахівців до формулювання ними життєвих завдань як завдань саморозвитку.

Крім цього слід зазначити, що науковець О. Штепа вивчаючи у своїй роботі принципи ресурсно-спрямованої концепції навчання зазначає, що концепція ресурсно-спрямованого навчання презентує можливість гармонійного співвідношення особистісної готовності студентів до майбутньої професійної діяльності та професійної компетентності, тобто психологічна ресурсність є основою та інструментом для реалізації професійних знань і умінь [16, с. 133–134].

Разом з тим, застосування ресурсно-орієнтованого навчання у практичній площині дозволить:

– розробляти методологію аналізу результативності державної політики у сфері захисту критичної інфраструктури;

– забезпечувати взаємодію національної системи захисту критичної інфраструктури з відповідними міжнародними системами, насамперед європейськими та євроатлантичними;

– виступати в установленому порядку замовником науково-дослідних робіт з питань захисту критичної інфраструктури та забезпечення національної системи стійкості.

За циклічним показником система підготовки кадрів для сфери захисту критичної інфраструктури поділяється на постійне (або безперервне) та періодичне навчання. Постійне (або безперервне) навчання відкриває довгострокові переваги щодо розширення навичок фахівців суб'єктів національної системи захисту критичної інфраструктури та збереження їх знань. Таке навчання сприяє генеруванню нових ідей і можливостей, загальному зростанню продуктивності особового складу суб'єктів національної системи захисту критичної інфраструктури, створює основу для гнучкості мислення, підвищує моральний дух. У сфері захисту критичної інфраструктури, де професіоналізм та інновації відіграють важливу роль, постійне навчання є ключем до успіху. Постійне навчання необхідне, щоб залишатися в тренді, стежити за останніми тенденціями і розвивати свої навички у зазначеній сфері.

Періодичне навчання проводиться в процесі службової (трудової) діяльності для того, щоб фахівець міг продовжувати виконувати свої службові обов'язки, передбачені його посадою. Періодичне навчання призначене для нагадування (або структурування) вже набутих знань, а також для ознайомлення з новими управлінськими, організаційними та технічними рішеннями.

Участь фахівців суб'єктів національної системи захисту критичної інфраструктури у постійному (або безперервному) та періодичному навчанні надасть змогу здійснити «освітній поштовх» до:

– створення та організації системи підготовки кадрів для сфери захисту критичної інфраструктури;

– організації підготовки (перепідготовки), підвищення кваліфікації та тренувань фахівців національної системи захисту критичної інфраструктури щодо забезпечення стійкості та захисту секторів критичної інфраструктури;

– розробки і затвердження програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування сфери захисту критичної інфраструктури, а також галузевих і регіональних планів та програм з протидії загрозам критичній інфраструктурі;

– розроблення нової галузі знань «Захист, безпека і стійкість сфери захисту критичної інфраструктури», програм навчання (підвищення кваліфікації), робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури.

Разом з тим, організація та забезпечення постійного (або безперервного) та періодичного навчання фахівців суб'єктів національної системи захисту критичної інфраструктури сприятиме:

– підготовці та перевірці персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури, організації навчань, тренінгів, спільних командно-штабних (тактико-спеціальних) навчань, спільних тренувань та занять із захисту (охорони, оборони), припинення злочинних дій, інцидентів та кібератак проти об'єктів критичної інформаційної інфраструктури;

– підвищенню комплексних знань (навичок, умінь) як персоналу, так і керівного складу операторів критичної інфраструктури, персоналу суб'єктів господарювання, які провадять діяльність, пов'язану із забезпеченням безпеки об'єктів критичної інфраструктури.

Система підготовки кадрів для сфери захисту критичної інфраструктури за бюджетним показником розподіляється на: кошти державного бюджету, відповідного місцевого бюджету, проєктів (програм) міжнародної технічної допомоги та інших форм міжнародного співробітництва відповідно до законодавства, власні кошти та інші джерела, не заборонені законодавством.

Сучасний світ сповнений непередбачуваностей, а отже, невизначеностей і неефективностей у регулюванні людського капіталу на ринках праці. У контексті широкомасштабного вторгнення російської федерації на територію України більшість вітчизняних роботодавців малоздатні передбачувати та замовляти специфіку людського ресурсу. Фокус на підготовку фахівців у сфері захисту критичної інфраструктури має певні обмеження у зв'язку, перш за все, із відсутністю відповідної галузі знань у сфері захисту критичної інфраструктури. Разом з тим оцінка розподілу державного замовлення на підготовку відповідних фахівців не може бути повноцінною також без аналізу інших часток бюджету, що спрямовані на фінансування закладів вищої освіти: наприклад, фінансування наукових та дослідницьких проєктів, капітальні інвестиції, повернені прибутки від контрактних місць чи підприємницьких проєктів тощо. Таким чином, враховуючи умови воєнного стану, вважаємо, що держава повинна прогнозувати забезпечення відповідних фахівців та коригувати постачання людського капіталу лише у секторах, які є стратегічно-важливими для розвитку держави, її національної безпеки і оборонного комплексу тощо.

Система підготовки кадрів для сфери захисту критичної інфраструктури за суб'єктами надання освітніх послуг розподіляється на: фізичних або юридичних осіб (заклади освіти, підприємства (установи, організації) будь-якої форми власності), що провадять освітню діяльність, міжнародні та іноземні установи (організації), зокрема ті, які реалізують відповідні проєкти (програми) міжнародної технічної допомоги.

Запропонована та розкрита класифікація системи підготовки кадрів для сфери захисту критичної інфраструктури надасть змогу Адміністрації Держспецзв'язку, яка забезпечує здійснення передбачених Законом України «Про критичну інфраструктуру» повноважень уповноваженого органу у сфері захисту критичної інфраструктури під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування, та іншим суб'єктам національної системи захисту критичної інфраструктури у подальшому

розглядати питання щодо удосконалення організаційно-технічного, методологічного та кадрового забезпечення, а саме:

– методології віднесення об’єктів до критичної інфраструктури, визначення їх стану, а також оцінки ефективності реагування на надзвичайні ситуації на таких об’єктах;

– систем моніторингу, прогнозування і підтримки прийняття рішень для національного ситуаційного центру;

– питань пов’язаних із започаткуванням цільових комплексних програм наукових досліджень та більш активного залучення приватного сектору до фінансування досліджень за тематикою захисту критичної інфраструктури;

– підготовки та перепідготовки кадрів за тематикою захисту критичної інфраструктури, а також організації спеціалізованих тренувань та учбових курсів на базі вже існуючих учбових центрів.

Продовжуючи дослідження слід розглянути також методи організації системи підготовки кадрів для сфери захисту критичної інфраструктури, які вирішують завдання щодо організації зазначеної системи відповідно до принципів професійної підготовки фахівців національної системи захисту критичної інфраструктури.

Вибір методів організації системи підготовки кадрів для сфери захисту критичної інфраструктури слід здійснювати враховуючи такі принципи:

– жоден з методів не є універсальним, але має чітко окреслену пізнавальну можливість;

– надійність методів забезпечується як їхньою обґрунтованістю, так і правилами застосування;

– оперативність та економічність дослідження не повинні шкодити якості даних;

– обґрунтування методу припускає розробку або відбір такого методу, який максимально відповідає вирішуваному завданню, не вимагаючи при цьому значних витрат для своєї реалізації.

Разом з тим слід зазначити, що основними проблемами, які виникають на етапі вибору методів дослідження за обраним напрямом, є:

– відсутність у відкритому доступі статистичної та аналітичної інформації про організацію системи підготовки кадрів для сфери захисту критичної інфраструктури, що у свою чергу не дозволяє широко використовувати кількісні методи дослідження, зокрема методи типу «результати – витрати», економічного аналізу, імітаційного моделювання, екстраполяції тощо;

– відсутність проведення серед суб'єктів національної системи захисту критичної інфраструктури відповідних емпіричних досліджень за обраним напрямом, що ускладнює застосування гіпотетико-дедуктивного методу, експерименту, інтерв'ю тощо;

– неможливість перевірення певних гіпотез, пов'язаних із удосконаленням механізмів формування та реалізації державної політики у сфері захисту критичної інфраструктури України, без розроблення Концепції системи підготовки кадрів для сфери захисту критичної інфраструктури та інших нормативно-правових і організаційно-розпорядчих актів, які б регламентували функціонування системи підготовки кадрів для сфери захисту критичної інфраструктури.

У зв'язку з цим, серед загально-наукових і конкретно-наукових методів, які достатньо висвітлені у сучасній літературі, та з метою дослідження системи підготовки кадрів для сфери захисту критичної інфраструктури, визначимо такі методи її організації:

– метод спостереження – метод наукового дослідження, що полягає в активному, систематичному, цілеспрямованому та планомірному сприйнятті того чи іншого об'єкта, в ході застосування якого одержуються знання про зовнішні сторони, властивості й відносини досліджуваного об'єкта. В рамках нашого дослідження метод спостереження доцільно застосовувати при відстеженні процесу розроблення Концепції системи підготовки кадрів для сфери захисту критичної інфраструктури на різних етапах її підготовки і

погодження, а також інших нормативно-правових і організаційно-розпорядчих актів із зазначеного питання;

– метод анкетування – метод отримання інформації шляхом надання письмових відповідей респондентами на запитання попередньо підготовлених бланків – анкет. Анкетування належить до групи тих методів, яка має назву «опитування». Метод анкетування може стати у пригоді при організації опитування керівного складу суб'єктів національної системи захисту критичної інфраструктури щодо визначення навчальних потреб, кількості співробітників, які підвищують професійну компетентність, методів і технологій навчання, які використовуються у службовій діяльності, основних проблем розвитку існуючої системи підвищення кваліфікації та її державного регулювання тощо;

– метод порівняння є пізнавальним процесом, що дає змогу виявити подібні та відмінні ознаки (риси) об'єктів, зіставляючи один об'єкт з іншим задля з'ясування їх співвідношення. Даний метод необхідно використовувати при зіставленні зарубіжних та вітчизняної систем розвитку професійної компетентності, у тому числі у сфері захисту критичної інфраструктури, що надасть змогу здійснити імплементацію найбільш успішного досвіду у службову діяльність;

– метод класифікації є сукупністю правил розподілу заданої чисельності і результату розподілу на підчисельність. Такий метод надасть змогу уточнювати види підвищення кваліфікації фахівців суб'єктів національної системи захисту критичної інфраструктури з урахуванням змін до законодавства про критичну інфраструктуру, державну службу та освіту в Україні;

– метод індивідуальних експертних оцінок – це використання думок експертів, які сформульовані особисто кожним із них самостійно без врахування думок інших експертів. До такого методу належать інтерв'ю та анкетування. Використовуючи такий метод з'явиться можливість сформувати підсумкову думку щодо проблем у сфері захисту критичної інфраструктури стосовно підвищення кваліфікації та шляхів їх розв'язання на основі думок

науковців та експертів, яких опитують індивідуально незалежно один від одного;

– статистичний метод дозволяє визначити рівняння зв'язку вхідних і вихідних параметрів, побудувати математичну модель процесу, установити взаємну залежність між різними факторами і технологічними результатами процесу, а також аналізувати параметри технологічного процесу. Даний метод доцільно використовувати для узагальнення результатів анкетувань та індивідуальних експертних оцінок шляхом систематизації і групування показників, аналізування варіації, динаміки і взаємозв'язків у сфері захисту критичної інфраструктури;

– метод інтеграції «дерева цілей» і поля діяльності об'єкта управління є структурованою та побудованою за ієрархічним принципом сукупністю цілей соціально-економічної системи. Цей метод визначає заходи, спрямовані на досягнення цілей розвитку системи підготовки кадрів для сфери захисту критичної інфраструктури з метою подальшого формування механізмів її державного регулювання;

– метод формально-логічного аналізу нормативно-правових баз є логічно структурованою і чітко фіксованою системою правил, яка побудована за принципом підпорядкованості та несуперечності норм. Завдяки такому методу з'явиться можливість виявити «прогалини» у нормативно-правовій базі, яка регулюватиме питання підвищення кваліфікації особового складу суб'єктів національної системи захисту критичної інфраструктури у розрізі її напрямів та видів;

– метод моделювання – це метод дослідження об'єктів пізнання (процесів, пристроїв, явищ), що ґрунтується на заміні конкретного об'єкта дослідження іншим, подібним до нього. Користуючись методом моделювання з'явиться можливість описати структуру системи підготовки кадрів для сфери захисту критичної інфраструктури, механізмів її державного регулювання та функціонування.

На нашу думку розглянуті методи організації системи підготовки кадрів для сфери захисту критичної інфраструктури нададуть змогу у подальшому:

– прискорити створення відповідної нормативно-правової бази, визначивши найвищим пріоритетом у цьому напрямі розробку та прийняття Концепції системи підготовки кадрів для сфери захисту критичної інфраструктури;

– вжити заходи у напрямі забезпечення інституційної підтримки запровадження Концепції системи підготовки кадрів для сфери захисту критичної інфраструктури, включаючи розбудову відповідної системи підготовки кадрів для сфери захисту критичної інфраструктури;

– запровадити системну роботу з населенням із загальної проблематики захисту критичної інфраструктури та забезпечення її стійкості зі створенням можливостей для отримання необхідних знань на безоплатній основі, у тому числі із застосуванням сучасних ІТ-технологій.

Висновки та перспективи подальших розвідок у даному напрямі. В контексті подальшого розвитку публічного управління в умовах воєнного стану, впровадження розглянутої класифікації та методів організації системи підготовки кадрів для сфери захисту критичної інфраструктури у службову діяльність надали би змогу реалізувати заходи щодо:

– зміцнення та удосконалення практичної складової освітнього процесу із збереженням достатнього рівня теоретичної та практичної підготовки;

– забезпечення взаємозв’язку різних систем (наука і освіта, наука і виробництво чи громадський сектор) для впровадження важливих змін, спрямованих на підвищення якості освіти у сфері захисту критичної інфраструктури;

– підвищення якості підготовки фахівців суб’єктів національної системи захисту критичної інфраструктури відповідно до реальних вимог ринку праці та забезпечення національної економіки кваліфікованими фахівцями;

– посилення ролі суб’єктів національної системи захисту критичної інфраструктури від формування змісту освітніх програм до оцінювання результатів навчання.

Література

1. Арсенович Л. А. Фактичний стан сфери кібербезпеки в контексті впровадження та перспектив застосування професійного стандарту «Фахівець із кібербезпеки». *Věda a perspektivy (Praha, Czech Republic).* 2022. № 7(14). С. 17–41.

2. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 16.10.2024).

3. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 16.10.2024).

4. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України від 19.09.2023 р. № 825-р. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (дата звернення: 16.10.2024).

5. Теленик С. Пріоритети адміністративно-правового регулювання державної політики України у сфері захисту критичної інфраструктури у контексті прийняття нової Стратегії національної безпеки України. *Право України*. 2019. № 10. С. 250–266.

6. Леоненко Н. А. Державна політика забезпечення безпекового середовища функціонування критичної інфраструктури в Україні. *Вісник Національного університету цивільного захисту України. Серія : Державне управління*. 2023. № 2. С. 162–169.

7. Дзяна Г. О. Система публічного управління як об’єкт критичної інфраструктури за критерієм "кібербезпека та захист інформації". *Національні інтереси України*. 2024. № 2. С. 370–379.

8. Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об’єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» : Указ Президента України від 17.10.2023 р. № 695/2023. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/695/2023#Text (дата звернення: 16.10.2024).

9. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 р. № 518. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 16.10.2024).

10. Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року : розпорядження Кабінету Міністрів України від 10.11.2023 р. № 1025-р. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text (дата звернення: 16.10.2024).

11. Про затвердження Положення про систему професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад : постанова Кабінету Міністрів України від 06.02.2019 р. № 106. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/106-2019-%D0%BF#Text (дата звернення: 16.10.2024).

12. Про трансформацію системи військової освіти : постанова Кабінету Міністрів України від 15.12.1997 р. № 1410. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text (дата звернення: 16.10.2024).

13. Про затвердження Положення про професійне навчання працівників

на виробництві : наказ Міністерства праці та соціальної політики України, Міністерства освіти і науки України від 26.03.2001 р. № 127/151. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/z0315-01#Text (дата звернення: 16.10.2024).

14. Про вищу освіту : Закон України від 01.07.2014 р. № 1556-VII. Дата оновлення: 16.10.2024. URL: https://zakon.rada.gov.ua/laws/show/1556-18#top (дата звернення: 16.10.2024).

15. Яценко С. Л. Особистісно орієнтоване навчання: теоретичний та прикладний аспекти. *Проблеми освіти: Наук-метод. зб. / Інститут інноваційних технологій і змісту освіти МОН України.* Київ, 2015. № 85. С. 231–237.

16. Штепа О. Принципи ресурсно-спрямованої концепції навчання. *Вісник Львівського університету. Серія : Психологічні науки*. 2018. № 2. С. 129–135.

References

1. Arsenovych, L.A. (2022), “The actual state of cyber security in the context of the implementation and prospects of application of the professional standard “Cyber Security Specialist””, *Věda a perspektivy (Praha, Czech Republic)*, vol. 7(14), pp. 17–41.

2. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine “On critical infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Accessed 16.10.2024).

3. Cabinet of Ministers of Ukraine (2017), Order “On the approval of the Concept of creating a state system for the protection of critical infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (Accessed 16.10.2024).

4. Cabinet of Ministers of Ukraine (2023), Order “On the approval of the National Plan for the Protection and Ensuring the Safety and Stability of Critical Infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (Accessed 16.10.2024).

5. Telenyk, S. (2019), “Priorities of administrative and legal regulation of the state policy of Ukraine in the field of critical infrastructure protection in the context of the adoption of the new National Security Strategy of Ukraine”, *Pravo Ukrainy*, vol. 10, pp. 250–266.

6. Leonenko, N.A. (2023), “State policy of ensuring a safe environment for the functioning of critical infrastructure in Ukraine”, *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriia : Derzhavne upravlinnia*, vol. 2, pp. 162–169.

7. Dzyana, G.O. (2024), “The public management system as a critical infrastructure object according to the criterion “cyber security and information protection””, *Natsionalni interesy Ukrainy*, vol. 2, pp. 370–379.

8. Office of the President of Ukraine (2023), Decree “On the decision of the National Security and Defense Council of Ukraine dated October 17, 2023 “On the organization of protection and ensuring the safety of the functioning of critical infrastructure and energy facilities of Ukraine in the conditions of military operations””, available at: https://zakon.rada.gov.ua/laws/show/695/2023#Text (Accessed 16.10.2024).

9. Cabinet of Ministers of Ukraine (2019), Resolution “On the approval of General requirements for cyber protection of critical infrastructure objects”, available at: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (Accessed 16.10.2024).

10. Cabinet of Ministers of Ukraine (2023), Order “On the approval of the plan of measures for the implementation of the Concept of ensuring the national system of stability until 2025”, available at: https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text (Accessed 16.10.2024).

11. Cabinet of Ministers of Ukraine (2019), Resolution “On the approval of the Regulation on the system of professional training of civil servants, heads of local state administrations, their first deputies and deputies, officials of local self-government and deputies of local councils”, available at: https://zakon.rada.gov.ua/laws/show/106-2019-%D0%BF#Text (Accessed 16.10.2024).

12. Cabinet of Ministers of Ukraine (1997), Resolution “On the transformation of the military education system”, available at: https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text (Accessed 16.10.2024).

13. Ministry of Labor and Social Policy of Ukraine, Ministry of Education and Science of Ukraine (2001), Order “On the approval of the Regulation on professional training of workers in production”, available at: https://zakon.rada.gov.ua/laws/show/z0315-01#Text (Accessed 16.10.2024).

14. The Verkhovna Rada of Ukraine (2014), The Law of Ukraine “On higher education”, available at: https://zakon.rada.gov.ua/laws/show/1556-18#top (Accessed 16.10.2024).

15. Yatsenko, S.L. (2015), “Personally oriented learning: theoretical and applied aspects”, *Problemy osvity: Nauk-metod. zb. / Instytut innovatsiinykh tekhnolohii i zmistu osvity MON Ukrainy*, Kyiv, vol. 85, pp. 231-237.

16. Shtepa, O. (2018), “Principles of the resource-oriented concept of education”, *Visnyk Lvivskoho universytetu. Seriia : Psykholohichni nauky*, vol. 2, pp. 129–135.

Стаття надійшла до редакції 24.10.2024 р.