

УДК 35.088.6:[004:007:351.86] (477)
DOI <https://doi.org/10.32851/tnv-pub.2022.5.1>

ДЕЯКІ ПИТАННЯ ЗАПРОВАДЖЕННЯ СИСТЕМИ ПІДГОТОВКИ ФАХІВЦІВ 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 Держспецзв'язку
ORCID: 0000-0001-7081-2838

Воєнні дії на всій території України, руйнування та пошкодження численних промислових підприємств, установ та організацій, у тому числі стратегічно важливих інфраструктурних об'єктів – все це та інші ризики вимагають від держави нових підходів до вирішення зазначених проблемних питань.

Забезпечення безпеки та безперерйного 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 здійснено аналіз нормативно-правового підґрунтя щодо підготовки фахівців у сфері захисту критичної інфраструктури (який вказує на відсутність нормативно-правових актів пов'язаних з підготовкою фахівців у сфері захисту критичної інфраструктури), узасаднено освітню практику щодо захисту критичної інфраструктури у різних провідних державах світу (які приділяють велику увагу процесу навчання та підготовці фахівців у сфері захисту критичної інфраструктури), та запропоновано механізм запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури, який розроблено для задоволення потреб країни у відповідних фахівцях та покращення рівня обізнаності всіх верств населення та його готовності протистояти викликам у сфері безпеки.

Ключові слова: критична інфраструктура, перепідготовка, підвищення кваліфікації, система підготовка фахівців, сфера захисту критичної інфраструктури.

Arsenovych L. A. Some issues of introducing a system of training critical infrastructure protection specialists

Military actions throughout Ukraine, destruction and damage of many industrial companies, institutions and organizations, including strategically important infrastructure facilities, – all these and other risks require the government to take new approaches to addressing the above-mentioned issues.

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.

The publication analyzes the regulatory basis for the training of critical infrastructure protection specialists (which shows the absence of any regulations related to the training of critical infrastructure protection specialists), summarizes the critical infrastructure protection education practices in various leading countries of the world (which pay considerable attention to training critical infrastructure protection specialists), and proposes a mechanism for introducing a system of training critical infrastructure protection specialists designed to meet the country's needs for the appropriate experts and to improve the awareness of all groups of the population and their readiness to resist security challenges.

Key words: *Critical infrastructure, retraining, advanced training, system of training specialists, critical infrastructure protection.*

Постановка проблеми та її зв'язок із важливими науковими і практичними завданнями. На теперішній час здатність країни та суспільства своєчасно розрізнити передумови катастроф та криз, які можуть негативно вплинути на критичну інфраструктуру, стала одним із ключових завдань національної безпеки і оборони.

Початок активних бойових дій на всій території України та масштабні зміни в різних сферах життєдіяльності держави призвели до необхідності формування ефективної і дієвої національної політики щодо захисту критично важливих об'єктів у разі виникнення та поширення надзвичайних ситуацій. Крім того, кризові явища, з якими стискається наше суспільство, показують, що необхідно кардинально змінити систему підготовки фахівців у сфері захисту критичної інфраструктури, а також розробити та впровадити ефективні механізми її функціонування.

У контексті проведення освітніх реформ у всіх сферах діяльності українського суспільства, питання підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері захисту критичної інфраструктури набуває особливої актуальності та потребує окремої уваги.

Аналіз останніх досліджень, в яких започатковано розв'язання проблеми та визначення невирішених раніше частин загальної проблеми, яким присвячена стаття. Наукові напрацювання вчених і практиків засвідчують, що професійна підготовка фахівців у сфері захисту критичної інфраструктури є одним із напрямів державної політики у сферах національної безпеки і оборони, без якого є неможливими створення та функціонування національної системи захисту критичної інфраструктури.

Як свідчать останні дослідження і публікації, проблеми професійного розвитку фахівців у сфері захисту критичної інфраструктури є малодослідженими. Так, кандидат юридичних наук С. Теленик у своїй статті встановлює перелік суміжних спеціальностей, які можуть бути затребувані в галузі захисту критичної інфраструктури та аналізує причини, що перешкоджають високій ефективності навчання та підвищення кваліфікації персоналу [1]. А науковці С. Белай, І. Євтушенко та В. Мацюк у своєму дослідженні аналізують теоретико-методологічне підґрунтя щодо підготовки фахівців з реагування на кризові ситуації на об'єктах критичної інфраструктури України, надають пропозиції щодо розвитку спеціалізації «Захист критичної інфраструктури та її стійкість» та практичні рекомендації в контексті розвитку створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури щодо розвитку державно-приватного партнерства, а також проведення міжвідомчих командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять [2].

Незважаючи на нещодавні (2020 – 2021 роки) дослідження вищевказаних науковців, які стосуються питань підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері захисту критичної інфраструктури, питанням основних теоретико-методологічних засад підготовки кадрів у зазначеній сфері приділено мало уваги, що й обумовило актуальність дослідження.

Метою статті є здійснення дослідження системи підготовки фахівців у сфері захисту критичної інфраструктури та надання практичних рекомендацій щодо подальшої її розбудови.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. На теперішній час Україна протистоїть одному із серйозніших безпекових викликів за всі роки свого становлення та своєї незалежності. Відкрита збройна агресія з боку російської федерації на всій території України, падіння економіки, пошкодження та руйнування багатьох підприємств, установ, організацій та інших інфраструктурних об'єктів – це ті реалії, з якими сьогодні зіштовхнулася Україна, і в яких повинна забезпечуватися безпека держави, суспільства, різноманітних інституцій, а також звичайних громадян України.

Зазначена ситуація перш за все сигналізує про те, що сектор безпеки нашої держави потребує ґрунтовного реформування, яке у подальшому необхідно здійснювати з урахуванням європейського та світового досвіду. Зазначені фактори роблять украй необхідним впровадження в Україні такого поняття як «захист критичної інфраструктури», яке активно застосовується у всіх провідних країнах світу як один із дієвих інструментів реалізації політики безпеки.

Незважаючи на те, що захист критичної інфраструктури є порівняно «молодою» безпековою концепцією, наразі в багатьох країнах світу існує безліч різноманітної інформації з цього питання, у тому числі щодо запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури, а також підвищення поінформованості населення стосовно захисту та забезпечення стійкості критичної інфраструктури.

Відзначаючи особливу роль вищої освіти як визначальної сили для формування фахівців у сфері захисту критичної інфраструктури, зважаючи на те, що потреба у таких фахівцях є актуальною та з подальшим розвитком високотехнологічного суспільства буде ще більше зростати, слід зазначити, що розвиток якісної освіти й науки потребує узгодженого вирішення конкретних практичних завдань у цій сфері. В умовах протистояння України агресії з боку російської федерації, становлення її як демократичної держави, прагнення щодо вступу до європейських та євроатлантичних структур, кількість та якість загроз і небезпек, спрямованих проти України, суттєво збільшуються. Виходячи з цього, проблематика національної безпеки стає особливо актуальною та гостро ставить питання про подальший розвиток системи підготовки фахівців у сфері захисту критичної інфраструктури.

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 [3, с. 60–61].

Сучасні підходи до започаткування системи підготовки фахівців у сфері захисту критичної інфраструктури враховують її нерозривний зв'язок з кібербезпекою, і усвідомлення цього факту знаходить свій відбиток у національному законодавстві.

Так, відповідно до Концепції створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 06 грудня 2017 року № 1009-р [4], одними із шляхів і способів розв'язання існуючих проблем у сфері захисту критичної інфраструктури, крім розроблення, виконання та перегляду програм забезпечення інформаційної безпеки та кібербезпеки, є створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури.

Як зазначено у Переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 19 червня 2019 року № 518 [5], власник/керівник об'єкта критичної інфраструктури повинен впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль рівня обізнаності.

Крім цього, відповідно до Закону України «Про критичну інфраструктуру» [6], що був прийнятий Верховною Радою України 16 листопада 2021 року, до завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належить, у тому числі, підготовка, перепідготовка, підвищення кваліфікації та тренування працівників національної системи захисту критичної інфраструктури. При цьому, організація взаємодії між суб'єктами національної системи захисту критичної інфраструктури здійснюється також шляхом проведення 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. У мирний час, реалізацію зазначених питань покладено на «новоспечену» Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України, що утворена постановою Кабінету Міністрів України від 12 липня 2022 року № 787 [7], а під час дії воєнного стану – на Держспецзв'язку, що передбачено Законом України від 18 жовтня 2022 року № 2684-IX [8].

У розрізі предмета даного дослідження слід констатувати, що на сьогодні в державі відсутній окремий підзаконний нормативно-правовий акт, який би консолідував усі елементи сфери захисту критичної інфраструктури, у тому числі й пов'язані з підготовкою фахівців для цієї сфери. Зазначений факт суттєво знижує ефективність нормативно-правового регулювання підготовки фахівців із захисту критичної інфраструктури.

Огляд відкритих інформаційних ресурсів дозволяє зробити висновок про те, що у чітко структурованому вигляді підготовка кадрів та населення щодо захисту об'єктів та систем критичної інфраструктури на даний момент існує лише у США. При цьому слід зазначити, що організаційно-практичні підходи до виконання цього завдання перебувають у стадії активного розвитку та виконуються Міністерством внутрішньої безпеки США (U.S. Department of Homeland Security, DHS). Це міністерство одноосібно відповідає за 7 з 16 секторів критичної інфраструктури США, а ще стосовно двох секторів воно ділить свою відповідальність з двома іншими державними агентствами. Відповідно, міністерство, на даний час

забезпечує реалізацію програм підготовки персоналу та навчання з питань захисту критичної інфраструктури за напрямками що стосуються хімічного сектору, комерційних об'єктів, гідротехнічних споруд, надання екстреної допомоги та стосовно ядерного сектору (ядерні реактори, ядерні та радіоактивні матеріали, відходи) [9].

Необхідність підготовки спеціалістів із захисту критичної інфраструктури добре усвідомлюється не тільки у США, а й в інших розвинутих країнах світу. Так, наприклад у Франції, яка виокремила критичну інфраструктуру та заклала правові основи для її захисту ще в 1997 році, питаннями планування безпекових заходів, навчання та розробки технологій безпеки, в тому числі стосовно сфери захисту критичної інфраструктури, займається підрозділ з державного захисту та безпеки (англ., State Protection and Security – PSE) при Генеральному секретаріаті з питань оборони та національної безпеки (фр., Secrétariat Général de la Défense et de la Sécurité Nationale, SGDSN).

У Німеччині, яка розпочала визначати і захищати критичну інфраструктуру однією з перших у Європі, підтримкою адміністрації та громад, гармонізацією федерального планування, аналізом досліджень, навчанням персоналу, стандартизацією та забезпеченням якості послуг у сфері захисту критичної інфраструктури опікується Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих (нім., Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK), яке було створено в травні 2004 року у складі Федерального міністерства внутрішніх справ (BMI).

А в Іспанії питання навчання персоналу з питань безпеки критичної інфраструктури покладено на Національний криптологічний центр (CCN), який є важливим підрозділом для захисту критичної інфраструктури у складі Національного центру розвідки (ісп., Centro Nacional de Inteligencia, CNI), що створений в 2002 році як національний розвідувальний та контррозвідувальний орган. Крім цього, координацією навчання та підготовкою персоналу Національної системи цивільного захисту Іспанії займається Головне управління з питань цивільного захисту (ісп., Dirección General de Protección Civil y Emergencias, DGPCE), яке є підрозділом MBC Іспанії та відповідає за розробку програми попередження надзвичайних ситуацій.

Узагальнення освітніх підходів до захисту критичної інфраструктури у різних провідних державах дозволяє сформулювати думку про те, що владні органи зазвичай приділяють досить важливу увагу процесу навчання та підготовці фахівців у сфері захисту критичної інфраструктури.

Як зазначалося, забезпечення і захист відповідної стійкості критичної інфраструктури є об'ємним завданням, до виконання якого може бути залучено широке коло осіб, як керівники вищих та середніх ланок управління державних органів, так і інші верстви населення. Зрозуміло, що відповідні аудиторії під час підготовки кадрів і населення країни щодо проблематики критичної інфраструктури необхідно визначати в залежності від ролі та обов'язків тієї чи іншої категорії осіб у процесі захисту стійкості критичної інфраструктури. Бажано, щоб через таке навчання пройшло якомога більше представників населення, робітників підприємств та компаній, керівників та управлінців різного рівня та з різними функціональними обов'язками [9].

Враховуючи зазначене, з метою розвитку підготовки кадрів з питань захисту та забезпечення стійкості критичної інфраструктури, необхідним є запровадження відповідного механізму, що можна зробити шляхом удосконалення законодавства, вивчення міжнародного досвіду та запозичення кращих практик (рис. 1).

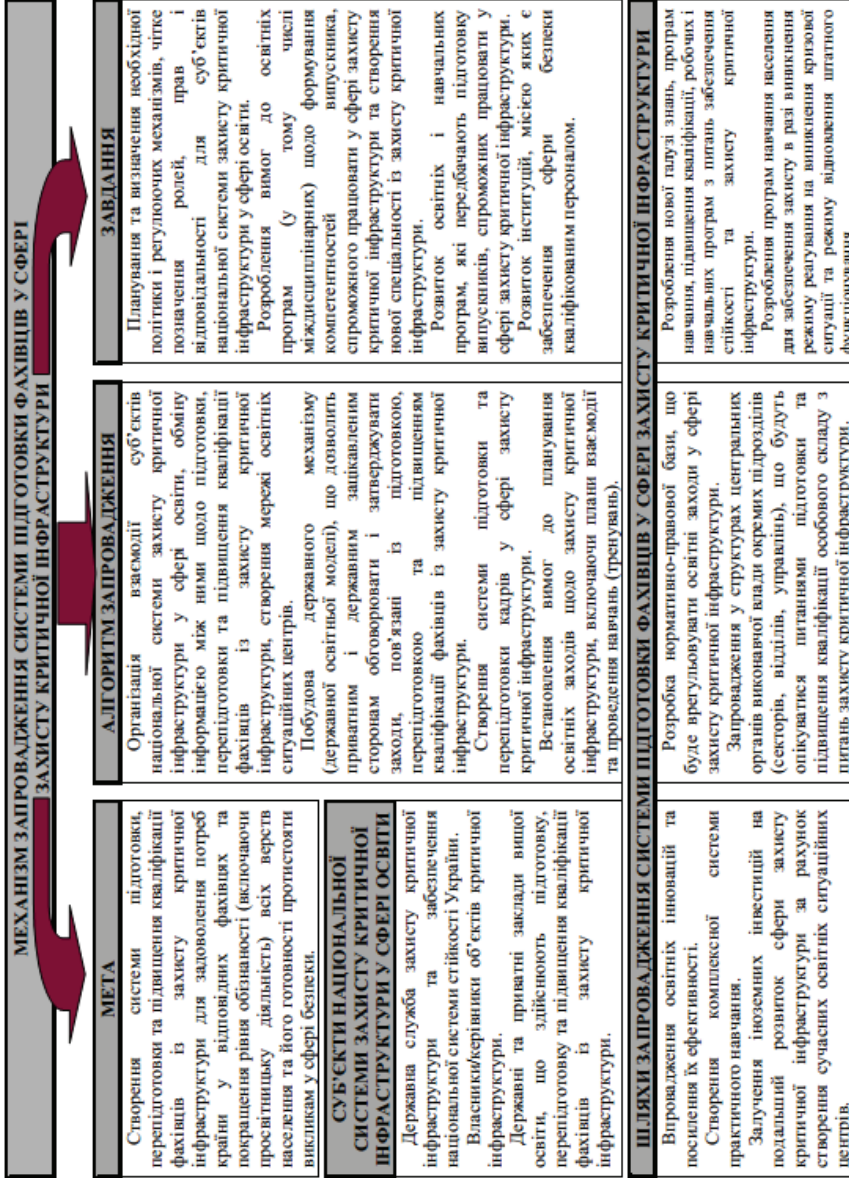


Рис. 1. Механізм запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури
Розробив автор

Розроблений проєкт – це механізм створений для забезпечення сталого розвитку держави, формування поведінки окремих груп людей та суспільства у цілому при виникненні загроз критичній інфраструктурі держави, розбудови та розвитку системи підготовки, перепідготовки та підвищення компетентності фахівців у сфері захисту критичної інфраструктури, що є важливими та своєчасними заходами із підвищення рівня національної безпеки і оборони держави.

Зазначений механізм спрямований на навчання персоналу об'єктів критичної інфраструктури та постійне його тренування, розробку рекомендацій, впровадження процедур та правил поведінки працівників об'єкта критичної інфраструктури при впливі загроз для мінімізації можливих збитків, підвищення інформованості персоналу об'єктів критичної інфраструктури та населення щодо можливих загроз і наслідків від них.

Суб'єктами національної системи захисту критичної інфраструктури у сфері освіти є:

Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України, яка 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 [7];

власники/керівники об'єктів критичної інфраструктури, в обов'язки яких входять питання щодо впровадження різноманітних програм підвищення обізнаності/навчання підлеглих працівників з питань інформаційної безпеки та забезпечення щорічного контролю за рівнем їхньої обізнаності;

державні та приватні заклади вищої освіти, що здійснюють підготовку, перепідготовку та підвищення кваліфікації фахівців із захисту критичної інфраструктури.

Крім того, в країні функціонує ряд наукових та науково-дослідних організацій, які потенційно спроможні зробити належний внесок у створення та функціонування системи підготовки фахівців у сфері захисту критичної інфраструктури. До цих установ слід віднести, насамперед, провідні українські університети – Київський національний університет імені Т.Г. Шевченка та Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»; заклади освіти сектору безпеки і оборони України – Національну академію Служби безпеки України, Національну академію внутрішніх справ України, Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ імені Ігоря Сікорського» (як окремий освітній заклад у складі Держспецзв'язку), Національний університет оборони України імені Івана Черняхівського, учбові та науково-дослідні заклади національної системи цивільного захисту України, наукові установи Національної академії наук України, Національний інститут стратегічних досліджень [9].

Процес створення в Україні дієвої та ефективної системи підготовки фахівців у сфері 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 запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури треба робити особливий акцент, який вказує на необхідність:

створення нормативно-правової бази з питань організації діяльності суб'єктів національної системи захисту критичної інфраструктури у сфері освіти;

створення організаційно-інституційної структури системи підготовки фахівців у сфері захисту критичної інфраструктури;

визначення повноважень, завдань та відповідальності суб'єктів національної системи захисту критичної інфраструктури у сфері освіти;

підвищення рівня навичок та компетентностей населення в державі з питань захисту критичної інфраструктури, а також рівня конкурентоспроможності країни щодо розвитку критичної інфраструктури;

створення певних індикаторів для контролю (моніторингу) стану підготовки фахівців у сфері захисту критичної інфраструктури.

Разом з тим виконання завдань, які визначені в рамках запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури, надади би змогу:

сформуванню засади освітнього державно-приватного партнерства у сфері захисту критичної інфраструктури на основі взаємної довіри, обміну інформацією та створення стимулів для спільного інвестування у здійснення відповідних освітніх заходів;

визначити права, обов'язки та відповідальність власників/керівників об'єктів критичної інфраструктури;

організувати взаємодію суб'єктів національної системи захисту критичної інфраструктури у сфері освіти, обмін інформацією між ними про освітні потреби шляхом розробки алгоритму обрахування довгострокової й короткострокової потреби у фахівцях із захисту критичної інфраструктури.

Продовжуючи дослідження слід зазначити, що не дивлячись на те що Україна володіє неабияким потенціалом з питань організації різноманітних освітніх заходів, на сьогодні фактично відсутня будь-яка освітня робота у сфері захисту критичної інфраструктури. У контексті зазначеної проблематики, впровадження освітніх інновацій, посилення їх ефективності, а також створення відповідної комплексної системи практичного навчання надади би можливість:

розробити кваліфікаційні вимоги до персоналу із захисту критичної інфраструктури;

реалізовувати у подальшому пілотні короткострокові програми професійного розвитку персоналу;

визначити вимоги до освітніх програм (у тому числі міждисциплінарних) щодо формування компетентностей випускника, спроможного працювати у сфері захисту критичної інфраструктури;

визначити опорні заклади освіти для реалізації усіляких освітніх пілотних проєктів.

В свою чергу створення сучасних освітніх ситуаційних центрів у сфері захисту критичної інфраструктури зможе забезпечити:

організацію та проведення відповідних навчань (за територіальним принципом) з питань захисту критичної інфраструктури у разі виникнення надзвичайних ситуацій та подій (реагування на загрози у сфері критичної інфраструктури);

практичне відпрацювання дій (сценаріїв) власниками/керівниками об'єктів критичної інфраструктури при реагуванні на загрози у сфері критичної інфраструктури;

проведення практичних (у тому числі командних) навчань з питань захисту критичної інфраструктури, зокрема в інтересах основних суб'єктів сектору безпеки і оборони України, участь у таких навчаннях у рамках заходів колективної оборони;

практичну підготовку вузькопрофільних фахівців сфери захисту критичної інфраструктури;

перевірку практичних навичок кандидатів, що претендують на зайняття відповідних посад на об'єктах критичної інфраструктури.

Рівень підготовки військовослужбовців, осіб начальницького складу, державних службовців та інших працівників повинен відповідати не лише сучасним потребам розвитку інформаційного суспільства, але й забезпечити здатність адаптуватись у процесі змін у різних сферах діяльності, знаходити рішення у складних ситуаціях, під час виконання своїх службових обов'язків. Зазначене потребує якісних змін, у тому числі нормативно-правового забезпечення у сфері захисту критичної інфраструктури. Зміни у законодавстві є однією з передумов підвищення ефективності заходів у сфері захисту критичної інфраструктури, у тому числі освітніх. Враховуючи зазначене, розробка освітньої нормативно-правової бази у сфері захисту критичної інфраструктури надасть поштовх до:

розвитку освіти у сфері захисту критичної інфраструктури та інтеграції кращих світових практик у систему підготовки фахівців для підвищення їх конкурентоспроможності на ринку праці;

удосконалення організації професійної підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері захисту критичної інфраструктури шляхом залучення в установленому порядку до такої діяльності закладів освіти, що здійснюють підготовку відповідних фахівців.

Для забезпечення плідної роботи спеціалістів у сфері захисту критичної інфраструктури слід не тільки ретельно здійснювати набір кадрів, а й приділяти також увагу організації їх підготовки. Особливу увагу при цьому потрібно приділяти практичній складовій навчання. Для цього необхідно не лише проводити навчання особового складу силами закладів освіти, але і створювати навчальні підрозділи з вивчення різноманітних питань що стосуються захисту критичної інфраструктури. Запровадження у структурах центральних органів виконавчої влади окремих підрозділів (секторів, відділів, управлінь), що будуть опікуватися питаннями підготовки та підвищення кваліфікації особового складу з питань захисту критичної інфраструктури, надасть змогу підготувати:

державних управлінців вищої ланки та керівників окремих структурних підрозділів (департаментів, управлінь, відділів) з питань забезпечення захисту інформаційних ресурсів, критичних бізнес/операційних процесів тощо на об'єкті критичної інфраструктури;

керівників середньої ланки управління (начальники секторів, відділів, управлінь та їх заступники у складі окремих структурних підрозділів) з питань дотримання вимог до забезпечення інформаційної безпеки під час взаємодії з постачальниками;

наукових співробітників та інженерно-технічний персонал з питань формування (надання, скасування) та контролю за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних;

спеціалістів з питань порядку резервування даних та компонентів об'єкта критичної інфраструктури, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів об'єкта у випадку виходу їх з ладу тощо;

відповідних фахівців з питань політики проведення внутрішнього аудиту інформаційної безпеки об'єкта критичної інфраструктури.

Необхідно зазначити також й про необхідність запровадження нової галузі знань (спеціальності), яка буде врегульовувати всі аспекти підготовки фахівців у сфері захисту критичної інфраструктури. Нині у чинному переліку галузей

знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти (постанова Кабінету Міністрів України від 29 квітня 2015 року № 266 [10]), сфера захисту критичної інфраструктури не виділена ані в якості окремої галузі знань, ані в якості окремої спеціальності. Таку ситуацію змінила вимога частини дев'ятої розділу VI Закону України «Про критичну інфраструктуру», відповідно до якої Міносвіти спільно з Державною службою захисту критичної інфраструктури та забезпечення національної системи стійкості України необхідно до 1 січня 2024 року забезпечити проведення науково-дослідної роботи щодо доповнення зазначеного переліку новою позицією у сфері забезпечення стійкості та захисту критичної інфраструктури. Такі нововведення зможуть беззаперечно «підштовхнути» до розроблення нових програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури, а також до впровадження нових освітніх ініціатив, що в свою чергу надасть захист від загроз у сфері державної безпеки, від кіберзагроз та від надзвичайних ситуацій.

На сьогодні, особливістю підготовки фахівців у сфері захисту критичної інфраструктури є динамічний розвиток новітніх інформаційно-комунікаційних технологій і, відповідно, змісту навчання. Ця проблема має вирішуватись своєчасним оновленням змісту навчання, інтеграцією базової освіти та більш гнучкою підготовкою.

Внаслідок широкого використання сучасних інформаційних технологій суспільство стало вразливим до різноманітних впливів, які все частіше стають інструментом управління об'єктами критичної інфраструктури держави, підприємств, установ і організацій.

Тому особливої актуальності набуває питання ефективного використання потенціалу фахівців у сфері захисту критичної інфраструктури. Професійний розвиток таких фахівців і, як наслідок, ефективна діяльність органів державної влади у зазначеній сфері є одним із пріоритетів українського уряду та перебуває на сьогодні у трансформаційному стані.

Проведений аналіз доводить, що для України формування нової культури безпеки зі збереженням за необхідності спеціалізації та індивідуалізації системи підготовки кадрів, підвищення кваліфікаційного рівня персоналу та забезпечення його високої мотивації професійної діяльності у сфері захисту критичної інфраструктури є справою державного рівня.

Висновки. Забезпечення безпеки та стійкості сфери захисту критичної інфраструктури в умовах воєнного стану є чи не найголовнішим для національної безпеки і оборони України. Зазначене питання великою мірою залежить від професіоналізму та рівня освіченості кадрів у даній сфері діяльності. Проведене дослідження ще раз наголошує, що питання підготовки та підвищення кваліфікації фахівців у сфері захисту критичної інфраструктури потребує значного поліпшення. Відтак запровадження запропонованої у статті системи підготовки фахівців у сфері захисту критичної інфраструктури надасть змогу:

задовольнити потреби країни у фахівцях, спроможних працювати у сфері захисту критичної інфраструктури, та забезпечити їх відповідну підготовку;

покращити обізнаність населення у питаннях безпеки критичної інфраструктури і посилити спроможність територіальних громад протистояти відповідним загрозам;

зміцнити державну систему забезпечення безпеки та стійкості критичної інфраструктури, посилити її захист і спроможність до швидкого відновлення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Теленик С. С. Напрями підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури / С. С. Теленик // Правові новели. 2020. № 10/2020. Т. 2. С. 91-99.
2. Белай С. В. Теоретико-методологічні засади підготовки кадрів у сфері захисту критичної інфраструктури України / С. В. Белай, І. В. Євтушенко, В. В. Мацюк // Вісник Національного університету цивільного захисту України. Серія : Державне управління. 2021. Вип. 2. С. 342-350.
3. Арсенович Л. А. Механізми формування та забезпечення функціонування системи підготовки фахівців у сфері кібербезпеки органів державної влади України : дис. ... доктора філософії : 281. Київ, 2021. 412 с.
4. 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>.
5. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України № 518 від 19.06.2019 р. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>.
6. Про критичну інфраструктуру : Закон України № 1882-IX від 16.11.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
7. 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>.
8. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України : Закон України № 2684-IX від 18.10.2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2684-20#Text>.
9. Проблема розбудови системи підготовки кадрів і населення для забезпечення стійкості критичної інфраструктури в Україні. Аналітична записка. URL: <https://niss.gov.ua/doslidzhennya/ekonomika/problema-rozbudovi-sistemi-pidgotovki-kadriv-i-naselennya-dlya?cfchl tk=LJPAVZIDpVJ52lnHulre7xlaFszac0u3bMFmfGXlHe4-1668019093-0-gaNycGzNCKU>.
10. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : постанова Кабінету Міністрів України № 266 від 29.04.2015 р. URL: <https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF>.

REFERENCES:

1. Telenyk S. S. (2020) Napriamy pidhotovky ta pidvyshchennia kvalifikatsii fakhivtsiv iz zakhystu krytychnoi infrastrukтуры [Areas of training and advanced training of critical infrastructure protection specialists]. *Pravovi novely*, Vup. 10/2020, 91-99.
2. Bielai S. V. (2021) Teoretyko-metodolohichni zasady pidhotovky kadriv u sferi zakhystu krytychnoi infrastrukтуры Ukrainy [Theoretical and methodological principles of personnel training in the field of protection of critical infrastructure of Ukraine]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriiia : Derzhavne upravlinnia*, Vup. 2, 342-350.
3. Arsenovych L. A. (2021). Mekhanizmy formuvannia ta zabezpechennia funktsionuvannia systemy pidhotovky fakhivtsiv u sferi kiberbezpeky orhaniv derzhavnoi vlady Ukrainy [Mechanisms of forming and ensuring the functioning of the system of training specialists in the field of cyber security of the state authorities of Ukraine]. *Dissertation of the Doctor of Philosophy*. Kyiv [in Ukrainian].
4. The Cabinet of Ministers of Ukraine (2017). Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastrukтуры [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>.

5. The Cabinet of Ministers of Ukraine (2019). Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu ob'ektiv krytychnoi infrastruktury [On the approval of General requirements for cyber protection of critical infrastructure objects]. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>.

6. The Verkhovna Rada of Ukraine (2021). Pro krytychnu infrastrukturu [About critical infrastructure]. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.

7. The Cabinet of Ministers of Ukraine (2022). Pro utvorennia Derzhavnoi sluzhby zakhystu krytychnoi infrastruktury ta zabezpechennia natsionalnoi systemy stiikosti 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>.

8. The Verkhovna Rada of Ukraine (2022). Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo povnovazhen upovnovazhenoho orhanu u sferi zakhystu krytychnoi infrastruktury Ukrainy [On making changes to some laws of Ukraine regarding the powers of the authorized body in the field of protection of critical infrastructure of Ukraine]. URL: <https://zakon.rada.gov.ua/laws/show/2684-20#Text>.

9. Problema rozbudovy systemy pidhotovky kadriv i naseleння dlia zabezpechennia stiikosti krytychnoi infrastruktury v Ukraini. Analitychna zapyska [The problem of building a system of training personnel and the population to ensure the stability of critical infrastructure in Ukraine. Analytical note]. URL: https://niss.gov.ua/doslidzhennya/ekonomika/problema-rozbudovi-sistemi-pidgotovki-kadriv-i-naseleння-dlya?_cf_chl tk=LJPAVZIDpVJ52lnHu_lre7xlaFszac0u3bMFmfGX IHe4-1668019093-0-gaNycGzNCKU.

10. The Cabinet of Ministers of Ukraine (2015). Pro zatverdzhennia pereliku haluzei znan i spetsialnostei, za yakymy zdiisniuietsia pidhotovka zdobuvachiv vyshchoi osvity [On approval of the list of fields of knowledge and specialties for which higher education applicants are trained]. URL: <https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF>.