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. 2025. № 2.

DOI: http://doi.org/10.32702/2307-2156.2025.2.17

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

МЕТОДОЛОГІЧНІ ПІДХОДИ ЩОДО ЗАСТОСУВАННЯ ЗАРУБІЖНОГО ДОСВІДУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ 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

METHODOLOGICAL APPROACHES TO IMPLEMENTING FOREIGN EXPERIENCE IN PROFESSIONAL TRAINING OF CRITICAL INFRASTRUCTURE PROTECTION SPECIALISTS

Підписання Угоди України з ЄС про асоціацію, визнання європейської інтеграції стратегічним зовнішньополітичним пріоритетом України, прийняття нового Закону України "Про критичну інфраструктуру" висувають нові завдання на шляху до європейського і світового освітнього простору для забезпечення високотехнологічного та інноваційного розвитку держави, потреб суспільства і ринку праці у кваліфікованих фахівцях.

На сьогодні одним із проблемних питань в Україні є підготовка фахівців нової якості, здатних творчо мислити, швидко орієнтуватися в сучасних інформаційних технологіях, приймати нестандартні рішення, вчитися і удосконалюватися протягом усього життя.

Підрозділи сфери захисту критичної інфраструктури за кордоном відіграють вагому роль у захисті національної безпеки і оборони своїх країн. Для їх належного функціонування країнами Європейського Союзу впроваджуються сучасні інформаційні технології, здійснюється сприяння інноваційним процесам у систему підготовки та підвищення кваліфікації фахівців, вдосконалюється відповідна нормативна база.

У процесі реалізації зазначених питань повною мірою необхідно використовувати досвід роботи університетів сусідніх країн Європи та співпрацю в рамках виконання міжнародних освітніх програм, що сприятиме інтеграції української освіти в європейський освітній та науковий простори.

При підготовці кваліфікованих фахівців сфери захисту критичної інфраструктури для потреб суб'єктів національної системи захисту критичної інфраструктури, безперечно, буде у нагоді досвід країн-членів Європейського Союзу щодо підготовки як своїх фахівців, так і спеціалістів України у зазначеній сфері.

У статті автором розглянуто та проаналізовано освітні підходи до захисту критичної інфраструктури у різних провідних державах світу, зарубіжний досвід (у практичній площині) при організації та проведенні освітніх заходів для українських фахівців сфери захисту критичної інфраструктури, досвід державних органів України, які розпочали освітні

заходи з питань захисту об'єктів критичної інфраструктури, а також зарубіжні освітні напрацювання, які роблять кіберзахист об'єктів критичної інфраструктури України надійнішим та ефективнішим.

The signing of the EU-Ukraine Association Agreement, the recognition of European integration as a strategic foreign policy priority of Ukraine, and the adoption of a new Law of Ukraine "On Critical Infrastructure" put forward new challenges on the way to the European and global educational environment to ensure high-tech and innovative development of the state, and to meet the needs of the society and the labor market for qualified specialists.

Today, one of the most challenging issues in Ukraine is the training of a new type of specialists who can think creatively, quickly navigate modern information technologies, make out-of-the-box decisions, learn and improve throughout their lives.

Critical infrastructure protection units abroad play an important role in protecting the national security and defense of their countries. To ensure their proper functioning, the EU countries introduce modern information technologies, promote innovative processes in the system of training and professional development of specialists, and improve the relevant regulatory framework.

In the process of implementing these issues, it is necessary to fully use the experience of universities in the neighboring European countries and benefit from the cooperation in the international educational programs, which will facilitate the integration of Ukrainian education into the European educational and scientific environment.

When training qualified critical infrastructure protection specialists for the needs of the entities of the national system of critical infrastructure protection, the experience of the EU member states in training both their specialists and Ukrainian specialists in this area will undoubtedly be useful.

In this article, the author reviews and analyzes educational approaches to critical infrastructure protection in various leading countries of the world, foreign

experience (in practical terms) in organizing and holding educational activities for Ukrainian critical infrastructure protection specialists, the experience of Ukrainian government agencies that have launched educational activities on critical infrastructure protection, as well as foreign educational developments that make cyber protection of Ukraine's critical infrastructure more reliable and effective.

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. Шлях європейської та євроатлантичної інтеграції є незворотним для України, це цивілізаційний і звичайний вибір, який зробив і відстоює ціною великих втрат український народ. За останні декілька років країна зробила дієві та рішучі кроки у напрямку зближення із Європейським Союзом. Водночас, із входженням до Європейського Союзу Україна не повинна «розчинитися» і «втратити себе» на європейському та світовому просторі. Отже, на сьогодні необхідно зрозуміти, яким чином національний досвід у різноманітних сферах різних країн Європейського Союзу, та світу в цілому, узгоджується з національним досвідом України, у тому числі в умовах воєнного стану.

На теперішній час, за всю історію незалежності України, наша держава протистоїть самому серйозному виклику своїй національній безпеці. Військова агресія російської федерації проти України, підвищення ймовірності скоєння на її території різноманітних терористичних актів, падіння економіки, руйнування та знищення численних об'єктів інфраструктури – все це визначає ті реалії сучасності, в яких сьогодні існує Україна, і в яких має забезпечуватися безпека її громадян, суспільства і держави в цілому.

Багато кому добре відомо, що у запровадженні відповідних реформ та підходів у тому чи іншому напрямі діяльності, ключову роль відіграє людський фактор. І захист або забезпечення безпеки критичної інфраструктури від будь яких видів загроз, звичайно, не може бути винятком.

З огляду на безпекову ситуацію, в якій перебуває Україна, а також на ті світові тенденції, які формують нові загрози та виклики безпеці у глобальному та регіональному вимірах, проблематику захисту критичної інфраструктури, взагалі, та підготовки кадрів для системи захисту критичної інфраструктури, зокрема, не можна не визнати як актуальну [1].

Аналіз останніх досліджень і публікацій. Вітчизняні фахівці у сфері захисту критичної інфраструктури неодноразово у своїх роботах розглядали як правові так і організаційні засади створення та функціювання зарубіжних систем захисту критичної інфраструктури. Так, науковці Національного університету водного господарства та природокористування Жемба А.Й., Клюха О.О. та Качан О.І. досліджуючи питання управління міжнародною політикою ЄС у сфері захисту критичної інфраструктури зазначають, що в Україні доцільно провести розробку або доопрацювати плани кризового управління критичною інфраструктурою, що в свою чергу потребує додаткової підготовки суб'єктів господарювання до надзвичайних ситуацій (що включає координовані зусилля з обліку працівників), надання екстрених житлових та альтернативних комутаційних послуг, взаємної допомоги між підприємствами та громадськими установами, у тому числі регулярний аналіз аварійних планів, включаючи навчання [2, с. 9–10].

У свою чергу дослідник Зубко Г.Ю. на підставі узагальнення зарубіжного досвіду у напрямі створення системи підготовки кадрів та населення з питань безпеки критичної інфраструктури наголошує на необхідності:

– створення профільних підрозділів з питань безпеки критичної інфраструктури та підготовки кадрів у профільних міністерствах;

– внесення змін до класифікатора професій з визначенням професій відповідно до визначених секторів критичної інфраструктури на усіх управлінських рівнях;

– розробки освітніх програм з відповідними програмними результатами навчання та компетентностями і навчальних програм для підвищення кваліфікації державних службовців і рівня поінформованості населення з питань безпеки критичної інфраструктури [3, с. 13].

Разом з тим, науковець Єрменчук О.П. здійснюючи аналіз європейського законодавства у сфері захисту критичної інфраструктури акцентує свою увагу на тому, що загалом стійкість критичної інфраструктури та її об'єктів у деяких державах розглядається не окремо, а як одна із складових забезпечення безпеки регіону або держави в цілому. Крім того, забезпечення стійкості об'єктів критичної інфраструктури досягається не тільки спеціальними заходами, а включає також підвищення інформованості персоналу об'єктів критичної інфраструктури та населення щодо можливих загроз та наслідків від них, навчання персоналу об'єктів критичної інфраструктури та постійне його тренування [4, с. 41].

Вищезазначені дослідження ще раз підказують, що для подальшої реалізації професійної підготовки фахівців національної системи захисту критичної інфраструктури в умовах воєнного стану необхідно виокремити та чітко регламентувати питання підготовки кадрів та населення у сфері захисту критичної інфраструктури, яка має здійснюватися на систематичній основі відповідно до освітніх потреб цільових аудиторій різними закладами освіти та науково-дослідними й експертними установами.

Формулювання цілей статті (постановка завдання). Метою статті є розгляд практичних підходів щодо застосування зарубіжного досвіду професійної підготовки фахівців у сфері захисту критичної інфраструктури.

Виклад основного матеріалу дослідження. Досвід провідних країн Європи свідчить, що захист критичної інфраструктури належить до основних напрямів державної політики з питань забезпечення державної безпеки. Нові та

небезпечні виклики регіональній і глобальній безпеці висувають на порядок денний завдання із побудови в Україні системи захисту критичної інфраструктури та наукової розробки зазначеної проблематики [5, с. 5].

Проблематика сфери захисту критичної інфраструктури, безперечно, є актуальним світовим феноменом. Її базові основи і принципи відомі у багатьох країнах багато років, проте, зі зростаючою світовою глобалізацією та інформатизацією, ця проблематика вже вийшла на перший план. Тому міжнародне співробітництво у сфері захисту критичної інфраструктури, у тому числі в освітній складовій, є вкрай важливим питанням сьогодення.

З початку вторгнення російської федерації на територію України стало очевидно, що винесення Україною проблематики захисту критичної інфраструктури на світовий рівень дозволяє з упевненістю розраховувати на те, що у подальшому багатьом питанням міжнародної співпраці та обміну передовим досвідом у цій сфері, у тому числі щодо професійної підготовки фахівців у сфері захисту критичної інфраструктури, в нашій країні буде приділятися відповідна увага.

Підтверджує таку думку Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р [6], очікуваними результатами якої, крім створення державної системи захисту критичної інфраструктури, налагодження ефективної взаємодії між усіма суб'єктами державної системи захисту критичної інфраструктури та гармонізації законодавства України у сфері захисту критичної інфраструктури із законодавством ЄС, є також міжнародне співробітництво у сфері захисту критичної інфраструктури та інтеграції України до міжнародних систем захисту критичної інфраструктури.

Крім цього, відповідно до Положення про Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України, затвердженого постановою Кабінету Міністрів України від 12 липня 2022 року № 787 [7], Державна служба захисту критичної інфраструктури та

забезпечення національної системи стійкості України, яка стане протягом 12 місяців після припинення чи скасування воєнного стану головним органом у системі центральних органів виконавчої влади, що забезпечуватиме формування та реалізацію державної політики у сфері захисту критичної інфраструктури та забезпечення національної системи стійкості, крім здійснення підготовки, перепідготовки, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури, опікуватиметься також взаємодією з відповідними міжнародними системами, насамперед європейськими та євроатлантичними.

Разом з тим, з метою посилення спроможності державних органів проводити ідентифікацію загроз, виявляти вразливості та оцінювати ризики національній безпеці Нацдержслужби, Міноборони та ДСНС України є відповідальними за забезпечення розроблення (з урахуванням міжнародного досвіду) та впровадження програм підвищення кваліфікації державних службовців та посадових осіб місцевого самоврядування з питань аналізу, управління ризиками та планування на основі спроможностей (розпорядження Кабінету Міністрів України від 10 листопада 2023 року № 1025-р «Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року» [8]).

Положення таких актів ще раз підкреслюють той факт, що запровадження системи підготовки кадрів для сфери захисту критичної інфраструктури в умовах воєнного стану потребує посилення зарубіжного партнерства та формування злагоджених дій на європейському просторі між усіма країнами Європейського Союзу.

Не дивлячись на те, що сфера захисту критичної інфраструктури є досить новою та не обстеженою концепцією, на теперішній час в світі існує безліч інформації з цього питання, у тому числі щодо професійної підготовки фахівців у сфері захисту критичної інфраструктури.

При цьому, характер тих чи інших завдань, пов’язаних із впровадженням такої системи вимагає організацію забезпечення потреб у навчанні в чималому

діапазоні цільових аудиторій для різних секторів критичної інфраструктури, а також створення широких можливостей як для поширення серед населення опорних знань про критичну інфраструктуру, так і отримання відповідної (спеціалізованої) вищої освіти.

Ефективному виконанню цих вимог безумовно може сприяти те, що у теперішній час триває процес бурхливого розвитку ІТ-технологій, результати якого дозволяють провідним країнам світу, корпораціям, неурядовим організаціям, залученим до цього процесу, значно урізноманітнити форми і методи навчання і на усіх рівнях та в усіх напрямах [1].

Навчання з питань захисту критичної інфраструктури в зарубіжних країнах – це система дидактичної та виховної діяльності органів влади, силових структур, соціальних організацій та об'єднань, які сприяють розповсюдженню ідей, знань та навичок, безпосередньо пов'язаних із захистом сфери критичної інфраструктури.

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 [9, с. 5].

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 напрямами що стосуються хімічного сектору, комерційних об'єктів, гідротехнічних споруд, надання екстреної допомоги та стосовно ядерного сектору (ядерні реактори, ядерні та радіоактивні матеріали, відходи) [1].

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) [9, с. 7].

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 МВС Іспанії та відповідає за розробку програми попередження надзвичайних ситуацій [9, с. 7].

Слід виділити досвід також Великої Британії. Так, структура системи забезпечення безпеки сфери критичної інфраструктури Великої Британії включає 13 секторів критичної інфраструктури, три з яких додатково поділені на 15 підсекторів. Діяльність щодо безпеки та стійкості критичної інфраструктури у рамках зазначених секторів та підсекторів координують 11 провідних урядових органів. У зв'язку із різким загостренням проблем кібербезпеки активну роботу з надання освітніх та навчальних послуг, у тому числі щодо критичної інфраструктури, на теперішній час провадить Національний центр кібербезпеки, яким, у тому числі, розробляються настанови щодо забезпечення кібербезпеки організацій державного сектору. Так, зазначеним центром підготовлено низку настанов і рекомендацій, які сприяють самостійній діяльності організацій та підприємств, серед яких слід виділити «10 кроків до кібербезпеки», «Настанова для кінцевого користувача приладу», «Принципи хмарної безпеки» тощо.

Останніми роками також і Румунія розпочала приділяти значну увагу питанням стійкості критичної інфраструктури визначивши свої підходи до цієї проблеми в стратегічних документах, що були ухвалені останнім часом. Так, Стратегія національної оборони Румунії передбачає заходи щодо розвитку ефективних інструментів зміцнення стійкості суспільства та критичної інфраструктури, які можна розділити на чотири основні напрями:

– інформаційна безпека: вдосконалення обізнаності щодо ворожих дій/впливу, що здійснюється в публічному просторі за допомогою класичних інструментів або інтернет-ЗМІ чи аналітичних центрів, підвищення спроможності освітніх, дослідницьких, аналітичних центрів та медіа-інституцій щодо виявлення та протидії дезінформаційним діям, що підтримуються ворожою державою чи недержавними гравцями;

– охорона здоров'я: підтримка санітарної освіти та освітніх програм для надзвичайних ситуацій;

– кібербезпека: започаткування всеосяжних програм для середньої та вищої освіти щодо онлайн-безпеки та боротьби з неправдивою/підробленою інформацією;

– захист критичної інфраструктури: підвищення обізнаності населення, центральних та місцевих державних установ, бізнес-середовища щодо важливості заходів для захисту критичної інфраструктури [10].

Надавати допомогу організаціям критичної інфраструктури для кращого запобігання, підготовки, реагування та відновлення після збоїв і несприятливих подій розпочали і в Австралії, шляхом створення у 2003 році довіреної мережі обміну інформацією (TISN). TISN забезпечує освітні форуми національного рівня для власників і операторів критичної інфраструктури для обговорення вразливостей критичної інфраструктури з відповідними урядовими установами та спільної роботи над розробкою стратегій і рішень для зменшення ризиків. TISN охоплює сотні членів, включаючи представників багатьох найбільших і найвідоміших компаній Австралії, а також урядів штатів і територій. Він складається з семи секторальних груп критичної інфраструктури та двох консультативних груп експертів. Члени TISN регулярно зустрічаються у своїх галузевих групах у безпечному, неконкурентному середовищі, щоб обмінюватися важливою інформацією, розробляти колективні освітньо-навчальні рішення для спільних проблем, а також проводити регулярні зустрічі та навчання між групами та з урядами штатів.

А в Фінляндії при Міністерстві економіки та зайнятості створено Національне агентство з надзвичайних ситуацій (NESA), яке має завдання проводити аналіз ризиків, координувати обмін інформацією, сприяти співробітництву між державним та приватним секторами та впроваджувати політику безпеки постачання в критичних секторах. Навчання, організовані NESA, допомагають операторам перевірити свої плани безперервності бізнесу та надають хороші можливості для вивчення уроків, особливо тих, що проводяться в реальних умовах. Тренування з реагування на надзвичайні

ситуації допомагають виявити слабкі місця та визначити пріоритетність покращень.

Крім цього, Фінляндія входить до системи транскордонного співробітництва з країнами північної Європи (Данія, Ісландія, Норвегія та Швеція) (NordBER) для підтримки стійкості електроенергетичної системи країни через її значну залежність від імпорту електроенергії взимку та через необхідність співпраці у разі транскордонної кризи. NordBER сприяє регулярним навчальним зустрічам між відповідними національними органами влади, відповідальними за питання передачі та розподілу електроенергії в надзвичайних ситуаціях, регіональним навчанням і координації політики. Структура NordBER дозволила створити механізм транскордонної координації на випадок великомасштабного дефіциту енергії, що впливає на одного з його членів.

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

Разом з тим, для більшості розвинутих країн, насамперед країн – членів ЄС та НАТО, загальновизнаними є низка основоположних підходів і принципів при створенні системи захисту критичної інфраструктури, у тому числі у сфері освіти, які почали реалізовуватися в Україні після повномасштабного вторгнення російської федерації на її територію.

Мова, перш за все, йде за Талліннський механізм, який започатковано у 2023 році як міжнародний формат підтримки стійкості цивільної інфраструктури України перед кіберзагрозами. Це комплексний захист, який поєднує як експертну, технологічну, так і освітню підтримку для України. Механізм передбачає підтримку проєктів із захисту критичної інфраструктури України, навчання фахівців, виявлення та блокування шкідливого програмного забезпечення, забезпечення супутникового зв’язку та координацію зусиль міжнародних партнерів.

Учасниками Талліннського механізму є 11 країн – Німеччина, Нідерланди, Естонія, Франція, Данія, Італія, Швеція, Велика Британія, Канада, Польща і США. Спостерігачами є НАТО та Європейський Союз. На національному рівні до роботи Талліннського механізму залучені Національний координаційний центр кібербезпеки, Міністерство цифрової трансформації України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство закордонних справ України та Служба безпеки України.

До створення Талліннського механізму міжнародна допомога Україні у забезпеченні кібербезпеки та критичної інфраструктури України була розрізненою, позбавленою системного підходу та централізованої координації. На сьогодні країни-учасниці Талліннського механізму зібрали більш ніж 200 мільйонів євро, щоб допомогти Україні захистити свою критичну інфраструктуру від російської кіберагресії. Рік скоординованої роботи Талліннського механізму зміг транслювати чіткий сигнал – Україна має партнерів, які продовжуватимуть допомагати їй у розбудові сфери критичної інфраструктури, як під час військової агресії, так і у довгостроковій перспективі.

Розбудовувати систему захисту критичної інфраструктури України у сфері освіти продовжують також Уряд Сполучених Штатів у рамках Програми «Development Cooperation Partnership» (DCP) та Уряд Естонської Республіки через Естонський центр міжнародного розвитку (ESTDEV) та Академію електронного управління Естонії (eGA). Одна з таких ініціатив – проєкт «Готовність кібербезпеки для критичної інфраструктури в Україні», що стартував наприкінці 2024 року за активної участі Держспецзв'язку. Проєкт передбачає проведення низки спеціальних тренінгів, які забезпечать підвищення кваліфікації фахівців державних установ та об'єктів критичної інфраструктури. Слід зазначити, що eGA співпрацює з Держспецзв'язку та іншими українськими кібербезпековими організаціями ще з 2020 року. За цей час було розроблено інструкції для державних установ щодо планування та

проведення тестування інформаційної безпеки, а також успішно проведено ряд навчань з кібербезпеки та захисту об'єктів критичної інфраструктури.

«В умовах агресії російської федерації проти України захист критичної інфраструктури є одним із найважливіших завдань держави. Кінетичні атаки на ці об'єкти часто супроводжуються масштабними кібератаками. Фахівці Держспецзв'язку разом із колегами з інших організацій постійно працюють над посиленням кіберзахисту, зокрема й на об'єктах критичної інфраструктури. Тож ми щиро вдячні нашим партнерам за їхню потужну підтримку – експертну, фінансову та дипломатичну. Вона є невід'ємною складовою посилення спроможностей фахівців протистояти загрозам у кіберпросторі», – підкреслив Голова Держспецзв'язку Олександр Потій [11].

Об'єднує свої зусилля Україна у сфері захисту критичної інфраструктури також з Іспанією. Так, у листопаді 2024 року представниками Держспецзв'язку в рамках виконання відповідних пунктів Угоди про співробітництво у сфері безпеки між Україною та Іспанією підписано Меморандум про взаєморозуміння з Національним центром захисту критичної інфраструктури Королівства Іспанія, який передбачає: проведення спільних навчань для суб'єктів національної системи захисту критичної інфраструктури України, обмін досвідом та наукову співпрацю, а також допомогу щодо узгодження українського законодавства з європейськими директивами CER (стійкість критичної інфраструктури) та NIS2 (кібербезпека).

Слід виділити також Угоду про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії і Північної Ірландії у частині сприяння розвитку спроможності захисту критичної інфраструктури України. Так, відповідно до Угоди, Сполучене Королівство продовжить залучати українських фахівців із досвідом забезпечення безпеки критичної інфраструктури для реалізації відповідних проєктів на своїй території, проведення спільних освітніх та навчальних програм для спеціалістів із захисту критичної інфраструктури, а також визначати джерела фінансування для розвитку захисту та стійкості критичної інфраструктури в різних секторах [12].

Дієвою є також Угода про співробітництво у сфері безпеки та довгострокову підтримку між Україною і Великим Герцогством Люксембург, яка визнала, що оборона, відновлення, реформи та європейські і євроатлантичні амбіції підсилюють Україну та Велике Герцогство Люксембург на шляху спільного розвитку. Так, з огляду на європейську перспективу України Люксембург сприятиме Україні в гармонізації її нормативних актів зі стандартами ЄС у сфері захисту критичної інфраструктури, та щодо організації та проведення спільних освітніх і навчальних програм для спеціалістів у сфері захисту критичної інфраструктури.

Питанням навчання та підготовки фахівців у сфері захисту критичної інфраструктури почав опікуватись й Національний авіаційний університет створивши на базі факультету екологічної безпеки, інженерії та технологій Центр безпеки та стійкості критичної інфраструктури. Місія Центру полягає у співпраці з основними зацікавленими сторонами у сфері безпеки сфери критичної інфраструктури по всій Україні, центрами передового досвіду, науковцями та профільними експертами з Північної Америки та Європейського Союзу. При цьому основними завдання Центру є:

– створення контенту для освіти і навчання з питань безпеки та стійкості критичної інфраструктури для використання в шкільній, професійно-технічній освіті, навчанні на робочому місці, бакалаврській (магістерській) освіті, військовій освіті, а також для урядових та галузевих лідерів, менеджерів та керівників;

– розроблення та розвиток тематичних досліджень з питань безпеки та стійкості критичної інфраструктури, заснованих на реальних подіях, що вплинули на українську критичну інфраструктуру протягом останнього десятиліття, які можуть бути використані для підтримки освіти і навчання з питань безпеки та стійкості критичної інфраструктури на довгі роки вперед;

– співпраця з власниками та операторами об’єктів критичної інфраструктури та іншими зацікавленими сторонами для розроблення базових

навчальних програм, які відповідають специфічним потребам кожної галузі критичної інфраструктури, визначеного в українському законодавстві [13].

Подальшим розвитком української сфери захисту критичної інфраструктури займається також Фонд цивільних досліджень та розвитку США в Україні (CRDF Global в Україні) та Державний Департамент США. Так, 02 жовтня 2024 року в Академії СБ України відкрили Навчальний ситуаційний центр кібербезпеки об'єкта критичної інфраструктури, що є значним кроком для підвищення якості здобувачів освіти. Відкриття Навчального центру стало можливе завдяки участі та перемозі у конкурсі під назвою «Гранти на покращення кібербезпеки для центральних органів влади та інституцій з розбудови спроможності України». Навчальний заклад при цьому отримав ІТ-обладнання для оснащення центру вартістю близько 50 тисяч доларів США. «Це значний крок для підвищення якості освіти наших здобувачів освіти. Адже наша молодь зможе отримати практичні навички керування ситуаційним центром кібербезпеки об'єкта критичної інфраструктури», – наголосив ректор Академії Андрій Черняк [14].

Велике значення має також зарубіжний досвід (у практичній площині) при організації та проведенні освітніх заходів для фахівців сфери захисту критичної інфраструктури. Так, 11 – 14 березня 2024 року у м. Лечче (Італія) за підтримки Офісу зменшення загроз Управління міжнародної безпеки та нерозповсюдження Державного департаменту США, Фонду цивільних досліджень та розвитку США відбувся практичний семінар «Розвиток університетських програм з безпеки та стійкості критичної інфраструктури» за проєктом «Захист критично важливої хімічної інфраструктури України від триваючої російської агресії». Учасниками української делегації стали представники Національного університету цивільного захисту України, які ознайомилися з кращими практиками захисту об'єктів критичної інфраструктури (пов'язаними з хімічним сектором), проведенням оцінки вразливості хімічних об'єктів, а також освітніми програмами з безпеки та

стійкості критичної інфраструктури для розбудови національної системи навчання у сфері захисту об’єктів критичної інфраструктури в Україні [15].

В свою чергу королівські інженерні фахівці британської армії також провели нову програму навчання, щоб допомогти Україні зміцнити її здатність захищати свою критично важливу національну інфраструктуру від нападів росії та рятувати життя цивільних осіб. Так, протягом 2024 року українські цивільні інженери пройшли спеціальний 2-тижневий курс у Великій Британії, щоб навчитися захищати критичну інфраструктуру від атак російських безпілотників і ракет. Навчання надало змогу покращити здатність України планувати захист своєї критично важливої інфраструктури від атак та навчити, як визначити найбільш вразливі елементи інфраструктури, потенційні відстані вибуху та вплив різної зброї та вибухових речовин, а також де найкраще розташувати фізичні та повітряні бар’єри, щоб допомогти захиститися від російських атак [16].

Не можливо не відмітити також й освітні заходи що організовуються з метою поєднання вимог зеленої економіки і поствоєнної відбудови України у сфері захисту критичної інфраструктури. Так, у липні 2023 року науковцями кафедри економічної і соціальної географії імені професора Олега Шаблія Національного університету «Львівська політехніка» та кафедри інжинірингу Університету Бірмінгема (Великобританія) організовано у межах проєкту «Twinning for Identity, Sovereignty and Resilience» міжнародний семінар «Транскордонна стійкість критичної транспортної інфраструктури в Україні та її вплив на економіку та суспільство», що відбувся у м. Варшава. В рамках семінару були розглянуті питання пов’язані із стійкістю та сталими рішеннями в адаптації інфраструктури в умовах поствоєнної відбудови, суспільно-географічними проблемами розвитку Львівської області, економічною ефективністю використання залізничних пасажирських маршрутів Західного регіону України, практичним використанням геологістики в транспортній галузі Західного регіону України, соціально-економічними передумовами функціонування приміського залізничного транспорту [17].

Приймає участь у підвищенні кваліфікації українських фахівців також й Республіка Польща. Так, у грудні 2023 року працівники підрозділів системи МВС України, Нацгвардії, ДСНС України, Державної прикордонної служби, Національної поліції України, ДМС України спільно з польськими колегами та представниками Федерального бюро розслідувань Посольства США у Варшаві взяли участь у міжнародному тренінгу з кібербезпеки, який був організований у рамках посилення співпраці з Україною Управлінням комунікації та інформаційних технологій Головного управління поліції в місті Щитно та керівництвом Академії поліції. Під час навчання представниками компаній WB Electronics, Netformers, CISCO, MCX і Comcert було організовано симуляційні ігри «Cyber Fortress», де були змодельовані різноманітні ситуації, пов'язані із кіберзахистом об'єктів критичної інфраструктури. Крім цього, за результатами тренінгу учасники розширили свої знання щодо захисту ІКТ-систем, загроз зовнішнього втручання, а також у сфері «OSINT» (розвідка відкритих джерел). Варто зазначити, що це були перші сумісні навчання такого типу, які спрямовані на підвищення професійної кваліфікації спеціалістів із безпеки об'єктів критичної інфраструктури, що в свою чергу надало можливість налагодити робочі контакти та обмінятися досвідом із колегами з Польщі [18].

Слід вказати також й на державні органи України, які розпочали освітні заходи з питань захисту об'єктів критичної інфраструктури. Так, на ресурсах апарату Ради національної безпеки і оборони України почала працювати онлайн-платформа «Безпека та стійкість критичної інфраструктури». Платформу отримано у рамках співпраці служби з питань безпеки критичної інфраструктури Апарату РНБО України з Державним Департаментом США та Фондом цивільних досліджень та розвитку США в Україні (CRDF Global) яка призначена для електронного навчання на безкоштовній основі усіх причетних до національної системи захисту критичної інфраструктури. Платформа містить перекладені українською мовою сім модулів дистанційного навчання з питань безпеки та стійкості критичної інфраструктури Інституту управління надзвичайними ситуаціями Федерального агентства з надзвичайних ситуацій

при Департаменті внутрішньої безпеки США і два модулі українських експертів з питань безпеки та стійкості критичної інфраструктури За даними РНБО України, на платформі вже зареєструвалися понад 1500 користувачів і більш як 500 з них отримали перші сертифікати [19].

Кіберстійкість державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури залежить не тільки від умов, які має створити держава, а й від ефективного захисту, який має бути побудований у кожній установі. Так, для підвищення спроможності з розбудови кіберзахисту державних установ Держспецзв'язку разом із проєктом ЄС «Підтримка комплексної реформи державного управління в Україні» (EU4PAR) та Нацдержслужби провела перше навчання для держслужбовців категорії «А» з побудови кіберзахисту в державних установах. Програма навчання була орієнтована на керівників, які мають стати лідерами змін у своїх установах у галузі кіберзахисту. Метою було дати слухачам розуміння специфіки загроз в українському кіберпросторі, які істотно зросли від початку кібервійни росії проти України, та ролі керівників у підвищенні кіберзахисту; запропонувати інструменти, які допоможуть у підвищенні кіберстійкості їхніх установ навіть в умовах браку коштів, та ознайомити з інфраструктурою кіберзахисту, яку будує держава [20].

«Програма з кіберзахисту від Держспецзв'язку є унікальним продуктом, який базується на практичному досвіді протистояння кібервійні, яка відбувається тут і зараз у режимі реального часу. Програму викладають ті, хто щодня захищає Україну та весь цивілізований світ від атак російських хакерів. Це ті знання та вміння, які вкрай необхідні для посилення стійкості України в цілому та публічної служби зокрема. Коли ми згадуємо цю програму серед колег в інших країнах Європи, відповідь в усіх одна: «Нам теж це потрібно!», – прокоментував керівник проєкту ЄС «Підтримка комплексної реформи державного управління в Україні» (EU4PAR)» Угіс Сікс [20].

Разом з тим, посиленням захисту об'єктів критичної інфраструктури почали плідно опікуватися й суб'єкти національної системи захисту критичної

інфраструктури спільно із зарубіжними представниками. Так, у січні 2024 року представниками Генерального штабу ЗС України, Адміністрації Держспецзв'язку, ДСНС України та Національного університету оборони України проведено курси підвищення кваліфікації фахівців з питань захисту об'єктів критичної інфраструктури. У навчаннях взяли участь представники обласних і військових адміністрацій, органів державної влади, операторів об'єктів критичної інфраструктури, а також фахівці країн Європейського Союзу, які відповідають за захист критичної інфраструктури. Підготовка фахівців дала можливість посилити теоретичні знання у сферах забезпечення енергетичної безпеки держави під час дії воєнного стану, функціонування загальної системи захисту та забезпечення безпеки і стійкості критичної інфраструктури України. За результатами підсумкового контролю наприкінці курсів випускники отримали знання щодо захисту об'єктів критичної інфраструктури, зокрема щодо:

– нормативної бази у сфері захисту критичної інфраструктури;

– основних аспектів енергетичної безпеки держави в ході відбиття широкомасштабної агресії російської федерації;

– порядку проведення моніторингу захисту об'єктів критичної інфраструктури, зокрема під час російської агресії;

– порядку категоризації об'єктів критичної інфраструктури;

– вимог щодо захисту критичних елементів об'єктів критичної інфраструктури;

– вимог та порядку проведення оцінювання стану захищеності об'єктів критичної інфраструктури;

– заходів пожежної, техногенної безпеки та цивільного захисту, які необхідно впроваджувати під час захисту критично-важливих елементів об'єктів критичної інфраструктури;

– взаємодії з підрозділами, які беруть участь в організації захисту об'єктів критичної інфраструктури [21].

В свою чергу освітньо-практичні заняття з основ кібергігієни та медіаграмотності для працівників критичної інфраструктури організовуються та проводяться також і на регіональному рівні. Так, у квітні 2024 року CRDF Global в Україні для представників ОВА, Ужгородського національного університету, Закарпаттяобленерго, обласного управління Пенсійного фонду України, БУВР Тиси, обласної клінічної лікарні імені А. Новака й інших установ та організацій організовано практичний семінар з питань ключових аспектів кібергігієни й кібербезпеки, підвищення рівня медіаграмотності та боротьби з дезінформацією та фейками. «В умовах війни вкрай важливо дбати про власну безпеку в цифровому середовищі, вміти розпізнавати дезінформацію, протистояти ворожим фейкам і шахрайським схемам. Зараз такі знання та навички особливо потрібні працівникам критичної інфраструктури», – підкреслив заступник голови Закарпатської обласної військової адміністрації Олександр Пацкан [22].

Крім цього, на початку 2024 року Ужгородським національним університетом, за підтримки Агентства США з міжнародного розвитку (USAID), на кафедрі твердотільної електроніки та інформаційної безпеки відкрито кіберполігон, що використовуватиметься, у тому числі, для підвищення кваліфікації та компетентності фахівців з кібербезпеки, учасників бойових дій, державних службовців, посадових осіб органів самоврядування з питань моделювання реалістичних сценаріїв кібератак на об’єкти критичної інфраструктури. Планується, що кіберполігон дасть змогу проводити науково-дослідну роботу та експерименти з використанням новітніх технологій та методик з кібербезпеки. В рамках відкриття кіберполігону Ужгородському національному університету було передано 40 одиниць комп’ютерного обладнання та 40 ліцензій на використання програмного забезпечення, що сприятиме розвитку культури кібербезпеки в суспільстві та популяризації професії кіберексперта [23].

Слід акцентувати увагу також на допомогу від міжнародних партнерів, яка робить кіберзахист об’єктів критичної інфраструктури України

надійнішим та ефективнішим. Так, Державний центр кіберзахисту Держспецзв'язку отримав нове серверне та мережеве обладнання і програмне забезпечення від Агентства США з міжнародного розвитку (USAID). Допомога надійшла в межах проєкту «Кібербезпека критично важливої інфраструктури України». Завдяки новому обладнанню Державний центр може краще захищати важливі державні об'єкти від кібератак, у тому числі шляхом проведення відповідних занять у тренінговому кіберцентрі. Зокрема, покращено роботу системи виявлення вразливостей і реагування на кіберінциденти, що допомагає забезпечити безперебійне надання послуг об'єктам критичної інфраструктури та надійніший захист від кіберзагроз. Програмне забезпечення було передано Національному центру резервування державних інформаційних ресурсів, що надало змогу швидше виявляти загрози та миттєво реагувати на небезпечні події у сфері інформаційної безпеки [24].

А у фізико-технічному інституті КПІ імені Ігоря Сікорського, за підтримки ініціативи USAID «Кібербезпека критично важливої інфраструктури України» відкрито навчальну лабораторію кібербезпеки автоматизованих систем керування, що дублює середовище промислової системи управління, моделюючи реальні ситуації у різних секторах критичної інфраструктури. Передбачається, що на базі навчальної лабораторії буде підготовлено орієнтовно 200 спеціалістів з інформаційної та кібернетичної безпеки, які у подальшому зможуть проводити практичні експерименти, залучаючи при цьому інших фахівців з кібербезпеки.

«Обладнання лабораторії допоможе студентам опанувати передові методи й рішення у сфері кібербезпеки з акцентом на оцінку вразливостей державних і приватних об'єктів критичної інфраструктури. А ще завдяки цій лабораторії в нашому університеті розроблятимуть окремі навчальні модулі в межах освітніх і сертифікатних програм», – зазначив ректор КПІ Анатолій Мельниченко [25].

Розбудовою освітньої складової сфери захисту критичної інфраструктури зайнялися і в Національному авіаційному університеті. Так, за підтримки CRDF

Global в Україні та Державного департаменту США, а також за участі Національного координаційного центру кібербезпеки при РНБО України та українського постачальника програм з кібернавчання Cyber Unit Technologies у серпні 2024 року відкрито Cyber Range UA – віртуальне середовище для емуляції інфраструктур та кібератак, яке доступне для всіх кіберспеціалістів країни. Одночасно на кіберполігоні можуть проходити тренування представники державних установ, підприємств критичної інфраструктури, приватних компаній, навчальних закладів та студенти Національного авіаційного університету. Поділені на різні команди, вони вчяться реагувати на інциденти в умовах, максимально наближених до реальних.

Наразі кіберполігон має 15 сценаріїв, які у віртуальному режимі здійснюють симуляцію реальних кібератак, з якими Україна стикнулася впродовж останніх років. Зокрема, кіберполігон симулює складні APT-атаки російських хакерських груп, які щоденно атакують Україну. «НАУ має готувати не тільки інженерів, які створюють та програмують БпЛА, але і потужних ІТ-фахівців. Це колосальна перевага для наших студентів – навчатися на ультрареалістичних сценаріях на рівні з провідними українськими фахівцями з кібербезпеки, та на практиці бачити специфіку активної протидії кіберзагрозам у різних секторах», – прокоментувала керівниця НАУ Ксенія Семенова [26].

Потужним «мотиватором» для реалізації питань пов’язаних із професійною підготовкою фахівців у сфері захисту критичної інфраструктури є надання грантів на здобуття освіти – грошової допомоги, яка надається для здобуття громадянином вищої освіти, або з метою перепідготовки та підвищення кваліфікації тощо. Так, проєктним офісом Національного університету «Львівська політехніка» відкрито конкурс на участь у програмі грантів від USAID «Кібербезпека критичної інфраструктури України», метою якої є підвищення національної готовності, зменшення ризиків та вразливостей у сфері кібербезпеки, а також зміцнення критичної інфраструктури України у

секторі кібербезпеки. Загальний бюджет програми – від 20 000 до 150 000 доларів США.

При цьому, основними цілями конкурсу є:

– розвиток кадрового потенціалу України у сфері кібербезпеки об'єктів критичної інфраструктури;

– розбудова стійкої індустрії кібербезпеки об'єктів критичної інфраструктури для стимулювання попиту і пропозиції українських рішень;

– прискорення розвитку людей, процесів і технологій на підтримку кібербезпеки в усіх секторах та об'єктах критично важливої інфраструктури України;

– розширення можливостей, оснащення й фінансування кібербезпеки підприємців та бізнесів у сфері кібербезпеки [27].

Слід зазначити, що проєкт USAID «Кібербезпека критичної інфраструктури України» з початку повномасштабного вторгнення російської федерації на територію України надав обладнання та програмне забезпечення для 25 закладів вищої освіти, оновив 11 освітніх програм з кібербезпеки для 8 українських університетів, та розробив нову програму, що повністю відповідає новим професійним стандартам з кібербезпеки, прийнятим наприкінці 2023 року. Крім цього, зазначеним проєктом оголошено програму стажування для студентів, щоб сприяти співпраці між університетами та операторами критичної інфраструктури, а також запущено програму підвищення кваліфікації для обраних викладачів, що відкриє доступ до нових знань, навичок та зв'язків у галузі, що необхідні для підвищення якості освіти у кібербезпеці. У поєднанні з державною підтримкою, такі зусилля здатні перетворити Україну на лідера в інноваційних підходах у сфері безпеки критичної інфраструктури.

З огляду на євроатлантичні устремління нашої держави, історичний вибір народу України, що підтверджується в черговий раз, вивчення освітніх підходів як на національному так і регіональному рівнях в країнах-членах Євросоюзу та в інших країнах є актуальним. Нині питання захисту загальноєвропейської

критичної інфраструктури є частиною загальної архітектури безпеки в ЄС, а створення національно-освітніх систем професійної підготовки фахівців у сфері захисту критичної інфраструктури – невід'ємною частиною забезпечення національної безпеки.

Висновки та перспективи подальших розвідок у даному напрямі. На основі зарубіжного досвіду можна виокремити такі узагальнені підходи до організації та забезпечення проведення професійної підготовки фахівців у сфері захисту критичної інфраструктури, що застосовуються як в країнах ЄС, так і в Україні за допомогою міжнародних партнерів:

– навчання залежно від масштабу та сфери охоплення можна поділити на багатонаціональні, національні, регіональні (місцеві), секторальні або галузеві, корпоративні та об'єктові;

– за формальністю освіти навчання забезпечується шляхом підвищення кваліфікації та стажування, що надає змогу набути компетентності пов'язані із здійсненням оцінки захищеності об'єктів критичної інфраструктури, загроз критичній інфраструктурі, визначенням вимог до забезпечення захисту та стійкості секторів критичної інфраструктури, а також координацією секторальних органів щодо забезпечення безпеки та стійкості сфери захисту критичної інфраструктури;

– за кількісним показником освітні заходи проводяться шляхом індивідуального та групового навчання, що може забезпечити відповідні умови для активної пізнавальної діяльності, самоконтролю та створення ситуації успіху в навчальній діяльності, а також реалізувати природне прагнення до спілкування, взаємодопомоги і співпраці;

– за часовим показником підвищення кваліфікації поділяється на довгострокове та короткострокове навчання;

– за формою навчання підготовка кадрів для сфери захисту критичної інфраструктури здійснюється шляхом заочного, дистанційного та мережевого навчання, що у подальшому дасть змогу відповідним фахівцям проводити оцінку загроз критичній інфраструктурі на національному рівні, а також

готувати рекомендації щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури відповідно до категорій об’єктів критичної інфраструктури.

Результати аналізу досвіду провідних країн світу свідчить про те, що Україна знаходиться на початку формування національної системи захисту критичної інфраструктури та системи підготовки кадрів для сфери захисту критичної інфраструктури. В умовах воєнного стану система підготовки кадрів зазначеної сфери потребує відповідної адаптації до світової практики, що у майбутньому дасть змогу забезпечити:

– підвищення комплексних знань (навичок, умінь) персоналу та керівного складу операторів критичної інфраструктури, персоналу суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури;

– підготовку персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури;

– навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

Беручи до уваги зарубіжні підходи щодо організації професійної підготовки фахівців у сфері захисту критичної інфраструктури, особливу увагу при забезпеченні функціонування системи підготовки кадрів для сфери захисту критичної інфраструктури необхідно акцентувати на:

– впровадження Концепції системи підготовки кадрів для сфери захисту критичної інфраструктури;

– розроблення інших нормативно-правових та організаційно-розпорядчих актів, які врегулювали би освітньо-суспільні відносини у сфері захисту критичної інфраструктури у відповідність до вимог сьогодення;

– запровадження обов’язкової періодичної атестації (переатестації) персоналу відповідального за забезпечення кіберзахисту та кібербезпеки суб’єктів критичної інфраструктури;

– введення в органах державної влади та на об’єктах критичної інфраструктури відповідних фахівців із кіберзахисту об’єктів критичної інфраструктури;

– запровадження порядку присвоєння (підтвердження) професійної кваліфікації фахівцям суб’єктів національної системи захисту критичної інфраструктури.

Сьогодні освітній напрям у сфері захисту критичної інфраструктури є складовою політики як на національному рівні окремих країн-членів ЄС та НАТО, так і на міжнародному рівні. Поступове втілення освітнього напряму у життя дозволить зміцнити національну систему захисту критичної інфраструктури, посиливши її здатність виконувати функції із забезпечення життєво важливих національних інтересів. Запровадження зарубіжних підходів до підготовки вітчизняних кадрів для сфери захисту критичної інфраструктури ще більше наблизить сучасні механізми управління в сфері національної безпеки України до тих, що впроваджені в країнах-членах ЄС та НАТО. Захист критичної інфраструктури в Україні має стати невід’ємною частиною загальноєвропейського механізму у сфері безпеки.

Література

1. 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 (дата звернення: 10.02.2025).

2. Жемба А. Й. Управління міжнародною політикою ЄС у сфері захисту критичної інфраструктури. *Наукові записки Національного університету "Острозька академія". Серія : Економіка*. 2022. № 27. С. 4–11.

3. Зубко Г. Ю. Розвиток інституційної спроможності держави у сфері безпеки та стійкості життєво важливої інфраструктури. *Прикарпатський юридичний вісник*. 2019. № 2. С. 9–14.

4. Єрменчук О. П. Європейський досвід захисту критичної інфраструктури: правовий аналіз та перспективи впровадження в Україні.

Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2018. № 2. С. 40–46.

5. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

6. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. Дата оновлення: 10.02.2025. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 10.02.2025).

7. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : постанова Кабінету Міністрів України від 12.07.2022 р. № 787. Дата оновлення: 10.02.2025. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (дата звернення: 10.02.2025).

8. 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: 10.02.2025. URL: https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text (дата звернення: 10.02.2025).

9. Арсенович Л. А. Деякі питання запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2022. № 5. С. 3–14.

10. Експерт НІСД: «Стратегія національної оборони Румунії передбачає заходи щодо розвитку ефективних інструментів зміцнення стійкості суспільства та критичної інфраструктури». URL: https://niss.gov.ua/news/statti/ekspert-nisd-stratehiya-natsionalnoyi-oborony-rumuniyi-peredbachaye-zakhody-shchodo (дата звернення: 10.02.2025).

11. Держспецзв’язку та eGA запускають проєкт з підвищення кіберстійкості критичної інфраструктури. URL: https://cip.gov.ua/ua/news/ssscip-and-ega-to-enhance-cyber-resilience-of-ukrainian-critical-infrastructure (дата звернення: 10.02.2025).

12. Угода про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії і Північної Ірландії. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-88277 (дата звернення: 10.02.2025).

13. Центр безпеки та стійкості критичної інфраструктури. URL: https://febit.nau.edu.ua/tsentr-bezpeky-ta-stiikosti-krytychnoi-infrastruktury/ (дата звернення: 10.02.2025).

14. В Академії СБУ відкрили Навчальний ситуаційний центр кібербезпеки об'єкта критичної інфраструктури. URL: https://www.nasbu.edu.ua/ua/news-1-8-667-v-akademii-sbu-vidkrili-navchalniy-situaciyniy-centr-kiberbezpeki-obekta-kritichnoi-infrastrukturi (дата звернення: 10.02.2025).

15. Представники НУЦЗ України стали учасниками практичного семінару «Розвиток університетських програм з безпеки та стійкості критичної інфраструктури». URL: https://surl.li/vkmvwt (дата звернення: 10.02.2025).

16. Інженери ЗСУ пройшли навчання із захисту критичної інфраструктури у Британії. URL: https://www.ukrinform.ua/rubric-ato/3776985-inzeneri-zsu-projsli-navcanna-iz-zahistu-kriticnoi-infrastrukturi-u-britanii.html (дата звернення: 10.02.2025).

17. Відбувся міжнародний семінар «Транскордонна стійкість критичної транспортної інфраструктури в Україні та її вплив на економіку та суспільство». URL: https://surl.li/dhumnt (дата звернення: 10.02.2025).

18. Спеціаліст Відділу захисту інформації ДМС України взяв участь у міжнародному тренінгу з кібербезпеки у Польщі. URL: https://dmsu.gov.ua/news/dms/15365.html (дата звернення: 10.02.2025).

19. РНБО запустила онлайн-платформу «Безпека та стійкість критичної інфраструктури». URL: https://www.ceskenoviny.cz/ukrinform/ukrajinsky/zprava.php?id=1221334 (дата звернення: 10.02.2025).

20. Підвищуємо кіберстійкість державних інформаційних ресурсів: Держспецзв'язку провела перший освітній курс із кіберзахисту для держслужбовців категорії «А». URL: https://scpc.gov.ua/uk/articles/225 (дата звернення: 10.02.2025).

21. Посилення захисту об’єктів критичної інфраструктури: спеціалісти Держспецзв’язку провели навчання для профільних фахівців. URL: https://cip.gov.ua/ua/news/posilennya-zakhistu-ob-yektiv-kritichnoyi-infrastrukturi-specialisti-derzhspeczv-yazku-proveli-navchannya-dlya-profilnikh-fakhivciv (дата звернення: 10.02.2025).

22. CRDF Global в Україні провела на Закарпатті чергові навчання з основ кібергігієни та медіаграмотності. URL: https://carpathia.gov.ua/news/crdf-global-v-ukraini-provela-na-zakarpatti-cherhovi-navchannia-z-osnov-kiberhihiieny-ta-mediahramotnosti (дата звернення: 10.02.2025).

23. У рамках реалізації Проєкту USAID «Кібербезпека критично важливої інфраструктури України» відкрито кіберполігон на кафедрі ТЕІБ. URL: https://www.uzhnu.edu.ua/uk/news/u-ramkah-realizatsiji-proyektu-USAID-kiberbezpeka--teIb-.htm (дата звернення: 10.02.2025).

24. ДЦКЗ Держспецзв’язку посилив захист критичної інфраструктури за підтримки Агентства США з міжнародного розвитку. URL: https://scpc.gov.ua/uk/articles/379 (дата звернення: 10.02.2025).

25. На базі КПІ відкрили лабораторію з кібербезпеки критичної інфраструктури. URL: https://dou.ua/lenta/news/new-lab-in-kpi/ (дата звернення: 10.02.2025).

26. На базі НАУ створили кіберполігон Cyber Range UA. URL: https://dou.ua/lenta/news/about-cyber-range-ua/?from=similar_posts (дата звернення: 10.02.2025).

27. Програма грантів від USAID «Кібербезпека критичної інфраструктури України». URL: https://lpnu.ua/news/prohrama-hrantiv-vid-usaid-kiberbezpeka-krytychnoi-infrastruktury-ukrainy (дата звернення: 10.02.2025).

References

1. Official website of the National Institute of Strategic Studies (2021), “The problem of building a system of personnel and population training to ensure the stability of critical infrastructure in Ukraine. Analytical note”, available at:

https://niss.gov.ua/doslidzhennya/ekonomika/problema-rozbudovi-sistemi-pidgotovki-kadriv-i-naselennya-dlya (Accessed 10 February 2025).

2. Zhemba, A.A. (2022), “Management of the EU's international policy in the field of critical infrastructure protection”, *Naukovi zapysky Natsionalnoho universytetu "Ostrozka akademiia". Seriia : Ekonomika,* vol. 27, pp. 4–11.

3. Zubko, G.Yu. (2019), “Development of the state's institutional capacity in the field of safety and stability of vital infrastructure”, *Prykarpatskyi yurydychnyi visnyk,* vol. 2, pp. 9–14.

4. Ermenchuk, O.P. (2018), “European experience of critical infrastructure protection: legal analysis and prospects for implementation in Ukraine”, *Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav,* vol. 2, pp. 40–46.

5. Ermenchuk, O.P. (2018), *Osnovni pidkhody do orhanizatsii zakhystu krytychnoi infrastruktury v krainakh Yevropy: dosvid dlia Ukrainy* [Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine], Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav, Dnipro, Ukraine.

6. 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: hhttps://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (Accessed 10.02.2025).

7. Cabinet of Ministers of Ukraine (2022), Resolution “On the establishment of the State Service for the Protection of Critical Infrastructure and Ensuring the National Stability System of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (Accessed 10.02.2025).

8. 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 10.02.2025).

9. Arsenovych, L.A. (2022), “Some issues of introducing a system of training specialists in the field of critical infrastructure protection”, *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruvannia,* vol. 5, pp. 3–14.

10. Official website of the National Institute of Strategic Studies (2021), “NISD expert: “The National Defense Strategy of Romania provides for measures to develop effective tools for strengthening the resilience of society and critical infrastructure”, available at: https://niss.gov.ua/news/statti/ekspert-nisd-stratehiya-natsionalnoyi-oborony-rumuniyi-peredbachaye-zakhody-shchodo (Accessed 10 February 2025).

11. The official website of the State Service for Special Communications and Information Protection of Ukraine (2025), “State Special Communications and eGA are launching a project to improve the cyber resilience of critical infrastructure”, available at: https://cip.gov.ua/ua/news/ssscip-and-ega-to-enhance-cyber-resilience-of-ukrainian-critical-infrastructure (Accessed 10 February 2025).

12. Official website of the President of Ukraine (2024), “Agreement on cooperation in the field of security between Ukraine and the United Kingdom of Great Britain and Northern Ireland”, available at: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-88277 (Accessed 10 February 2025).

13. Official website of the National Aviation University (2024), “Center for Security and Resilience of Critical Infrastructure”, available at: https://febit.nau.edu.ua/tsentr-bezpeky-ta-stiikosti-krytychnoi-infrastruktury/ (Accessed 10 February 2025).

14. The official website of the National Academy of the Security Service of Ukraine (2024), “The Training Situational Center for Cyber Security of a Critical Infrastructure Object was opened at the SBU Academy”, available at: https://www.nasbu.edu.ua/ua/news-1-8-667-v-akademii-sbu-vidkrili-navchalniy-situaciyniy-centr-kiberbezpeki-obekta-kritichnoi-infrastrukturi (Accessed 10 February 2025).

15. Official website of the National University of Civil Defense of Ukraine (2024), “Representatives of the National Center of Ukraine became participants in the practical seminar “Development of university programs on security and stability of

critical infrastructure", available at: https://surl.li/vkmvwt (Accessed 10 February 2025).

16. The official website of the Ukrinform publication (2023), "Engineers of the Armed Forces of Ukraine received training in the protection of critical infrastructure in Britain", available at: https://www.ukrinform.ua/rubric-ato/3776985-inzeneri-zsu-projsli-navcanna-iz-zahistu-kriticnoi-infrastrukturi-u-britanii.html (Accessed 10 February 2025).

17. The official website of the Lviv Polytechnic National University (2023), "The international seminar "Cross-border sustainability of critical transport infrastructure in Ukraine and its impact on the economy and society" was held", available at: https://surl.li/dhumnt (Accessed 10 February 2025).

18. Official website of the State Migration Service of Ukraine (2023), "A specialist of the Department of Information Protection of the Ministry of Internal Affairs of Ukraine took part in an international training on cyber security in Poland", available at: https://dmsu.gov.ua/news/dms/15365.html (Accessed 10 February 2025).

19. Official site of Czech news (2024), "NSDC launched the online platform "Security and stability of critical infrastructure", available at: https://www.ceskenoviny.cz/ukrinform/ukrajinsky/zprava.php?id=1221334 (Accessed 10 February 2025).

20. The official website of the State Center for Cyber Protection of the State Special Communications (2022), "We are increasing the cyber resilience of state information resources: the State Intelligence Service conducted the first educational course on cyber protection for civil servants of category "A", available at: https://scpc.gov.ua/uk/articles/225 (Accessed 10 February 2025).

21. The official website of the State Service for Special Communications and Information Protection of Ukraine (2024), "Strengthening the protection of critical infrastructure objects: State Special Communications specialists conducted training for specialized specialists", available at: https://cip.gov.ua/ua/news/posilennya-zakhistu-ob-yektiv-kritichnoyi-infrastrukturi-specialisti-derzhspeczv-yazku-proveli-navchannya-dlya-profilnikh-fakhivciv (Accessed 10 February 2025).

22. The official website of the Transcarpathian Regional Military Administration (2024), “CRDF Global in Ukraine conducted regular training on the basics of cyber hygiene and media literacy in Transcarpathia”, available at: https://carpathia.gov.ua/news/crdf-global-v-ukraini-provela-na-zakarpatti-cherhovi-navchannia-z-osnov-kiberhihiieny-ta-mediahramotnosti (Accessed 10 February 2025).

23. Official website of the Uzhhorod National University (2024), “As part of the implementation of the USAID Project “Cybersecurity of Critically Important Infrastructure of Ukraine”, a cyber training ground was opened at the TEIB department”, available at: https://www.uzhnu.edu.ua/uk/news/u-ramkah-realizatsiji-proyektu-USAID-kiberbezpeka--teIb-.htm (Accessed 10 February 2025).

24. The official website of the State Center for Cyber Protection of the State Special Communications (2024), “The State Intelligence Service has strengthened the protection of critical infrastructure with the support of the United States Agency for International Development”, available at: https://scpc.gov.ua/uk/articles/379 (Accessed 10 February 2025).

25. The official website of the DOU publication (2024), “A laboratory for cyber security of critical infrastructure was opened on the basis of KPI”, available at: https://dou.ua/lenta/news/new-lab-in-kpi/ (Accessed 10 February 2025).

26. The official website of the DOU publication (2024), “The Cyber Range UA cyber polygon was created on the basis of NAU”, available at: https://dou.ua/lenta/news/about-cyber-range-ua/?from=similar_posts (Accessed 10 February 2025).

27. The official website of the Lviv Polytechnic National University (2024), “USAID grant program “Cybersecurity of critical infrastructure of Ukraine”, available at: https://lpnu.ua/news/prohrama-hrantiv-vid-usaid-kiberbezpeka-krytychnoi-infrastruktury-ukrainy (Accessed 10 February 2025).

Стаття надійшла до редакції 15.02.2025 р.