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. № 1.

DOI: http://doi.org/10.32702/2307-2156.2025.1.15

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

НАПРЯМИ ПОЛІПШЕННЯ МАЙСТЕРНОСТІ ТА ФАХОВОЇ ПІДГОТОВКИ ФАХІВЦІВ СУБ'ЄКТІВ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ ОБ'ЄКТІВ 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

WAYS OF IMPROVING THE SKILLS AND PROFESSIONAL TRAINING OF SPECIALISTS ENGAGED AT ENTITIES OF THE NATIONAL SYSTEM OF CRITICAL INFRASTRUCTURE PROTECTION IN THE CONTEXT OF ENSURING CYBERSECURITY AND CYBERPROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES

Динамічний розвиток української держави потребує практично щорічної корекції концептуальних підходів до розвитку сфери захисту критичної інфраструктури. Система вищої освіти стає стратегічною сферою формування професійних компетентностей фахівців національної системи захисту критичної інфраструктури відповідно до потреб світового ринку праці. Виникає гостра потреба в адаптації даних питань не тільки на законодавчому, нормативно-правовому, економічному рівні, але і в динамічній перебудові загальної мети та стратегічних напрямів реформування всіх ланок освіти згідно зі світовими стандартами. Українська держава будує власну національну систему захисту критичної інфраструктури та відповідну систему підготовки кадрів для сфери захисту критичної інфраструктури.

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

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

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

У статті автором запропоновано запровадження присвоєння (підтвердження) професійної кваліфікації фахівцям суб'єктів національної системи захисту критичної інфраструктури, які забезпечують кібербезпеку та кіберзахист об'єктів критичної інфраструктури, на базі Кваліфікаційного

центру інформаційних технологій та кібербезпеки Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації Держспецзв'язку, що в умовах воєнного стану може стати потужним важелем до створення, впровадження, розвитку та забезпечення функціонування національної системи захисту критичної інфраструктури.

The dynamic development of the Ukrainian state requires an almost annual adjustment of conceptual approaches to the advance in critical infrastructure protection. The higher education system becomes a strategic area of raising professional competences in specialists of the national critical infrastructure protection system to cater for the global labor market. It is getting highly relevant to adapt these issues not only in legal, regulatory and economic terms, but also in terms of dynamic restructuring of the general goal and strategic directions of reforming all education sectors to be consistent with the world standards. The Ukrainian state is developing its own national system of critical infrastructure protection and the appropriate system to train personnel for the critical infrastructure protection.

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

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

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

training critical infrastructure protection specialists.

In the article, the author proposes to introduce the process of assignment (verification) of professional qualifications for the specialists engaged at entities of the national system of critical infrastructure protection who ensure cybersecurity and cyberprotection of critical infrastructure facilities, based in the Information Technology and Cybersecurity Qualification Center of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection of the State Service of Special Communications and Information Protection of Ukraine, which in the martial law context can become a powerful driver to create, implement, develop and ensure the national system of critical infrastructure protection.

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. Протягом останнього десятиліття економіка України виходить на новий технологічний рівень – інноваційний, що спирається на знання. У центрі нової економіки стоїть людина, її знання, компетенція, спеціалізація, кваліфікація. У той самий час стан конкуренції на ринку вимагає від підприємств, установ, організацій та органів державної влади України швидкого оновлення виробництва, продукції або відповідних послуг, постійного впровадження інновацій у всі сфери діяльності [1, с. 13].

Необхідність гарантованого задоволення потреб суб'єктів національної системи захисту критичної інфраструктури в людських ресурсах під час повномасштабного вторгнення російської федерації в Україну, спрямованість стратегічного курсу України на інтеграцію в європейський та євроатлантичний безпековий простір, забезпечення реалізації стратегічних цілей та завдань

реформування сектору безпеки і оборони, досягнення взаємосумісності суб'єктів національної системи захисту критичної інфраструктури з відповідними підрозділами держав - членів НАТО обумовлюють формування Адміністрацією Держспецзв'язку, яка забезпечує здійснення передбачених Законом України «Про критичну інфраструктуру» [2] повноважень уповноваженого органу у сфері захисту критичної інфраструктури під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування, стратегічного бачення щодо подальшого розвитку системи підготовки кадрів для сфери захисту критичної інфраструктури.

Побудова сфери захисту критичної інфраструктури в Україні є логічним продовженням розбудови держави. Діяльність у зазначеній сфері передбачає сукупність заходів та засобів щодо забезпечення безпеки та стійкості критичної інфраструктури, яка в умовах воєнного стану потребує як захисту, так і покращення. Разом з тим, визначення законодавчих вимог до принципів (пріоритетів, завдань, підходів) щодо захисту критичної інфраструктури, впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, створення системи раннього виявлення загроз критичній інфраструктурі, а також формування системи підготовки кадрів для сфери захисту критичної інфраструктури є основною метою розвитку зазначеної сфери.

Аналіз останніх досліджень і публікацій. Як свідчать дослідження і публікації, проблеми поліпшення майстерності та фахової підготовки фахівців суб'єктів національної системи захисту критичної інфраструктури, у тому числі військовослужбовців та осіб начальницького складу, а також питання їх професійного розвитку та навчання є малодослідженими. У контексті нашого дослідження необхідно виділити публікацію доцента кафедри публічного управління та права комунального закладу вищої освіти «Дніпровська академія неперервної освіти» Дніпропетровської обласної ради» Сергія Якименка та начальника факультету підготовки спеціалістів військової розвідки та сил спеціальних операцій Військової академії (м. Одеса) Юрія Гикала, які

розкриваючи питання удосконалення системи професійної підготовки військовослужбовців в контексті трансформації системи військової освіти доходять до висновку, що система професійної підготовки військовослужбовців потребує постійного удосконалення. Основним завданням удосконалення є забезпечення військовослужбовців необхідними знаннями, вміннями та навичками для ефективного виконання своїх обов'язків у різних умовах. Одним із напрямків удосконалення системи професійної підготовки є трансформація системи військової освіти. Зокрема, перегляд методів навчання та впровадження інновацій в систему освіти [3, с. 62].

Також слід звернути увагу на дослідження науковців кафедри морально-психологічного забезпечення діяльності військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного Берези Р.П., Геруса О.П. та Годованського О.О., які досліджували питання інтерактивного навчання як основу ефективної підготовки сучасного військовослужбовця. Зазначені науковці дійшли до висновку, що активне використання у військовій педагогічній практиці сучасних інтерактивних методів та форм є запорукою підвищення ефективності навчання, виховання та освіти у підготовці військовослужбовця, який, за своїми професійними характеристиками, є здатним протистояти викликам військових дій, що стали реальністю вже на початку XXI століття, зокрема, у неоголошеній російсько-українській війні [4, с. 86].

Крім цього цікавим є дослідження завідувача кафедри мовної підготовки Інституту Військово-Морських Сил Національного університету «Одеська морська академія» Беньковської Н.Б., якою визначено основні компетенції військовослужбовця, а також розглянуто основні чинники, які впливають на його розвиток. Так, науковиця зазначає, що професійна компетентність військовослужбовців обов'язково повинна містити особистісний та соціальний компоненти, що визначаються активністю особистості до спільної діяльності в команді та реалізації поставленої мети, а також формуватися на основі теоретичних знань, практичних умінь, значущих особистісних якостей та

життєвого досвіду, що зумовлює їх готовність до здійснення професійних обов'язків та забезпечення високого рівня самореалізації та конкурентоспроможності [5, с. 106].

Незважаючи на деяку кількість прикладних та фундаментальних робіт, які розкривають деякі аспекти професійного розвитку вищезазначених осіб, питанням удосконалення системи професійної підготовки фахівців національної системи захисту критичної інфраструктури у контексті забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури приділено мало уваги, що й обумовлює актуальність дослідження.

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

Виклад основного матеріалу дослідження. Будь-яка діяльність неможлива без кадрового забезпечення та професійної (або фахової) підготовки особового складу. Це повною мірою стосується і сфери захисту критичної інфраструктури. Підвищена відповідальність за результати своєї діяльності, відсутність готового алгоритму дій для всіх можливих ситуацій, широкий діапазон спеціальних знань та навичок потребують підвищеної уваги до системи підготовки кадрів для сфери захисту критичної інфраструктури.

В умовах повномасштабного вторгнення російської федерації на територію України військовослужбовцям, особам начальницького складу та іншим фахівцям суб'єктів національної системи захисту критичної інфраструктури, у тому числі співробітникам Держспецзв'язку, доводиться виконувати свої службові обов'язки з подвоєною енергією, що в свою чергу вимагає від них високої відповідальності, напруженості, майстерності та фахової підготовки. У зв'язку з цим актуалізується питання про структуру та побудову професіоналізму кожного фахівця, критерії та показники його сформованості. Такі знання є цінною підмогою для керівників усіх рівнів щодо ефективної та дієвої побудови управлінського процесу формування досвіду та відповідної здатності у зазначених осіб в умовах воєнного стану.

Майстерність та фахова підготовка фахівців суб'єктів національної системи захисту критичної інфраструктури, у тому числі військовослужбовців та осіб начальницького складу, які опікуються питаннями забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури, складається з:

– професійних знань, умінь та навичок, а також ступеня їх реалізації та впровадження у військовій (службовій, трудовій) діяльності;

– досягнення високих, стабільних та ефективних результатів у своїй діяльності;

– професійної самостійності, мислення та інтуїції у вирішенні завдань військової (службової, трудової) діяльності;

– оптимального професійно-психологічного стану, відсутності перевантаження і втоми при виконанні службово-бойових завдань;

– ступеня усвідомлення значущості своєї професії, розуміння свого призначення (місії), оцінки обрання діяльності по захисту Вітчизни, її територіальної цілісності та недоторканості;

– володіння декількома видами військово-професійної діяльності (спеціальностями) в рамках професії.

Зміст понять «майстерність» та «фахова підготовка» не є «застиглим» утворенням. Про майстерність та фахову підготовку фахівців суб'єктів національної системи захисту критичної інфраструктури можна говорити тільки тоді, коли постійно зростає ефективність професійної діяльності, коли розширюється та поповнюється діапазон завдань, що виконуються, а система знань (умінь, навичок) постійно збагачується та помножується. Розвиток даних понять може здійснюватися різним чином, у тому числі шляхом підготовки, здобуття ступеня вищої освіти за іншою спеціальністю, підвищення кваліфікації, професійного навчання (бойової підготовки), самоосвіти, а також за результатами складання відповідних іспитів при присвоєнні (підтвердженні) класної (професійної) кваліфікації.

Основними функціями майстерності та фахової підготовки фахівців, які опікуються питаннями забезпечення кібербезпеки та кіберзахисту об'єктів

критичної інфраструктури, є: нормативна, результативна, ціннісно-смислова, комунікативна, а також перетворювальна. Так, нормативна і результативна функції дозволяють розкрити діяльнісний компонент – володіння військово-професійною діяльністю на високому рівні, а також здатність впроваджувати свій професійний розвиток. В свою чергу, за допомогою ціннісно-смислової, комунікативної та перетворювальної функцій можна виявити особистісний компонент, який є системоутворюючим для всіх компонентів майстерності та фахової підготовки військовослужбовця (особи начальницького складу, працівника), та який розкривається в особистісному розвитку суб'єкта до рівня професіонала при наявності продуктивної «Я-концепції», основу якої складають уявлення про самого себе.

Крім функцій майстерності та фахової підготовки фахівців, які опікуються питаннями забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури, необхідно виділити також їх критерії, які є результатом проведеного аналізу наукової літератури та керівних документів. Так, такими критеріями є військово-професійна (службово-професійна) діяльність, щоденні відносини, особистісно-професійний розвиток, оптимізація служби (праці), а також загальні її результати. Виділені критерії свідчать, що майстерність та фахову підготовку вищезазначених фахівців необхідно розглядати як системну якість суб'єкта, що відображає його можливості реалізувати задані нормативи діяльності, а також як системну якість діяльності, що характеризує рівень продуктивності та успішності.

Деякі аспекти удосконалення майстерності та фахової підготовки фахівців із забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури висвітлено також в нормативно-правових актах. Так, відповідно до Переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 19 червня 2019 року № 518 [6], під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають

фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки.

Необхідно також акцентувати увагу на заходах з реалізації Концепції забезпечення національної системи стійкості до 2025 року, затвердженої розпорядженням Кабінету Міністрів України від 10 листопада 2023 року № 1025-р [7], які розкривають питання щодо ідентифікації загроз, виявлення вразливостей, оцінювання та пріоритезації ризиків національній безпеці, запобігання виникненню кризових ситуацій, реагування на загрози і кризові ситуації, а також подолання наслідків виникнення загроз або настання кризових ситуацій. Так, відповідно до затвердженого Урядом плану, в рамках проведення аналізу загроз та ризиків для найбільш важливих сфер життєдіяльності суспільства і держави Адміністрації Держспецзв'язку та Міносвіти доручено забезпечити науково-методичне супроводження фахівців, відповідальних за забезпечення кіберзахисту об'єктів кібербезпеки та кіберзахисту, зокрема об'єктів критичної інфраструктури. Разом з тим, на секторальні органи у сфері захисту критичної інфраструктури, Адміністрацію Держспецзв'язку, Мінекономіки, Міносвіти, Нацдержслужбу, Національне агентство кваліфікацій та функціональні органи у сфері захисту критичної інфраструктури покладено завдання щодо забезпечення розроблення переліку посад та кваліфікаційних характеристик для фахівців, відповідальних за забезпечення захисту об'єктів критичної інфраструктури. Крім цього, Міносвіти, Адміністрація Держспецзв'язку, Нацдержслужба, секторальні та функціональні органи у сфері захисту критичної інфраструктури є відповідальними за започаткування підготовки фахівців, відповідальних за забезпечення захисту об'єктів критичної інфраструктури.

Питання забезпечення кіберзахисту об'єктів критичної інфраструктури акцентовано також у заходах на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України, затверджених розпорядженням Кабінету Міністрів України від 19 грудня 2023 року № 1163-р [8], які передбачають залучення суб'єктів національної системи кібербезпеки до міжнародних програм навчання

і підвищення кваліфікації персоналу. Так, МЗС України, Апарат РНБО України, Адміністрація Держспецзв'язку, Мінфін, Мінекономіки, Нацполіція, СБУ, Міноборони, Генштаб ЗС України, СЗР, Адміністрація Держприкордонслужби та Нацбанк є відповідальними за забезпечення участі представників основних суб'єктів національної системи кібербезпеки та об'єктів критичної інфраструктури у навчаннях та підвищенні кваліфікації за міжнародними програмами.

Положення даних актів ще раз підкреслюють той факт, що система підготовки кадрів для сфери захисту критичної інфраструктури на сьогодні перебуває у стадії становлення, потребує організації та проведення різноманітних освітніх заходів, розроблення відповідних навчальних програм та методик, а також проведення регулярних навчань щодо попередження і реагування на загрози критичній інфраструктурі.

Розвиток системи підготовки фахівців у сфері захисту критичної інфраструктури та їх професійна сертифікація у галузі безпеки інформації, кібербезпеки та кіберзахисту є актуальним завданням для посилення кіберстійкості України. В умовах повномасштабного вторгнення російської федерації на територію України наша держава фактично стала майданчиком російських кібероперацій та на сьогодні набула значного досвіду щодо протидії ворожим атакам у кіберпросторі. Зазначене призводить до дефіциту кваліфікованих кадрів у сфері кібербезпеки та кіберзахисту. Таким чином одним із шляхів розв'язання цієї проблеми є необхідність створення системи професійної підготовки та сертифікації кадрів у сфері захисту критичної інфраструктури, яка б надала змогу враховувати вимоги ринку праці до компетентностей працівників, гармонізувати чинне законодавство сфери вищої освіти й соціально-трудових відносин, сприяти національному та міжнародному визнанню кваліфікацій, здобутих в Україні, а також налагоджувати ефективну взаємодію всіх напрямів розвитку суспільства у сфері захисту критичної інфраструктури.

Освітнє навчання стосується будь-яких систематичних дій, що здійснюються людьми, які завершили початковий цикл безперервної освіти, для покращення своїх знань, навичок та оцінок, а також розвитку відносин з іншими людьми для адекватного виконання професійних завдань [9, с. 525].

Процес професійної підготовки фахівців національної системи захисту критичної інфраструктури має свої особливості. Він проводиться в умовах постійної службової готовності та характеризується різко вираженою практичною направленістю. Підготовка проходить в умовах розумового та інтелектуального напруження, а процес навчання знаходиться в безпосередній залежності від технічних можливостей суб'єкта національної системи захисту критичної інфраструктури.

Враховуючи зазначене, з метою професіоналізації особового складу складових сил оборони, у тому числі військовослужбовців та осіб начальницького складу, які забезпечують кібербезпеку та кіберзахист об'єктів критичної інфраструктури, інтеграції діючих стандартів освіти, професійних стандартів, нормативно-правової бази для забезпечення сил оборони військовими фахівцями, надання широкого спектру професійних знань та розвитку креативного мислення упродовж військової (службової, трудової) кар'єри, необхідним є введення відповідного механізму, що можна зробити шляхом розробки та запровадження порядку присвоєння (підтвердження) професійної кваліфікації фахівцям суб'єктів національної системи захисту критичної інфраструктури (рис. 1).

Розроблений механізм розвитку та зростання власної професійної підготовки, який покладено в основу порядку присвоєння (підтвердження) професійної кваліфікації фахівцям суб'єктів національної системи захисту критичної інфраструктури, які забезпечують кібербезпеку та кіберзахист об'єктів критичної інфраструктури, забезпечує потребу у кваліфікованому персоналі суб'єктів національної системи захисту критичної інфраструктури та найбільш ефективно використовує його потенціал шляхом побудови службової (військової) кар'єри.

Рис. 1. Порядок присвоєння (підтвердження) професійної кваліфікації фахівцям суб' єктів національної системи захисту критичної інфраструктури з питань кібербезпеки та кіберзахисту об' єктів критичної інфраструктури

Джерело: розробка автора

Запропонований порядок передбачає поетапне присвоєння (підтвердження) професійної кваліфікації фахівцям суб'єктів національної системи захисту критичної інфраструктури (спеціалістам Адміністрації Держспецзв'язку (уповноваженого органу у сфері захисту критичної інфраструктури України), Збройних Сил України, інших військових формувань, СБ України, правоохоронних та розвідувальних органів, ДСНС України, секторальних та функціональних органів, операторів критичної інфраструктури суб'єктів національної системи захисту критичної інфраструктури, підприємств (установ, організацій) які провадять діяльність із забезпеченням безпеки та стійкості критичної інфраструктури), які забезпечують кібербезпеку та кіберзахист об'єктів критичної інфраструктури, на базі Кваліфікаційного центру інформаційних технологій та кібербезпеки Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації Держспецзв'язку.

Кваліфікаційний центр інформаційних технологій та кібербезпеки – суб'єкт, уповноважений Національним агентством кваліфікацій здійснювати:

– оцінювання і визнання, у відповідності до професійних стандартів у сфері інформаційної безпеки та кібербезпеки Національної рамки класифікації, результатів навчання, здобутих особами шляхом формальної, неформальної або інформальної освіти;

– присвоєння та/або підтвердження відповідних професійних кваліфікацій;

– визнання відповідних професійних кваліфікацій, здобутих у інших країнах на підставі сертифікату про акредитування такого кваліфікаційного центру.

Основними завданнями Кваліфікаційного центру інформаційних технологій та кібербезпеки є:

– оцінювання та визнання результатів навчання, присвоєння та/або підтвердження професійних кваліфікацій за процедурами, які дають змогу оцінити результати навчання, здобуті шляхом формальної, неформальної та

інформальної освіти, з видачою особі документів про присвоєння та/або підтвердження відповідних професійних кваліфікацій;

– визнання професійних кваліфікацій, здобутих у інших країнах, з видачою особі відповідних документів.

Професійна кваліфікація (повна професійна кваліфікація) – це визнана або присвоєна/підтверджена суб'єктом, уповноваженим на це законодавством, та засвідчена відповідним документом стандартизована сукупність здобутих особою компетентностей та/або результатів навчання, що дає змогу здійснювати всі трудові функції, визначені відповідним професійним стандартом [10].

Для успішного проходження процедури оцінювання здобувач професійної кваліфікації має здобути компетентності, знання, вміння та навички відповідної професійної кваліфікації. При цьому здобувач повинен бути обізнаним та освіченим фахівцем з питань кібербезпеки та кіберзахисту об'єктів критичної інфраструктури. Так, такі професійні кваліфікації як «Розробник систем захисту інформації», «Провідний розробник систем захисту інформації» передбачають здатність:

– аналізувати проєктні обмеження, компроміси та детальний проєкт системи захисту критичної інфраструктури, а також розглядати підтримку її життєвого циклу;

– проєктувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки об'єктів критичної інфраструктури;

– розробляти вимоги до безпеки об'єкта критичної інфраструктури та її врахування в усіх системах захисту інформації або прикладних програмах;

– розробляти стратегії зменшення ризиків для усунення вразливостей із урахуванням рекомендацій щодо зміни заходів безпеки у системі захисту критичної інфраструктури або системних компонентах;

– забезпечувати діяльність із проєктування та розвитку кібербезпеки належним (у тому числі задокументованим) чином;

– оцінювати системи кібербезпеки або продукти, що сприяють кібербезпеці;

– здійснювати заходи щодо тестування та оцінки систем безпеки об’єктів критичної інфраструктури та сертифікації;

– впроваджувати проєкти системи безпеки об’єктів критичної інфраструктури для нових або наявних систем захисту інформації;

– здійснювати технічне керівництво профільними розробниками систем захисту інформації;

– взаємодіяти з представниками секторальних та функціональних органів суб’єктів національної системи захисту критичної інфраструктури, операторів критичної інфраструктури та підприємств (установ, організацій), які провадять діяльність із забезпеченням безпеки та стійкості критичної інфраструктури, щодо технологічних питань відповідного спрямування;

– взаємодіяти із зовнішніми партнерами в межах визначених повноважень.

Разом з тим, для присвоєння (або підтвердження) таких професійних кваліфікацій як «Аудитор систем менеджменту інформаційної безпеки» та «Провідний аудитор систем менеджменту інформаційної безпеки» здобувачу необхідно вміти:

– планувати здійснювати та документувати проведення внутрішнього аудиту інформаційних систем і технологій об’єктів критичної інфраструктури, визначати для цього ефективні методи та процедури;

– визначати, аналізувати та оцінювати ризики, пов’язані з інформаційними системами та технологіями, здійснювати прогнозування потенційних загроз та виявляти вразливості системи безпеки об’єктів критичної інфраструктури;

– розробляти та впроваджувати стратегічні плани для функціонування та розвитку інформаційної інфраструктури секторальних та функціональних органів суб’єктів національної системи захисту критичної інфраструктури, операторів критичної інфраструктури та підприємств (установ, організацій), які

провадять діяльність із забезпеченням безпеки та стійкості критичної інфраструктури;

– визначати методи та процедури для здійснення заходів контролю та оцінки ефективності функціонування інформаційних систем, незалежних оглядів та планових аудитів;

– використовувати аналітичні методи та інструменти для оцінки ефективності інформаційних систем, виявлення слабких місць і потенційних загроз безпеці об’єктам критичної інфраструктури, а також для розробки стратегій поліпшення інформаційної безпеки.

В свою чергу, фахівець, що претендує на присвоєння (або підтвердження) професійної кваліфікації «Керівник команди з аудиту систем менеджменту інформаційної безпеки», зобов’язаний знати:

– концепції і протоколи комп’ютерних мереж, а також методології забезпечення мережевої безпеки об’єктів критичної інфраструктури;

– закони, нормативно-правові та організаційно-розпорядчі акти, політики і етичні норми, та як вони пов’язані з кібербезпекою і приватністю системи захисту критичної інфраструктури;

– принципи кібербезпеки і приватності суб’єктів національної системи захисту критичної інфраструктури;

– класифікацію кіберзагроз та вразливостей об’єктів критичної інфраструктури;

– механізми контролю доступу до хостів/мереж (списки контролю доступу, списки повноважень тощо).

Крім цього, при підготовці до присвоєння (або підтвердження) таких професійних кваліфікацій як «Фахівець з планування політики та стратегії кібербезпеки» та «Провідний фахівець з планування політики та стратегії кібербезпеки» відповідний спеціаліст повинен орієнтуватися у питаннях забезпечення:

– інформаційної та/або кібербезпеки, а також захисту персональних даних;

– порядку адаптивного планування, а також планування в кризових умовах та з урахуванням обмеження часу;

– аналізу кризових ситуацій з метою забезпечення суспільної та персональної безпеки, захисту кіберресурсів, стійкості та надійності об’єктів критичної інфраструктури;

– вимог (рекомендацій) кращих міжнародних практик (NIST, ISO, ENISA, BSI, MITRE ATT&CK тощо), законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки;

– управління ризиками (методами оцінювання та оброблення ризиків), а також сучасними і перспективними кібертехнологіями.

Необхідно також відмітити, що фахівці Адміністрації Держспецзв’язку (уповноваженого органу у сфері захисту критичної інфраструктури України), ЗС України, інших військових формувань, СБ України, правоохоронних та розвідувальних органів, ДСНС України, секторальних та функціональних органів, операторів критичної інфраструктури суб’єктів національної системи захисту критичної інфраструктури та підприємств (установ, організацій) які провадять діяльність із забезпеченням безпеки та стійкості критичної інфраструктури, при проходженні процедури оцінювання повинні вміти:

– для професійних кваліфікацій «Аудитор інформаційних технологій (з кібербезпеки)» та «Провідний аудитор інформаційних технологій (з кібербезпеки)»: визначати необхідний рівень складності тесту для конкретної системи; проводити аудити або огляди технічних систем; розробляти звітні документи за результатами аудиту інформаційних систем; розробляти план тестування системи безпеки (наприклад, окремого компонента, процесу інтеграції, системи, процесу приймання системи); проводити сканування вразливостей і розпізнавання вразливостей в системах безпеки; розпізнавати та класифікувати різні типи вразливостей і пов’язаних з ними атак; використовувати інструменти мережевого аналізу для визначення вразливостей (наприклад, fuzzing, nmap, тощо);

– для професійних кваліфікацій «Аналітик загроз безпеки» та «Провідний аналітик загроз безпеки»: визначати та характеризувати всі відповідні аспекти операційного середовища; використовувати кілька пошукових систем та інструментів для проведення пошуку з відкритим кодом; проводити дослідження з використанням Web-сайтів/сторінок, що не індексуються пошуковими системами; збирати точні та повні дані з джерел, які використовуються для розвідки, оцінювання та/або планування; виявляти, відстежувати й оцінювати тактики, методи та процедури, які використовуються суб'єктами кіберзагроз, шляхом аналізу даних, інформації та кібердослідних даних із відкритих і власних джерел; визначати критичні цільові елементи, щоб включити критичні цільові елементи для кібердомену;

– для професійних кваліфікацій «Молодший фахівець з реагування на інциденти кібербезпеки», «Фахівець з реагування на інциденти кібербезпеки» та «Провідний фахівець з реагування на інциденти кібербезпеки»: розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак; виявляти вторгнення на хост і мережу за допомогою технологій виявлення вторгнень; виявляти вразливості в захищених системах (наприклад, сканування вразливостей і перевірка відповідності); проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки; проводити сканування вразливостей і розпізнавати вразливості в системах безпеки; зберігати цілісність доказів відповідно до стандартних оперативних процедур або національних стандартів; застосовувати методики виявлення вторгнень з боку хоста та мережі за допомогою технологій виявлення вторгнень;

– для професійних кваліфікацій «Конструктор систем кібербезпеки» та «Провідний конструктор систем кібербезпеки»: визначати та пріоритезувати суттєві спроможності систем або бізнес-функцій, необхідних для часткового або повного відновлення системи після її повної відмови; перекладати функціональні вимоги в потреби захисту (тобто, контролі безпеки); застосовувати принципи кібербезпеки і приватності при формуванні вимог об'єкта критичної інфраструктури (стосовно конфіденційності, цілісності,

доступності, автентифікації і неспростовності); проєктувати інтеграції апаратних і програмних рішень; застосовувати методи проєктування; документувати та приводити у відповідність інформаційну безпеку об’єкта критичної інфраструктури, архітектуру кібербезпеки та вимоги техніки безпеки системи протягом всього життєвого циклу закупівлі; застосовувати інструменти, методи і техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем; застосовувати процеси планування захисту програм; застосовувати загальні мережеві протоколи та протоколи маршрутизації (наприклад, TCP/IP), послуги (наприклад, веб-пошти, DNS) та їх взаємодії для забезпечення мережевих зв’язків;

– для професійних кваліфікацій «Фахівець із кібердосліджень та розробок систем безпеки», «Провідний фахівець із кібердосліджень та розробок систем безпеки» та «Професіонал з кібердосліджень та розробок систем безпеки»: досліджувати і оцінювати наявні технології і стандарти з метою задоволення вимог суб’єктів національної системи захисту критичної інфраструктури; оцінювати ефективність застосованих вимог чинних законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки; оцінювати необхідність проведення інжинірингу програмного забезпечення та систем забезпечення кібербезпеки на конкретному об’єкті; враховувати у дослідницькій та проєктній діяльності виявлені вразливості мережевої інфраструктури; використовувати інструменти мережевого аналізу для визначення вразливостей систем; ідентифікувати вразливості мережевої інфраструктури та програмного забезпечення у сфері кібербезпеки; розроблювати стратегії оцінювання та обробки ризиків; проводити аналіз ризиків, коли прикладна програма або система зазнають суттєвих змін; здійснювати огляди безпеки та виявляти пробіли в архітектурі безпеки;

– для професійних кваліфікацій «Фахівець з оцінки заходів захисту інформації (з кібербезпеки)» та «Провідний фахівець з оцінки заходів захисту інформації (з кібербезпеки)»: застосовувати принципи, моделі, методи і засоби управління мережевими системами (наприклад, наскрізний моніторинг

пропускної здатності системи); організовувати процеси планування, включаючи підготовку функціональних і спеціальних планів підтримки, підготовки і забезпечення технічного листування; визначати аномалії в цільової мережі (наприклад, вторгнення, потік даних або їх обробки, цільове впровадження нових технологій); використовувати віртуальні машини (наприклад, Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, тощо); виявляти проблеми кібербезпеки і приватності, які виникають при з'єднаннях внутрішніх та зовнішніх замовників та організацій-партнерів; визначати вимоги до інфраструктури тестування і оцінювання (співробітники, полігони, засоби, прилади); використовувати шифрування інфраструктури відкритих ключів (PKI) та можливостей цифрового підпису в програмних додатках (наприклад, електронна пошта S/MIME, SSL-трафік).

У свою чергу спеціалісти секторальних та функціональних органів, а також операторів критичної інфраструктури суб'єктів національної системи захисту критичної інфраструктури, при проходженні процедури оцінювання повинні мати такі навички:

– для професійних кваліфікацій «Молодший фахівець з підтримки інфраструктури кіберзахисту», «Фахівець з підтримки інфраструктури кіберзахисту» та «Провідний фахівець з підтримки інфраструктури кіберзахисту»: здійснювати налаштування датчиків; здійснювати встановлення та налаштування інструментів та прикладного програмного забезпечення системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS); здійснювати встановлення та налаштування SIEM-системи; здійснювати встановлення та налаштування антивірусного програмного забезпечення; здійснювати встановлення та налаштування міжмережевого екрану; виконувати захист мережевих комунікацій; характеризувати та аналізувати мережевий трафік з метою виявлення аномальної активності та потенційних загроз мережевим ресурсам; перехоплювати та аналізувати мережевий трафік, пов'язаний з шкідливими діями, використовуючи засоби моніторингу мережі;

здійснювати підтримку баз даних (резервне копіювання, відновлення, видалення даних, файлів лог-журналу, тощо); здійснювати адміністрування операційної системи (ведення облікових записів, резервне копіювання та відновлення даних файлів лог-журналу тощо); здійснювати захист мережі від шкідливого програмного забезпечення (наприклад, NIPS/HIPS, обмеження/запобігання впливу зовнішніх пристроїв, фільтрацію спаму); застосовувати концепції архітектури безпеки мереж, включаючи топологію, протоколи, компоненти і принципи (наприклад, застосунки з «ешелонованим захистом); оцінювати засоби контролю безпеки на основі принципів і доктрин кібербезпеки (наприклад, стандарти «CIS CSC», NIST SP 800-53, керівні принципи кібербезпеки тощо);

– для професійних кваліфікацій «Фахівець сфери захисту інформації» та «Провідний фахівець сфери захисту інформації»: визначати (формулювати) потреби щодо захисту інформації, що обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників); визначати (формулювати) потреби щодо захисту інформації, що озвучується на об’єктах інформаційної діяльності підприємства (організації); визначати (формулювати) потреби до кібербезпеки в електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників); визначати та аналізувати вимоги щодо захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності підприємства (організації); здійснювати попередню оцінку достатності потреб і вимог користувачів (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту; застосовувати політики безпеки для досягнення цілей безпеки системи; аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки; використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації;

– для професійних кваліфікацій «Молодший адміністратор безпеки мереж і систем», «Адміністратор безпеки мереж і систем» та «Провідний адміністратор безпеки мереж і систем»: користуватися загальнодоступними мережевими інструментами (ping, traceroute, nslookup); діагностувати несправні системні компоненти (сервери); встановлювати оновлення системи та компонентів (серверів, пристроїв, мережевих пристроїв); застосовувати принципи кібербезпеки та приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації та неспростовності); налаштовувати та використовувати програмні засоби захисту комп'ютерів (програмні фільтри, антивірусна програма й антишпигунське програмне забезпечення); проводити планування, управління та обслуговування систем/серверів; застосовувати принципи кібербезпеки та приватності при формуванні організаційних вимог (що стосуються конфіденційності, цілісності, доступності, автентифікації та неспростовності).

Таким чином порядок присвоєння (підтвердження) професійної кваліфікації фахівцям суб'єктів національної системи захисту критичної інфраструктури орієнтований на визначення індивідуально-професійного розвитку кожного фахівця сфери захисту критичної інфраструктури. При цьому досягнення таких фахівців поєднують їхні характеристики, що відображають об'єктивні та неупереджені результати пізнавальної діяльності – навички, досвід, знання, уміння, предметні компетентності тощо. Звісно, впровадження зазначеного порядку присвоєння (підтвердження) професійної кваліфікації можливе тільки після ефективних нормативно-правових змін у відповідних актах.

Необхідно також відмітити, що для участі у присвоєнні (підтвердженні) професійної кваліфікації фахівець суб'єктів національної системи захисту критичної інфраструктури визначає для себе правила і стиль поведінки, які є допоміжними в його професійному розвитку. До зазначених правил і стилів належать: постійне підвищення свого фахового та професійного рівня; вміння розставляти пріоритети і розраховувати час; розуміння особистих сильних і

слабких сторін; відповідальність за доручену справу; відстоювання власних поглядів; сприйняття конструктивної критики та формування вірних висновків.

Крім цього, присвоєння (підтвердження) професійної кваліфікації фахівцям суб'єктів національної системи захисту критичної інфраструктури у контексті забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури, дасть змогу:

– спеціалістам Адміністрації Держспецзв'язку (уповноваженого органу у сфері захисту критичної інфраструктури України), ЗС України, інших військових формувань, СБ України, правоохоронних та розвідувальних органів, ДСНС України – оволодіти аналітичним мисленням і системністю, комунікативними вміннями, навичками ефективно-міжособистісної взаємодії, умінням прогнозувати розвиток тієї чи іншої ситуації, мислити у масштабному та реалістичному форматі;

– фахівцям підприємств (установ, організацій) які провадять діяльність із забезпеченням безпеки та стійкості критичної інфраструктури – опанувати здатність до уміння розв'язувати нестандартно-професійні проблеми, виконувати складні і відповідальні завдання, приймати самостійні рішення, прагнути до постійного підвищення власного професіоналізму, реалістично сприймати свої здібності і можливості;

– керівникам секторальних та функціональних органів суб'єктів національної системи захисту критичної інфраструктури, а також операторам критичної інфраструктури – розвивати особисті цілі та інтереси, індивідуальні потреби, цінності й мотиви, розширювати особистісно-орієнтовану спрямованість, формувати необхідні якості лідера та професіонала, формувати службово-професійні компетентності у підлеглого особового складу.

Впровадження у службову діяльність порядку присвоєння (підтвердження) професійної кваліфікації фахівцям суб'єктів національної системи захисту критичної інфраструктури забезпечить: якість та безперервність набуття відповідного досвіду; розвиток професійної компетентності; відповідні умови для конкуренції серед співробітників

національної системи захисту критичної інфраструктури; сучасну єдину та гнучку систему професійного розвитку; належні умови для реалізації права на професійне зростання.

Висновки та перспективи подальших розвідок у даному напрямі. Фахові дослідження підкреслюють, що в сучасному світі підготовка кадрів у сфері захисту критичної інфраструктури не може обмежуватися лише отриманням вищої освіти за певною спеціальністю. Для збереження відповідної конкурентоспроможності військовослужбовцям, особам начальницького складу та іншим фахівцям необхідно постійно підвищувати власну кваліфікацію на засадах «освіти протягом життя», різноманітність та множинність форм і методів якої відкриває перспективний напрям для професійного розвитку. Саме тому будь-який секторальний та функціональний орган суб'єкту національної системи захисту критичної інфраструктури, а також оператор критичної інфраструктури повинний сприяти розвитку своїх працівників.

Завдяки своїй новизні дане дослідження має перспективу подальшої інтеграції його результатів у розвиток української професійної освіти з підготовки кадрів для сфери захисту критичної інфраструктури та продовження на шляху формування та реалізації державної політики у сфері захисту критичної інфраструктури України.

Література

1. Арсенович Л. А. Впровадження професійного стандарту «Фахівець із кібербезпеки» як інструменту подальшого розвитку системи підготовки кадрів у сфері кібербезпеки. *Sciences of Europe (Praha, Czech Republic).* 2021. № 83. С. 12–23.

2. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 11.01.2025. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 11.01.2025).

3. Якименко С. Удосконалення системи професійної підготовки військовослужбовців в контексті трансформації системи військової освіти. *Вісник Дніпровської академії неперервної освіти. Серія : Публічне управління та адміністрування.* 2023. № 2. С. 60–63.

4. Береза Р. П. Інтерактивне навчання як основа ефективної підготовки сучасного військовослужбовця. *Інноваційна педагогіка*. 2022. № 52(1). С. 81–86.

5. Беньковська Н. Б. Ретроспективний аналіз поняття "професійна компетентність військовослужбовців Збройних сил України". *Педагогічні науки: теорія та практика*. 2022. № 1. С. 100–107.

6. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 р. № 518. Дата оновлення: 11.01.2025. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 11.01.2025).

7. 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: 11.01.2025. URL: https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text (дата звернення: 11.01.2025).

8. Про затвердження плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 19.12.2023 р. № 1163-р. Дата оновлення: 11.01.2025. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (дата звернення: 11.01.2025).

9. Leonid Arsenovych, Oleksandr Nikolaievsky, Olena Skliarenko, Leonid Lytvynenko, Ivan Kydriavskyi. Organization of Training with the Use of Digital Technologies for Ensuring Cybersecurity in the Educational Space. *WSEAS Transactions on Computer Research*. 2024. № 12. pp. 524-536.

10. Про внесення змін до деяких законодавчих актів України щодо функціонування національної системи кваліфікацій : Закон України від 01.04.2022 р. № 2179-IX. Дата оновлення: 11.01.2025. URL: https://zakon.rada.gov.ua/laws/show/2179-20#top (дата звернення: 11.01.2025).

References

1. Arsenovych, L.A. (2021), “Implementation of the professional standard "Cybersecurity Specialist" as a tool for the further development of the system of personnel training in the field of cyber security”, *Sciences of Europe (Praha, Czech Republic)*, vol. 83, pp. 12–23.

2. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine “On critical infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Accessed 11.01.2025).

3. Yakymenko, S. (2023), “Improving the system of professional training of military personnel in the context of the transformation of the military education system”, *Visnyk Dniprovskoi akademii neperervnoi osvity. Seriia : Publichne upravlinnia ta administruvannia,* vol. 2, pp. 60–63.

4. Bereza, R.P. (2022), “Interactive training as a basis for effective training of a modern military serviceman”, *Innovatsiina pedahohika,* vol. 52(1), pp. 81–86.

5. Benkovska, N.B. (2022), “Retrospective analysis of the concept of "professional competence of servicemen of the Armed Forces of Ukraine”, *Pedahohichni nauky: teoriia ta praktyka,* vol. 1, pp. 100–107.

6. Cabinet of Ministers of Ukraine (2019), Resolution “On the approval of General requirements for cyber protection of critical infrastructure objects”, available at: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (Accessed 11.01.2025).

7. 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 11.01.2025).

8. Cabinet of Ministers of Ukraine (2023), Order “On the approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (Accessed 11.01.2025).

9. Arsenovych, L. Nikolaievsky, O. Skliarenko, O. Lytvynenko, L. Kydriavskyi, I. (2024), “Organization of Training with the Use of Digital Technologies for Ensuring Cybersecurity in the Educational Space”, *WSEAS Transactions on Computer Research,* vol. 12, pp. 524–536.

10. The Verkhovna Rada of Ukraine (2022), The Law of Ukraine “On making changes to some legislative acts of Ukraine regarding the functioning of the national system of qualifications”, available at: https://zakon.rada.gov.ua/laws/show/2179-20#Text (Accessed 11.01.2025).

Стаття надійшла до редакції 14.01.2025 р.