

---

## CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

---

DOI 10.20535/2411-1031.2024.12.1.306276

УДК 004.056.5:614.876.4

БОГДАН НИКОЛАЄНКО,  
АНДРІЙ МІСЮРА,  
АНТОН СТОРЧАК,  
ПАВЛО ДІМІТРОВ

### ПІДГОТОВКА ФАХІВЦІВ ЯК ОДИН З АСПЕКТІВ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Одним із напрямів державної політики у сфері забезпечення національної безпеки є розбудова багаторівневої ефективної національної системи забезпечення безпеки та стійкості критичної інфраструктури. Ключовим фактором будь-якої системи, як у сфері забезпечення національної безпеки, так і в інших сферах, є людський капітал, його здатність аналізувати ризики та загрози, визначати вразливості, опановувати новітні технології, знаходити нестандартні креативні рішення для протистояння сучасним викликам. Таким чином, важливим аспектом стає підготовка кваліфікованих фахівців, які володіють системними знаннями та навичками.

Встановлено необхідність надання системних знань фахівцям та керівникам, які безпосередньо вирішують завдання забезпечення захисту та стійкості об'єктів критичної інфраструктури. Визначено поточний стан системи підготовки фахівців у сфері захисту критичної інфраструктури України та проаналізовано основні форми організації навчання та підготовки персоналу у цій сфері. Встановлено завдання на основі аналізу наявних професій та попиту на ринку праці визначити набір професій, які доцільно залучати до виконання завдань із забезпечення безпеки та стійкості критичної інфраструктури. Аналіз підготовки та підвищення кваліфікації фахівців у сфері захисту та стійкості критичної інфраструктури показав необхідність і можливість створення національної системи освіти і навчання з питань захисту та стійкості критичної інфраструктури в Україні.

Проаналізовано наявні професії та попит на ринку праці. Визначено набір професій, які доцільно залучати до виконання завдань із забезпечення безпеки та стійкості критичної інфраструктури. Такими професіями, після їх остаточного затвердження, можуть стати: керівник структурного підрозділу з питань захисту та стійкості критичної інфраструктури та фахівець із захисту та стійкості критичної інфраструктури. Розроблені або оновлені професійні стандарти у сфері захисту та стійкості критичної інфраструктури стануть основою для адаптації освітніх програм закладів вищої освіти відповідно до попиту ринку праці.

**Ключові слова:** безпека, стійкість, критична інфраструктура, класифікатор професій, національна безпека.

**Постановка проблеми.** На даний час в Україні тривають активні процеси зі створення національної системи стійкості. Стратегією національної безпеки України, затвердженою Указом Президента України від 14 вересня 2020 року № 392 [1], запровадження такої системи віднесено до основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки. Багаторівнева комплексна національна система стійкості має сприяти формуванню відповідних спроможностей для забезпечення здатності держави і суспільства своєчасно ідентифікувати загрози, виявляти

вразливості та оцінювати ризики національній безпеці, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу, але не обмежуючись ними.

Мета, основні принципи, напрями, механізми і строки запровадження та функціонування національної системи стійкості визначені Концепцією забезпечення національної системи стійкості, затвердженою Указом Президента України від 27 вересня 2021 року № 479 [2]. Відповідно до положень вказаної Концепції, впроваджувана система має передбачати забезпечення функціонування таких базових елементів:

- 1) гарантована дієвість та спроможність до повноцінного функціонування системи державних органів, їх інституційна стійкість;
- 2) безпека та захищеність об'єктів критичної інфраструктури, зокрема:
  - стійке постачання продовольства, водопостачання, енергопостачання, постачання теплової енергії;
  - стійке функціонування транспортних систем;
  - кібербезпека;
  - захищеність та безперебійне функціонування інформаційних та комунікаційних послуг;
  - забезпечення оборони та правопорядку;
  - здатність системи охорони здоров'я функціонувати в умовах посиленних навантажень;
- 3) спроможність єдиної державної системи цивільного захисту до дій в умовах загрози чи виникнення надзвичайних ситуацій;
- 4) здатність ефективно реагувати на неконтрольоване масове переміщення людей;
- 5) суспільна стійкість, зокрема, до інформаційних впливів;
- 6) фінансово-економічна стійкість, зокрема, безперервність основних бізнес-процесів.

Отже, безпека та захищеність об'єктів критичної інфраструктури є складовою частиною забезпечення національної безпеки України, що закріплено статтею 4 Закону України «Про критичну інфраструктуру» (далі – Закон) [3].

Слід зазначити, що ефективність виконання поставленого завдання безпосередньо залежить від рівня знань, умінь, навичок та компетенцій представників суб'єктів національної системи захисту критичної інфраструктури, які безпосередньо виконують функції у даній сфері. Відповідно, зростає потреба у створенні системи підготовки та навчання керівників та персоналу, задіяних у плануванні та виконанні заходів, спрямованих на забезпечення безпеки та стійкості об'єктів критичної інфраструктури.

Набутий практичний досвід застосування нормативно-правових актів, існуючих методичних розробок та напрацювань у сфері захисту та стійкості критичної інфраструктури свідчить про необхідність запровадження цілісної системи навчання, підготовки, перепідготовки та підвищення кваліфікації відповідних фахівців різних рівнів управління національної системи захисту критичної інфраструктури України.

**Аналіз останніх досліджень і публікацій.** За останній час в Україні проблематика досліджень проблем організації та забезпечення підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері захисту та стійкості критичної інфраструктури набула своєї актуальності. Можливі шляхи організації системи підготовки висвітлювались у роботах О. Суходолі [4]–[6], В. Басистого [7]. Підходи до забезпечення національної безпеки та організації основних процесів у цій сфері у сучасних умовах розкриті у дослідженнях В. Горбуліна, А. Місюри [8], Г. Ситника, В. Абрамова [9]. Теоретичні та практичні аспекти забезпечення національної системи стійкості в умовах мінливості й невизначеності безпекового середовища досліджувались у роботах О. Резнікової [10].

В підсумковому звіті «Дослідження доцільності запровадження системи освіти і навчання з питань безпеки та стійкості критичної інфраструктури в Україні» [11] вказано,

що проблематика досліджень проблем організації та забезпечення підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері захисту та стійкості критичної інфраструктури набула своєї актуальності. Вивчено міжнародний досвід та практики підготовки фахівців. Запропонована «умовна» дорожня карта з організації навчання та освіти у сфері захисту критичної інфраструктури в Україні.

Аналітична записка центру безпекових досліджень Національного інституту стратегічних досліджень *«Пріоритетні завдання формування системи навчання фахівців у сфері захисту критичної інфраструктури»* містить огляд основних форм організації навчання та підготовки персоналу у сфері захисту критичної інфраструктури. Запропоновано перелік спеціальностей, навчальних дисциплін, базових компетенцій та програмних результатів навчання, які мають сформулювати вимоги до змісту освітніх програм з питань захисту критичної інфраструктури.

В аналітичній записці центру безпекових досліджень Національного інституту стратегічних досліджень *«Проблема розбудови системи підготовки кадрів і населення для забезпечення стійкості критичної інфраструктури в Україні»* розглянуто проблему створення системи підготовки кадрів і населення для захисту та забезпечення стійкості критичної інфраструктури в Україні на основі передового зарубіжного досвіду та найкращої практики, зокрема досвіду діяльності у рамках Міністерства внутрішньої безпеки США (U.S. Department of Homeland Security, DHS) та Всесвітнього інституту з фізичної ядерної безпеки (World Institute for Nuclear Security).

**Метою статті** є аналіз актуальності створення системи підготовки та підвищення кваліфікації фахівців у сфері захисту та стійкості критичної інфраструктури, а також дослідження основних проблем формування такої системи та визначення основних напрямів їх вирішення.

**Виклад основного матеріалу дослідження.** Слід зазначити, що в умовах повномасштабної збройної агресії РФ критична інфраструктура України, її окремі системи та елементи залишаються одними із пріоритетних цілей для збройних сил та спеціальних служб країни-агресора. Спектр загроз є надзвичайно широкий: від ударів засобами повітряного нападу до організації здійснення терористичних атак, актів диверсій та кібератак на об'єктах критичної інфраструктури. Також актуальними залишаються загрози природного та техногенного характеру. У відповідь на ці виклики Україна вживає заходів для посилення захисту своєї критичної інфраструктури, включаючи вдосконалення системи кібербезпеки, модернізацію захисних споруд і систем оповіщення, а також проведення регулярних тренувань і навчань для персоналу. Крім того, важливою є міжнародна співпраця, яка дозволяє обмінюватися досвідом і технологіями, а також отримувати підтримку у вигляді ресурсів і консультацій від міжнародних партнерів.

Критична інфраструктура України поділена на 24 сектори: паливно-енергетичний; цифрові технології; захист інформації; харчова промисловість та агропромисловий комплекс; державний матеріальний резерв; охорона здоров'я; ринки капіталу та організовані товарні ринки; фінансовий сектор; транспорт і пошта; системи життєзабезпечення; промисловість; сектор громадської безпеки; цивільний захист населення і територій; охорона навколишнього природного середовища; сектор оборони; правосуддя; виконання кримінальних покарань, тримання під вартою та утримання військовополонених; державна реєстрація; наукові дослідження та розробки; вибори та референдуми; соціальний захист; інформаційний сектор; державна влада та місцеве самоврядування [12]. Кожен з цих секторів є надзвичайно важливим для забезпечення національної безпеки та стабільності країни. Зокрема, паливно-енергетичний сектор забезпечує енергетичну незалежність, тоді як цифрові технології і захист інформації є ключовими для кібербезпеки. Харчова промисловість та агропромисловий комплекс гарантують продовольчу безпеку, а охорона здоров'я – медичну допомогу населенню. В умовах поточних загроз, Україна активно працює над посиленням захисту цих секторів, впроваджуючи новітні технології, підвищуючи рівень готовності та співпрацюючи з міжнародними партнерами для обміну досвідом та ресурсами.

Для вирішення завдань щодо захисту та стійкості критичної інфраструктури Законом передбачена національна система захисту критичної інфраструктури. Ця система має забезпечити ефективну реалізацію поставлених завдань щодо захисту об'єктів критичної інфраструктури в умовах трансформації існуючих ризиків і загроз, а також появи нових, у тому числі пов'язаних із швидким розвитком технологій. Побудова дієвої системи захисту є складним завданням, яке створює нові виклики для нашої країни та потребує значних зусиль. При цьому суттєво підвищується цінність людського фактору як ключового елемента національної системи захисту. Якісно підготовлені фахівці, володіючи необхідними знаннями, навичками та відповідними компетенціями, повинні вирішувати складні комплексні завдання забезпечення безпеки та стійкості критичної інфраструктури. Також суттєво зростає потреба у підвищенні рівня комплексних знань, навичок і вмінь персоналу та керівного складу операторів критичної інфраструктури, які займаються забезпеченням безпеки об'єктів критичної інфраструктури та реагуванням на кризові ситуації на таких об'єктах. Важливим аспектом є постійне навчання та професійний розвиток, що дозволяє оперативно реагувати на нові загрози та забезпечувати стійкість критичної інфраструктури.

За цих умов постає актуальним питання створення системи освіти, підготовки та підвищення кваліфікації фахівців у сфері захисту та стійкості критичної інфраструктури. Розбудова такої системи є необхідним елементом для створення, підтримки та розвитку кадрового потенціалу, який вирішуватиме широке коло завдань: аналізуватиме реальні та потенційні ризики і загрози, реагуватиме на складні комплексні виклики та прийматиме ефективні управлінські, організаційні, інженерно-технічні та інші рішення, необхідні для досягнення цілей і вирішення завдань, визначених українським законодавством. Фахівцям необхідно володіти знаннями щодо особливостей операційного середовища, розуміти структуру та ієрархію систем, взаємні впливи, регуляторні чинники та нормативно-правове забезпечення. Вони повинні вміти оцінювати ризики та загрози, визначати критерії стійкості та безпеки об'єктів критичної інфраструктури, а також виявляти та усувати вразливості. Без цих знань неможливе адекватне планування заходів захисту та забезпечення стійкості об'єктів.

За цих умов постає актуальним питання створення системи освіти, підготовки та підвищення кваліфікації фахівців у сфері захисту та стійкості критичної інфраструктури. Розбудова такої системи є необхідним елементом для створення, підтримки та розвитку кадрового потенціалу, який вирішуватиме широке коло завдань: аналізуватиме реальні та потенційні ризики і загрози, реагуватиме на складні комплексні виклики та прийматиме ефективні управлінські, організаційні, інженерно-технічні та інші рішення, необхідні для досягнення цілей і вирішення завдань, визначених українським законодавством.

Система підготовки кадрів має охоплювати досить широку аудиторію: державні службовці, власники та оператори об'єктів критичної інфраструктури, представники секторальних та функціональних органів у сфері захисту критичної інфраструктури та інших суб'єктів національної системи захисту. Фахівцям необхідно володіти знаннями щодо особливостей операційного середовища, розуміти структуру та ієрархію систем, взаємні впливи, регуляторні чинники та нормативно-правове забезпечення. Вони повинні вміти оцінювати ризики та загрози, визначати критерії стійкості та безпеки об'єктів критичної інфраструктури, а також виявляти та усувати вразливості. Без цих знань неможливе адекватне планування заходів захисту та забезпечення стійкості об'єктів.

Для ефективного функціонування системи освіти і підготовки фахівців необхідно створити навчальні програми, що включатимуть теоретичну підготовку та практичні тренінги. Важливим є також впровадження новітніх технологій навчання, таких як симуляції та моделювання кризових ситуацій, що дозволяють відпрацювати навички в умовах, максимально наближених до реальних. Крім того, міжнародна співпраця та обмін досвідом з країнами-партнерами є критично важливими. Вивчення найкращих світових практик та їх адаптація до українських реалій допоможе підвищити рівень підготовки фахівців. Розвиток таких програм і систем підготовки фахівців є довгостроковою інвестицією у безпеку країни, яка забезпечить її стійкість перед сучасними викликами та загрозами.

Слід зазначити, що Законом поставлено завдання щодо проведення науково-дослідної роботи щодо доповнення Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, новою позицією у сфері забезпечення стійкості та захисту критичної інфраструктури. За результатами вказаної роботи має бути підготовлено проєкт відповідного рішення та пропозиції Кабінету Міністрів України щодо програм навчання, підвищення кваліфікації, робочих і навчальних програм. Це завдання також визначене Національним планом захисту та забезпечення безпеки та стійкості критичної інфраструктури, затвердженим розпорядженням Кабінету Міністрів України від 19 вересня 2023 р. № 825-р [13].

Зазначене дослідження доцільності запровадження системи освіти і навчання з питань безпеки та стійкості критичної інфраструктури в Україні (далі – Дослідження) було проведено, результатом якого 18 січня 2024 року було представлено підсумковий звіт [11]. Основним висновком за результатами Дослідження стала рекомендація щодо розгляду можливості створення в Україні на базі наявних закладів вищої освіти освітнього закладу, завдання якого полягало б в організації співпраці з потенційними споживачами сфери захисту критичної інфраструктури, центрами передового досвіду, відповідними інституціями у сфері безпеки та стійкості критичної інфраструктури, вітчизняними та закордонними провідними спеціалістами та науковцями.

Доцільно підкреслити, що створення такого освітнього закладу сприятиме розвитку кадрового потенціалу, який зможе ефективно реагувати на сучасні виклики та загрози. Співпраця з міжнародними партнерами дозволить впроваджувати кращі світові практики, що підвищить рівень підготовки фахівців. Важливо також забезпечити безперервний процес навчання та підвищення кваліфікації, який буде включати як теоретичні знання, так і практичні навички, зокрема використання симуляцій та інших сучасних методів навчання. Таким чином, результати Дослідження не тільки підкреслюють актуальність створення системи освіти та навчання у сфері захисту критичної інфраструктури, але й визначають конкретні кроки для реалізації цієї ініціативи, спрямованої на зміцнення національної безпеки України.

Система навчання, підготовки та перепідготовки спеціалістів у сфері захисту критичної інфраструктури може охоплювати різні форми та методи, зокрема: проведення окремих заходів (відомчі, міжвідомчі та міжнародні навчання та тренінги, короткострокові курси) у рамках форматів підвищення професійної кваліфікації; перепідготовки персоналу (навчальні програми у очній та заочній формі) з оволодіння новими спеціальностями чи підвищення професійного рівня; навчання персоналу в рамках програм професійної, передвищої та вищої освіти. Водночас система вищої освіти, у рамках якої можливо запровадити необхідні освітні програми, має сприяти формуванню бази для підготовки фахівців та сприяти розвитку інших форм підготовки персоналу та населення з питань захисту критичної інфраструктури.

Слід зазначити, що в Україні започатковано процес дослідження проблем підготовки фахівців у сфері захисту критичної інфраструктури. При цьому, актуальним питанням постає огляд та аналіз наявних систем підготовки та перепідготовки кадрів, які можуть містити проблеми у зазначеній сфері. Особливість та складність у розробці освітніх програм, програм підготовки, перепідготовки та підвищення кваліфікації полягає у необхідності забезпечення міждисциплінарного підходу. За результатами Дослідження встановлено, що на даний час в навчальних програмах вищих навчальних закладів практично відсутня проблематика захисту ті стійкості об'єктів критичної інфраструктури. Окремі питання у цій сфері стали включатися до освітніх програм за спеціальностями «цивільний захист», «кібербезпека та захист інформації», «національна безпека» та «публічне управління та адміністрування».

Система професійної освіти в Україні розвивається в динаміці разом зі світовими тенденціями, які стосуються лібералізації форм професійного навчання. В Україні має сформуватися гнучка система підготовки кадрів у сфері захисту критичної інфраструктури, яка дозволяє швидко реагувати на зміни попиту на ринку праці.

Зокрема, створено та функціонує Національне агентство кваліфікацій, яке, серед іншого, забезпечує підтримку Національної рамки кваліфікацій; бере участь у прогнозуванні потреб ринку праці у кваліфікаціях персоналу; створює та веде Реєстр кваліфікацій (що містить базу даних професійних стандартів).

Реєстр кваліфікацій [14] містить перелік суб'єктів, які здійснюють підготовку/підтвердження кваліфікації кадрів за певними професіями (кваліфікаційні центри). Реєстр адаптується до вимог законодавства та потреб ринку праці. Цей процес вже розпочався, і до нього можуть долучитися різні суб'єкти системи професійної освіти. Кваліфікаційні центри можуть мати різні форми власності та створюватися закладами вищої освіти, суб'єктами господарювання, фізичними особами тощо.

Аналіз інформації про потреби ринку праці дозволяє зрозуміти необхідність розроблення, впровадження або перегляду професійних стандартів [15]. Професійний стандарт [16] встановлює вимоги до компетентностей працівників, які слугують основою для формування професійних кваліфікацій в освітньому процесі. Професійні стандарти є основою для адаптації освітніх програм закладів вищої освіти відповідно до мінливого попиту ринку праці.

Інструментом стимулювання попиту на фахівців у сфері захисту критичної інфраструктури та формування вимог до відповідних компетентностей може стати розроблення професійних стандартів [17]. Прикладом такої політики є розроблення комплексу професійних стандартів у сфері кібербезпеки. Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) реформує систему підготовки кадрів у сфері кібербезпеки з урахуванням вимог ринку праці. До державного класифікатора професій додано нові професії у сфері кібербезпеки та інформаційної безпеки. Для цих професій розробляються професійні стандарти у сфері кібербезпеки.

Постає завдання на основі аналізу наявних професій та попиту на ринку праці визначити набір професій, які доцільно залучати до виконання завдань із забезпечення безпеки та стійкості критичної інфраструктури.

Додатковим варіантом підвищення обізнаності з питань захисту критичної інфраструктури може стати формування системи навчання для керівників і персоналу органів державної влади та промисловості. Система підготовки кадрів у сфері цивільного захисту може надати інноваційні ідеї для розвитку освіти у сфері захисту критичної інфраструктури. В Україні розвивається система підготовки новопризначених керівників і персоналу центральних, місцевих органів виконавчої влади та промисловості у сфері цивільного захисту. Створено систему навчальних центрів, які проводять короткострокові курси з питань цивільного захисту та безпеки життєдіяльності [18].

У Національному класифікаторі України ДК 003:2010 “Класифікатор професій” [19] (далі – КП) проаналізовано наявність номенклатури професій, посад та професійних звань, пов'язаних із захистом об'єктів критичної інфраструктури. За результатами цього аналізу можна зробити ряд висновків. У КП є суттєва прогалина – у ньому повністю відсутні професії та посади, безпосередньо пов'язані з управлінням національною системою захисту об'єктів критичної інфраструктури в цілому та діяльністю її об'єктів і суб'єктів, зокрема. Серед усього масиву посад у КП лише вісімдесят шість безпосередньо пов'язані із захистом об'єктів критичної інфраструктури. До них належать:

- керівник (із захисту інформації) підприємства (установи, організації);
- начальник (воєнізованого, газорятувального, гірничорятувального, авіаційного, пожежного) підрозділу;
- Голова Державної воєнізованої гірничорятувальної служби;
- командир відділення (цивільна оборона);
- магістр (цивільний захист) – інспектор з радіаційної безпеки;
- розробник систем інформаційної безпеки;
- аналітик з безпеки інформаційно-комунікаційних систем;

- аналітик з оцінювання вразливостей;
- аналітик загроз безпеці;
- аналітик систем інформаційної безпеки;
- аудитор інформаційних технологій (*кібербезпека*);
- спеціаліст з інформаційної безпеки / заходів із захисту інформації (*кібербезпеки*);
- аналітик з фінансової та економічної безпеки;
- професіонал у сфері фінансової та економічної безпеки;
- аудитор систем безпечності харчових продуктів, тощо.

Також у складі КП відсутні посади, пов'язані з управлінням системою захисту об'єктів критичної інфраструктури на національному, регіональному, галузевому, місцевому та об'єктовому рівнях, як це визначено статтею 7 Закону. Це безпосередньо стосується необхідності існування спеціалізованих посад в Уповноваженому органі у сфері захисту критичної інфраструктури в Україні, а також у функціональних та галузевих органах у цій сфері. Ця потреба поширюється на місцеві органи виконавчої влади та військово- цивільні адміністрації, а також на операторів об'єктів критичної інфраструктури як зазначено у статтях 16-21 Закону.

Слід зазначити, що у [11] приведено 38 пропозицій щодо внесення змін до КП.

Водночас, з метою виконання плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року, щодо розроблення переліку посад та кваліфікаційних характеристик для фахівців, відповідальних за забезпечення захисту об'єктів критичної інфраструктури, Адміністрація Держспецзв'язку, на основі узагальнення пропозицій від секторальних та функціональних органів у сфері захисту об'єктів критичної інфраструктури, звернулася до Міністерства економіки України з пропозицією включення до КП наступних двох професій:

1. “Керівник структурного підрозділу з питань захисту та стійкості критичної інфраструктури” (код КП-1229.7) з урахуванням встановлених функцій та задач, як керівника підрозділу, який відповідальний за розроблення та підтримку планів, стратегій та політики із забезпечення захисту та стійкості критичної інфраструктури та заходи для їх підтримки та узгодження з ініціативами підприємства (установи, організації) у сфері забезпечення захисту та стійкості критичної інфраструктури з дотриманням регуляторних вимог;

2. “Фахівець із захисту та стійкості критичної інфраструктури” (код КП-2490.1) з урахуванням встановлених функцій та задач, як фахівця, що розробляє та підтримує плани, стратегії та політики у сфері захисту та стійкості критичної інфраструктури та заходи для їх підтримки та узгодження з ініціативами підприємства (установи, організації) у сфері забезпечення захисту та стійкості критичної інфраструктури з дотриманням регуляторних вимог.

Після остаточного формування Мінекономіки проєкту змін до КП він буде затверджений в установленому порядку.

Слід зазначити, що включення до КП нових назв професій дозволить Держспецзв'язку із широким колом заінтересованих сторін виконати вимоги статті 96 “Кодексу законів про працю в Україні”, стаття 39 Закону України “Про освіту”, статті 6 Закону України “Про оплату праці” та з урахуванням досвіду громадського об'єднання Національної освітньої ініціативи сформувавши вимоги до компетентностей працівників сфери захисту та стійкості критичної інфраструктури, що стане основою створення системи професійної кваліфікації даного напрямку, а також підвищення ефективності системи захисту та стійкості критичної інфраструктури держави та суспільства, критичних інфраструктур країни.

**Висновки та перспективи подальших досліджень.** Отже проведений аналіз питання підготовки та підвищення кваліфікації фахівців у сфері захисту та стійкості критичної інфраструктури показав, що нинішній стан захисту та стійкості критичної інфраструктури свідчить про необхідність і можливість створення національної системи освіти і навчання з питань захисту та стійкості критичної інфраструктури в Україні.

Здійснений аналіз щодо потреби ринку праці захисту та стійкості критичної інфраструктури дозволяє зрозуміти необхідність розроблення, впровадження або перегляду професійних стандартів, в котрих встановлюються вимоги до компетентностей працівників, які слугують основою для формування професійних кваліфікацій в освітньому процесі. Розроблені або оновлені професійні стандарти в сфері захисту та стійкості критичної інфраструктури стануть основою для адаптації освітніх програм закладів вищої освіти відповідно до мінливого попиту ринку праці.

Слід зазначити, що на основі аналізу наявних професій та попиту на ринку праці авторами визначено набір професій, які доцільно залучати до виконання завдань із забезпечення безпеки та стійкості критичної інфраструктури. Такими професіями, після їх остаточного затвердження, можуть стати: керівник структурного підрозділу з питань захисту та стійкості критичної інфраструктури та фахівець із захисту та стійкості критичної інфраструктури.

Водночас, це дозволить розгорнути в країні діяльність щодо розроблення професійних стандартів, створення кваліфікаційних центрів та формування системи професійної сертифікації кадрів у відповідності до кращих вітчизняних та міжнародних практик у сфері захисту та стійкості критичної інфраструктури.

Нові назви професій є актуальними та важливими саме у цей складний для країни час. Перехід сфери захисту та стійкості критичної інфраструктури на міжнародні стандарти є пріоритетною основою для всього суспільства.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Рада національної безпеки і оборони України. (2020, Вер. 14). *Рішення Ради національної безпеки і оборони України “Про Стратегію національної безпеки України”*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>. Дата звернення: Квіт. 15, 2024.
- [2] Рада національної безпеки і оборони України. (2021, Вер. 27). *Рішення Ради національної безпеки і оборони України “Концепція забезпечення національної системи стійкості”*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/n0065525-21#Text>. Дата звернення: Квіт. 15, 2024.
- [3] Верховна Рада України. (2021, Листоп.16). *Закон України 1882-IX, Про критичну інфраструктуру*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>. Дата звернення: Квіт. 15, 2024.
- [4] Д.С. Бірюков, та С.І. Кондратов, *Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад*, О.М. Суходоля, Ред. Київ: НІСД, 2016.
- [5] Ю. Дорохіна, “Розвиток системи захисту критичної інфраструктури в Україні”, *Право та суспільство*, №7, с. 69-73, 2018.
- [6] S. Kondratov et al., *Developing The Critical Infrastructure Protection System in Ukraine: monograph*, O. Sukhodolia, Ed. Kyiv, Ukraine: NISS, 2017.
- [7] V. Basystyi, “Research on Critical Infrastructure Protection education in Ukraine”, *ResearchGate*. [Online]. Available: [https://www.researchgate.net/publication/372851978\\_Research\\_on\\_Critical\\_Infrastructure\\_Protection\\_education\\_in\\_Ukraine](https://www.researchgate.net/publication/372851978_Research_on_Critical_Infrastructure_Protection_education_in_Ukraine). Accessed on: Ap. 15, 2024.
- [8] V. Horbulin, *The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from ukrainian*. Kharkiv, Ukraine: Folio, 2017.
- [9] Г.П. Ситник та ін, *Шляхи удосконалення системи державного управління забезпеченням національної безпеки України: монографія*. Київ, Україна: Майстер книг, 2012.
- [10] О.О. Резнікова, *Національна стійкість в умовах мінливого безпекового середовища. монографія*. Київ, Україна: НІСД, 2022.



- [11] R.S. Beers, and A. Lazari, *Study on the feasibility of introducing a system of education and training on critical infrastructure security and resilience in Ukraine. Final report*. Jan. 18, 2024, 120 p.
- [12] Кабінет Міністрів України (2020, Жовт. 9) *Постанова Кабінету Міністрів України №1109. Перелік секторів критичної інфраструктури*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text>. Дата звернення: Квіт. 15, 2024.
- [13]. Кабінет Міністрів України (2023, Вер. 9) *Розпорядження Кабінету Міністрів України №825-р. Про затвердження Національного плану*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text>. Дата звернення: Квіт. 15, 2024.
- [14]. Кабінет Міністрів України (2021, Черв. 16) *Постанова Кабінету Міністрів України № 6203. Про затвердження Положення про Реєстр кваліфікацій*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/620-2021-%D0%BF>. Дата звернення: Квіт. 15, 2024.
- [15]. Кабінет Міністрів України (2017, Трав. 31) *Постанова Кабінету Міністрів України № 373 Про затвердження Порядку розроблення, запровадження та перегляду професійних стандартів*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/373-2017-%D0%BF#n11>. Дата звернення: Квіт. 15, 2024.
- [16]. Відомості про професійні стандарти. [Електронний ресурс]. Доступно: <https://register.nqa.gov.ua/profstandarts>. Дата звернення: Квіт. 15, 2024.
- [17]. Методичні рекомендації щодо розроблення професійних стандартів. [Електронний ресурс]. Доступно: <https://nqa.gov.ua/news/metodicni-rekomendacii-sodo-rozroblenna-profesijnih-standartiv/>. Дата звернення: Квіт. 15, 2024.
- [18]. Кабінет Міністрів України (2013, Жовт. 23) *Постанова Кабінету Міністрів України № 819. Про затвердження Порядку проведення навчання керівного складу та фахівців, діяльність яких пов'язана з організацією і здійсненням заходів з питань цивільного захисту*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/819-2013-%D0%BF#n9>. Дата звернення: Квіт. 15, 2024.
- [19]. Національний класифікатор України. Класифікатор професій ДК 003:2010. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/rada/show/va327609-10#Text>. Дата звернення: Квіт. 15, 2024.

Стаття надійшла до редакції 17.05.2024.

## REFERENCE

- [1] National Security and Defense Council of Ukraine. (2020, Sept.14). *Decision of the National Security and Defense Council of Ukraine “On the National Security Strategy of Ukraine”*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>. Accessed on: Apr. 15, 2024.
- [2] National Security and Defense Council of Ukraine. (2021, Sept.27). *Decision of the National Security and Defense Council of Ukraine “The concept of ensuring the national resilience system”*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/n0065525-21#Text>. Accessed on: Apr. 15, 2024.
- [3] Verkhovna Rada of Ukraine. (2021, Nov.16). *Law of Ukraine 1882-IX About critical infrastructure*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>. Accessed on: Apr. 15, 2024.
- [4] D.S. Biryukov, and S.I. Kondratov, *Green book on critical infrastructure protection in Ukraine: coll. mat. of int. exp. meet.*, O. Sukhodolia, Ed. Kyiv, Ukraine: NISS, 2016.
- [5] Y. Dorokhina, “Development Of Critical Informational Infrastructure Protection System In Ukraine”, *Law & Society (untill 2019)*, no. 7, pp. 69-73, 2018.
- [6] S. Kondratov et al., *Developing The Critical Infrastructure Protection System in Ukraine: monograph*, O. Sukhodolia, Ed. Kyiv, Ukraine: NISS, 2017.

- [7] V. Basystyi, “Research on Critical Infrastructure Protection education in Ukraine”, *ResearchGate*. [Online]. Available: [https://www.researchgate.net/publication/372851978\\_Research\\_on\\_Critical\\_Infrastructure\\_Protection\\_education\\_in\\_Ukraine](https://www.researchgate.net/publication/372851978_Research_on_Critical_Infrastructure_Protection_education_in_Ukraine). Accessed on: Ap. 15, 2024.
- [8] V. Horbulin, *The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from ukrainian*. Kharkiv, Ukraine: Folio, 2017.
- [9] H.P. Sytnyk et al., *Ways to improve the system of public administration of national security of Ukraine: monograph*. Kyiv, Ukraine: Master of books, 2012.
- [10] O. Reznikova, *National resilience in a changing security environment: monograph*. Kyiv, Ukraine: NISS, 2022.
- [11] R.S. Beers, and A. Lazari, *Study on the feasibility of introducing a system of education and training on critical infrastructure security and resilience in Ukraine. Final report*. Jan. 18, 2024, 120 p.
- [12] Cabinet of Ministers of Ukraine (2020, Oct. 9) *Resolution of the Cabinet of Ministers of Ukraine №1109. List of critical infrastructure sectors*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text>. Accessed on: Ap. 15, 2024.
- [13]. Cabinet of Ministers of Ukraine (2023, Sept. 9) *Order of the Cabinet of Ministers of Ukraine №825-p. On approval of the National Plan*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text>. Accessed on: Ap. 15, 2024.
- [14]. Cabinet of Ministers of Ukraine (2021, June 16) *Resolution of the Cabinet of Ministers of Ukraine № 6203. On approval of the Regulation on the Register of Qualifications*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/620-2021-%D0%BF>. Accessed on: Ap. 15, 2024.
- [15]. Cabinet of Ministers of Ukraine (2017, May 31) *Resolution of the Cabinet of Ministers of Ukraine № 373 On Approval of the Procedure for Development, Implementation and Review of Professional Standards*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/373-2017-%D0%BF#n11>. Accessed on: Ap. 15, 2024.
- [16]. Information on professional standards. [Online]. Available: <https://register.nqa.gov.ua/profstandarts>. Accessed on: Ap. 15, 2024.
- [17]. Guidelines for the development of professional standards. [Online]. Available: <https://nqa.gov.ua/news/metodicni-rekomendacii-sodo-rozroblenna-profesijnih-standartiv>. Accessed on: Ap. 15, 2024.
- [18]. Cabinet of Ministers of Ukraine (2013, Oct. 23) *Resolution of the Cabinet of Ministers of Ukraine № 819. On Approval of the Procedure for Training of Management Personnel and Specialists Whose Activities Are Related to the Organisation and Implementation of Civil Protection Measures*. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/819-2013-%D0%BF#n9>. Accessed on: Ap. 15, 2024.
- [19]. National Classifier of Ukraine. Classifier of professions DC 003:2010. [Online]. Available: <https://zakon.rada.gov.ua/rada/show/va327609-10#Text>. Accessed on: Ap. 15, 2024.

BOHDAN NIKOLAIENKO,  
ANDRII MISIURA,  
ANTON STORCHAK,  
PAVLO DIMITROV

## **TRAINING OF SPECIALISTS AS ONE OF THE ASPECTS OF RESILIENCE OF CRITICAL INFRASTRUCTURE**

**Abstract:** One of the directions of state policy in the field of ensuring national security is the development of a multi-level effective national security and resilience system for critical infrastructure. A key factor in any system, whether in the field of national security or in other spheres,

is human capital, its ability to analyze risks and threats, identify vulnerabilities, master new technologies, and find innovative solutions to address modern challenges. Thus, an important aspect becomes the training of qualified professionals who possess systemic knowledge and skills.

The need to provide systemic knowledge to specialists and managers directly addressing the tasks of ensuring the protection and resilience of critical infrastructure has been established. The current state of the training system for specialists in the field of critical infrastructure protection in Ukraine has been identified, and the main forms of organizing training and personnel preparation in this area have been analyzed. Tasks have been established based on an analysis of existing professions and labor market demand to determine a set of professions that are expedient to involve in ensuring the security and resilience of critical infrastructure. An analysis of the training and qualification enhancement of specialists in the field of critical infrastructure protection and resilience has shown the necessity and possibility of creating a national education and training system on critical infrastructure protection and resilience in Ukraine.

Professions and labor market demand have been analyzed, and a set of professions expedient to involve in ensuring the security and resilience of critical infrastructure has been determined. After their final approval, these professions could include: the head of a structural unit responsible for the protection and resilience of critical infrastructure and a specialist in the protection and resilience of critical infrastructure. Developed or updated professional standards in the field of critical infrastructure protection and resilience will serve as a basis for adapting educational programs of higher education institutions according to the labor market demand.

**Keywords:** security, resilience, critical infrastructure, professional classification, national security.

**Ніколаєнко Богдан Анатолійович**, кандидат технічних наук, доцент, головний спеціаліст департаменту захисту критичної інфраструктури Адміністрації Держспецзв'язку, Київ, Україна, ORCID <https://orcid.org/0000-0002-6888-5947>, [nikolaienko\\_iszzi@ukr.net](mailto:nikolaienko_iszzi@ukr.net).

**Місюра Андрій Олександрович**, головний спеціаліст департаменту захисту критичної інфраструктури Адміністрації Держспецзв'язку, Київ, Україна, ORCID 0009-0005-8254-5251, [a.misiura.cip@gmail.com](mailto:a.misiura.cip@gmail.com).

**Сторчак Антон Сергійович**, кандидат технічних наук, доцент кафедри кібербезпеки та захисту інформації, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-5267-3122, [storchakanton@gmail.com](mailto:storchakanton@gmail.com)

**Дімітров Павло Євстафійович**, науковий співробітник Науково-дослідного інституту воєнної розвідки, Київ, Україна, ORCID <https://orcid.org/0009-0007-6184-8223>, [strenia@ukr.net](mailto:strenia@ukr.net).

**Nikolaienko Bohdan**, PhD in engineering, associate professor, chief specialist of the department of the critical infrastructure protection Administration of the State Service of Special Communications and Information Protection of Ukraine, Kyiv, Ukraine.

**Misiura Andrii**, chief specialist of the department of the critical infrastructure protection Administration of the State Service of Special Communications and Information Protection of Ukraine, Kyiv, Ukraine.

**Storchak Anton**, PhD in engineering, associate professor at the cybersecurity and information security academic department, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

**Dimitrov Pavlo**, researcher at the Military Intelligence Research Institute, Kyiv, Ukraine.