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. № 5.

DOI: http://doi.org/10.32702/2307-2156.2025.5.12

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

КОНЦЕПТУАЛЬНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ПІДГОТОВКИ КАДРІВ ДЛЯ СФЕРИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

L. A. 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

CONCEPTUAL AND METHODOLOGICAL PRINCIPLES FOR THE FORMATION OF STATE POLICY FOR TRAINING CRITICAL INFRASTRUCTURE PROTECTION PERSONNEL

Стан розвитку інформаційного суспільства й критичної інформаційної інфраструктури України визначає професійні вимоги до державних суб'єктів національної системи захисту критичної інфраструктури і операторів

критичної інфраструктури при підготовці фахівців у сфері захисту критичної інфраструктури. Зазначена сфера почала суттєво розвиватися в останнє десятиліття, особливо після повномасштабного вторгнення російської федерації на територію України, при цьому поняття критичної інфраструктури в Україні законодавчо визначено лише у листопаді 2021 року.

Відповідно концептуальні та методологічні засади формування державної політики підготовки кадрів для сфери захисту критичної інфраструктури, а також понятійно-категоріальний апарат професійної діяльності у зазначеній сфері не є остаточно визначеним як на законодавчому, так і практично-науковому рівні.

У сучасних умовах проблема забезпечення кіберзахисту та кібербезпеки національної системи захисту критичної інфраструктури переходить із рівня захисту інформації на окремому об'єкті критичної інфраструктури на рівень створення єдиної системи захисту критичної інфраструктури держави як складової національної безпеки, що відповідає державним пріоритетам у реформуванні сектору безпеки і оборони України.

Сфера захисту критичної інфраструктури сьогодні – це не лише об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, а передусім людський ресурс. І більшість представників органів державної влади України, задіяних у функціонуванні національної системи захисту критичної інфраструктури, відзначають незадовільний стан кадрового забезпечення фахівцями відповідних суб'єктів та усієї системи підготовки кадрів для сфери захисту критичної інфраструктури.

У статті автором охарактеризовано систему підготовки кадрів для сфери захисту критичної інфраструктури, надано їй визначення, сформулювано таке поняття, як кібернавчання, а також розкрито дефініцію «фахівець сфери захисту критичної інфраструктури», що є передумовами розвитку процесу підготовки відповідних фахівців, підвищення їх кваліфікації у

сфері захисту критичної інфраструктури з урахуванням усіх аспектів діяльності та сфер життя держави.

The development state of the information society and critical information infrastructure of Ukraine determines professional requirements for state entities within the national critical infrastructure protection system and critical infrastructure operators in the training of specialists in the critical infrastructure protection field. This subject area commenced its significant development in the last decade, especially after the full-scale invasion of the Russian Federation into Ukraine, whereas the concept of critical infrastructure in Ukraine was legislatively defined only in November 2021. Accordingly, the conceptual and methodological principles for the formation of state policy for training critical infrastructure protection personnel, as well as the conceptual and categorical apparatus of professional activities in this field, are not finally defined both at the legislative and practical-scientific levels.

In modern conditions, the problem of ensuring cyber defense and cyber security of the national critical infrastructure protection system shifts from the level of information protection at a separate critical infrastructure facility to the level of creating a unified system to protect the state's critical infrastructure as a national security component that meets state priorities in reforming the security and defense sector of Ukraine.

The current sphere of critical infrastructure protection includes not only infrastructure facilities, systems, their components and the entirety thereof, which are important for the economy, national security and defense, but above all, human resources. Moreover, most representatives of Ukrainian government bodies involved in the functioning of the national critical infrastructure protection system note the unsatisfactory staffing by specialists of the relevant entities and the entire system of training personnel for the critical infrastructure protection sector.

In this article, the author gives an account of the system of training personnel for the critical infrastructure protection field, gives its definition, formulates the

concept of cyber training and reveals the meaning of "critical infrastructure protection specialist", which are prerequisites to further develop the process of training relevant specialists and improve their qualifications in critical infrastructure protection, taking into account all aspects of the state's activities and spheres of life.

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. Важливим питанням є розгляд та трактування освітніх понять, що необхідно в ході дослідження і уточнення різних аспектів сфери захисту критичної інфраструктури в розрізі підготовки фахівців для національної системи захисту критичної інфраструктури. Разом з тим, термінологія для дослідження даного напряму може слугувати не тільки теоретично-практичним підґрунтям при виборі відповідної методології, але й виявляти певні недоліки щодо її єдиної класифікації, систематизації та узагальнення на належному науково-практичному (науково-теоретичному) рівні та в процесі ефективного застосування за умов узгодження із чинним законодавством у сфері захисту критичної інфраструктури.

Понятійно-категоріальний апарат державно-управлінської науки в освітній сфері захисту критичної інфраструктури потребує суттєвої розбудови, наукового редагування та переосмислення. Система формування освітніх дефініцій у сфері захисту критичної інфраструктури, яка на сьогодні будується за принципом змістовного віднесення термінів відповідно до певних категорій та критеріїв, вимагає дієвого розвитку задля її удосконалення.

Нинішні світові тенденції свідчать про розширення та поглиблення сфер

практично-професійної діяльності й освіти, що пов’язане із швидкою динамікою розвитку ІТ-складової життєдіяльності людини і суспільства, у тому числі у сферах кібербезпеки, кіберзахисту, захисту критичної інфраструктури.

Аналіз останніх досліджень і публікацій. Проблемою підготовки фахівців для сфери захисту критичної інфраструктури переймались сучасні дослідники. Так, науковцем Євсєєвим В.О. розроблено і теоретично обґрунтовано модель підготовки кадрів у сфері захисту критичної інфраструктури в системі вищої освіти, яка ураховує сучасні специфічні організаційно-управлінські механізми формування системи підготовки фахівців у сфері захисту критичної інфраструктури у межах вищої освіти, передові тенденції розвитку й забезпечення якості освітньої діяльності та вищої освіти, сучасні принципи реалізації закладами вищої освіти освітніх (освітньо-професійних) програм, а також визначає порядок взаємодії стейкхолдерів у процесі розроблення і реалізації зазначених програм підготовки кадрів для суб’єктів національної системи захисту критичної інфраструктури. Вченим підкреслено, що особливостями розробленої моделі є комплексність, поетапність реалізації, динамічність, взаємопов’язаність складників та інтеграція системи забезпечення якості тощо [1].

А науковець Теленик С.С., вивчаючи напрями підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури, доходить до висновку, що національні класифікатори не передбачають поділу видів економічної діяльності та професій, пов’язаних із захистом критичної інфраструктури, що в свою чергу призводить до того, що в офіційному державному переліку галузей знань та спеціальностей відсутня відповідна категорія. Автором статті також встановлено перелік суміжних спеціальностей, які можуть бути затребувані в галузі захисту критичної інфраструктури. Вчений відводить важливе місце аналізу причин, що перешкоджають високій ефективності навчання та підвищення кваліфікації персоналу, що дає змогу розробити пропозиції щодо вдосконалення існуючої нормативної бази та завдань для органів виконавчої влади України [2, с. 97].

Разом з тим, вчені С. Бєлай, І. Євтушенко та В. Мацюк у своєму дослідженні надають пропозиції щодо розвитку спеціалізації «Захист критичної інфраструктури та її стійкість», практичні рекомендації в контексті розвитку створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури щодо розвитку державно-приватного партнерства, а також пропонують проводити міжвідомчі командно-штабні, тактико-спеціальні навчання, спільні тренування та заняття [3, с. 342].

Здійснений аналіз не вичерпує результати усіх досліджень щодо професійної підготовки фахівців для сфери захисту критичної інфраструктури. Натомість роботи вищезазначених науковців ще раз підкреслюють затребуваність та актуальність сфери підготовки таких фахівців, реалізація та впровадження якої стане значним кроком вперед у забезпеченні національної безпеки України.

Формулювання цілей статті (постановка завдання). Метою статті є розгляд концептуальних та методологічних засад формування державної політики підготовки кадрів для сфери захисту критичної інфраструктури.

Виклад основного матеріалу дослідження. Відзначаючи головуючу роль вищої освіти як суттєвої сили для формування образу високорозвинутого суспільства, у тому фахівців у сфері захисту критичної інфраструктури, зважаючи на те, що потреба у таких фахівцях є надзвичайно актуальною та з подальшим розвитком ІТ-суспільства буде ще більше зростати, необхідно зазначити, що розвиток якісної освіти й науки потребує узгодженого вирішення відповідних теоретично-практичних завдань для сфери захисту критичної інфраструктури. В умовах ведення бойових дій на території України, становлення її як демократичної та незалежної держави, прагнення щодо вступу до євроатлантичних та європейських структур, кількість різноманітних загроз і небезпек, спрямованих проти України, суттєво збільшуються. Враховуючи зазначене, проблематика національної безпеки стає найактуальною та гостро ставить питання про розвиток системи підготовки фахівців для сфери захисту критичної інфраструктури.

Процес професійної підготовки фахівців для сфери захисту критичної інфраструктури в Україні на сьогоднішній день проходить період становлення та потребує досліджень і відповідної стандартизації. На наш погляд, аналіз чинних нормативно-правових актів і напрацювань сучасних науковців у сфері захисту критичної інфраструктури, враховуючи деякі прогалини у законодавстві, надасть змогу охарактеризувати систему підготовки кадрів для сфери захисту критичної інфраструктури, дати їй визначення, сформулювати таке поняття, як кібернавчання, розкрити дефініцію «фахівець сфери захисту критичної інфраструктури», що у подальшому дозволить визначити основні шляхи удосконалення підготовки професіоналів обраного профілю.

Система підготовки кадрів у будь-якій сфері діяльності завжди буде унікальною. На профіль, конфігурацію та функціонування такої системи впливає цілий комплекс відповідних чинників: від особливостей законодавства до розподілу повноважень між державними органами, від менталітету та рівня освіти співробітників (населення) до їх комп'ютерної грамотності, від суспільної (громадської) та соціальної відповідальності до розвитку державно-приватного партнерства у цій сфері тощо. При цьому комплексний характер завдань, пов'язаних зі створенням такої системи, вимагає забезпечення постійних потреб у навчанні в широкому діапазоні цільових аудиторій, створення перспектив та можливостей як для розповсюдження серед співробітників опорних і базових понять та знань (підвищення інформованості), так і отримання додаткової вищої освіти.

На національному рівні Закон України від 16 листопада 2021 року № 1882-IX «Про критичну інфраструктуру» [4], Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р [5], а також Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, затверджений постановою Кабінету

Міністрів України від 11 листопада 2020 року № 1176 [6], є основними документами, в яких вперше згадується про запровадження системи підготовки кадрів для сфери захисту критичної інфраструктури.

Так, відповідно до Закону України від 16 листопада 2021 року «Про критичну інфраструктуру» державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури, здійснюють, у тому числі, організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури. Крім цього, державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється також шляхом створення системи підготовки кадрів для сфери захисту критичної інфраструктури. Саме цей документ, що має, на наш погляд, теоретично-практичне направлення, можна вважати точкою відліку у сфері підготовки фахівців національної системи захисту критичної інфраструктури.

Разом з тим, Концепцією створення державної системи захисту критичної інфраструктури, схваленою розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р, яка визначає основні напрями, механізми і строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління у сфері захисту критичної інфраструктури, передбачено створення на загальнодержавному рівні системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури.

Крім цього, відповідно до Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, затвердженого постановою Кабінету Міністрів України від 11 листопада 2020 року № 1176, міжвідомча робоча група з питань проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, готує пропозиції

щодо шляхів і напрямів вдосконалення системи підготовки кадрів та науково-технічної підтримки розвитку національної системи кібербезпеки.

Зазначимо, що зміст будь-якого явища – це його сутність, внутрішня особливість, отже, зміст національної системи захисту критичної інфраструктури і становитимуть її певні ознаки та особливості. Як тлумачить словник сучасної української мови, під системою розуміється сукупність будь-яких елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням [7, с. 368]. Таким чином, наприклад, під системою підготовки кадрів для сфери захисту критичної інфраструктури буде матися на увазі сукупність органів (підрозділів, формувань), які задіяні у забезпеченні національної системи захисту критичної інфраструктури.

Продовжуючи дослідження, охарактеризуємо систему підготовки кадрів для сфери захисту критичної інфраструктури, зіставляючи її з основними складовими системи освіти України, яка на теперішній час переживає процес глибинної трансформації в умовах розвитку цифрового суспільства.

Система освіти України, як і кожна суспільно-економічна система, базується на трьох основних складниках: інституційна складова (перш за все, нормативно-правове забезпечення); мережа закладів освіти, органи управління у сфері освіти, інші учасники освітньої діяльності, які забезпечують функціонування системи; механізми та інструментарій регулювання відносин між всіма зацікавленими сторонами [8].

Інституційна складова на теперішній час системи підготовки кадрів для сфери захисту критичної інфраструктури запроваджується, перебуває на етапі становлення і розвитку, та складається поки що з вищезазначених нормативно-правових документів. Враховуючи багатовекторність, різноманітність та різнобічність сфери захисту критичної інфраструктури, підготовка здобувачів вищої освіти для зазначеної сфери здійснюється майже за всіма галузями знань і спеціальностями, які передбачені в Україні (постанова Кабінету Міністрів України від 29 квітня 2015 року № 266 «Про затвердження переліку галузей

знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» [9]) (таблиця 1).

Таблиця 1. Інформація щодо підготовки здобувачів вищої освіти для сфери захисту критичної інфраструктури

Найменування галузі знань	**Найменування спеціальності**	**Сектор критичної інфраструктури**	**Кількість закладів освіти, що провадять освітню діяльність**
Культура, мистецтво та гуманітарні науки	B14 Організація соціокультурної діяльності	Соціальний захист	24
Соціальні науки, журналістика, інформація та міжнародні відносини	C5 Соціологія	Соціальний захист	24
	C7 Журналістика	Інформаційний сектор	51
Бізнес, адміністрування та право	D1 Облік і оподаткування	Фінансовий сектор	9
	D2 Фінанси, банківська справа, страхування та фондовий ринок		
	D4 Публічне управління та адміністрування	Інформаційний сектор	51
	D8 Право	Правосуддя	18
Природничі науки, математика та статистика	E2 Екологія	Охорона навколишнього природного середовища	45
Інформаційні технології	F2 Інженерія програмного забезпечення	Цифрові технології	33
		Захист інформації	49
	F3 Комп’ютерні науки	Цифрові технології	33
		Захист інформації	49
	F4 Системний аналіз та наука про дані	Цифрові технології	33
		Захист інформації	49
	F5 Кібербезпека та захист інформації	Цифрові технології	33
		Захист інформації	49
	F6 Інформаційні системи і технології	Цифрові технології	33
		Захист інформації	49
	F7 Комп’ютерна інженерія	Цифрові технології	33
		Захист інформації	49

Продовження таблиці 1.

Найменування галузі знань	**Найменування спеціальності**	**Сектор критичної інфраструктури**	**Кількість закладів освіти, що провадять освітню діяльність**
Інженерія, виробництво та будівництво	G1 Хімічні технології та інженерія	Промисловість	22
	G2 Технології захисту навколишнього середовища	Охорона навколишнього природного середовища	45
	G3 Електрична інженерія	Охорона навколишнього природного середовища	45
		Промисловість	22
	G4 Енерговиробництво	Охорона навколишнього природного середовища	45
		Промисловість	22
	G5 Електроніка, електронні комунікації, приладобудування та радіотехніка	Цифрові технології	33
		Промисловість	22
	G6 Інформаційно-вимірювальні технології	Цифрові технології	33
		Промисловість	22
	G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка	Цифрові технології	33
		Промисловість	22
	G10 Металургія	Паливно-енергетичний сектор	21
		Промисловість	22
	G11 Машинобудування	Паливно-енергетичний сектор	21
		Промисловість	22
	G12 Авіаційна та ракетно-космічна техніка	Паливно-енергетичний сектор	21
		Промисловість	22
	G13 Харчові технології	Харчова промисловість та агропромисловий комплекс	39
	G14 Деревообробні та меблеві технології	Промисловість	22
	G15 Технології легкої промисловості		
	G16 Гірництво та нафтогазові технології	Паливно-енергетичний сектор	21
	G17 Архітектура та містобудування	Промисловість	22
	G20 Видавництво та поліграфія		
	G21 Біотехнології та біоінженерія	Охорона здоров'я	18
	G22 Біомедична інженерія		

Продовження таблиці 1.

Найменування галузі знань	**Найменування спеціальності**	**Сектор критичної інфраструктури**	**Кількість закладів освіти, що провадять освітню діяльність**
Сільське, лісове, рибне господарство та ветеринарна медицина	H1 Агрономія	Харчова промисловість та агропромисловий комплекс	39
	H2 Тваринництво	Харчова промисловість та агропромисловий комплекс	39
	H7 Агроінженерія		
Охорона здоров'я та соціальне забезпечення	I1 Стоматологія	Охорона здоров'я	18
	I2 Медицина		
	I3 Педіатрія		
	I4 Медична психологія		
	I5 Медсестринство		
	I6 Технології медичної діагностики та лікування		
	I7 Терапія та реабілітація		
	I8 Фармація		
	I9 Громадське здоров'я		
	I10 Соціальна робота та консультування	Соціальний захист	24
	I11 Дитячі та молодіжні служби		
Транспорт та послуги	J5 Морський та внутрішній водний транспорт	Транспорт і пошта	56
	J6 Авіаційний транспорт		
	J7 Залізничний транспорт		
	J8 Автомобільний транспорт		
Безпека та оборона	K1 Державна безпека	Сектор оборони	22
	K2 Безпека державного кордону		
	K3 Національна безпека		
	K4 Управління інформаційною безпекою	Сектор оборони	22
		Інформаційний сектор	51
	K5 Військове управління	Сектор оборони	22
	K6 Забезпечення військ (сил)		
	K7 Озброєння та військова техніка		
	K8 Пожежна безпека	Цивільний захист населення і територій	3
	K9 Правоохоронна діяльність	Сектор громадської безпеки	15
		Правосуддя	18
		Виконання кримінальних покарань	18
	K10 Цивільна безпека	Цивільний захист населення і територій	3

Джерело: авторська розробка

Органом управління для закладів вищої освіти є, звісно, Міністерство освіти і науки України незалежно від того, чи перебувають такі заклади у прямому підпорядкуванні чи у сфері управління Міністерства. Відповідно до статті 52 Закону України «Про освіту» [10] учасниками освітнього процесу у закладах вищої освіти є наукові, науково-педагогічні та педагогічні працівники; здобувачі вищої освіти та інші особи, які навчаються у закладах вищої освіти; фахівці-практики, які залучаються до освітнього процесу на освітньо-професійних програмах та інші працівники закладів вищої освіти. Не дивлячись на те, що протягом останніх років (в умовах воєнного стану) як прийом так і випуск студентів за спеціальностями, які можна віднести до секторів критичної інфраструктури, знизився, є всі передумови стверджувати, що система підготовки кадрів для сфери захисту критичної інфраструктури у переважній більшості забезпечується учасниками освітньої діяльності, зберігаючи при цьому відповідну затребуваність у таких учасниках.

Серед механізмів системи освіти України сучасні науковці виділяють механізми удосконалення розвитку освіти (кадрово-мотиваційний, організаційно-функціональний, нормативно-правовий) та інтегровані механізми розвитку освіти (міжнародного співробітництва, стратегічного фінансування, науково-освітньої локалізації), які при комплексному застосуванні формують державну освітню політику. Інструментами реалізації вищезазначених механізмів визнано засоби, прямі і непрямі форми, методи та прийоми, використовуючи які держава послідовно і систематично впливає на кон’юнктуру ринку освітніх послуг і діяльність закладів вищої освіти з метою підтримки оптимальних організаційних, соціальних, педагогічних, правових, кадрових, матеріально-фінансових та інших умов їх розвитку, забезпечення високоякісних освітніх послуг, рівного доступу до освіти, інтеграції української освітньої сфери у європейський простір [11].

Не зважаючи на те, що нормативно-правова база у зазначеному аспекті перебуває на етапі становлення, а також враховуючи те, що механізми та інструменти системи освіти України, які мають як теоретичне, так і практичне

значення, можуть так само застосовуватися і в системі підготовки кадрів для сфери захисту критичної інфраструктури, слід констатувати, що система, яка досліджується, заснована відповідно до чинного законодавства та перебуває на початковому шляху її розбудови.

Стаття 1 Закону України «Про освіту» визначає систему освіти як сукупність складників освіти, рівнів і ступенів освіти, кваліфікацій, освітніх програм, стандартів освіти, ліцензійних умов, закладів освіти та інших суб'єктів освітньої діяльності, учасників освітнього процесу, органів управління у сфері освіти, а також нормативно-правових актів, що регулюють відносини між ними [10].

Зважаючи на охарактеризовану систему підготовки кадрів для сфери захисту критичної інфраструктури, сутність захисту критичної інфраструктури в системі національної безпеки України, а також наявну в актах законодавства термінологічну базу щодо забезпечення захисту критичної інфраструктури в Україні, нами пропонується така узагальнювальна дефініція зазначеної системи: *система підготовки кадрів для сфери захисту критичної інфраструктури – комплекс засад, принципів та складників освітньої діяльності, спрямованих на реалізацію та забезпечення сталого розвитку національної системи захисту критичної інфраструктури шляхом підготовки фахівців в обсязі, необхідному для забезпечення потреб суб'єктів національної системи захисту критичної інфраструктури та підвищення компетентності населення України та фахівців різних сфер діяльності з питань захисту критичної інфраструктури.*

Сучасна інформатизація українського суспільства суттєво вплинула на всі складові системи вищої освіти, яка активно впроваджує ІТ-технології сучасності в науково-навчальний процес з метою пошуку та впровадження нових можливостей використання останніх світових досягнень у галузі електронних комунікацій для підвищення якості освітньо-педагогічного процесу. Аналіз педагогічної реальності використання можливостей освітньо-навчального простору показує його пряму залежність від сучасних

інформаційно-комунікаційних технологій. І якщо формальна вища освіта (здобуття ступенів вищої освіти, наукових ступенів, підвищення кваліфікації) має ознаки спеціально організованого та захищеного інформаційно-комунікаційного та педагогічного середовища, то неформальна освіта (здобуття ступеня вищої освіти за іншою спеціальністю, навчання за програмами тематичних (фахових) постійно діючих і короткострокових семінарів (тренінгів, спеціалізованих короткострокових курсів), стажування, наставництво) й інформальна освіта (самоосвіта) фактично залишаються беззахисними об’єктами впливу під час використання мережі Інтернет або соціальних мереж і часто потрапляють у пастки кіберзлочинців. На наш погляд зазначена проблема потребує міждисциплінарного аналізу й обговорення, у тому числі в інтересах сфери захисту критичної інфраструктури.

На підґрунтях формування та виконання заходів Національної програми інформатизації, спрямованих, у тому числі, на реалізацію завдань із створення та модернізації об’єктів критичної інформаційної інфраструктури, захисту інформації та кіберзахисту, а також засад забезпечення кібербезпеки України, за яких забезпечується кібербезпека об’єктів критичної інфраструктури, у науковців сформувалось нове поняття «кібернавчання», яке має різні смислові характеристики, відрізняється своєю багатомірністю, але не має офіційного визначення у чинній нормативно-правовій базі. Формування глобального кібернетичного суспільства з притаманними йому кібермовою, кіберкультурою, кібермисленням, криптовалютою вже стало очевидним. Тож нагального дослідження потребують питання підвищення обізнаності співробітників і зменшення ризиків людських помилок, створення надійної основи для кіберстійкості держави та суспільства в умовах широкомасштабної війни російської федерації проти України та її агресії у глобальному кіберпросторі.

У цьому аспекті можна погодитись із думкою Зінченко О.І., аспірантки кафедри політології Харківського національного університету імені В.Н. Каразіна, яка у своїй статті досліджує вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського регіону в умовах сучасних

геополітичних викликів. Науковиця зазначає, що Українська влада розвиває співпрацю з європейськими державами, сприяючи зростанню кібербезпеки на континенті, що в свою чергу, охоплює спільні навчання з кіберзахисту, обмін досвідом та технологіями у сфері кібербезпеки, а також створення спеціалізованих організацій для боротьби з кіберзагрозами. Разом з тим Зінченко О.І. зазначає, що Європейський регіон активно посилив заходи кіберзахисту, орієнтуючись на загрози, пов'язані з конфліктом в Україні. Серед ключових кроків – ЄС організовує регулярні кібернавчання, такі як Cyber Europe, що дозволяють тестувати захист критичної інфраструктури [12, с. 156].

Разом з тим, співробітники ЗС України Живило Є.О. та Черноног О.О. вивчаючи проблемні питання в підготовці складових сил оборони та безпеки України зазначають, що покращення навичок національних кібергруп швидкого реагування потрібно зосередити на: обміні інформацією про кібератаки та кіберінциденти, проведенні спільних кібероперацій та розслідуваннях міжнародних кіберзлочинів, регулярних спільних кібернавчаннях та тренінгах, обміні досвідом та найкращими практиками із відповідними підрозділами держав – членів НАТО [13, с. 19].

В свою чергу група науковців у складі В. Горлинського та Б. Горлинського, співробітників Держспецзв'язку, вивчаючи освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі зазначають, що з огляду на воєнну агресію російської федерації, посилення кібератак і озброєних нападів на об'єкти критичної інфраструктури держави і необхідності забезпечення захисту кіберпростору України в умовах постійних загроз життю і здоров'ю, постає питання щодо адаптації підготовки фахівців з кібербезпеки до професійної діяльності в умовах воєнного стану і підвищеного ризику [14, с. 272].

Підвищена увага до проблем кібернавчання для потреб сфери захисту критичної інфраструктури спостерігається і в провідних країнах світу. Це обумовлено загальною тенденцією зниження рівня професійної (спеціальної) підготовки випускників закладів вищої освіти і, насамперед, у сфері отримання

практичних навичок ефективної діяльності під час впровадження та застосування інноваційних ІТ-технологій. При цьому невід'ємною складовою забезпечення кіберзахисту та кібербезпеки суб'єктів критичної інфраструктури будь-якої держави є питання розбудови, удосконалення, поліпшення та нарощування систем наукових досліджень з цих питань. Найбільших успіхів у підготовці фахівців для потреб сфери захисту критичної інфраструктури у світі досягли США, Японія, КНР та країни – члени блоку НАТО.

Процес кіберосвіти, кібернавчання та створення в Україні дієвої системи підготовки кадрів для сфери захисту критичної інфраструктури необхідно розглядати, виходячи в першу чергу, з реалій та можливостей. Звісно, не можна не враховувати як позитивний, так і негативний досвід вищезазначених країн, у яких вже впроваджені та функціонують аналогічні системи. Тому на аналізі передового світового досвіду зі створення національної системи захисту критичної інфраструктури необхідно робити особливий акцент. Процес забезпечення кібербезпеки у кожній країні має специфічні та своєрідні особливості, які також обов'язково мають бути враховані. Тому поєднання власних ініціатив, напрацювань і досвіду, додаючи розроблену та впроваджену освітню нормативно-правову базу, треба обирати як найбільш доцільний та раціональний підхід при формулюванні такого поняття, як «кібернавчання».

Освіта є основою інтелектуального, духовного, фізичного і культурного розвитку особистості, її успішної соціалізації, економічного добробуту, запорукою розвитку суспільства, об'єднаного спільними цінностями і культурою, та держави. Метою освіти є всебічний розвиток людини як особистості та найвищої цінності суспільства, її талантів, інтелектуальних, творчих і фізичних здібностей, формування цінностей і необхідних для успішної самореалізації компетентностей, виховання відповідальних громадян, які здатні до свідомого суспільного вибору та спрямування своєї діяльності на користь іншим людям і суспільству, збагачення на цій основі інтелектуального, економічного, творчого, культурного потенціалу Українського народу,

підвищення освітнього рівня громадян задля забезпечення сталого розвитку України та її європейського вибору [10].

Схожі завдання, цілі і мету ставить перед собою суспільство, громадськість, сучасність, та, звісно, держава щодо трансформації багатьох освітніх аспектів і процесів, які вже за своєю сутністю є віджилими та навіть неефективними, але які досі присутні у галузі освіти, у більш сучасно-новітні та технологічні з використанням інформаційно-комунікаційних та ІТ-технологій, стрімкий розвиток та поширення яких вже сьогодні впливають на розвиток і життєдіяльність будь-якої людини, галузі, у тому числі сфери захисту критичної інфраструктури.

Аналіз вітчизняних і зарубіжних наукових розвідок показує, що протягом останніх 10 років сучасні вчені, науковці та учасники освітнього процесу до поняття «навчання» здебільшого додають слово «cyber» (кібер), що за своєю суттю пов'язане з використанням ІТ-технологій і комп'ютерної техніки, тобто пов'язане з кіберпростором та кіберсередовищем. І такі зміни та новації не можливо ігнорувати, так як високотехнологічне виробництво та модернізація усіх галузей економіки, у тому числі галузі освіти в умовах воєнного стану, за допомогою інформаційно-комунікаційних та цифрових технологій, вже є пріоритетом економічного розвитку та піднесення України.

Сьогодні у світової та європейської освітньої спільноти є всі підстави стверджувати, що ІКТ – це у переважній більшості освітні та навчальні технології, які вже на повну силу та потужність почали демонструвати свої освітньо-навчальні можливості із використанням програмних і технічних засобів (кіно-, аудіо-, відеозаписи, комп'ютери, телекомунікаційні мережі) задля організації, забезпечення та підтримки навчальних, комунікаційних та інформаційних освітніх процесів, як в теоретичному, так і практичному аспектах.

Слід звернути увагу і на те, що запровадження новітніх елементів та понять у процес сучасної ІТ-освіти передбачається на всіх рівнях освітньо-навчального процесу. Останніми роками і, напевно, найчастіше під час

службової (робочої) діяльності або в мас-медіа ми чуємо такі слова та словосполучення, як «воркшоп», «івент», «вебінар», «кібертренер», «кібертренінг», «медіаосвіта», «онлайн – платформа», «хакатон», «корпоративний блог» та інші, які так чи інакше ми у нашій уяві пов'язуємо із новими методами та формами навчання у сфері кібернетичної освіти. І хоча нормативно-правових або організаційно-розпорядчих актів, які б на рівні держави або державних органів тлумачили такі дефініції поки що немає, за допомогою таких новацій як в України, так і у всьому світі здійснюється підвищення рівня та якості знань громадян цифровій грамотності, а також формування їх освітніх компетентностей та навичок, що безумовно відноситься до такого поняття, як кібернавчання.

Таким чином, узагальнюючи трактування терміну «кібернавчання», визначимо особливості, що йому притаманні: постійне зростання можливостей впливу на складові кібернетичних систем; необхідність постійного оновлення знань з питань кібербезпеки, кіберзахисту об'єктів критичної інфраструктури; швидка зміна електронних, кібернетичних та інфокомунікаційних технологій; особливості курсу кібербезпеки та кіберзахисту; велика кількість специфічних складових кібербезпеки, кіберзахисту об'єктів критичної інфраструктури; різні

рівні здатності та готовності до навчання тих, хто навчається, у тому числі і дистанційного.

Враховуючи зазначене, першочерговими завданнями кібернавчання необхідно визнати: формування та впровадження ґрунтовної національної політики цифровізації освіти як пріоритетної складової частини реформи освіти та розбудови сфери захисту критичної інфраструктури; створення відповідних цифрових освітянських ІТ-платформ для використання у навчальному процесі, у тому числі у сфері захисту критичної інфраструктури; визначення конкретних ініціатив підключення освітніх класів до широкосмугового Інтернету; підготовка, адаптація та організація доступу до мультимедійних технологій, а

також створення та реалізація сучасних моделей забезпечення студентів та закладів освіти комп'ютерними засобами.

Враховуючи думки кола вчених, науковців, особливості та першочергові завдання кібербезпеки, кіберзахисту, у тому числі в інтересах суб'єктів національної системи захисту критичної інфраструктури, нами пропонується така узагальнювальна дефініція: *кібернавчання – використання цифрових платформ, впровадження нових освітніх та інформаційних технологій, застосування передових форм організації освітнього та навчального процесу, а також сучасних навчально-методичних матеріалів, які в сукупності є основою для всебічного розвитку людини та добробуту населення в цілому.* Таке формулювання стане можливим лише тоді, коли ідеї, дії, ініціативи та відповідні програми, які стосуються розвитку сфери кіберзахисту та сфери захисту критичної інфраструктури, будуть інтегровані та впроваджені, зокрема, в національні, регіональні, галузеві, відомчі стратегії і програми розвитку кібернетичної освіти та національної системи захисту критичної інфраструктури.

У рамках дослідження доречно звернутися також до поняття «фахівець сфери захисту критичної інфраструктури», тому що саме такий фахівець є як суб'єктом, так і об'єктом державної політики у сфері захисту критичної інфраструктури одночасно. Так, науковці Держспецзв'язку та науково-дослідного інституту воєнної розвідки Б. Ніколаєнко, А. Місюра, А. Сторчак та П. Дімітров вивчаючи деякі аспекти підготовки фахівців для сфери захисту критичної інфраструктури зазначають, що якісно підготовлені фахівці, володіючи необхідними знаннями, навичками та відповідними компетенціями, повинні вирішувати складні комплексні завдання забезпечення безпеки та стійкості критичної інфраструктури. Вчені акцентують свою увагу на те, що таким 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 [15, с. 105].

Науковці Національного інституту стратегічних досліджень Суходоля О.М. та Кравченко С.О. вивчаючи спеціальні компетентності випускників магістерської програми в сфері захисту критичної інфраструктури за спеціальністю 281 (на теперішній час – D 4), визначені на основі положень Закону України «Про критичну інфраструктуру», наголошують, що такі фахівці по закінченню відповідного закладу освіти повинні мати здатність:

– аналізувати державну політику в сфері захисту критичної інфраструктури та її окремих секторах, розробляти рішення щодо політики та механізми їх впровадження;

– організовувати діяльність суб'єктів національної системи захисту критичної інфраструктури та забезпечувати їх взаємодію відповідно до вимог чинної нормативно-правової бази;

– надавати експертну оцінку нормативно-правовим актам та самостійно готувати їх проєкти в даній сфері;

– застосовувати сучасну методологію аналізу та оцінювання захищеності, ризиків і загроз на національному, секторальному, місцевому, об'єктовому рівні критичної інфраструктури;

– визначати потреби та планувати заходи щодо захисту та забезпечення стійкості критичної інфраструктури, життєво важливих функцій та послуг;

– розробляти та застосовувати механізми регулювання діяльності операторів критичної інфраструктури [16, с. 167].

В свою чергу кандидат юридичних наук Теленик С.С. досліджуючи напрями підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури приходить до висновку, що питання забезпечення безпеки та стійкості критичної інфраструктури є чи не найголовнішим для національної безпеки держави. Значною мірою воно залежить від професіоналізму, рівня освіченості кадрів у галузі, що своєю чергою стане запорукою безперебійної роботи об'єктів критичної інфраструктури та галузі в цілому [2, с. 97].

У процесі тлумачення зазначених понять з метою визначення сутності термінів «фах», «фахівець» і «спеціаліст» звернемося до Великого тлумачного словника сучасної української мови, де пояснюється, що «фах – вид заняття, трудової діяльності, що вимагає певної підготовки і є основним засобом до існування; професія…. основна кваліфікація, спеціальність», а фахівець – це той, хто досконало володіє якимсь фахом, має високу кваліфікацію, глибокі знання з певної галузі науки, техніки, мистецтва тощо; спеціаліст [17, с. 1530]. Тоді як спеціаліст – це той, хто досконало володіє певною спеціальністю, має глибокі знання в якій-небудь галузі науки, техніки, мистецтва тощо; фахівець. Це той, хто досяг високої майстерності в чому-небудь, знавець чогось [17, с. 1364].

Так, доктор фізико-математичних наук Джалладова І.А., професор кафедри комп'ютерної математики та інформаційної безпеки Київського національного економічного університету імені Вадима Гетьмана, здійснюючи історичний огляд підготовки фахівців з інформаційної безпеки, підкреслює, що компетентний фахівець зобов'язаний стати еталоном суб'єкта безпечної інформаційної діяльності і при цьому знатися на питаннях інформаційної безпеки в усіх аспектах: юридичних, психологічних, соціально-історичних, педагогічних, програмно-технічних. Адже інформація (інформаційні ресурси, цінності) та її інфраструктура – це та основа, з якою їм доведеться працювати і жити в XXI столітті [18, с. 64].

Ще одна група вчених у складі С. Голованя, С. Лєнкова, В. Дорошка та Л. Щербака визначають кваліфікаційні вимоги до фахівця (спеціаліста) з інформаційної безпеки, зазначаючи, що окрім суто спеціальних знань, пов'язаних із механізмом захисту, він повинен володіти знаннями про об'єкт (предмет) захисту та ефективність застосування даного механізму. Так, фахівець (спеціаліст) з інформаційної безпеки повинен оволодіти знаннями не тільки зі своєї галузі, але й суміжних галузей. Фахівець (спеціаліст) з управління системою обробки інформації, крім спеціальних знань з теорії управління, повинен оволодіти знаннями технологій обробки інформації та

механізмів її захисту. Фахівець (спеціаліст) з проєктування повинен оволодіти ґрунтовними спеціалізованими знаннями. Така відмінність вимагає здійснення класифікації фахівців/спеціалістів з урахуванням їхнього функціонального включення в систему та розуміння певних базових знань, що ґрунтуються на загальносистемних закономірностях [19, с. 47].

Науковець Пашорін В.І., визначивши співвідношення між категоріями «інформаційна безпека» та «кібербезпека», зазначає про суттєві розбіжності в сфері застосування зазначених понять, а також наголошує на тому, що фахівець з інформаційної безпеки, виходячи з визначення, може навіть не розумітися в ІТ-технологіях так, як фахівець з кібербезпеки. При цьому вчений акцентує увагу на тому, що відрізнити спеціаліста з кібербезпеки від спеціаліста з інформаційної безпеки можна за сертифікацією. Сертифікацій на тему кібербезпеки та інформаційної безпеки у світі величезна кількість, але є декілька найпоширеніших та найбільш популярних. Для спеціалістів з кібербезпеки це такі сертифікати: CEH (Certified Ethical Hacker), CISSP (Certified Information System Security Professional), CCSP (Cisco Certified Security Professional). У спеціалістів з інформаційної безпеки поширеними є сертифікати CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), ISO 27001 Lead Implementer, а також ISO 27001 Lead Auditor [20, с. 28–29].

Вчений Бобро Д.Г. вивчаючи методологію оцінки рівня критичності об’єктів інфраструктури, враховуючи досвід провідних країн світу, а також роботи українських фахівців щодо захисту критичної інфраструктури, приходить до висновку про створення Національного центру з питань захисту критичної інфраструктури та мережі галузевих (територіальних) ситуаційних центрів, фахівці якого мають оцінювати загрози та ризики критичній інфраструктурі, формувати перелік та проводити ранжування об’єктів інфраструктури за їх критичністю, розробляти плани реагування та оцінювати ефективність їх виконання [21, с. 84].

Група науковців Грицюк Ю.І. та Рак Т.Є., досліджуючи процес забезпечення інформаційної безпеки структурних підрозділів МНС України, дійшли висновку, що найбільш важливими напрямами діяльності фахівців із захисту інформації є: спостереження, аналіз, оцінювання та прогнозування джерел загроз і рівнів їх небезпек, ступеня внутрішньої та зовнішньої уразливості; відпрацювання стратегії та тактики захисту інформації, планування попередження нападу, укріплення потенційними зв'язками, варіювання мережевими ресурсами забезпечення інформаційної безпеки; відбір сил і засобів протидії, нейтралізації та недопущення інформаційних атак, мінімізації шкоди від них; протистояння джерелам загроз природного, технічного або антропогенного характеру системам забезпечення інформаційної безпеки; управління наслідками інциденту (від інформаційних атак, інформаційних операцій, інформаційних воєн).

В умовах воєнного стану сфера захисту критичної інфраструктури перетворюється на одне з найактуальніших завдань Уряду. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим від значних кібернетичних впливів, які все частіше стають ефективним інструментом російської федерації на шляху досягнення мети щодо несилового контролю та управління як об'єктами критичної інфраструктури держави, підприємств, установ, організацій, так і окремо взятими громадянами, їх об'єднаннями.

Аналіз наукових напрацювань і досліджень у сфері захисту критичної інфраструктури, кібер- та інформаційної безпеки дозволяє конкретизувати сутнісне значення дефініції «фахівець сфери захисту критичної інфраструктури», яке вбачається сформулювати таким чином: *фахівець сфери захисту критичної інфраструктури – це спеціаліст галузі, яка є важливою для економіки та національної безпеки і оборони, який досконало володіє технологією побудови державної системи захисту критичної інфраструктури, теорією проєктування, моделювання та конструювання систем управління доступом, комп'ютерних та інформаційних систем, об'єктів і ресурсів, які є*

критично важливими для функціонування суспільства, соціально-економічного розвитку держави, а також підходами, засобами та технологіями захисту та стійкості критичної інфраструктури, адміністрування систем та мереж.

Вичерпно сформульована та детермінована термінологія є першим кроком, що допоможе фахівцям сфери захисту критичної інфраструктури виконувати їх головне професійне завдання – забезпечення функціювання національної системи захисту критичної інфраструктури. Тому вже на етапі підготовки таких фахівців важливо ведення та підтримка всіма суб'єктами освітнього процесу єдиного тезауруса сфери захисту критичної інфраструктури.

Висновки та перспективи подальших розвідок у даному напрямі. Експертні дослідження свідчать, що в сучасному світі підготовка кадрів у сфері захисту критичної інфраструктури не може обмежуватися лише отриманням вищої освіти у закладах освіти за відповідною спеціальністю. Для збереження належної конкурентоспроможності та професійного рівня цим фахівцям необхідно перманентно підвищувати свою кваліфікацію на засадах так званої концепції безперервної освіти (або «освіти протягом життя»), множинність форм та методів якої відкриває ще один широкий та перспективний напрям для галузевого кібербезпекового державно-приватного партнерства [22, с. 24].

Отже, понятійно-категоріальний апарат підготовки кадрів для сфери захисту критичної інфраструктури є тією ланкою, яка створює передумови розвитку процесу підготовки кадрів, підвищення їх кваліфікації в цьому напрямі з урахуванням усіх аспектів діяльності та сфер життя держави, у тому числі в галузі міжнародного співробітництва, та має здійснюватися на інтеграційних засадах кореляції всіх складників кібернетичної безпеки.

Література

1. Євсєєв В. О. Модель підготовки кадрів у сфері захисту критичної інфраструктури в системі вищої освіти. *Наукове видання «Честь і закон»*. 2024. № 4(91).

2. Теленик С. С. Напрями підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури. *Правові новели*. 2020. № 10(2). С. 91–99.

3. Бєлай С. В. Теоретико-методологічні засади підготовки кадрів у сфері захисту критичної інфраструктури України. *Вісник Національного університету цивільного захисту України. Серія : Державне управління.* 2021. № 2. С. 342–350.

4. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 27.04.2025. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 27.04.2025).

5. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. Дата оновлення: 27.04.2025. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 27.04.2025).

6. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : постанова Кабінету Міністрів України від 11.11.2020 р. № 1176. Дата оновлення: 27.04.2025. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (дата звернення: 27.04.2025).

7. Єрошенко О. О. *Великий тлумачний словник сучасної української мови* / ред. О. О. Єрошенко. Донецьк, ТОВ «Глорія Трейд», 2012. 864 с.

8. Освіта в Україні: базові індикатори. Інформаційно-статистичний бюлетень. URL: https://mon.gov.ua/storage/app/media/nova-ukrainska-shkola/1serpkonf-informatsiyniy-byuleten.pdf (дата звернення: 27.04.2025).

9. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти : постанова Кабінету Міністрів України від 29.04.2015 р. № 266. Дата оновлення: 27.04.2025. URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF (дата звернення: 27.04.2025).

10. Про освіту : Закон України від 05.09.2017 р. № 2145-VIII. Дата оновлення: 27.04.2025. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 27.04.2025).

11. Якайтіс І. Б. Механізми державного управління інноваційним розвитком вищої освіти в Україні : автореф. дис…. канд. наук. з держ. упр. : 25.00.02. Івано-Франківськ, 2018. 22 с.

12. Зінченко О. І. Вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського регіону. *Політикус*. 2024. № 5. С. 154–158.

13. Живило Є. О. Міжнародні кібернавчання Locked Shields – 2022. Проблемні питання в підготовці складових сил оборони та безпеки України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 1. С. 19–24.

14. Горлинський В. Освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі. *Information Technology and Security*. 2024. № 12 (2). С. 268–282.

15. Ніколаєнко Б. Підготовка фахівців як один з аспектів стійкості критичної інфраструктури. *Information Technology and Security*. 2024. № 12 (1). С. 102–112.

16. Суходоля О. М. Загальні підходи до розробки освітніх програм у сфері захисту критичної інфраструктури за спеціальністю «Публічне управління та адміністрування». *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування.* 2024. № 35 (74). С. 164–171.

17. Бусел В. Т. *Великий тлумачний словник сучасної української мови* / ред. В. Т. Бусел. Київ, Перун, 2005. 1728 с.

18. Джалладова І. А. Політика інформаційної безпеки: науково-прикладні аспекти і проблеми підготовки фахівців. *Моделювання та інформаційні системи в економіці.* 2015. № 91. С. 57–75.

19. Бистрова Б. В. Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США : дис. ... канд. пед. наук : 13.00.04 / Інст. пед. освіти і освіти дорос. НАПН України. Київ, 2018. 254 с.

20. Пашорін В. І. Термінологічні та освітні аспекти кібербезпеки. *Безпека соціально-економічних процесів в кіберпросторі* : матеріали Всеукр. наук.-практ. конф., м. Київ, 27 берез. 2019 р. Київ, 2019. 244 с. С. 28–30.

21. Бобро Д. В. Методологія оцінки рівня критичності об'єктів інфраструктури. *Стратегічні пріоритети*. 2016. № 3. С. 77–85.

22. Арсенович Л. А. Шляхи формування рівня цифрової компетентності фахівців у сфері кібербезпеки в умовах розвитку цифрового суспільства. *Наукові інновації та передові технології (Серія «Державне управління»): журнал.* 2022. № 3(5). С. 10–26.

References

1. Yevseev, V.A. (2024), "Model of personnel training in the field of critical infrastructure protection in the higher education system", *Naukove vydannia «Chest i zakon»*, vol. 4(91).

2. Telenyk, S.S. (2020), "Areas of training and advanced training of critical infrastructure protection specialists", *Pravovi novely,* vol. 10(2), pp. 91–99.

3. Bielai, S.V. (2021), "Theoretical and methodological principles of personnel training in the field of protection of critical infrastructure of Ukraine", *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriia : Derzhavne upravlinnia*, vol. 2, pp. 342–350.

4. 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 27.04.2025).

5. Cabinet of Ministers of Ukraine (2017), Order "On the approval of the Concept of creating a state system for the protection of critical infrastructure", available at: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (Accessed 27.04.2025).

6. Cabinet of Ministers of Ukraine (2020), Resolution "On the approval of the Procedure for conducting a review of the state of cyber protection of critical information infrastructure, state information resources and information, the

requirement for the protection of which is established by law", available at: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (Accessed 27.04.2025).

7. Yeroshenko, O.O. (2012), *Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy* [A large explanatory dictionary of the modern Ukrainian language], TOV "Hloriia Treid", Donetsk, Ukraine.

8. The official website of the Ministry of Education and Science of Ukraine (2018), "Education in Ukraine: basic indicators. Informational and statistical bulletin", available at: https://mon.gov.ua/storage/app/media/nova-ukrainska-shkola/1serpkonf-informatsiyniy-byuleten.pdf (Accessed 27.04.2025).

9. Cabinet of Ministers of Ukraine (2015), Resolution "On the approval of the list of fields of knowledge and specialties for which the training of applicants for higher and professional pre-higher education is carried out", available at: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF (Accessed 27.04.2025).

10. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "About education", available at: https://zakon.rada.gov.ua/laws/show/2145-19#Text (Accessed 27.04.2025).

11. Yakaitis, I.B. (2018), "Mechanisms of state management of innovative development of higher education in Ukraine", Ph.D. Thesis, Ivano-Frankivsk, Ukraine.

12. Zinchenko, O.I. (2024), "The influence of the political situation in Ukraine on the cyber security problems of the European region", *Politykus*, vol. 5, pp. 154–158.

13. Zhyvylo, Y.O. (2022), "International cyber training Locked Shields - 2022. Problematic issues in the training of the defense and security forces of Ukraine", *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, vol. 1, pp. 19–24.

14. Horlynskyi, V. (2024), "Educational priorities for the training of cyber security specialists in the conditions of martial law in the state", *Information Technology and Security*, vol. 12(2), pp. 268–282.

15. Nikolaienko, B. (2024), “Training of specialists as one of the aspects of the stability of critical infrastructure”, *Information Technology and Security,* vol. 12(1), pp. 102–112.

16. Sukhodolia, O.M. (2024), “General approaches to the development of educational programs in the field of critical infrastructure protection in the specialty “Public management and administration””, *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia*, vol. 35(74), pp. 164–171.

17. Busel, V.T. (2005), *Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy* [A large explanatory dictionary of the modern Ukrainian language], Perun, Kyiv, Ukraine.

18. Dzhalladova, I.A. (2015), “Information security policy: scientific and applied aspects and problems of training specialists”, *Modeliuvannia ta informatsiini systemy v ekonomitsi,* vol. 91, pp. 57–75.

19. Bystrova, B.V. (2018), “Professional training of bachelors in cyber security in higher educational institutions of the USA”, Ph.D. dissertation, Inst. ped. education and adult education. NAPN of Ukraine, Kyiv, Ukraine.

20. Pashorin, V.I. (2019), “Terminological and educational aspects of cyber security”, *Bezpeka sotsialno-ekonomichnykh protsesiv v kiberprostori* [Security of socio-economic processes in cyberspace], Vseukr. nauk.-prakt. konf. [Vseukr. science and practice conf], Kyiv, Ukraine, 27 berez. 2019, pp. 28–30.

21. Bobro, D.B. (2016), “Methodology for assessing the level of criticality of infrastructure objects”, *Stratehichni priorytety,* vol. 3, pp. 77–85.

22. Arsenovych, L.A. (2022), “Ways of forming the level of digital competence of specialists in the field of cyber security in the conditions of the development of a digital society”, *Naukovi innovatsii ta peredovi tekhnolohii (Seriia «Derzhavne upravlinnia»): zhurnal,* vol. 3(5), pp. 10–26.

Стаття надійшла до редакції 29.04.2025 р.