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. 2024. № 9.

DOI: http://doi.org/10.32702/2307-2156.2024.9.5

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

ВПРОВАДЖЕННЯ ОСВІТНЬОЇ КАРТИ РОЗВИТКУ ФАХІВЦЯ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ІНСТРУМЕНТУ ПОДАЛЬШОГО РОЗВИТКУ СИСТЕМИ 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

IMPLEMENTATION OF AN EDUCATIONAL MAP FOR TRAINING AND DEVELOPMENT OF CRITICAL INFRASTRUCTURE PROTECTION SPECIALISTS AS A TOOL FOR FURTHER DEVELOPMENT OF THE CRITICAL INFRASTRUCTURE PROTECTION PERSONNEL TRAINING SYSTEM

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

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

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

Забезпечення безпеки та безперебійного функціонування об'єктів критичної інфраструктури значною мірою залежить від так званого «людського фактору». Саме рівень підготовленості фахівців, їхні компетенції, розуміння специфіки діяльності об'єктів та механізмів здійснення взаємодії багато в чому зумовлюють успіх справи в цілому. Огляд і первинна систематизація наукових праць за обраною темою дозволив встановити, що попри значний інтерес дослідників до підготовки фахівців із захисту критичної інфраструктури поза увагою вчених залишаються суттєві аспекти даного питання.

У статті автором запропоновано для подальшого впровадження освітню карту розвитку фахівця у сфері захисту критичної інфраструктури, подальше впровадження якої у освітній процес суб'єктів національної системи захисту критичної інфраструктури стане справжньою реалізацією у службову діяльність питань що стосуються єдності методологічних засад у сфері критичної інфраструктури, їх координованості, державно-приватного партнерства, безпеки, захисту та охорони інформації з обмеженим доступом,

міжнародного співробітництва, а також принципу «навчання впродовж життя» для тих фахівців, які безпосередньо забезпечують запобігання проявам несанкціонованого втручання на об'єктах критичної інфраструктури, прогнозування та запобігання кризовим ситуаціям на таких об'єктах.

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

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

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

Safety and uninterrupted operation of critical infrastructure facilities largely depends on the so-called "human factor". It is the qualification of specialists, their competences, understanding of how the facilities operate and how the interaction occurs that largely determine the overall success in this area. The study and initial systematization of scientific works dedicated to the chosen topic helped us find out that despite significant interest of researchers in the training of critical infrastructure protection specialists, essential aspects of this issue still remain outside the attention of scientists.

In the article, the author proposes an educational map for further implementation, which is designed for training and development of critical infrastructure protection specialists, and which further integration in the training process of entities of the national critical infrastructure protection system will lead to

true putting into work practice of issues related to the harmonization and consistency of critical infrastructure methodologies, their coordination, public-private partnership, security, protection and security of classified information, international cooperation, as well as the principle of "lifelong training" for those specialists who are directly involved in the prevention of unauthorized interference at critical infrastructure facilities, forecasting and prevention of emergencies at such facilities.

Ключові слова: *критична інфраструктура, національна система захисту критичної інфраструктури, освітня карта, підвищення кваліфікації, сфера захисту критичної інфраструктури.*

Keywords: *critical infrastructure, national system of critical infrastructure protection, educational map, advanced training, critical infrastructure protection.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Науково-технічний прогрес останнім часом докорінно змінив сучасне світобачення: на сьогодні, в умовах воєнного стану, інформаційні технології у поєднанні з сферою захисту критичної інфраструктури відіграють важливу роль у розвитку країни та населення. За останні роки інформація стала настільки міцним чинником розвитку громадянського суспільства, що приводить, у тому числі, до запровадження єдиних підходів до організації управління об'єктами державної системи захисту критичної інфраструктури на державному та місцевому рівні, а також до визначення засад взаємодії суб'єктів, що залучені до захисту критичної інфраструктури державних органів та суб'єктів господарювання.

В умовах повномасштабного вторгнення на територію України, швидкий розвиток та загальне впровадження сучасних інформаційних технологій у сферу захисту критичної інфраструктури, формування всеохоплюючого кіберпростору призводить до появи нових ризиків (загроз) у сферах національної безпеки, які розповсюджуються як у кіберпросторі, так і в сфері захисту критичної інфраструктури безпосередньо. Кібернетичні загрози

впливають на усі сфери громадської, суспільної діяльності (безпекову, правову, соціальну, політичну, економічну, інфраструктурну тощо), а також на сферу забезпечення безпеки критичної інфраструктури задаючи шкоди суб'єктам національної системи захисту критичної інфраструктури.

У цьому аспекті передумовою до формування ефективної та дієвої системи підготовки кадрів для сфери захисту критичної інфраструктури в умовах розвитку цифрового суспільства України буде повна й відкрита освітня взаємодія держави та приватного сектора, без якого неможливо побудувати ефективну освіту у сфері захисту критичної інфраструктури.

Аналіз останніх досліджень і публікацій. Наукові напрацювання практиків і вчених у сфері захисту критичної інфраструктури засвідчують, що професійна підготовка фахівців у зазначеній сфері є одним із напрямів державної політики у сфері національної безпеки, без якого є неможливими відновлюваність, функціональність, безперервність роботи, стійкість і цілісність критичної інфраструктури і відповідно – соціально-економічний та науково-технічний розвиток країни.

Як свідчать останні публікації та наукові дослідження, проблеми професійного розвитку фахівців для сфери захисту критичної інфраструктури є малодослідженими. Так, науковець Теленик С.С. у своїй науковій статті встановлює 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 у свою чергу, дає змогу розробити пропозиції щодо вдосконалення існуючої нормативної бази та завдань для органів виконавчої влади України [1, с. 97].

У свою чергу професор Національної академії Національної гвардії України Бєлай С.В., співробітник Інституту підготовки юридичних кадрів для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого Євтушенко І.В. та співробітник Національної академії Служби безпеки України Мацюк В.В. у своїй спільній науковій статті

пропонують пропозиції щодо розвитку спеціалізації «Захист критичної інфраструктури та її стійкість», а також надають практичні рекомендації в контексті розвитку створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури щодо розвитку державно-приватного партнерства та проведення міжвідомчих командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять [2, с. 342].

Крім цього, фахівець відділу енергетичної та техногенної безпеки Національного інституту стратегічних досліджень Кондратов С.І. у своїй аналітичній записці розглядає проблему створення системи підготовки кадрів для захисту та забезпечення стійкості критичної інфраструктури в Україні на основі передового зарубіжного досвіду та найкращих практик, сформулювавши при цьому низку конкретних рекомендацій для міністерств і відомств України [3].

Незважаючи на певну кількість досліджень, які стосуються актуальних питань підготовки фахівців у сфері захисту критичної інфраструктури, питанням підготовки кадрів для зазначеної сфери приділено мало уваги, що й обумовлює актуальність дослідження.

Формулювання цілей статті (постановка завдання). Метою статті є розгляд теоретичних підходів до удосконалення механізмів формування системи підготовки кадрів для сфери захисту критичної інфраструктури.

Виклад основного матеріалу дослідження. Відповідно до законодавства України заходи із забезпечення захисту критичної інфраструктури в умовах воєнного стану у межах своєї компетенції безпосередньо здійснюють:

– Кабінет Міністрів України, Центральна виборча комісія та Національний банк України;

– Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, Національна комісія з цінних паперів та фондового ринку та Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації;

– Апарат Ради національної безпеки і оборони України, Адміністрація Держспецзв'язку, Служба безпеки України, Збройні Сили України, інші військові формування, утворені відповідно до законів України, правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності, а також Державна служба України з надзвичайних ситуацій;

– Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом, секторальні та функціональні органи, та інші міністерства та центральні органи виконавчої влади;

– місцеві органи виконавчої влади, органи місцевого самоврядування, оператори критичної інфраструктури, а також підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Видами діяльності у сфері захисту критичної інфраструктури є:

– забезпечення безпеки та стійкості критичної інфраструктури, визначення законодавчих підходів щодо її захисту;

– впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, ліквідацію та/або мінімізацію наслідків реалізованих загроз, зниження ризику реалізації можливих загроз, кризових ситуацій та інших їх видів;

– створення системи раннього виявлення загроз критичній інфраструктурі, а також умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури;

– запровадження державно-приватного партнерства, взаємодії суб'єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури, а також забезпечення міжнародного співробітництва у зазначеній сфері.

Відповідно до Закону України «Про критичну інфраструктуру» [4], нормативно-правових актів Президента України та Кабінету Міністрів України,

суб’єкти національної системи захисту критичної інфраструктури безпосередньо забезпечують:

– запобігання проявам несанкціонованого втручання в функціонування системи захисту критичної інфраструктури та попередження кризових ситуацій, що порушують безпеку критичної інфраструктури;

– розвиток функціонування національної системи захисту критичної інфраструктури шляхом розроблення відповідної нормативно-правової та нормативно-технічної бази;

– розроблення та реалізацію державних цільових програм із захисту критичної інфраструктури, а також відповідного комплексу заходів з контролю за ризиками безпеки на об’єктах критичної інфраструктури;

– розроблення методології аналізу результативності державної політики у сфері захисту критичної інфраструктури, а також аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури;

– взаємодію національної системи захисту критичної інфраструктури з європейськими та євроатлантичними системами.

І одним із таких напрямів, який є стрижневим у всій сфері захисту критичної інфраструктури, є створення системи підготовки кадрів для сфери захисту критичної інфраструктури, який застосовується шляхом підготовки, перепідготовки, підвищення кваліфікації персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури.

На сьогодні відсутня єдина методологія в системі підготовки кадрів для сфери захисту критичної інфраструктури як на державному, так і на приватному рівнях. Відсутність методичного забезпечення навчання, єдиних освітньо-керівних документів, розбіжність у поглядах на мету, зміст та завдання підготовки з питань захисту критичної інфраструктури знижує якість підготовки фахівців у зазначеній сфері та її ефективність для всієї країни в цілому.

Крім того, рівень підготовки, перепідготовки та підвищення кваліфікації персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної

інфраструктури має ризики до послаблення через недостатню цифрову грамотність. Так, спостерігається певне гальмування процесів цифрових перетворень у країні через:

– не усвідомлення цифрових навичок та цифрової грамотності як в суспільстві, так і в органах державної влади;

– невідповідність рівня підготовки людського капіталу з питань цифрових навичок вимогам цифрової економіки та суспільства;

– відсутність нормативної бази та затвердженого стандарту цифрових компетентностей, їх дескрипторів та описів по кожній окремій галузі по сферах економічної діяльності та основних професійних групах;

– неузгодженість вимог до рівня володіння цифровими компетентностями різних категорій працівників, відсутність єдиних обґрунтованих затверджених вимог до цифрової компетентності в професійних стандартах та посадових обов'язках різних категорій працівників [5, с. 10].

При цьому на сучасному етапі розвитку освіти серед базових парадигм щодо підготовки кадрів як для сфери захисту критичної інфраструктури, так і для сектору безпеки і оборони України в цілому, є компетентнісна парадигма, яка спрямована на формування у майбутніх фахівців зазначеної сфери цифрових, стратегічних компетентностей, форсайт передбачень тощо.

Необхідність подальшої розбудови системи підготовки кадрів для сфери захисту критичної інфраструктури підкреслюють також і сучасні вчені, які вже протягом семи років з моменту схвалення Концепції створення державної системи захисту критичної інфраструктури (розпорядження Кабінету Міністрів України від 6 грудня 2017 року № 1009-р) [6], сповіщають і нагадують у наукових роботах про нагальність розвитку сфери захисту критичної інфраструктури в освітньому напрямку. Так, наприклад група науковців Національного авіаційного університету (Щербак Л.М., Гнатюк С.О., Сидоренко В.М. та Шаховал О.А.) при проведенні аналізу методів розрахунку критичності інформаційних систем зазначають, що вибір методів розрахунку критичності залежить від конкретних обставин, а саме: масштабу і складу

інформаційної системи, інформації, що обробляється в цій системі, складу і використовуваних засобів безпеки, а також наявності кваліфікованих експертів [7, с. 29].

У свою чергу вчені Ткаченко І.В., Козачок В.А., Гахов С.О. та Дмітрієв В.Є. при проведенні оцінки стану кібербезпеки об'єктів критичної інформаційної інфраструктури зазначають, що якість оцінки буде залежати від:

– визначення основного переліку індексів щодо оцінки кібербезпеки типових для даного об'єкту критичної інфраструктури, а також від здійснення збагачення (уточнення) даних моделі шляхом введення регіональних індексів;

– здійснення кореляції, виявлення залежностей між індексами та визначення дельти часу;

– застосування технології великих даних для роботи з структурованими та не структурованими даними, а також від вибору технології машинного навчання, що буде здійснювати обробку даних моделі, її тренування та перенавчання [8, с. 55].

Крім цього, група вчених у складі завідувача кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка Бурячка В.Л., професора спеціальної кафедри Національної академії Служби безпеки України Богуша В.М., професора кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка Борсуковського Ю.В., старшого викладача кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка Складанного П.М. та керівника проєктів департаменту безпеки ПАТ «Укрсоцбанк» Борсуковської В.Ю. аналізуючи професійно-орієнтовані моделі компетентностей основних суб'єктів національної системи кібербезпеки зазначають, що для виконання завдань у системі забезпечення національної системи кібербезпеки фахівці повинні бути підготовленими до здатності:

– формувати та реалізовувати державну політику щодо кіберзахисту об'єктів критичної інформаційної інфраструктури;

– забезпечувати управління аудитом інформаційної безпеки на об’єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, визначення порядку їх атестації (переатестації);

– координації, організації та проведення аудиту захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на уразливість;

– формувати вимоги щодо впровадження та використання системи безперервного навчання персоналу об’єктів критичної інформаційної інфраструктури методам та способам особистого кіберзахисту [9, с. 284–285].

Вищезазначені дослідження ще раз підтверджують, що система підготовки кадрів для сфери захисту критичної інфраструктури має враховувати вимоги теперішнього ринку праці і відповідати загальносвітовим критеріям якості та ефективності. Цього вимагає інформаційне суспільство, що характеризується активним поширенням нових ІТ-технологій, розвитком конкуренції в сфері захисту критичної інфраструктури та зростанням її ролі.

Необхідність подальшої розбудови системи підготовки кадрів для сфери захисту критичної інфраструктури підкреслюють також нещодавно прийняті нормативно-правові акти, що спрямовані на забезпечення функціонування національної системи захисту критичної інфраструктури. Так, наприклад, постановою Кабінету Міністрів України від 12 липня 2022 року № 787 [10], створено Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України, одними із основних завдань якої є забезпечення підготовки, перепідготовки, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури, а також участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури.

Слід відмітити також розпорядження Кабінету Міністрів України від 19 вересня 2023 року № 825-р «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» [11], яке

передбачає виконання заходів щодо:

– розроблення та затвердження галузевих, регіональних планів та програм з протидії загрозам критичній інфраструктурі, включаючи плани взаємодії, відновлення об’єктів критичної інфраструктури, а також плани проведення навчань та тренувань;

– затвердження секторальних програм підготовки персоналу щодо забезпечення стійкості та захисту критичної інфраструктури та проведення на постійній основі спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак;

– проведення навчань та тренінгів, підготовки та перевірки персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури;

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

Крім цього, відповідно до розпорядження Кабінету Міністрів України від 10 листопада 2023 року № 1025-р «Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року» [12], суб’єктам національної системи захисту критичної інфраструктури передбачено забезпечити розроблення:

– переліку посад та кваліфікаційних характеристик для фахівців, відповідальних за забезпечення захисту об’єктів критичної інфраструктури;

– програм підвищення кваліфікації державних службовців, працівників державних органів, що входять до складу сектору безпеки та оборони, посадових осіб органів управління та органів місцевого самоврядування з питань кібербезпеки та захисту критичної інфраструктури.

Положення даних актів ще раз наголошують на певну кількість повноважень суб’єктів національної системи захисту критичної інфраструктури, серед яких необхідно виділити проведення регулярних навчань

щодо попередження і реагування на загрози критичній інфраструктурі, організацію та проведення різноманітних освітніх заходів, а також розроблення відповідних програм та методик, сценаріїв реагування на загрози критичній інфраструктурі.

Враховуючи необхідність створення системи підготовки кадрів для сфери захисту критичної інфраструктури та підвищення компетентності її фахівців, а також з метою організації навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури автором дослідження розроблено освітню карту розвитку фахівця у сфері захисту критичної інфраструктури (рис. 1), подальше впровадження якої у освітній процес суб'єктів національної системи захисту критичної інфраструктури стане справжньою реалізацією у службову діяльність питань що стосуються єдності методологічних засад у сфері критичної інфраструктури, їх координованості, державно-приватного партнерства, безпеки, захисту та охорони інформації з обмеженим доступом, міжнародного співробітництва, а також принципу «навчання впродовж життя» для тих фахівців, які безпосередньо забезпечують запобігання проявам несанкціонованого втручання на об'єктах критичної інфраструктури, прогнозування та запобігання кризовим ситуаціям на таких об'єктах.

Зазначена освітня карта відображає внутрішню логіку формування у курсантів (студентів) індивідуально-особистісного стилю освітньо-пізнавальної діяльності, показує вибір індивідуальної стратегії пізнавальної діяльності, зображує індивідуальний маршрут та просування ним використовуючи алгоритмізацію окремих навчальних дій, які підібрано із урахуванням індивідуальних особливостей курсанта (студента) та кола його пізнавальних інтересів. Самостійний вибір оптимальної освітньої стратегії, а також відповідного освітньо-індивідуального маршруту є оптимальними організаційними формами для подальшого формування особистісно-індивідуального стилю пізнавальної діяльності курсантів (студентів).

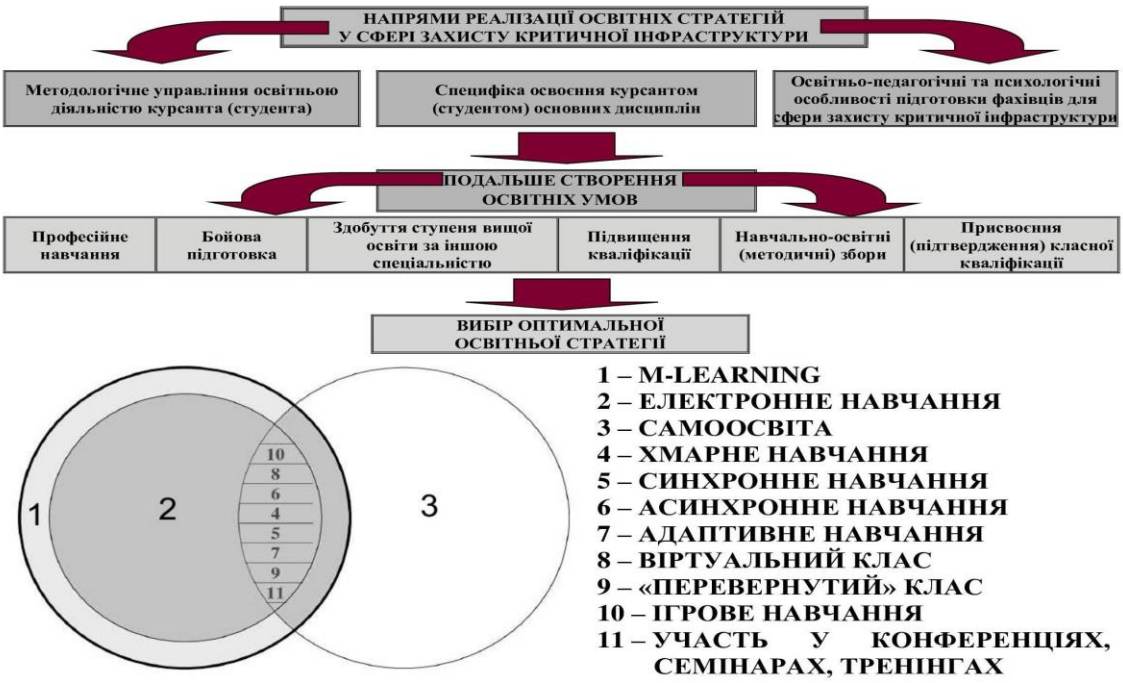

Рис. 1. Освітня карта розвитку фахівця у сфері захисту критичної інфраструктури

Джерело: Розробив автор

Вибір відповідної освітньої стратегії професійної підготовки фахівців у сфері захисту критичної інфраструктури відбувається шляхом визначення напряму підготовки того чи іншого фахівця, що у подальшому дає змогу розвивати певні компетентності відповідного спеціаліста. Таким чином, «рухаючись» індивідуальним освітнім маршрутом фахівці (курсанти, студенти) занурюються в пізнавально-навчальну сутність освітньої стратегії, вибирають оптимальні шляхи своїх навчальних дій, що дає можливість доводити або пояснювати їхню правомірність та правильність.

Освітня карта розвитку фахівця у сфері захисту критичної інфраструктури освіщає загальну логіку професійної підготовки фахівців у зазначеній сфері, а також надає навчально-ціннісне забарвлення тим знанням, що засвоюються та використовуються у професійній діяльності таких фахівців.

Освітніми умовами в рамках реалізації освітніх стратегій захисту критичної інфраструктури є:

– професійне навчання – це організований за відповідним планом процес навчання і виховання особового складу з метою підтримання на належному рівні набутих знань та удосконалення практичних навичок;

– бойова підготовка – це система навчально-виховних заходів, що проводиться з метою навчання військовослужбовців та їхньої підготовки до виконання завдань за призначенням;

– здобуття ступеня вищої освіти за іншою спеціальністю – це освітній процес здобуття вищої освіти відповідного ступеня за обраними спеціальностями відповідно до стандартів вищої освіти з метою задоволення потреб суб'єктів національної системи захисту критичної інфраструктури у кваліфікованих кадрах;

– підвищення кваліфікації – навчання з метою оновлення та вдосконалення умінь, знань, навичок і здатності виконувати додаткові завдання та обов'язки у межах отриманої спеціальності для провадження професійної діяльності, у тому числі в органах і підрозділах суб'єктів національної системи захисту критичної інфраструктури;

– навчально-освітні (методичні) збори – основна форма підготовки будь-яких фахівців, яка спрямована на відновлення (набуття, удосконалення) індивідуальних спроможностей, необхідних під час дій на посадах, у тому числі у складі підрозділів суб'єктів національної системи захисту критичної інфраструктури;

– присвоєння (підтвердження) класної кваліфікації – освітньо-навчальний показник, що відповідає певному рівню майстерності та фахової підготовки військовослужбовця (особи начальницького складу) до виконання ним завдань за призначенням і присвоюється за результатами складання відповідних іспитів.

У свою чергу оптимальними освітніми стратегіями у сфері захисту критичної інфраструктури для подальшого розвитку її фахівців є:

– m-learning (або мобільне навчання) – це нове явище в освіті, яке стало популярним у 2020 – 2021 роках, коли освітня сфера, у тому числі у сфері критичної інфраструктури, перебудовувалася на тлі пандемії коронавірусу.

З технологічної точки зору, мобільне навчання – це передача і отримання навчальної інформації з використанням технологій WAP або GPRS на будь-який портативний мобільний пристрій, за допомогою якого можна отримати матеріали, відповісти на питання у форумі, зробити тест тощо.

Технологія mobile learning передбачає навчання в будь-який час та з будь-якого місця. З використанням технологій m-learning можливо досить дієво та ефективно реалізувати весь дидактичний цикл з вивчення дисципліни, що включає в себе лекції, практичні заняття, семінари, іспити тощо.

Використання технологій mobile learning суттєво підвищить якість виконання основних функцій освітнього процесу у сфері захисту критичної інфраструктури за рахунок:

надання слухачам постійного доступу до освітньо-інформаційних ресурсів, адміністративних ресурсів закладу освіти, плану-графіку навчання, запланованих освітніх заходів, а також до оперативного одержання повідомлень про хід навчального процесу;

багатопланової перевірки рівня умінь, знань і навичок фахівця, а також ступеня засвоєння освітнього матеріалу із застосуванням індивідуальних (групових, творчих) проєктів, тестових завдань, лабораторних і практичних робіт тощо;

методичної та консультативної підтримки в груповому і індивідуальному режимах;

постійного забезпечення слухачів інформацією про результати їхнього навчально-освітнього процесу.

Перевагами мобільного навчання є можливість:

організовувати освітньо-навчальний процес незалежно від часу і місця за допомогою мобільних пристроїв;

використання «кишенькових» комп’ютерів під час занять, що дозволить підвищувати співпрацю між учасниками освітнього процесу;

використання словників та інших засобів для вивчення іноземних мов.

Крім цього слід зазначити, що m-learning по своїй суті реалізує принципи відкритого навчання: використання сучасних інформаційно-комунікаційних технологій, модульність, а також гнучкість. У мобільному навчанні на перше місце становляться такі дидактичні принципи як доступність, інтерактивність та мультимедійність.

Разом з тим, m-learning має такі недоліки як: невисокий рівень захисту особистої інформації; труднощі із доступом до мережі Інтернет; малий розмір екрану та клавіш на мобільних пристроях; висока вартість початкових вкладень в організацію мобільного навчання.

Крім цього, можливості мобільних пристроїв, безумовно, необхідно використовувати в освітньо-навчальному процесі сфери захисту критичної інфраструктури, адже вони невід'ємно поєднуються з входженням України в загальний інформаційний простір Європейського Союзу та всього світу, а також розширюють можливості доступу до навчальної інформації та традиційних форм навчання. Поєднання традиційних форм навчання з новими мобільними технологіями забезпечить досягнення головних цілей навчання у переважної кількості здобувачів освіти;

– електронне навчання (або e-learning) – це система навчання, що побудована з використанням інформаційно-комунікаційних технологій, та яка дозволяє забезпечувати викладання освітньо-навчальних курсів, а також отримувати певну інформацію та спілкуватися студентам і викладачам між собою незалежно від місця та часу знаходження.

E-learning активно використовується у сфері захисту критичної інфраструктури в найрозвинутіших країнах світу та дозволяє:

забезпечувати доступність до певної освітньої платформи у будь-який час та в будь-якому місці;

використовувати сучасні та різноманітні методи та засоби навчання (відео, текст, тести тощо);

одночасно звертатися до будь-якої кількості студентів та до багатьох джерел навчальної інформації;

використовувати спеціальні форми контролю якості освітньо-навчальних досягнень;

забезпечувати можливість спілкування у режимі онлайн за межами навчальних аудиторій;

застосовувати у освітньому процесі нові досягнення ІТ-технологій, які надають можливість входження людини у світовий інформаційний простір.

Однак, незважаючи на низку переваг, електронне навчання має деякі недоліки. Якщо говорити про застосування e-learning у дистанційній освіті, то слухачі часто відчувають нестачу особистісного контакту. Нестача живої взаємодії для багатьох стає причиною зниження успішності та мотивації у навчанні.

Ще один мінус – технічні вимоги та навички. Наприклад, щоб викладати курс онлайн, необхідний доступ в мережу Інтернет, техніка для зйомок і знання, як її використовувати. Студентам у цей же час потрібне стабільне Інтернет-з'єднання, а також смартфон, планшет, комп'ютер або ноутбук для перегляду та завантаження навчальних матеріалів.

Крім цього слід зазначити, що m-learning є більш традиційним підходом до освіти з використанням сучасних ІТ-технологій, у той час як e-learning є більш інтерактивною, доступною та гнучкою формою освіти, що поєднує в собі використання унікальних методів онлайн-навчання та сучасних інформаційних технологій;

– самоосвіта – самостійно-пізнавальна діяльність людини, спрямована на задоволення загальнокультурних запитів, підвищення професійної кваліфікації, а також на досягнення пізнавальних інтересів у будь-якій сфері діяльності, у тому числі у сфері захисту критичної інфраструктури. Самоосвіта є умовою особистого розвитку, самоствердження, самонавчання, та є складовою навчання людини протягом всього життя.

Самоосвіта тісно пов'язана з самореалізацією, оскільки дозволяє слухачам досягати своїх потенційних можливостей у різних сферах життя. Через самоосвіту виявляються та розвиваються таланти, здібності та інтереси,

що веде до більшої освіченості та розширення світогляду. Це створює міцну основу для самозадоволення, даючи знайти сенс у своєму житті;

– хмарне навчання надає широкі можливості для створення різних навчально-освітніх ситуацій, в яких слухачі можуть освоювати і відпрацьовувати відповідні навички, у тому числі у сфері захисту критичної інфраструктури.

Хмарні технології – це можливість безлічі фізичних серверів бути загальним обчислювальним середовищем, у тому числі у сфері освіти. Сервіси хмарних обчислень є додатками, доступ до яких забезпечується через мережу Інтернет за допомогою браузера або інших мережевих застосувань. Суть хмарних технологій полягає в перенесенні обробки даних з власних персональних комп'ютерів, ноутбуків і робочих станцій на сервери всесвітньої мережі Інтернет.

Впровадження хмарних сервісів у освітній процес дає змогу об'єднатися в єдиній онлайн-платформі та забезпечити подальший розвиток професійного потенціалу та життєвих компетенцій через використання інформаційно-комунікаційних технологій.

Хмарні технології мають багато переваг, які призводять до їх широкого використання в різних галузях. «Плюсами» хмарного навчання сфери захисту критичної інфраструктури є: гнучкість та масштабованість; ефективне використання ресурсів; доступність та надійність; самообслуговування та автоматизація; економія витрат; глобальний доступ; безпека; швидке впровадження нових функцій та оновлень. Зазначені переваги нададуть змогу:

збільшувати (або зменшувати) використання освітніх ресурсів згідно зі змінними потребами, оптимізувати використання відповідного обладнання, а також забезпечити високий рівень ефективності в порівнянні з традиційними моделями власних серверів;

забезпечити достатній рівень доступності та надійності до навчальних послуг, самостійно керувати освітніми ресурсами, запускати віртуальні машини, налаштовувати сервіси та автоматизувати багато навчальних процесів;

отримувати доступ до своїх даних та освітніх ресурсів з будь-якого місця, а також впроваджувати нові функції та оновлення, забезпечуючи користувачам доступ до останніх освітніх технологій без необхідності самостійного оновлення відповідної інфраструктури.

Незважаючи на деяку кількість переваг, існують і певні недоліки у використанні хмарного навчання сфери захисту критичної інфраструктури, а саме: залежність від Інтернету; приватність та безпека даних; відмова від контролю над інфраструктурою; можливість виникнення проблем безпеки; вартість; обмежені можливості настроювання; відсутність контролю над місцезнаходженням даних; можливість зміни вартості послуг. Зазначені недоліки можуть впливати на:

наявність стабільного Інтернет-з'єднання та доступ до даних та сервісів;

конфіденційність та безпеку даних, а також на виникнення інцидентів безпеки;

обмеження можливостей користувачів налаштовувати інфраструктуру та програмне забезпечення під їхні потреби, а також на контроль над тим, де фізично знаходяться відповідні дані;

– синхронне навчання – це проведення заняття в режимі реального часу в обраному цифровому середовищі та передбачає взаємодію між суб'єктами дистанційного навчання. Під час проведення такого навчання учасники одночасно перебувають в електронному освітньому середовищі або спілкуються за допомогою засобів аудіо-, відеоконференції.

Звісно, є також і технологічні обмеження, які означають, що одночасно говоритиме лише хтось один, і на екрані можна побачити не всіх учасників водночас, якщо їх достатньо багато. Лише в синхронному форматі можна організувати безпосередню взаємодію учнів у малих групах, швидко обговорити питання та прийняти відповідне рішення.

Однак, синхронне навчання вимагає онлайн-присутності в чітко визначений час, що може бути проблемою, особливо коли є кілька осіб з графіками, що накладаються. Відповідна частина синхронного заняття йде на

узгодження технічних перешкод, перепитування й уточнення через непередбачувані перебої зі зв’язком та інші організаційні моменти;

– асинхронне навчання – це режим більш самостійного навчання, яке, водночас, підтримується вчителем з використанням відповідних цифрових інструментів. Такий режим передбачає роботу за власним графіком та у власному темпі й максимально використовує переваги змішаного навчання.

Асинхронний режим означає взаємодію між собою із затримкою в часі, застосовуючи інтерактивні освітні платформи (електронну пошту, соціальні мережі, форуми тощо). Це дозволяє опановувати матеріал, орієнтуючись на власне розуміння, а не на темп решти групи.

Разом з тим, асинхронне навчання може давати відчуття ізольованості та вимагати високої самодисципліни та розвиненого вміння керувати своїм часом, що, у свою чергу, може бути досить складним, зокрема за відсутності попереднього досвіду такої роботи;

– адаптивне навчання – підхід до освіти, який забезпечує індивідуальне навчання використовуючи персоналізовану технологію відповідно до унікальних потреб кожного слухача. За допомогою такої методики, можна зрозуміти сильні та слабкі сторони кожного слухача, а також отримати більше впевненості та залученості у процесі навчання.

Адаптивне навчання – це освітньо-навчальний інструмент, який використовує доповнену реальність і штучний інтелект, що в свою чергу надасть змогу сфері захисту критичної інфраструктури в освітньому напрямку:

забезпечити багатофункціональне, інтерактивне та адаптивне навчальне середовище;

створювати віртуальні 3D моделі, експерименти (симуляції), які збільшують зрозуміння складних понять та процесів;

створювати інтерактивні заняття з використанням інтуїтивно зрозумілого конструктора;

зробити процес навчання більш динамічним та цікавим, спонукаючи слухачів активно залучатися в процес навчання;

забезпечити інтеграцію з різними системами управління навчанням, сервісами відеозв’язку та популярними календарними додатками;

забезпечити динамічне (персоналізоване) та високоефективне навчальне середовище, яке допомагатиме слухачам досягати своїх академічних цілей;

– віртуальний клас – це навчально-освітній простір, де слухачі можуть давати та отримувати віртуальні уроки, що призначені для віддалених зустрічей та спілкування. «Складовими» віртуального класу є відеоконференцзв’язок (для живого спілкування з використанням веб-камери), цифрова дошка (для візуальної допомоги та підтримки матеріалів), обмін миттєвими повідомленнями (для більш чіткого обміну ідеями та доставки інформації), субчати (для індивідуального підходу за необхідності) та відео (для повторного перегляду та обміну, кращого розуміння та гнучкої передачі знань).

Перевагами використання віртуальних класів у сфері захисту критичної інфраструктури є можливість замінити особисті зустрічі на віртуальні, заощадити час та ресурси на подорожах, забезпечити велику гнучкість та комфорт, персоналізувати процес навчання, а також організувати навчання у ділових та особистих цілях тощо.

На теперішній час віртуальні класи є актуальними як ніколи. Вони пропонують комплексний функціонал, здатний замінити звичайні виїзні заняття. І якщо для закладів освіти це не так критично, то при користуванні суб’єктами національної системи захисту критичної інфраструктури це значно підвищуватиме професійний рівень своїх співробітників. Віртуальні класи дозволять зосередитися на викладанні (навчанні) та вирішувати більшість потенційних проблем з онлайн-освітою;

– «перевернутий» клас являє собою різновид змішаного навчання, головною особливістю якого є те, що завдання для слухачів організовується в онлайн-середовищі, що сприяє, в свою чергу, тісній співпраці з слухачами на заняттях.

Перевагами зазначеної освітньої стратегії є такі фактори:

викладач отримує час для індивідуальної роботи з кожним слухачем та може одразу зосередитися на виконанні практичних завдань;

слухач може самостійно передивлятися матеріал, робити у разі необхідності паузу або повертатися до необхідних фрагментів;

відеоматеріали доступні для всіх слухачів – і для тих, хто був на уроці, і для тих, хто з якоїсь причини був відсутній;

слухач може у будь-який момент звернутися до необхідних матеріалів.

Разом з тим, слухачі не можуть поставити запитання вчителю безпосередньо у той момент, коли воно виникає, а також деякі слухачі можуть не виконувати відповідні завдання, що є недоліками «перевернутого» класу;

– ігрове навчання (гейміфікація) – це застосування принципів гри в неігровому середовищі. Від інших ігрових форматів відрізняється фокусом на досягненні конкретної цілі, а не на власне грі. На гейміфікованих заняттях слухачі здобувають не оцінки, а бали досвіду, значки, просуваються в загальному рейтингу, що заохочує їх до подальших звершень. Ігрове навчання здатне суттєво полегшити вивчення багатьох складних предметів та спрощувати запам’ятовування нового матеріалу, у тому числі із використанням флешкарток та вікторин. Гейміфікація навчання – ефективний та дієвий спосіб утримати увагу та підвищити мотивацію;

– участь у конференціях, семінарах, тренінгах – форма групової роботи за участю запрошених, мета якої – обмін інформацією з певної теми. Іншими словами, це вид освітньої діяльності спрямованої на підвищення кваліфікації.

Подальше впровадження освітньої карти розвитку фахівця у сфері захисту критичної інфраструктури надасть змогу забезпечити:

– підготовку (перепідготовку, підвищення кваліфікації, тренування) працівників національної системи захисту критичної інфраструктури;

– організацію системи підготовки персоналу, навчання (тренування) щодо забезпечення стійкості та захисту секторів критичної інфраструктури;

– розроблення нової галузі знань (програм навчання, підвищення кваліфікації, робочих і навчальних програм) з питань забезпечення стійкості та захисту критичної інфраструктури;

– навчання населення з питань захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування;

– проведення навчань (тренінгів, підготовку та перевірку персоналу) з питань охорони, безпеки та захисту об’єктів критичної інфраструктури;

– проведення спільних командно-штабних (тактико-спеціальних) навчань, спільних тренувань та занять із захисту (охорони, оборони, припинення) злочинних дій, інцидентів та кібератак проти об’єктів критичної інформаційної інфраструктури;

– підвищення комплексних знань (навичок, умінь) персоналу та керівного складу операторів критичної інфраструктури, персоналу суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, з питань реагування на кризові ситуації на таких об’єктах.

Крім цього, запровадження освітньої карти розвитку фахівця у сфері захисту критичної інфраструктури у службову діяльність суб’єктів національної системи захисту критичної інфраструктури надасть змогу забезпечити конкурентоспроможність при прийомі на службу (роботу), кар’єрне зростання і підвищення зарплати, систематизацію знань, а також поглиблення професійних компетентностей і навичок.

Разом з тим, запропонований проєкт освітньої карти розвитку фахівця у сфері захисту критичної інфраструктури в контексті подальшого розвитку системи підготовки кадрів для сфери захисту критичної інфраструктури можна використовувати для:

– створення навчальних програм (тренінгів, освітніх курсів (ресурсів), спрямованих на підвищення рівня володіння професійними компетентностями;

– створення більш деталізованих (професійних) навчально-освітніх

програм у сфері захисту критичної інфраструктури;

– проведення тестування, сертифікації (опитування) тощо;

– системного збору статистичних даних щодо рівня володіння цифровими компетентностями окремих категорій працівників сфери захисту критичної інфраструктури;

– розробки (внесення) змін у професійні стандарти та стандарти вищої освіти сфери захисту критичної інфраструктури.

Висновки та перспективи подальших розвідок у даному напрямі. На сьогодні в Україні система підготовки кадрів для сфери захисту критичної інфраструктури перебуває у трансформаційному стані. Закон України «Про критичну інфраструктуру» та затверджена Урядом Концепція створення державної системи захисту критичної інфраструктури жодним чином не вирішує цієї проблеми, залишаючи осторонь ключові проблеми забезпечення і контролю якості та визнання освіти у сфері захисту критичної інфраструктури. Не існує офіційної статистики з цих питань, відсутні спеціальні навчальні концепції та освітні програми. Тому для України вкрай важливо найближчим часом вжити дієві заходи для подолання відставання у цій сфері.

Дослідження експертів свідчать, що в сучасному світі підготовка кадрів для сфери захисту критичної інфраструктури не може обмежуватися лише отриманням вищої освіти у закладах освіти за тією чи іншою спеціальністю. Для збереження відповідного професійного рівня та конкурентоспроможності фахівцям зазначеної сфери необхідно постійно підвищувати свою кваліфікацію на засадах концепції безперервної освіти (або «освіти протягом життя»). Можливі декілька варіантів роботи в цьому напрямі, серед яких здобуття ступеня вищої освіти за іншою спеціальністю, підвищення кваліфікації, участь у навчально-освітніх (методичних) зборах тощо.

Навчання протягом життя виходить на першорядні позиції у світових навчально-освітніх процесах – це диктується світовими тенденціями сучасного розвитку людства. Такий підхід, на наш погляд, дозволить кардинально змінити систему підготовки кадрів у сфері захисту критичної інфраструктури. Адже до

цього часу, у переважній більшості, вона зорієнтована на запити тогочасності. Сучасна ж світова економіка потребує кадрів, готових працювати та навчатись в умовах конкуренції, тобто в інноваційній економіці.

Використання та подальше впровадження освітньої карти розвитку фахівця у сфері захисту критичної інфраструктури для потреб суб'єктів національної системи захисту критичної інфраструктури стане дієвим та ефективним інструментом навчання, який дозволить рухатися власною навчально-освітньою траєкторією та розширить коло навчальних задач і збагатить їх сучасним змістом. Практична площина засвідчує, що ніяка теорія не буде реалізована (впроваджена) в освітній діяльності, якщо для її введення не буде розроблений відповідний алгоритм. Тому надалі вектор досліджень у сфері захисту критичної інфраструктури необхідно спрямовувати на створення освітньої медіатехнології як цілісної системи підготовки кадрів для сфери захисту критичної інфраструктури в умовах розвитку цифрового суспільства України.

Література

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

2. 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.

3. Проблема розбудови системи підготовки кадрів і населення для забезпечення стійкості критичної інфраструктури в Україні. Аналітична записка. URL: https://www.niss.gov.ua/sites/default/files/2016-12/kadry-d370c.pdf (дата звернення: 14.09.2024).

4. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 14.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 14.09.2024).

5. Арсенович Л. А. Удосконалення механізмів формування системи підготовки кадрів у сфері кібербезпеки в умовах державно-приватної взаємодії. *Науковий вісник: державне управління.* 2022. № 1. С. 6–27.

6. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. Дата оновлення: 14.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 14.09.2024).

7. Щербак Л. Метод визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації. *Безпека інформації*. 2017. № 1. С. 27–38.

8. Ткаченко І. В. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідковування кризових індикаторів. *Сучасний захист інформації*. 2020. № 1. С. 54–57.

9. Бурячок В. Л. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання*. 2018. № 5. С. 277–291.

10. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : постанова Кабінету Міністрів України від 12.07.2022 р. № 787. Дата оновлення: 14.09.2024. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (дата звернення: 14.09.2024).

11. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України від 19.09.2023 р. № 825-р. Дата оновлення: 14.09.2024. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (дата звернення: 14.09.2024).

12. Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року : розпорядження Кабінету Міністрів України від 10.11.2023 р. № 1025-р. Дата оновлення: 14.09.2024.

URL: https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text (дата звернення: 14.09.2024).

References

1. Telenyk, S.S. (2020), “Directions of training and advanced training of specialists in the protection of critical infrastructure”, *Pravovi novely*, vol. 10, pp. 91–99.

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

3. Kondratov, S.I. (2016), “The problem of developing a system of personnel and population training to ensure the stability of critical infrastructure in Ukraine. Analytical note”, available at: https://www.niss.gov.ua/sites/default/files/2016-12/kadry-d370c.pdf (Accessed 14 September 2024).

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 14 September 2024).

5. Arsenovych, L.A. (2022), “Improving the mechanisms of formation of the personnel training system in the field of cyber security in the conditions of public-private interaction”, *Naukovyi visnyk: derzhavne upravlinnia*, vol. 1, pp. 6–27.

6. Cabinet of Ministers of Ukraine (2017), Order “On the approval of the Concept of creating a state system for the protection of critical infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (Accessed 14 September 2024).

7. Shcherbak, L. (2017), “The method of determining the level of importance of critical information infrastructure objects in the field of civil aviation”, *Bezpeka informatsii*, vol. 1, pp. 27–38.

8. Tkachenko, I.V. (2020), “Assessment of the state of cyber security of critical information infrastructure during the identification and monitoring of crisis indicators”, *Suchasnyi zakhyst informatsii*, vol. 1, pp. 54–57.

9. Buryachok, V.L. (2018), “Model of training specialists in the field of information and cybernetic security in higher education institutions of Ukraine”, *Informatsiini tekhnolohii i zasoby navchannia*, vol. 5, pp. 277–291.

10. Cabinet of Ministers of Ukraine (2022), Resolution “On the establishment of the State Service for the Protection of Critical Infrastructure and Ensuring the National Stability System of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (Accessed 14 September 2024).

11. Cabinet of Ministers of Ukraine (2023), Order “On the approval of the National Plan for the Protection and Ensuring the Safety and Stability of Critical Infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (Accessed 14 September 2024).

12. Cabinet of Ministers of Ukraine (2023), Order “On the approval of the plan of measures for the implementation of the Concept of ensuring the national system of sustainability until 2025”, available at: https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text (Accessed 14 September 2024).

Стаття надійшла до редакції 15.09.2024 р.