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. № 7.

DOI: http://doi.org/10.32702/2307-2156.2025.7.7

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

ШЛЯХИ РОЗВИТКУ ФУНКЦІОНУВАННЯ ЦЕНТРІВ КІБЕРБЕЗПЕКИ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ НАЦІОНАЛЬНОЇ СИСТЕМИ 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

WAYS OF ENHANCING CYBERSECURITY CENTERS OPERATIONS IN THE CONTEXT OF ENSURING THE SECURITY OF THE NATIONAL CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

Підвищення дієвості та ефективності функціонування національної системи кібербезпеки на сьогодні є першорядним завданням для забезпечення сталого і безпечного функціонування національної системи захисту критичної інфраструктури. Її функціонально-нормативне визначення полягає у створенні умов для об'єднання зусиль суб'єктів забезпечення кібербезпеки при вирішенні завдань щодо підвищення рівня кіберстійкості критичної інформаційної інфраструктури держави, яка охоплює як об'єкти критичної інфраструктури, так і комунікаційно-інформаційні та інші системи, сталість та надійність функціонування яких критично важлива для функціонування державних органів, підприємств, установ і організацій всіх форм власності.

Виходячи з вищезазначеного, можна розуміти, що система підготовки кадрів для сфери захисту критичної інфраструктури – така система, яка допоможе у майбутньому об'єднати зусилля суб'єктів забезпечення кібербезпеки і суб'єктів національної системи захисту критичної інфраструктури та створити умови для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, зокрема через реалізацію заходів спрямованих на захист національних інформаційних ресурсів, кіберзахист об'єктів критичної інформаційної інфраструктури, забезпечення їх кіберстійкості, стабільне функціонування інформаційної інфраструктури державного та приватного секторів економіки.

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.

У статті автором запропоновано впровадження методики розрахунку вартості послуг з організації та проведення освітніх заходів у сфері кібербезпеки (кібертренінгів, кіберзмагань) для потреб суб'єктів національної

системи захисту критичної інфраструктури, що надасть у подальшому забезпечити розвиток мережі центрів реагування на кібератаки та кіберінциденти, а також подальшу розбудову мережі центрів, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки.

Enhancing effectiveness and efficiency of the national cybersecurity system is currently a priority task for ensuring a stable and safe functioning of the national critical infrastructure protection system. Its purpose and guiding principles are to create conditions to foster collaboration of the cybersecurity assurance entities while solving tasks related to enhancing the cyber resilience of the critical information infrastructure of the state encompassing both critical infrastructure facilities, and communication and information as well as the other systems, stable and reliable functioning of which is crucial for the state authorities, enterprises, institutions and organizations of all forms of ownership.

Based on the above it is obvious that the system of training personnel for the critical infrastructure protection is designed to foster future collaboration among the cybersecurity assurance entities and the entities of the national critical infrastructure protection system, and to create conditions for safe functioning of the cyberspace, its use in the interests of the individual, society and the state, in particular through implementation of the measures aimed at protection of the national information resources, cyber protection of critical information infrastructure facilities, ensuring their cyber resilience, stable functioning of the information infrastructure of public and private economy sectors.

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.

In the article the author proposes to implement the methodology for

calculating the cost of services to arrange and conduct educational events in the field of cybersecurity (cybersecurity trainings and competitions) for the entities of the national critical infrastructure protection system aimed at further expanding the network of cyberattack and cyber incident response centers, and further developing the network of centers for consolidating and sharing cybersecurity expertise.

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. У зв'язку зі стрімким розвитком цифрових технологій відбувається трансформація різних сфер суспільного життя. Завдяки відкритому та вільному кіберпростору розширюються свободи і можливості соціуму, стимулюється відповідальна та ефективна робота органів державної влади і відбувається активне залучення громадян до публічного управління. З іншого боку цифрові трансформації держави і суспільства розширили ландшафт загроз національній безпеці й ставлять перед державою та суспільством нові виклики, які вимагають адаптованої та інноваційної відповіді. Українська економіка, публічне управління та надання основних державних послуг відтепер спираються на цілісність кіберпростору та на інфраструктуру, системи та дані, які лежать в його основі, а втрата довіри до цієї цілісності поставить під загрозу переваги застосування процесів цифрових трансформацій. Будь-які збої, навіть ті, які спочатку обмежувалися однією організацією або одним сектором, можуть мати каскадні наслідки в глобальному сенсі, що потенційно призведе до негативних наслідків для суспільства і держави [1, с. 18].

На сьогодні, в умовах воєнного стану, забезпечення кібербезпеки об'єктів

критичної інфраструктури є пріоритетом у системі національної безпеки України. Впровадження та реалізація такого пріоритету здійснюється шляхом посилення спроможностей національної системи кібербезпеки, а також національної системи захисту критичної інфраструктури для відбиття та протидії кіберзагрозам у сучасному безпековому середовищі.

Розповсюдження та поширення різноманітних кіберзагроз на майже усі сфери життєдіяльності людини та вдосконалення інструментарію їх реалізації зумовлює і підштовхує до необхідності зміни стратегії і тактики протидії ним. При цьому швидке виявлення вразливостей і кібератак, поширення інформації про них для мінімізації можливої шкоди набуває все більшої значимості.

Аналіз останніх досліджень і публікацій. Проблемні питання у сферах кібербезпеки та безпеки критичної інфраструктури розглядають у своїх працях і вітчизняні науковці. Так, Топчій В.В., директор навчально-наукового інституту права Державного податкового університету, та Бодунова О.М., завідувач кафедри правничої лінгвістики Державного податкового університету, розглядаючи проблемні питання забезпечення кібербезпеки в Україні зазначають, що основними засадами до запобігання кіберзлочинності є, у тому числі, підготовка фахівців з кібербезпеки, організація тренінгів для співробітників правоохоронних органів і суддів щодо специфіки кіберзлочинів, а також створення спеціалізованих підрозділів, такі як підрозділи кіберполіції, центри реагування на кіберінциденти (CERT) тощо. Вчені приходять до висновку, що одними із основних напрямів забезпечення кібербезпеки в Україні є як зміцнення освітніх програм для підготовки кадрів у сфері кіберзахисту, так і створення регіональних центрів кібербезпеки для оперативного реагування на загрози, які суттєво впливають на безпеку національної системи захисту критичної інфраструктури [2, с. 667, 669].

У свою чергу Ю.В. Завгородня, доцент кафедри політичних теорій Національного університету «Одеська юридична академія», вивчаючи у своїй статті питання діяльності України в умовах повномасштабного вторгнення щодо боротьби з кіберзагрозами та формування публічного політичного

декламування стратегічних цілей зазначає, що важливої уваги потребує підготовка фахівців у сфері кібербезпеки через розширення освітніх програм та курсів з кіберзахисту в університетах і спеціалізованих навчальних закладах, а також стимулювання приватного сектора до участі в підготовці кадрів, зокрема через державно-приватне партнерство, створення навчальних центрів та стажування для молодих спеціалістів [3, с. 64].

Разом з тим, науковець Кавин С.Я. досліджуючи питання правового гарантування інформаційної безпеки, зокрема у сфері кіберзахисту в державах Центрально-Східної Європи в контексті аналізу їхніх національних Стратегій кібербезпеки та відповідних нормативно-правових актів, констатує, що у відповідних структурах країн Центрально-Східної Європи з метою впровадження ефективного й оперативного механізму протидії кіберзагрозам створюються національні центри кібербезпеки, до складу яких також входять і команди швидкого реагування на кіберінциденти (CERT) [4, с. 56].

Наукові праці вищезазначених фахівців ще раз сигналізують про необхідність розроблення та реалізації державно-освітньої політики для потреб сфери кібербезпеки та сфери захисту критичної інфраструктури у контексті створення й розбудови в Україні навчальних галузевих центрів із кібербезпеки та стійкості критичної інфраструктури на базі закладів вищої освіти та інших навчальних центрів.

Формулювання цілей статті (постановка завдання). Метою статті є розгляд концептуальних та методологічних засад функціонування центрів кібербезпеки у контексті забезпечення безпеки національної системи захисту критичної інфраструктури.

Виклад основного матеріалу дослідження. Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя [5].

Забезпечення кібербезпеки України як стану захищеності інтересів людини, суспільства та держави в кіберпросторі, у тому числі в інтересах суб'єктів національної системи захисту критичної інфраструктури, що досягається застосуванням сукупності правових (організаційних, інформаційних) заходів, має базуватися також на дійовій освітній складовій, у тому числі на розвитку мережі відповідних кіберцентрів, що будуть реагувати на кібератаки та кіберінциденти.

Так, відповідно до Указу Президента України від 26 серпня 2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [5] для досягнення стратегічної цілі «Національна кіберготовність та надійний кіберзахист» Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю має забезпечити посилення національної кіберготовності та кіберзахисту шляхом забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти та утворення центрів, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері, що стосується у повній мірі і суб'єктів національної системи захисту критичної інфраструктури.

Такі ж самі завдання закладено у План реалізації Стратегії кібербезпеки України, уведеного в дію Указом Президента України від 1 лютого 2022 року № 37/2022 [6], відповідно до якого забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти покладено на Кабінет Міністрів України та суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки (протягом другого півріччя 2025 року), а утворення центрів, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері – на Кабінет Міністрів України, Національну академію наук України та основні суб'єкти національної системи кібербезпеки (протягом другого півріччя 2025 року).

Більш детально питання розвитку мережі відповідних кіберцентрів

розкрито у плані заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України (розпорядження Кабінету Міністрів України від 19 грудня 2023 року № 1163-р [7]), відповідно до якого Мінцифри, Адміністрації Держспецзв'язку, Міносвіти та Національній академії наук доручено утворення мережі регіональних центрів підвищення компетенцій та розвитку інновацій (centers of excellence) у сфері кібербезпеки, стійкості критичної інформаційної інфраструктури та цифрових технологій безпеки для створення та впровадження навчально-методичних комплексів з розроблення місцевих програм підвищення стійкості територіальних громад до кризових ситуацій у зв'язку з припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій.

Необхідно акцентувати увагу також на план заходів на 2025 рік з реалізації Стратегії кібербезпеки України (розпорядження Кабінету Міністрів України від 07 березня 2025 року № 204-р [8]), завдання якого передбачають, у тому числі, забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти. Так, СБ України є відповідальна за посилення технічних спроможностей системи центрів забезпечення кібербезпеки СБ України з метою її сталого функціонування на національному та регіональному рівні, МВС та Нацполіції доручено забезпечити створення галузевого (секторального) центру реагування на інциденти з кібербезпеки в системі МВС, а на Адміністрацію Держспецзв'язку покладено обов'язки щодо створення регіонального центру реагування на інциденти з кібербезпеки.

Варто підкреслити зміни і на законодавчому рівні, що були прийняті Верховною Радою України у березні 2025 року (Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [9]), якими внесено, у тому числі, зміни до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [10]. Так, на Держспецзв'язку відповідно до визначених завдань

покладено обов’язки забезпечення функціонування регіональних центрів кіберзахисту, що є дієвим кроком щодо забезпечення безпеки національної системи захисту критичної інфраструктури.

Крім цього, варто зупинитись також на рішенні Уряду щодо суттєвого розширення повноважень Адміністрації Держспецзв’язку у частині функціонування національної системи обміну інформацією про кіберінциденти, кібератаки та кіберзагрози (постанова Кабінету Міністрів України від 4 червня 2025 року № 669 [11]). Так, Адміністрація Держспецзв’язку створює та забезпечує функціонування кваліфікаційного центру за групами кваліфікацій у сферах безпеки інформації та кіберзахисту, а також забезпечує функціонування регіональних центрів кіберзахисту.

Зазначені акти ще раз підкреслюють необхідність створення національної системи управління інцидентами, проведення наукових досліджень у сферах кібербезпеки, кіберзахисту, захисту критичної інфраструктури, реформування системи підготовки та підвищення кваліфікації кадрів у сфері кібербезпеки, впровадження системи підготовки кадрів для сфери захисту критичної інфраструктури в процесі забезпечення кіберзахисту та кібербезпеки її суб’єктів, а також розгортання навчальних програм, курсів, тренінгів з кібернавчання для всіх верств населення.

Прикладом можуть слугувати вже започатковані навчальні кіберцентри, які прямо чи опосередковано опікуються проблематикою кібербезпеки і кіберзахисту критичної інфраструктури. І таким першим прикладом в Україні є відкриття 13 травня 2021 року Державного центру реагування на кіберінциденти – Кіберцентру UA30, який створений з метою реагування на комп’ютерні надзвичайні події та здобуття навичок та знань у сфері кіберзахисту. До його складу входить також оновлений тренінговий майданчик з унікальною технологією відпрацювання реальних сценаріїв кібератак у навчальному середовищі. За словами Голови Держспецзв’язку Олександра Потія Україні потрібно 5 – 6 подібних команд реагування на комп’ютерні надзвичайні події для забезпечення повноцінного захисту у кіберпросторі.

Питання розвитку мережі кіберцентрів для посилення національної кіберготовності та кіберзахисту, обміну досвідом, підтримки інновацій та різноманітних розробок у цій сфері активно розглядається також іноземними партнерами, насамперед державами-членами НАТО. Прикладом є Об'єднаний центр передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), що забезпечує боротьбу з кібератаками й кіберзахист інформаційних систем, а також навчання та підготовку фахівців з кіберзахисту НАТО. На сьогодні зазначений центр є одним з ключових елементів системи НАТО з розвитку спроможностей у сфері кібернетичної оборони. Крім цього, на початку березня 2022 року представники 27 держав-членів НАТО прийняли рішення щодо надання Україні статусу країни-учасниці Об'єднаного центру передових технологій з кібероборони.

Водночас, британська компанія Glasswall вклала 18 мільйонів фунтів стерлінгів (694 млн грн) у програму з усунення кіберзагроз від шкідливих файлів. У Швеції нещодавно створили національний центр кібербезпеки. При цьому до 2025 року планувалось витратити на розвиток центру 440 мільйонів шведських крон (1,4 мільярда гривень). А міністерство оборони Люксембургу підписало контракт з естонською компанією CybExer. За три роки естонці побудують кіберполігон для Люксембургу, на якому будуть створені можливості для підвищення кіберзахисту країни [12].

Враховуючи зазначене, з метою забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти, подальшої розбудови мережі центрів, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, а також підтримку освітніх інновацій та розробок необхідним є впровадження методики розрахунку вартості послуг з організації та проведення освітніх заходів у сфері кібербезпеки (кібертренінгів, кіберзмагань) для потреб суб'єктів національної системи захисту критичної інфраструктури.

Розрахунок вартості послуг з організації та проведення освітніх заходів у сфері кібербезпеки (кібертренінгів, кіберзмагань) групується за статтями прямих і накладних витрат. До прямих витрат відносяться витрати на заробітну

плату та пов’язані з нею нарахування та витрати на матеріали (за необхідністю). До накладних витрат відносяться – амортизація обладнання, витрати на підтримку програмного забезпечення, комунальні витрати, адміністративно-управлінські витрати та інші.

Вартість одного людино-дня як показника трудомісткості надання послуг не є сталою величиною і може змінюватись в залежності від факторів, які впливають на його складові, зокрема, на величину накладних витрат. До основних факторів впливу відносять: обсяг та час надання послуг, рівень

компетентності слухачів, а також кількість фахівців у підрозділі, що надають послуги.

Розрахунок прямих витрат (ПВ) проводиться за такими формулами:

а) розрахунок витрат на оплату праці структурного підрозділу в день проводиться таким чином:

$$Ф^{дз(\%)} = \frac{Ф^{дз}}{Ф^{зз}}$$

де $Ф^{дз}$ – фонд додаткової зарплати;
$Ф^{зз}$ – загальний заробітний фонд;

$$Ф^{пп\ (день)} = \frac{\sum_{I=1}^{n} ЗЗ^{i}}{30} X (100\% + Ф^{дз(\%)})$$

де n – кількість фахівців в підрозділі, що безпосередньо надають послуги;

$ЗЗ^{i}$ – заробітна плата і-го працівника підрозділу;

б) відрахування на соціальні заходи ($ВС^{з1}$) проводиться так:

Закон України «Про збір та облік єдиного внеску на загальнообов’язкове державне соціальне страхування» [13] визначає правові та організаційні засади забезпечення збору та обліку єдиного внеску на загальнообов’язкове державне соціальне страхування, умови та порядок його нарахування і сплати та повноваження органу, що здійснює його збір та ведення обліку.

Згідно Закону України «Про Державний бюджет України на 2025 рік» [14] мінімальна заробітна плата з 01 січня 2025 року становить 8000 грн. Водночас частиною п’ятою статті 8 Закону України «Про збір та облік єдиного

внеску на загальнообов'язкове державне соціальне страхування» установлено порядок нарахування розміру єдиного внеску для кожної категорії платників, якщо база його нарахування не перевищує розміру мінімальної заробітної плати, встановленої законом на місяць, за який отримано дохід. У такому разі сума єдиного внеску розраховується як добуток розміру мінімальної зарплати, встановленої законом на місяць, за який отримано дохід (прибуток), та ставки єдиного внеску (22%);

в) розрахунок витрат на матеріали (за необхідністю) ($В^{мат}$) проводиться наступним чином:

$$В^{мат}= \sum_{I=1}^{n} M_i S_i$$

де M_i – кількість і-го найменування матеріалів, витрачених для проведення робіт;

S_i – вартість і-го найменування матеріалів, витрачених для проведення робіт.

Таким чином, прямі витрати (ПВ) розраховуються за такою формулою:

$$ПВ= Ф^{пп\ (день)} + ВС^{з1} + В^{мат}.$$

Розрахунок накладних витрат (НВ) проводиться за такими формулами:

а) розрахунок амортизації обладнання проводиться таким чином:

$$В^{аморт}= \sum_{I=1}^{n} \frac{S^i_{обл}}{E^i}$$

де $S_{обл}$ – ціна обладнання, а Е – експлуатаційний час;

б) обрахунок витрат на пролонгацію ліцензій на програмне забезпечення проводиться так:

$$В^{прогр}= \sum_{I=1}^{n} \frac{S^i_{пз}}{E^i}$$

де $S_{пз}$ – ціна програмного забезпечення, а Е – тривалість ліцензії;

в) розрахунок комунальних витрат (електроенергії) проводиться наступним чином:

$$В^{ком} = J \times R \times 24$$

де J – поточна ціна за 1 кВт, а R – витрати електроенергії (кВт) за 1 годину;

г) розрахунок адміністративно-управлінських витрат (на оплату праці керівництва підрозділу та підрозділів забезпечення) визначається як добуток відношення фонду оплати праці фахівців підрозділу, що надає послуги, до фонду оплати праці функціональних підрозділів, та фонду оплати праці підрозділу, який безпосередньо надає послугу з проведення кібертренінгів (кіберзмагань):

$$Ф^{пз} = \frac{Ф^{пп}}{Ф^{фп}} X\ Ф^{пз}$$

де $Ф^{пп}$ – фонд оплати підрозділу, що надає послугу, $Ф^{фп}$ – фонд зарплати всіх функціональних підрозділів, а $Ф^{пз}$ – фонд зарплати підрозділів забезпечення та адміністративних підрозділів;

д) відрахування на соціальні заходи ($ВС^{з2}$);

Таким чином, накладні витрати (НВ) розраховуються за такою формулою:

$$НВ = В^{аморт} + В^{прогр} + В^{ком} + Ф^{пз} + ВС^{з2} + В^{інші}$$

де $В^{інші}$ – інші витрати, до яких належать відрахування у межах норм передбачених законодавством України.

Розрахунок загальної вартості 1 дня робіт з організації та проведення освітніх заходів у сфері кібербезпеки (кібертренінгів, кіберзмагань) для потреб суб'єктів національної системи захисту критичної інфраструктури проводиться за такою формулою:

$$В^{1} = \frac{ПВ + НВ}{n}$$

де n – кількість навчальних кіберкласів.

Розрахунок собівартості послуг з організації та проведення освітніх заходів у сфері кібербезпеки (кібертренінгів, кіберзмагань) для потреб суб'єктів національної системи захисту критичної інфраструктури здійснюється за такою формулою:

$$В^{соб} = В^{1} \sum_{I=1}^{n} Т^{i}К^{i}$$

де n – кількість робіт (днів проведення кібертренінгів, кіберзмагань);

При цьому граничні норми коефіцієнту визначення трудомісткості робіт будуть виглядати так (таблиця 1):

Таблиця 1. Граничні норми коефіцієнту визначення трудомісткості робіт

Назва	**Трудовитрати ($Т^{i}$) (підрозділ/день)**	**Коефіцієнт ($К^{i}$)**	**Примітки**
Вступні випробування	1	к= {0,1…1}	к – пропорційно кількості слухачів
Проведення тренінгів	Відповідно до Програми підготовки фахівців з кібербезпеки	к= {1…3}	к – обернено-пропорційно середньому рівню компетентності групи
Розробка сценаріїв	90	к= {1...90}	за необхідності

Джерело: авторська розробка

Продовжуючи дослідження є необхідність розрахунку коефіцієнта рівня компетентності слухача навчальної групи, який виражається як залежність трудомісткості роботи від середнього фахового рівня групи слухачів.

Таким чином, середній рівень компетентності групи визначається як середнє арифметичне рівня компетентності слухачів навчальної групи, а саме:

$$Р^{гр} = \frac{1}{n} \sum_{I=1}^{n} Р^{i}$$

де n – кількість слухачів в групі, а $Р^{i}$ – рівень компетентності і-го слухача.

Слід зазначити, що рівень компетентності кожного слухача визначається на підставі вступних випробувань та/або співбесіди, які передбачають перевірку здатності до опанування програм та/або спецкурсів підготовки фахівців із кібербезпеки та кіберзахисту на основі здобутих раніше компетентностей (таблиця 2).

Таблиця 2. Порядок визначення рівня компетентності слухача навчальної групи

Рівень компетентності	Назва рівня компетентності	Опис рівня компетентності
3	висока компетентність	У слухача набутий великий досвід роботи, який часто практикується у практичній ситуації. Слухач має здатність до прийняття самостійних рішень, а також уміння розв'язувати нестандартні проблеми і виконувати складні завдання.
2	середня компетентність	У слухача є певний досвід роботи, який час від часу застосовується у практичній ситуації. Слухач має здатність до прийняття не складних самостійних рішень, а також уміння розв'язувати відповідні проблеми і виконувати не складні завдання.
1	низька компетентність	У слухача малий досвід роботи, який майже не застосовується у практичній ситуації. Слухач має низьку здатність до прийняття не складних самостійних рішень, а також уміння розв'язувати прості проблеми і завдання.
0	компетентність відсутня	У слухача немає досвіду та знань, які можна застосувати у будь-якій практичній ситуації.

Джерело: авторська розробка

У сучасному світі, де цифрові технології швидко розвиваються, а кібератаки стають дедалі складнішими та витонченішими, попит на фахівців з кібербезпеки для потреб національної системи захисту критичної інфраструктури зростає. В Україні, як і в усьому світі, кібербезпека є важливим пріоритетом для Президента України, Уряду, бізнесу та індивідуальних користувачів через збільшення кіберзагроз, що вимагає висококваліфікованих спеціалістів для захисту інформаційних активів суб'єктів національної системи захисту критичної інфраструктури.

Стрімкий розвиток ІТ-технологій та постійне ускладнення кіберзагроз ставлять перед суб'єктами національної системи захисту критичної інфраструктури нові виклики у сфері кібербезпеки. Ефективна та дієва підготовка фахівців з кібербезпеки потребує використання безпечних та реалістичних освітньо-навчальних середовищ, які дозволять моделювати різноманітні кіберсценарії атак та відпрацьовувати стратегії кіберзахисту. Центри реагування на кібератаки та кіберінциденти або іншими словами

кіберполігони стають невід'ємним інструментом для тестування навичок та тренувань відповідних фахівців у цій галузі.

На сьогодні є багато реалістичних рішень, розроблених різноманітними ІТ-компаніями, які використовують цифрові технології та підходи до управління і оркестрації віртуальними кіберсередовищами. В умовах відкритої кібервійни з боку російської федерації багато організацій прагнуть мати власне кіберсередовище, що буде адаптоване під необхідні потреби та вимоги. Створення власної кіберплатформи є трудним та ресурсномістким організаційним процесом, що потребує серйозних фінансових та матеріально-технічних ресурсів. Зважаючи на обмеженість ресурсів та високу вартість таких проєктів, виникає необхідність у ефективному управлінні відповідними освітньо-навчальними кіберполігонами для потреб суб'єктів національної системи захисту критичної інфраструктури.

Створення кваліфікаційних центрів за групами кваліфікацій у сферах безпеки інформації та кіберзахисту (регіональних центрів кіберзахисту, центрів реагування на кібератаки та кіберінциденти, кіберполігонів) в інтересах суб'єктів національної системи захисту критичної інфраструктури забезпечить формування основ для:

– дослідження в кіберпросторі (або через кіберпростір) комплексних кібердій;

– відпрацювання теоретичних та прикладних принципів побудови програмно-технічних засобів, форм і способів протидії гібридним впливам в кіберпросторі;

– цілодобового оперативного чергування в системі національної і загальноєвропейської інформаційної і кібербезпеки з використанням сил і засобів того чи іншого кіберполігону;

– проведення на постійній основі різносторонніх міжнародних та національних навчань з питань інформаційної і кібербезпеки;

– впровадження стандартів альянсу НАТО і досягнення взаємосумісності суб'єктів національної системи захисту критичної інфраструктури з країнами-

членами НАТО у сфері інформаційної і кібербезпеки;

– підготовки, перепідготовки і підвищення кваліфікації як військових так і цивільних фахівців у галузі інформаційної і кібербезпеки в країнах-членах та країнах-партнерах альянсу за національними стандартами і стандартами НАТО;

– впровадження перспективних фундаментальних і прикладних наукових досліджень у сфері кібербезпеки;

– ефективного вирішення наукових завдань і виконання дослідницьких функцій у сфері кібербезпеки.

Запровадження регіональних центрів кіберзахисту надасть уповноваженому органу у сфері захисту критичної інфраструктури України (Адміністрації Держспецзв'язку) змогу:

– здійснювати аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, а також надавати оцінку стану її захищеності;

– забезпечувати підготовку, перепідготовку, підвищення кваліфікації та тренування працівників національної системи захисту критичної інфраструктури;

– розробляти комплекс заходів з контролю за ризиками безпеки, виявляти, запобігати та ліквідовувати наслідки інцидентів безпеки на об'єктах критичної інфраструктури;

– попереджувати кризові ситуації, що порушують безпеку критичної інфраструктури;

– розвивати та забезпечувати функціонування національної системи захисту критичної інфраструктури;

– забезпечувати функціонування системи обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури;

– створювати бази даних щодо загроз і вразливостей критичній інфраструктурі;

– розробити нову галузь знань для потреб суб'єктів національної системи захисту критичної інфраструктури, впроваджувати програми навчання, підвищення кваліфікації, робочі і навчальні програми з питань забезпечення

стійкості та захисту критичної інфраструктури.

Участь працівників функціональних та секторальних органів сфери захисту критичної інфраструктури у підвищенні кваліфікації на базі центрів безпеки інформації та кіберзахисту забезпечить:

– пришвидшення процесів цифрової трансформації в Україні;

– підвищення рівня цифрових навичок та цифрових компетентностей серед особового складу суб'єктів національної системи захисту критичної інфраструктури;

– підвищення конкурентоспроможності працівників шляхом оволодіння новими цифровими навичками та цифровими компетентностями;

– зменшення ризиків виникнення небезпек під час користування Інтернетом;

– координацію дій на рівні органів виконавчої влади з питань розвитку цифрових навичок та цифрових компетентностей;

– створення індикаторів для моніторингу стану розвитку цифрових навичок та цифрових компетентностей.

Введення у складі Збройних Сил України та інших складових сектору безпеки і оборони України, які відносяться до суб'єктів національної системи захисту критичної інфраструктури, регіональних центрів кіберзахисту надасть можливість:

– здійснювати аналіз стану забезпечення кадрами національної системи захисту критичної інфраструктури та підготовку пропозицій щодо її удосконалення;

– брати участь у розробленні галузевих індикаторів стану кібербезпеки об'єктів критичної інфраструктури;

– прогнозувати та виявляти потенційні та реальні загрози у сфері кібербезпеки об'єктів критичної інфраструктури;

– забезпечити розроблення і впровадження суб'єктами національної системи захисту критичної інфраструктури механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, а також

усунення їх чинників та негативних наслідків;

– здійснювати заходи щодо забезпечення кіберзахисту об’єктів критичної інфраструктури та захисту технологічних процесів на виробництві у реальному секторі економіки;

– узгоджувати і координувати діяльність суб’єктів національної системи захисту критичної інфраструктури, які забезпечують кібербезпеку України.

Участь співробітників суб’єктів національної системи захисту критичної інфраструктури у навчаннях та тренінгах на базі регіональних центрів кіберзахисту надасть змогу у подальшому:

– створювати соціальні ініціативи, спрямовані на підвищення рівня цифрових навичок та цифрових компетентностей;

– запроваджувати програми, спрямовані на підвищення рівня обізнаності щодо небезпек у цифровому середовищі;

– удосконалити професійні стандарти з урахуванням затверджених рамок професійних цифрових компетентностей;

– запровадити сертифікацію цифрових навичок для працівників сфери захисту критичної інфраструктури;

– розробити програми підготовки, перепідготовки та підвищення кваліфікації фахівців сфери захисту критичної інфраструктури відповідно до професійних рамок цифрових компетентностей.

Висновки та перспективи подальших розвідок у даному напрямі. Динамічний розвиток української держави потребує практично щорічної корекції концептуальних підходів до розвитку інформаційних технологій та питань кібербезпеки у суспільстві. Система вищої освіти стає стратегічною сферою формування професійних компетентностей фахівців відповідно до потреб світового ринку праці. Виникає гостра потреба в адаптації даних питань не тільки на законодавчому, нормативно-правовому, економічному рівні, але і в динамічній перебудові загальної мети та стратегічних напрямів реформування всіх ланок освіти згідно зі світовими стандартами. Українська держава будує власну національну систему ІТ-індустрії та відповідну сферу кібербезпеки [15].

Кібербезпека є одним із найважливіших напрямів у сучасній цифровій індустрії, який швидко розвивається та має найвищий попит. В умовах постійних кіберзагроз і кібератак на інформаційні системи України, попит на висококваліфікованих фахівців у цій галузі продовжує стрімко зростати. Розвиток цифрових технологій і поява нових типів кіберзагроз роблять цю професію однією з найбільш перспективних і багатообіцяючих у секторі інформаційних технологій.

Кібербезпека критичної інфраструктури – це один із важливих пріоритетів національної безпеки України. Держспецзв'язку спільно з іншими суб'єктами національної системи захисту критичної інфраструктури постійно працює над удосконаленням системи кібербезпеки об'єктів критичної інфраструктури, і розбудова її освітньо-навчальної складової є одним із важливих інструментів у цій роботі.

Зараз триває перша у світі кібервійна, і Україна займає в ній активну позицію, задає головний напрям та знаходить нові способи і методи протистояти кіберзагрозам. Об'єкти критичної інфраструктури та інші заклади, установи та організації мають бути максимально захищені від різноманітних кібератак. Тож створення кваліфікаційних центрів у сферах безпеки інформації та кіберзахисту, регіональних центрів кіберзахисту, центрів реагування на кібератаки та кіберінциденти, а також кіберполігонів – перший та найважливіший крок на цьому шляху.

Література

1. Гавриляк В. Б. Державні механізми провадження кібербезпеки в Україні : дис. ... доктор. філософії : 281. Харків, 2021. 230 с.

2. Топчій В. В. Проблемні питання забезпечення кібербезпеки в Україні. *Аналітично-порівняльне правознавство.* 2025. № 1. С. 664–669.

3. Завгородня Ю. В. Державна політика в сфері кібербезпеки в умовах повномасштабної війни. *Актуальні проблеми політики.* 2024. № 74. С. 62–66.

4. Кавин С. Я. Правові засади забезпечення кібербезпеки в державах –

членах Європейського Союзу. *Актуальні проблеми держави і права.* 2020. № 87. С. 51–58.

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України” : Указ Президента України від 26.08.2021 р. № 447/2021. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 22.06.2025).

6. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року “Про План реалізації Стратегії кібербезпеки України” : Указ Президента України від 01.02.2022 р. № 37/2022. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/37/2022#n5 (дата звернення: 22.06.2025).

7. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 19.12.2023 р. № 1163-р. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (дата звернення: 22.06.2025).

8. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 р. № 204-р. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (дата звернення: 22.06.2025).

9. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 р. № 4336-IX. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/4336-IX#Text (дата звернення: 22.06.2025).

10. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 22.06.2025).

11. Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : постанова Кабінету Міністрів України від 04.06.2025 р. № 669. Дата оновлення: 22.06.2025. URL: https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-polozhennia-pro-administratsiiu-derzhavnoi-sluzhby-s669040625 (дата звернення: 22.06.2025).

12. Перший кіберцентр в Україні. Як він захищатиме державу і кожного з нас?. URL: https://www.epravda.com.ua/columns/2021/05/14/673864/ (дата звернення: 22.06.2025).

13. Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування : Закон України від 08.07.2010 р. № 2464-VI. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2464-17#top (дата звернення: 22.06.2025).

14. Про Державний бюджет України на 2025 рік : Закон України від 19.11.2024 р. № 4059-IX. Дата оновлення: 22.06.2025. URL: https://zakon.rada.gov.ua/laws/show/4059-20 (дата звернення: 22.06.2025).

15. Арсенович Л. А. Сучасний стан організації кіберосвіти в умовах особливого періоду. *Державне управління: удосконалення та розвиток.* 2022. № 9.

References

1. Havryliak, V.B. (2021), "State mechanisms of implementation of cyber security in Ukraine", Ph.D., Kharkiv, Ukraine.

2. Topchii, V.V. (2025), "Problematic issues of cyber security in Ukraine", *Analitychno-porivnialne pravoznavstvo,* vol. 1, pp. 664–669.

3. Zavhorodnia, Y.V. (2024), "State policy in the field of cyber security in conditions of full-scale war", *Aktualni problemy polityky,* vol. 74, pp. 62–66.

4. Kavyn, S.Y. (2020), "Legal principles of ensuring cyber security in the member states of the European Union", *Aktualni problemy derzhavy i prava,* vol. 87, pp. 51–58.

5. Office of the President of Ukraine (2021), Decree “On the decision of the National Security and Defense Council of Ukraine dated On May 14, 2021, “On the Cybersecurity Strategy of Ukraine””, available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text (Accessed 22.06.2025).

6. Office of the President of Ukraine (2022), Decree “On the decision of the National Security and Defense Council of Ukraine from On December 30, 2021, “On the Implementation Plan of the Cybersecurity Strategy of Ukraine””, available at: https://zakon.rada.gov.ua/laws/show/37/2022#n5 (Accessed 22.06.2025).

7. Cabinet of Ministers of Ukraine (2023), Order “On the approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (Accessed 22.06.2025).

8. Cabinet of Ministers of Ukraine (2025), Order “On the approval of the 2025 action plan for the implementation of the Cybersecurity Strategy of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (Accessed 22.06.2025).

9. The Verkhovna Rada of Ukraine (2025), The Law of Ukraine “On making changes to some laws of Ukraine regarding information protection and cyber protection of state information resources, objects of critical information infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/4336-IX#Text (Accessed 22.06.2025).

10. The Verkhovna Rada of Ukraine (2006), The Law of Ukraine “On the State Service of Special Communications and Information Protection of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/3475-15#Text (Accessed 22.06.2025).

11. Cabinet of Ministers of Ukraine (2025), Resolution “On making changes to the Regulations on the Administration of the State Service for Special Communications and Information Protection of Ukraine”, available at: https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-polozhennia-pro-administratsiiu-derzhavnoi-sluzhby-s669040625 (Accessed 22.06.2025).

12. The official website of the Internet edition of “Economic Truth” (2021), “The first cyber center in Ukraine. How will he protect the state and each of us?”, available at: https://www.epravda.com.ua/columns/2021/05/14/673864/ (Accessed 22.06.2025).

13. The Verkhovna Rada of Ukraine (2010), The Law of Ukraine “On the collection and accounting of a single contribution to mandatory state social insurance”, available at: https://zakon.rada.gov.ua/laws/show/2464-17#top (Accessed 22.06.2025).

14. The Verkhovna Rada of Ukraine (2024), The Law of Ukraine “On the State Budget of Ukraine for 2025”, available at: https://zakon.rada.gov.ua/laws/show/4059-20 (Accessed 22.06.2025).

15. Arsenovych, L.A. (2022), “The current state of the organization of cyber education in the conditions of a special period”, *Derzhavne upravlinnia: udoskonalennia ta rozvytok,* vol. 9.

Стаття надійшла до редакції 24.06.2025 р.