Yaroslav Pushak, Doctor of Economic Sciences, Professor
Lviv State University of Internal Affairs
Lviv, Ukraine

Nataliia Trushkina, Candidate of Economic Sciences,
Senior Researcher
Research Center for Industrial Development Problems
of National Academy of Sciences of Ukraine
Kharkiv, Ukraine

DOI: https://doi.org/10.30525/978-9934-26-306-4-8

FORMATION OF A NATIONAL EDUCATIONAL SYSTEM FOR TRAINING PERSONNEL IN THE FIELD OF INFORMATION SECURITY MANAGEMENT

ФОРМУВАННЯ НАЦІОНАЛЬНОЇ ОСВІТНЬОЇ СИСТЕМИ ПІДГОТОВКИ КАДРІВ У СФЕРІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

На даний час в умовах війни актуалізуються проблеми підготовки та підвищення кваліфікації кадрів у сфері інформаційної та кібернетичної безпеки. Це відповідає основним положенням законів України «Про стимулювання розвитку цифрової економіки в Україні», «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України, розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації», у яких йдеться про створення системи підготовки кадрів та підвищення компетентності фахівців різних видів економічної діяльності з питань кібербезпеки та кіберзахисту.

Отже, для модернізації національної освітньої системи в умовах російської агресії проти України необхідним є розроблення й реалізація комплексу заходів з підготовки та підвищення кваліфікації кадрів у сфері управління інформаційною безпекою [1–3] з урахуванням сучасних викликів. Серед них можна вказати такі: активне застосування цифрових технологій та інформаційних систем при організації бізнес-процесів [4; 5]; формування необхідного кадрового та інфраструктурного забезпечення [6; 7] розвитку

університетської освіти на засадах публічно-приватного партнерства тощо.

За даними Державної служби статистики України, частка видатків на вищу освіту у ВВП становила у 2021 р. лише 1,3% (у 2010 р. – 2,3%). Питома вага видатків на вищу освіту складала у 2021 р. 2,5% загальних видатків зведеного бюджету (у 2000 р. – 4,7%), а у загальному обсязі видатків зведеного бюджету на освіту – 16,5% (у 2000 р. – 32,3%).

Як свідчить статистичний аналіз, кількість студентів, які здобували вищу освіту за напрямом підготовки «Інформаційна безпека» (галузь знань «Безпека»), скоротилася за 2018–2022 рр. на 99,9%, а випущених із закладів вищої освіти (університети, академії, інститути) – на 99,6% (табл. 1). За цей період підготовка фахівців здійснювалася за освітньо-кваліфікаційним рівнем «бакалавр».

Таблиця 1

Підготовка фахівців у закладах вищої освіти за напрямом підготовки «Інформаційна безпека» (ІБ)

Навчальні роки	Кількість студентів, які здобували вищу освіту		Кількість випущених фахівців із ЗВО	
	усього	З них за напрямом підготовки ІБ	усього	З них за напрямом підготовки ІБ
2018/2019	242487	1175	171150	525
2019/2020	39271	38	133413	471
2020/2021	10676	3	26892	37
2021/2022	1418	1	7963	2

Джерело: складено на основі статистично-інформаційних матеріалів, які розміщено у розділі «Освіта» на офіційному сайті Державної служби статистики України

Глобальне дослідження Ernst & Young Global Information Security Survey 2018-19 «Кібербезпека – більше, ніж захист?» показує, що кібербезпека залишається важливим питанням порядку денного більшості компаній та організацій (в опитуванні взяли участь понад 1400 керівників найбільших міжнародних компаній з доходами від 10 млн дол. США). При цьому 60% організацій стверджують, що співробітники, які безпосередньо відповідальні за забезпечення інформаційної безпеки, не є членами рад директорів. Як зазначено у Звіті Центру кібербезпеки Всесвітнього економічного форуму (WEF) «Глобальні перспективи кібербезпеки до 2022 року», 59% усіх

респондентів вважають складним адекватно реагувати на інцидент кібербезпеки через брак кваліфікованих фахівців у їхній команді.

У сучасних умовах підвищеного попиту на професіоналів у сфері кібербезпеки продовжує зростати дефіцит кваліфікованих кадрів. Так, у результаті дослідження «Cybersecurity Workforce Study» виявлено, що глобальна нестача кадрів у сфері кібербезпеки становила у 2022 р. 3,4 млн осіб, при цьому 70% організацій мають незакриті вакансії. Багато держав працюють над зменшенням цього дефіциту. А великі компанії, такі як Google, Microsoft, IBM, запроваджують різні ініціативи, які спрямовано на навчання та підвищення кваліфікації персоналу у сфері кібербезпеки. Тим часом Всесвітній економічний форум спільно з кількома компаніями запустив освітню онлайн-платформу «Cybersecurity Learning Hub». Метою цього проєкту є навчання та удосконалення навичок фахівців з проблем кібербезпеки для забезпечення якісної роботи у цій сфері.

Якщо розглядати Україну, то слід відмітити, що заклади вищої освіти щороку випускають близько 2 тис. фахівців у сфері кібербезпеки та захисту інформації. Але цієї кількості недостатньо, щоб покрити потреби ринку інформаційних послуг. Крім цього, суттєва проблема полягає у відсутності практичних навичок студентів. Тому для вирішення даної проблеми заклади вищої освіти, які здійснюють підготовку фахівців у сфері безпеки інформаційних і комунікаційних систем, укладають меморандуми з Державною службою спеціального зв'язку та захисту інформації України. Відповідно до укладених меморандумів про співпрацю студенти мають можливості проходити навчання у Тренінговому центрі UA30, де здобувають практичні навички, відпрацьовуючи сценарії протидії кібератакам на спеціальних тренажерах.

На думку заступника Голови Державної служби спеціального зв'язку та захисту інформації України з питань цифрового розвитку, цифрових трансформацій і цифровізації В. Жори [8], для вирішення актуальних проблем нестачі необхідної кількості кадрів у сфері кібербезпеки і недостатніх практичних навичок випускників потрібна ґрунтовна системна робота бізнесу і держави (табл. 2).

Отже, для поліпшення ситуації при підготовці кадрів у сфері управління інформаційною безпекою необхідно якісно змінювати систему вітчизняної вищої освіти, яка має адаптуватися до принципово нових вимог ринків праці та інформаційно-комунікаційних послуг. Це, у першу чергу, обумовлено трансформацією

системи підготовки кадрів у сфері кібербезпеки з урахуванням умов воєнного і повоєнного періодів.

Таблиця 2

Ключові питання співпраці держави і бізнесу у напрямі підвищення кваліфікації кадрів з управління інформаційною безпекою

Пріоритетні напрями співпраці	Суть
Активна участь бізнесу при формуванні вимог до знань і компетенцій фахівців із кібербезпеки	Україна впроваджує досвід США і країн ЄС у сфері освіти за спеціальністю «Кібербезпека»
Підтримка освітніх ініціатив і молодих талантів у сфері кібербезпеки	Деякі українські компанії пропонують програми стажування для студентів; ІТ-компанії в Україні взаємодіють із закладами вищої освіти для підготовки кадрів
Організація національних змагань і навчальних тренінгів для розвитку практичних навичок у студентів	У ЄС розвитком кадрового потенціалу у сфері кібербезпеки на найвищому рівні займається Європейське агентство з мережевої та інформаційної безпеки

Джерело: складено на основі [8]

Для цього варто реалізовувати національний освітній проєкт, який має охоплювати такі важливі складові: 1) зміцнення кіберстійкості держави за рахунок тісної співпраці закладів вищої освіти з урядом України (Міністерством цифрової трансформації України, Державною службою спеціального зв'язку та захисту інформації України та Радою національної безпеки і оборони України); 2) підтримка університетів для збільшення кількості фахівців у сфері управління інформаційною безпекою та поліпшення якості їх навчання; 3) підвищення кваліфікації експертів із кібербезпеки за допомогою навчальних і практичних тренінгів і вебінарів; 4) налагодження контактів між українськими закладами вищої освіти із міжнародною академічною та університетською спільнотою.

З метою успішного впровадження даного освітнього проєкту, у першу чергу, пропонується внести зміни і доповнення до Стратегії національної безпеки України і Стратегії інформаційної безпеки України в частині створення належних інституційних умов для формування кадрового потенціалу у сфері кібербезпеки. Встановлено, що доцільно розробити й схвалити Концепцію розвитку

цифрової економіки та суспільства України на 2023–2027 роки, у якій визначити механізми підготовки кадрів у сфері інформаційної безпеки держави у контексті цифрових трансформацій, а також затвердити План щорічних заходів щодо її реалізації. Це й стане напрямом подальших наукових досліджень.

Література:

1. Bezpartochna O., Pushak Ya., Trushkina N. Current issues of information security management during the state of martial. *Current issues of security management during martial law*: scientific monograph. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2022. P. 8–19.
2. Пушак Я.Я., Трушкіна Н.В. Правове забезпечення економічної безпеки держави в умовах Індустрії 4.0. *Цифрова економіка та економічна безпека*. 2022. Вип. 1(01). С. 135–142. DOI: https://doi.org/10.32782/dees.1-22
3. Бойко О.В., Пушак Я.Я., Трушкіна Н.В. Формування сучасної парадигми інформаційної безпеки національної економіки: теоретичні засади. *Вісник післядипломної освіти. Сер.: Соціальні та поведінкові науки*. 2022. Вип. 22(51). С. 139–160. DOI: https://doi.org/10.32405/2522-9931-2022-22(51)-139-160
4. Trushkina N. Development of the information economy under the conditions of global economic transformations: features, factors and prospects. *Virtual Economics*. 2019. Vol. 2. № 4. P. 7–25. DOI: https://doi.org/10.34021/ve.2019.02.04(1).
5. Kryshtanovych S., Prosovych O., Panas Y., Trushkina N., Omelchenko V. Features of the Socio-Economic Development of the Countries of the World under the influence of the Digital Economy and COVID-19. *International Journal of Computer Science and Network Security*. 2022. Vol. 22. No. 1. P. 9–14. DOI: https://doi.org/10.22937/IJCSNS.2022.22.2.2
6. Khaustova V., Tirlea M. R., Dandara L., Trushkina N., Birca I. Development of Critical Infrastructure from the Point of View of Information Security. *UNIVERS STRATEGIC – Revistă de Studii Strategice Interdisciplinare și de Securitate*. 2023. Anul XIV. Nr. 1(53). P. 170–188.
7. Current issues of the management of socio-economic systems in terms of globalization challenges: scientific monograph. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2023. 679 p.
8. Жора В. Кібербезпека потребує кадрів: чому держава та бізнес повинні співпрацювати. *Економічна правда*. 2023. 27 лютого. URL: https://www.epravda.com.ua/columns/2023/02/27/697467