DOI: https://doi.org/10.36059/978-966-397-306-7-54

ТРАНСФОРМАЦІЯ СИСТЕМИ ПІДГОТОВКИ КАДРІВ ТА ПІДВИЩЕННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ФАХІВЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ

Трушкіна Н.В.
кандидат економічних наук, старший дослідник, докторант,
старший науковий співробітник
сектору промислової політики та інноваційного розвитку
відділу промислової політики та енергетичної безпеки,
Науково-дослідний центр індустріальних проблем розвитку
Національної академії наук України
м. Харків, Україна

В останні роки спостерігається тенденція зміни парадигми інформаційної безпеки України [1–3] у напрямі цифрової трансформації економічних систем. Сучасний етап цифровізації національної економіки в умовах Індустрії 4.0 характеризується інтеграцією широкого спектру кіберфізичних систем, великих баз даних, штучного інтелекту, блокчейну, інноваційних і фінансових технологій, інформаційних інфраструктур, цифрових платформ і сервісів тощо. Однак це, у свою чергу, призводить до появи кіберзагроз і ризиків інформаційної безпеки держави. І особливо це пов'язано з повномасштабною вторгненням росії на територію України.

Тому 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 освітню діяльність у сфері інформаційних технологій; створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки та кіберзахисту.

Отже, для успішного функціонування національної системи університетської освіти в Україні в умовах війни доцільним є розроблення й реалізація комплексу заходів з підготовки та підвищення кваліфікації кадрів у сфері управління інформаційною безпекою з урахуванням сучасних викликів. Серед них можна назвати стрімкий

розвиток цифрової економіки [4–5]; формування необхідного кадрового та інфраструктурного забезпечення [6], дієвої моделі публічно-приватного партнерства та належного контролю за кіберзахистом тощо.

На підставі статистичного аналізу виявлено ряд проблем, які стримують ефективний розвиток вищої освіти в Україні. Так, 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 аналіз, кількість студентів, які здобували вищу освіту за напрямом підготовки «Інформаційна безпека» (галузь знань «Безпека»), скоротилася за 2018–2022 рр. на 99,9 % (з 1175 до 1 особи), а випущених із закладів вищої освіти (університети, академії, інститути) – на 99,6 % (з 525 до 2 осіб). За цей період підготовка фахівців здійснювалася за освітньо-кваліфікаційним рівнем «бакалавр».

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 [7], для вирішення актуальних проблем нестачі необхідної кількості кадрів у сфері кібербезпеки і недостатніх практичних навичок випускників потрібна ґрунтовна системна робота бізнесу і держави. Суть даної співпраці полягає у такому: 1) 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». Стандарти для перших шести професій розроблено Державною службою спеціального зв'язку та захисту інформації України за підтримки проєкту USAID «Кібербезпека критично важливої інфраструктури України». У 2023 р. буде продовжено роботу ще над 14 стандартами); 2) підтримка освітніх ініціатив і молодих талантів у сфері кібербезпеки (деякі українські компанії пропонують програми стажування для студентів; IT-компанії в Україні взаємодіють із закладами вищої освіти для підготовки кадрів); 3) змагання та тренінги для розвитку практичних навичок у студентів (наприклад, у Європейському Союзі розвитком кадрового потенціалу у сфері кібербезпеки на найвищому рівні займається Європейське агентство з мережевої та інформаційної безпеки (ENISA), яке формує політику в цьому напрямі. Щорічно ENISA проводить Європейський челендж з кібербезпеки (ECSC), завданням якого є залучення та розвиток молодих талантів. У 2023 р. в Україні вперше проведено національні змагання з кібербезпеки UA30CTF за підтримки проєкту EU4DigitalUA, що фінансується Європейським Союзом).

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. 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.

Список використаних джерел:

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 [Dezvoltarea infrastructurii critice din punct de vedere al securității informațiilor]. *UNIVERS STRATEGIC – Revistă de Studii Strategice Interdisciplinare şi de Securitate*. 2023. Anul XIV. Nr. 1(53). P. 170–188.

7. 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/