context of the UN SDG. Therefore, the principles of cooperation formulated in the R&I-2021 Strategy, namely academic freedom, research ethics and integrity, gender equality, diversity and inclusiveness, open data and open science, international standards of R&I activities, evidence-informed policymaking turned into a categorical imperative of researchers, innovators and educators around the world.

Key words: *strategy, European Union, Research and Innovation (R&I), international cooperation, approach.*

УДК 378.09:004.056](477:410)(045)

Ольга Ящук
Київський національний лінгвістичний університет
ORCID ID 0000-0003-2991-0801
DOI 10.24139/2312-5993/2021.09/250-264

КІБЕРБЕЗПЕКА: ПОРІВНЯЛЬНІ АСПЕКТИ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В КОНТЕКСТІ ПІДГОТОВКИ КАДРІВ В УКРАЇНІ Й ВЕЛИКІЙ БРИТАНІЇ

Тенденції технологічної еволюції цифрового суспільства зумовлюють формування запиту на професії, які є запорукою захищеності громадян у нестабільних умовах. У контексті сучасних загроз і викликів питання забезпечення ринку праці кваліфікованими фахівцями в галузі кібербезпеки є пріоритетом державної політики, що потребує вдосконалення освітньої бази для їхньої підготовки. У статті висвітлено сутність термінів, що визначають специфіку приналежності до діяльності в галузі кібербезпеки. Проаналізовано чинники затребуваності й аспекти професійної діяльності кіберфахівців в Україні та Великій Британії. Виокремлено гуманітарний складник оптимізації підготовки кадрів для кібербезпекової галузі.

Ключові слова: *кібербезпека, фахівець із кібербезпеки, кіберпростір, професійна діяльність, професія, підготовка, університет, розвиток, аспект, сучасний.*

Постановка проблеми. У наш час затребуваність суспільством підготовлених кваліфікованих кадрів у галузі кібербезпеки зумовлена повсюдним упровадженням інноваційних інформаційно-комп'ютерних технологій, що призводить до зміни форм, способів, інструментів діяльності сучасного громадянина у вимірі цифрової дійсності. Зростає попит на професіоналів, коло компетентностей яких уможливлює забезпечення захисту й міцності всіх ланок «цифрового ланцюга» – численних сфер людської активності, що передбачають перехід у віртуальну, цифрову площину або залежать від безперебійного функціонування комп'ютерно-комунікаційних мереж та електронних сервісів.

Долучимося до думки українських науковців щодо усвідомленості того факту, що сьогодні «перед національною освітою поставлено якісно нові завдання, що відображають нові світові тенденції» (Бєлова, 2021, с. 489). У цьому сенсі у вітчизняних закладах вищої освіти, зокрема, технічних університетах, відбуваються позитивні зрушення щодо сучасного

формату підготовки фахівців із кібербезпеки – до освітньої діяльності в цьому напрямі залучаються кваліфіковані інженерно-педагогічні кадри, напрацьовується освітньо-нормативне підґрунтя, що регулює механізм підготовки майбутніх кіберфахівців, створюються програми, проєкти, заходи, спрямовані на реалізацію творчого потенціалу й формування їхнього практичного досвіду. Разом із тим, професійна система підготовки кадрів для кібергалузі ще не сформована настільки потужно, щоб упевнено стверджувати про її фундаментальність і ефективність у вітчизняному сегменті: розробленості потребує методологія вишколу, взаємоузгодженості – зміст, завдання, вимоги та результат підготовки; актуальними залишаються матеріально-технічні аспекти забезпечення.

У зазначеному контексті окреслюється необхідність досліджувати освітній досвід країн, уряди яких маркують розвиток кібербезпекової галузі як пріоритет, що є запорукою економічної стабільності й державної непорушності. З огляду на це проаналізуємо аспекти, дотичні до розуміння призначеності професії в галузі кібербезпеки, зокрема, через призму порівняльного досвіду Великої Британії як однієї з найбільш потужних держав світу за рівнем розвитку інноваційних технологій і світового взірця якості освіти.

Аналіз актуальних досліджень. У розділі 2 тексту чинної «Стратегії кібербезпеки України» (2021) щодо стану реалізації положень «Стратегії…» від 2016 р. зазначено, що «було докладено зусиль до становлення та розвитку національної системи кібербезпеки», однак «невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства» і, крім того, «недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки» (*Про рішення Ради…,* 2021). З-поміж низки описаних у документі передумов, що формують загрози для національного кіберпростору, визначено, зокрема, «невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців із питань кібербезпеки та кіберзахисту…» (*Про рішення Ради…,* 2021). Визнання актуальності проблеми на державному рівні в нашій країні засвідчує, що в такому потужному сегменті національної безпекової політики як у найближчій (особливо в зв’язку з гібридною агресією, від якої потерпає наша країна), так і у віддаленій (з огляду на постійний науково-технічний розвиток і вдосконалення комп’ютерних технологій, що створює також ризики їхнього недоброчесного використання) перспективах триватиме складна, кропітка

робота, зокрема, у напрямі забезпечення кібербезпекової галузі кваліфікованими, компетентними кадрами.

У цій площині, незважаючи на порівняно молодий, у реаліях фахової підготовки у вітчизняній системі вищої освіти, вік професії, назва якої в широкому сенсі відома як «фахівець із кібербезпеки», науковцями вироблено певний досвід теоретичного, методичного, освітньо-нормативного контекстів вишколу майбутніх кіберфахівців, що засвідчують наукові роботи Б. Бистрової (вивчено проблематику професійної підготовки бакалаврів із кібербезпеки в закладах вищої освіти США) (2018), Б. Брайко (досліджено специфіку професійної підготовки магістрів із кібербезпеки в університетах Великої Британії) (2020), І. Діордіци (висвітлено недоліки в проєктуванні освітньо-нормативної бази підготовки фахівців із кібербезпеки) (2017), О. Євсюкової (проаналізовано особливості підготовки фахівців у сфері кібербезпеки у вимірі розвитку сучасного суспільства) (2021), О. Матвійчук-Юдіної (визначено концепцію формування компетентностей фахівців у сфері інформаційних технологій та кібербезпеки (2019). Разом із тим, зважаючи на чинник часу щодо гармонізації освітньо-професійної підготовки фахівців кібергалузі з випереджальним європейським освітнім досвідом, ми прагнемо послідовно продовжувати вивчення проблемних аспектів, акцентуація на яких уможливить детальніше розкриття сутності фаху в галузі кібербезпеки в сучасному вимірі й розроблення алгоритму оптимізації підготовки кадрів для цієї професійної сфери.

Мета статті. Вивчення аспектів професійної підготовки кіберфахівців є концептуальною частиною пошукувань, що формують зміст нашого наукового дослідження. Метою статті є висвітлення в зіставному контексті окремих чинників, що сприяють формуванню чіткішого уявлення про специфіку діяльності в галузі кібербезпеки в Україні й Великій Британії.

Методи дослідження. Наш науковий пошук сфокусовано в порівняльній площині; напрацювання матеріалу статті за своєю специфікою спирається на метод аналізу. Логіку викладу сформовано на основі порівняльного аналізу нормативно-законодавчої бази, джерел, репрезентованих українськими та британськими інформаційними ресурсами й наукових досліджень учених.

Виклад основного матеріалу. Парадигма цифровізації як вияву сучасного етапу науково-технічного прогресу й мегатренду технологічного розвитку суспільства ґрунтується на використанні інноваційних технологій, що трансформують зміст і способи людської діяльності в багатьох сферах. Спостережено, що в ХХ столітті «людство, використовуючи сучасні

інформаційно-комунікаційні технології, розширило значення інформації в якості ресурсу свого розвитку, збільшено й значення інтелектуальних можливостей громадян», а в наш час потужним ресурсом, що дає змогу істотно збільшити ефективність та продуктивність діяльності, є цифрові дані та мережеві транзакції як ключові фактори та засоби виробництва (Соснін, 2020; Україна 2030Е…). У цьому контексті чітких обрисів набуває питання сталості кіберпростору – віртуального електронного середовища, у якому процеси збереження, модифікації, обміну інформації і даних зумовлені взаємодією обчислювального складника, функціонуванням електронних комунікаційних мереж, роботою електронних комунікацій, опосередкованої відповідними технічними засобами й пристроями. Вирішення проблем забезпечення стійкості кіберпростору до втручань – від зловмисних маніпуляцій із особистими даними до збоїв у системі критичної інфраструктури (банки, енергетика, виробництво тощо) в глобальних масштабах підпадає в зону компетентностей фахівців із кібербезпеки. Попит на кіберфахівців зумовлений, передусім, необхідністю забезпечення програмного та технічного захисту інформації, що становить державну або комерційну таємницю в таких сферах: приватні й державні підприємства різного профілю; науково-дослідні установи; органи державного управління та місцевого самоврядування; підрозділи кіберполіції Міністерства внутрішніх справ; Державна податкова служба; Державна митна служба; Державна служба спеціального зв’язку та захисту інформації; банківські установи та бізнес-структури; підрозділи захисту інформації залізничного та повітряного транспорту (*Національний університет…*). Зазначений контекст транслює ідею про те, що фахівець із кібербезпеки – це охоронець порядку в цифрову епоху (Cybersecurity guide). Водночас слушною є думка дослідника проблематики кібербезпеки І. Діордіци, який відзначає гуманістичний складник змісту професійної діяльності фахівців із кібербезпеки, пов’язуючи її «не з власне технічними питаннями, а із захистом прав людини через повноцінне функціонування суспільних і державних інституцій, розвиток громадянського суспільства» (Діордіца, 2017, с. 52).

Незважаючи на об’єктивні труднощі, зумовлені, передусім, політичною й економічною нестабільністю в нашій державі, й освітніми, що наразі тривають, реформами на всіх рівнях на шляху до консолідації з вимогами ЄС, вітчизняна технічна вища освіта, узгоджуючись із ритмом часу і потребами сьогодення, долає непростий шлях трансформації її змісту з переорієнтацією підготовки фахівців для реального життя та практичної реалізації вмінь і знань у професійній діяльності. Так, кадровий потенціал

для кібергалузі забезпечується, у першу чергу, технічними закладами вищої освіти України. Зокрема, мають напрацьовану навчально-методичну базу для підготовки кіберфахівців Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» (Фізико-технічний інститут, кафедра інформаційної безпеки), Національний авіаційний університет (факультет кібербезпеки, комп'ютерної та програмної інженерії, кафедра безпеки інформаційних технологій), Національний технічний університет «Харківський політехнічний інститут» (факультет комп'ютерних та інформаційних технологій, кафедра обчислювальної техніки та програмування), Національний університет «Львівська політехніка» (Інститут комп'ютерних технологій, автоматики та метрології, кафедра захисту інформації), Державний університет «Одеська політехніка» (Інститут бізнесу, економіки та інформаційних технологій, кафедра кібербезпеки та програмного забезпечення), Вінницький національний технічний університет (факультет інформаційних технологій та комп'ютерної інженерії, кафедра вищої математики; факультет менеджменту та інформаційної безпеки, кафедра менеджменту та безпеки інформаційних систем). І це далеко не повний перелік освітніх інституцій в Україні, керівництво яких усвідомлює гостроту запиту ринку праці й суспільства на кіберфахівців і перспективність розвитку кібербезпекової галузі в сучасному вимірі цифровізації як мегатренду глобальної спільноти.

Для чіткішого розуміння змісту діяльності, що маркується зазначеним професіонімом (слід зауважити, що таке узагальнене формулювання назви професії відсутнє в Національному класифікаторі України ДК 003:2010 «Класифікатор професій»), звернімося до обґрунтування сутності поняття «кібербезпека». На сайтах випускових кафедр, що залучають абітурієнтів і займаються підготовкою майбутніх фахівців із кібербезпеки за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології») подається роз'яснювальна інформація щодо змісту спеціальності, цілей, завдань підготовки й перспектив працевлаштування, у контексті якої кібербезпека визначається як «застосування технологій і методів захисту комп'ютерних систем, мереж, програм і даних у кіберпросторі від несанкціонованого доступу, зміни, знищення та інших кіберзагроз», «інженерна спеціальність, призначена для підготовки фахівців, які володіють набором засобів забезпечення безпеки кіберсередовища, ресурсів організацій і користувачів» (Інформаційний сайт абітурієнта ТНТУ; ІСТ). На думку М. Грайворонського (кафедра інформаційної безпеки Фізико-технічного інституту НТУУ «КПІ ім.

І. Сікорського»), розширеність предмету кібербезпеки ґрунтується на підставах того, що «кіберпростір охоплює і комп'ютерні мережі, і всі пристрої, які в цих мережах працюють, і всі комп'ютерні технології, і людей, які ці технології і пристрої застосовують». Отже, робота фахівця з кібербезпеки масштабована до вияву вразливості в системі, відстеження надзвичайних подій у мережі, установлення захисного софту й обладнання, вживання заходів для нейтралізації кіберзагроз (ДУІТЗ).

Поняття «фахівець із кібербезпеки» ввібрало достатньо широкий зміст діяльності з погляду професійних можливостей і компетентностей; разом із тим, у реальному професійному середовищі таких фахівців диференціюють відповідно до специфіки обраного напряму й сукупності методів, що використовуються для забезпечення безпеки відповідного об'єкта. Зазначений аспект наразі відображено в оновленому Національному класифікаторі України ДК 003:2010 «Класифікатор професій» через унесення (відповідно до тенденцій розвитку сучасного суспільства й потреб ринку праці) переліку «професійних назв роботи» за спільним кодом професії 2139.2. Фахівці кібербезпекової сфери розмежовуються за зонами професійної компетентності, що, таким чином, значно розширює діапазон застосування знань і вмінь. Так, випускник технічного університету або технічного факультету закладу вищої освіти, працевлаштовуючись, може орієнтуватися на перелік відповідних професій у КП: аналітик загроз безпеки, аналітик систем захисту інформації та оцінки вразливостей, аналітик з безпеки інформаційно-телекомунікаційних систем, дізнавач (сфера кібербезпеки та захисту інформації), експерт-криміналіст (сфера кібербезпеки та захисту інформації), експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації), слідчий з кіберзлочинів, фахівець з криптографічного захисту інформації, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець з підтримки інфраструктури кіберзахисту, фахівець з реагування на інциденти кібербезпеки, фахівець з тестування систем захисту інформації, фахівець з технічного захисту інформації, фахівець сфери захисту інформації (*Наказ…,* 2021). Принагідно зазначимо доцільність звіряння назв професій за Національним класифікатором України ДК 003:2010 «Класифікатор професій» з метою уникнення термінологічної плутанини й розуміння аспектів і напрямів професійної діяльності осіб у тій чи іншій галузі. Так, відповідно до «КП», «фахівець» – це складник назв певних професійних робіт. В описі розділу класифікації відповідної професії передбачається, що фахівець володіє знаннями в одній чи більше галузях

природознавчих, технічних і гуманітарних наук і має освітню кваліфікацію за початковим (коротким циклом) рівнем вищої освіти і в окремих випадках – першим (бакалаврським) рівнем вищої освіти» (*Наказ…,* 2021; Національний класифікатор). На противагу зазначеному, «у повсякденному житті ми сприймаємо «фахівця» як людину, що володіє спеціальними знаннями й навичками в будь-якій галузі, простіше кажучи – майстра своєї справи» (Носіков, 2021). У «Словнику української мови» фахівець тлумачиться як «той, хто досконало володіє якимось фахом, має високу кваліфікацію, глибокі знання з певної галузі науки, техніки, мистецтва тощо; спеціаліст» (*Словник…*). Тобто, вже усталений у професійному й суспільному обігу професіонім «фахівець із кібербезпеки» розширено маркує задіяність у кібербезпековій галузі й використовується в загальному контексті володіння професійною справою. Водночас, конкретніші, прикладні аспекти фахового змісту діяльності в сфері кібербезпеки зафіксовані в зазначених вище назвах професійних робіт у «КП».

У професійній лексиці англійської мови віднесеність до діяльності в кібербезпековій галузі передається через професіонім, семантика якого вирізняється узагальненістю позначуваного фаху – «cyber security specialist» («фахівець із кібербезпеки»). Поліваріантність терміна «кібербезпека» знаходить вияв у позначенні ним галузі діяльності; спеціальності (в українській освітньо-нормативній документації – «125 Кібербезпека»), а, наприклад, на сайті Ради кібербезпеки Сполученого Королівства кібербезпека тлумачиться як «мультидисциплінарна професія» (UK Cyber security council). З прив’язкою до цього визначення подано назви спеціалізацій («specialisms»), зумовлених відповідними напрямами (секторами) діяльності: цифрова криміналістика (digital forensics), cyber threat intelligence (розвідка кіберзагроз), cyber security management (управління кібербезпекою), secure operations (безпечні операції), incident response (реагування на інцидент), network monitoring & intrusion detection (моніторинг мережі та виявлення втручань), cryptography & communications security (криптографія та безпека комунікацій), identity & access management (управління ідентіфікацією та доступом), data protection & privacy (захист даних і конфіденційність), secure system architecture & design (архітектура та проєктування безпечної системи), secure system development (розробка безпечної системи), security testing (тестування безпеки), cyber security governance & risk management (управління кібербезпекою та ризиками), cyber security audit & assurance (аудит та забезпечення кібербезпеки) (*UK Cyber security council*). Важливо

підкреслити, що в реаліях акумулювання британського освітньо-професійного досвіду в цій сфері всі ці грані реалізації кібербезпекової діяльності вписані в гуманістичну парадигму взаємовідносин, що ґрунтуються на сукупності психологічних складників, морально-етичних принципів і ціннісних ставлень. Передусім, мова йде про людиноорієнтованість комп'ютерів і комп'ютерних технологій; розуміння шляхів взаємодії людини з цифровими системами або через їх застосування: розуміти принципи розроблення для цільових користувачів і також розуміти, як працюють і як використовують ці системи зловмисники. Важливе значення також надається врахуванню таких психолого-соціальних складників професійної інтеракції, як практичність (зручність і простота використання), довіра, практика співпраці, соціальна інтегрованість, громадянськість, культурне розмаїття та взаємозв'язок мікросоціальних взаємодій і глобальних структур (*Cyber security Oxford*). Такий зразок мікрорівня соціальних відносин в умовах освітньо-професійної діяльності вписується в зміст гуманістичного дискурсу, в якому «загальнолюдські цінності, їх внутрішній ідейний потенціал і соціально-культурний зміст експліцитно транспонуються на весь духовний простір сучасної цивілізації» (Матвієнко, 2005, с.60). На таких засадах здійснюється вишкіл фахівців із кібербезпеки у взірцевих закладах освіти, що репрезентують британську вищу освіту як бренд, насамперед, Оксфордському університеті з його потужною, що базується на фундаментальній методології й інноваційних технологіях, школою кібербезпеки «Cyber security Oxford» – спільнотою дослідників та експертів галузі; Кембріджському університеті (Cambridge Cybercrime Centre – Кембриджський центр кіберзлочинності – мультидисциплінарна ініціатива кафедри комп'ютерних наук і технологій, Інституту кримінології та юридичного факультету) (*Cyber security Oxford; University of Cambridge*). Грунтовні програми підготовки кіберфахівців мають університети Великої Британії, з великої кількості яких кібербезпеку вивчають, зокрема, у Лондонському університеті Метрополітен, Бристольському університеті, Норвічському університеті, Кентському університеті, Сасекському університеті, Единбурзькому університеті, Дублінський університеті.

Аналіз стану кібербезпеки, принципи державної політики в цьому напрямі й перспективи розвитку галузі в Сполученому Королівстві зафіксовано в «Національній стратегії кібербезпеки» на 2016-2021 роки, у передмові якої зазначено, що Сполучене Королівство – «один із світових лідерів серед цифрових націй». У документі наголошується на тому, що

«значною мірою добробут громадян залежить від здатності захистити технології, дані від великої кількості загроз, що стоять перед суспільством» (National Cyber Security Strategy). Водночас, незважаючи на те, що Велика Британія – одна з країн світу з найрозвинутішою економікою й із усталеною еталонною системою освіти, потребують вирішення питання, що стосуються нарощування людського ресурсу для забезпечення британського ринку праці кваліфікованими кадрами в галузі кібербезпеки. Такі проблеми існують і, зокрема, знаходять вияв у низькому рівні підготовки кадрів; нестачі кваліфікованих кадрів і знань, щоб задовольнити потреби в кібербезпеці в масштабах державного і приватного секторів; низькому рівні обізнаності про кібербезпеку серед персоналу в компаніях. Дефіцит фахівців у кібергалузі зумовлений недостатньою кількістю молодих людей, які обирають цю професію; недостатнім висвітленням концепцій кібернетичної та інформаційної безпеки в програмах комп'ютерних курсів; нестачею кваліфікованих викладачів для підготовки цієї професії (*National Cyber Security Strategy*).

Шляхи подолання згаданих проблем вбачаються у визначенні сукупності довгострокових, скоординованих заходів, які повинні прийняти урядові органи, підприємства, освітні установи та наукові організації для того, щоб забезпечити стабільну підготовку сертифікованих фахівців із кібербезпеки відповідно до необхідних стандартів (*National Cyber Security Strategy*). У цьому контексті суттєву допомогу в реалізації державної політики розвитку кібербезпекового виміру надає Рада кібербезпеки Великої Британії, саморегулівний орган у сфері освіти та кваліфікацій. Будь-яка організація, яка зацікавлена в просуванні, підтримці та розвитку кібербезпекових професій, може подати заявку на членство (в Раді…). Діяльність органу полягає в пропагуванні, популяризації професії в межах Сполученого Королівства і забезпеченні високих професійних стандартів через призму передових практик та інтелектуального лідерства, надання інструментів для розвитку кар'єри й освітніх ресурсів у секторі кібербезпеки, вплив на уряд, промисловість та наукові кола (RealWire; The UK Cyber security council).

Потужне підґрунтя для реалізації плану розвитку кібербезпекової галузі сформоване Національним центром кібербезпеки Великої Британії, що активно функціонує на засадах використання знань із кібербезпеки для надання практичних рекомендацій організаціям, використання галузевого й академічного досвіду для розвитку можливостей кібербезпеки у Великій

Британії, підтримки важливих організації Великої Британії, широкого громадського сектору, промисловості (*National cyber security centre*).

Отже, міцність взаємозв'язку інформаційного й кібернетичного просторів, зокрема їхніх національних сегментів, а також трансформована в такій парадигмі цифрова активність громадян і комплекс електронних сервісів, що опосередковують життєдіяльність сфер суспільства, – все це, безумовно, потребує розбудови потужного фундаменту для здійснення «охоронних» кібербезпекових заходів кваліфікованими, освіченими кадрами.

Висновки та перспективи подальших наукових розвідок. Здійснений у статті аналіз складників, що формують концепцію забезпечення кадрів і зміст професійної діяльності в галузі кібербезпеки переконує в тому, що в цій царині існує широке коло питань, які потребують подальшого ретельного вивчення в зіставній площині соціально-економічних, професійних, освітніх, педагогічних реалій, проблем, тенденцій, ідей, цінностей, закумульованих в українському та британському досвіді з метою розбудови цілісної парадигми підготовки кіберфахівців на тлі актуальних запитів суспільства і глобальних викликів, що трансформують його потреби, виводячи сучасну спільноту на новий технологічний рівень розвитку.

Одним із важливих чинників професійного творення кадрів є «міждисциплінарна педагогічно-психологічна підготовка фахівців для подальшого саморозвитку і праці в різних галузях освіти, науки та інженерії» (*Системи технічного захисту інформації,* 2020). Такий підхід вимагає обґрунтованої необхідності вивчення майбутніми кіберфахівцями дисциплін гуманітарного циклу й іноземних мов зокрема. Так, програмні результати навчання (п. 7, ПРН 1) освітньо-професійної програми для бакалаврів спеціальності 125 «Кібербезпека» (Фізико-технічний інститут «КПІ ім. І. Сікорського») орієнтовані на застосовування «знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації» (*Системи технічного захисту інформації,* 2020). Прогресивним кроком і маркером далекоглядності в усвідомленні британським урядом значущості іноземних мов для вмонтування інформації про проблематику, розвиток і перспективи кібербезпеки в глобалізаційний контекст є відображення безпекової політики в шести іншомовних (арабською, португальською, китайською, французькою, російською, іспанською мовами) варіантах «Національної стратегії кібербезпеки» Сполученого Королівства (GOV. UK…).

У такому гуманітарному вимірі викладений у статті зміст дослідницького пошуку зорієнтований на долучення до наукового

порівняльного дослідження про специфіку іншомовної підготовки фахівців із кібербезпеки в технічних університетах Великої Британії. Висвітлення ж сутності професійної підготовки й діяльності фахівців є необхідною передумовою для наукової експертизи проблематики іншомовного навчання й обґрунтування актуальності іншомовної підготовки майбутніх кіберфахівців.

Резюмуємо вищезазначене думкою про те, що розгортання кіберпростору, зумовлене інтенсивним розробленням інноваційних цифрових технологій, які активно впроваджуються в сфери життя суспільства, створює запит на обмін професійною інформацією і співробітництво в галузі кібербезпеки в міжнародному вимірі, що ґрунтується на здійсненні комунікації іноземними мовами. Беручи до уваги начасність такого дискурсу, з'ясування проблем іншомовної підготовки кіберфахівців буде формувати зміст наших подальших наукових розвідок.

ЛІТЕРАТУРА

Бєлова, В. В. До питання про проблему управління освітою в зарубіжжі: термінологічний аспект. *Педагогічні науки: теорія, історія, інноваційні технології, 3 (107),* 489-501. Режим доступу: https://pedscience.sspu.edu.ua/wp-content/uploads/2021/11/32021-%D1%84%D1%96%D0%BD%D0%B0%D0%BB.pdf (Belova, V. V. (2021). To the question about the problem of management of education abroad: terminological aspect. *Pedagogical sciences: theory, history, innovative technologies, 3 (107),* 489-501. Retrieved from: https://pedscience.sspu.edu.ua/wp-content/uploads/2021/11/32021-D1%84%D1%96%D0%BD%D0%B0%D0%BB.pdf).

Бистрова, Б. В. (2018). *Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США* (автореф. дис. ... канд. пед. наук: 13.00.04). Київ (Bystrova, B. V. (2018). *Professional training of bachelors in cybersecurity in the US higher education institutions* (PhD thesis abstract). Kyiv).

Брайко, Б. В. (2020). *Професійна підготовка магістрів з кібербезпеки в університетах Великої Британії* (автореф. дис. ... канд. пед. наук: 13.00.04). Хмельницький (Braiko B. V. (2020). *Professional training of masters in cyber security at UK Universities* (PhD thesis abstract). Khmelnytskyi).

Діордіца, І. В. (2017). Освітні стандарти підготовки фахівців із кібербезпеки. *Національний юридичний журнал: теорія і практика, 1,* 50-53. Режим доступу: http://www.jurnaluljuridic.in.ua/archive/2017/1/12.pdf (Diorditsa, I. V. (2017). Educational standards for training cyber security professionals. *National law journal: theory and practice, 1,* 13-21. Retrieved from: http://www.jurnaluljuridic.in.ua/archive/2017/1/12.pdf).

ДУІТЗ [сайт]. Кібербезпека. Режим доступу: https://onat.edu.ua/kiberbezpeka/ (SUITC [site]. *Cyber security*. Retrieved from: https://onat.edu.ua/kiberbezpeka/).

Євсюкова, О. В. (2021). Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. *Державне управління: удосконалення та розвиток, 2.* Режим доступу: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf (Evsyukova, O. V. (2021). Features of training of specialists in the field of cyber security: current

challenges and prospects. *Public administration: improvement and development, 2.* Retrieved from: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf).

Інформаційний сайт абітурієнта ТНТУ. Спеціальність 125 «Кібербезпека». Режим доступу: https://vstup.tntu.edu.ua/speciality/125-kiberbezpeka.html (*Information site of TNTU entrant. Specialty 125 «Cyber security».* Retrieved from: https://vstup.tntu.edu.ua/speciality/125-kiberbezpeka.html).

ІСТ. Яка різниця між спеціальностями 12-ої галузі? Режим доступу: https://www.ist.knu.ua/web/news/yaka-riznitsya-mij-spetsialnostyami-12-oyi-galuzi (*IST. What is the difference between the specialties of the 12th field of knowledge?* Retrieved from: https://www.ist.knu.ua/web/news/yaka-riznitsya-mij-spetsialnostyami-12-oyi-galuzi).

Матвієнко, О. В. (2005). *Стратегії розвитку середньої освіти у країнах Європейського Союзу.* Київ: Ленвіт (Matviienko, O. V. (2005). *Strategies of development of secondary education in the countries of the European Union.* Kyiv: Lenvit).

Матвійчук-Юдіна, О. В. (2019). Концепція формування професійних компетентностей фахівців з інформаційних технологій та кібербезпеки. *Наукоємні технології, 3(43),* 330-342. Режим доступу: file:///C:/Users/admin/Downloads/19747.pdf (Matviichuk-Yudina, O. V. (2019). The concept of forming professional competencies of specialists in information technology and cyber security. *Science intensive technologies, 3(43),* 330-342. Retrieved from: file:///C:/Users/admin/Downloads/19747.pdf).

Наказ Міністерства економіки України «Про затвердження Зміни № 10 до національного класифікатора ДК 003:2010» (2021). Режим доступу: https://zakon.rada.gov.ua/rada/show/v0810930-21#n10 (*Order of Ministry of Economy of Ukraine «On approval of Amendment № 10 to the national classifier DK 003: 2010»* (2021). Retrieved from: https://zakon.rada.gov.ua/rada/show/v0810930-21#n10).

Національний класифікатор України «Класифікатор професій ДК 003:2010». Режим доступу: https://zakon.rada.gov.ua/rada/show/va327609-10#Text (*National Classifier of Ukraine "Classifier of professions DK 003:2010".* Retrieved from: https://zakon.rada.gov.ua/rada/show/va327609-10#Text).

Національний університет «Львівська політехніка». Інформація для абітурієнтів. Режим доступу: https://lpnu.ua/zi/abituriientu (*Lviv Polytechnic National University. Information for entrants.* Retrieved from: https://www.cybersecurity.ox.ac.uk/research https://lpnu.ua/zi/abituriientu).

Носіков, О. М. (2021). «Фахівець» за наказом. *Перша кадрова газета «Консультант кадровика». Професійна класифікація, 9 (117).* Режим доступу: https://kadrhelp.com.ua/oformlennya-dokumentiv-za-novym-dstu-41632020. (Nosikov, O. M. (2021). "Specialist" by order. *The first personnel newspaper "HR consultant". Professional classification, 9 (117).* Retrieved from: https://kadrhelp.com.ua/oformlennya-dokumentiv-za-novym-dstu-41632020).

НТУУ «КПІ» Фізико-технічний інститут. Кафедра інформаційної безпеки. Питання і відповіді – для абітурієнтів. Режим доступу: http://is.ipt.kpi.ua/faq-dlya-abituriyentiv (*NTUU "KPI" Institute of physics and technology. Department of*

information security. Questions and answers – for university entrants. Retrieved from: http://is.ipt.kpi.ua/faq-dlya-abituriyentiv).

Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». *Указ Президента України № 447/2021 від 26.08.2021.* Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (On the decision of the National security and defense Council of Ukraine of May 14, 2021 "On the cyber security Strategy of Ukraine". *Decree of the President of Ukraine № 447/2021 of August 26, 2021.* Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021#n12).

Системи технічного захисту інформації (2020). *Освітньо-професійна програма першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».* Київ: КПІ ім. І. Сікорського. Режим доступу: http://ptmip.ipt.kpi.ua/wp-content/uploads/sites/6/2020/12/OPP-125-Bakalavr-FTSZI-2020-R8-december-020.pdf (Technical information protection systems (2020). *Educational and professional program of the first (bachelor's) level in the specialty 125 "Cyber security" in the field of knowledge 12 "Information technology".* Kyiv: KPI named after I. Sikorsky. Retrieved from: http://ptmip.ipt.kpi.ua/wp-content/uploads/sites/6/2020/12/OPP-125-Bakalavr-FTSZI-2020-R8-december-2020.pdf).

Словник української мови. Академічний тлумачний словник. Режим доступу: http://sum.in.ua/s/fakhivecj (*Ukrainian language dictionary. Academic explanatory dictionary.* Retrieved from: http://sum.in.ua/s/fakhivecj).

Соснін, О. В. (2020). *Цифровізація як нова реальність України. LexInform. Юридичні новини України*. Режим доступу: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/ (Sosnin, O. V. (2020). *Digitalization as a new reality of Ukraine. LexInform. Legal news of Ukraine*. Retrieved from: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/

Український інститут майбутнього. Україна 2030Е – країна з розвинутою цифровою економікою. Режим доступу: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (*Ukrainian Institute for the Future. Ukraine 2030E is a country with a developed digital economy*. Retrieved from: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html).

Cybersecurity guide. How to become a cybersecurity specialist. Retrieved from: https://cybersecurityguide.org/careers/security-specialist/

Cyber security Oxford. Research. Retrieved from: https://www.cybersecurity.ox.ac.uk/research

GOV. UK. Policy paper overview: National Cyber Security Strategy 2016 to 2021. Retrieved from: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

National cyber security centre. About the NCSC. Retrieved from: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

National Cyber Security Strategy 2016-2021. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

RealWire. UK Cyber Security Council opens membership application process. Retrieved from: https://www.realwire.com/releases/UK-Cyber-Security-Council-opens-membership-application-process

The UK Cyber Security Council. The role of the Council and the influence of CyBOK. Retrieved from: https://cybok.org/media/downloads/Roddy_UK_Cyber_Security_Council_and_CyBOK_presentation_2_March_2021.pdf

UK Cyber security council. Qualifications. Retrieved from: https://www.ukcybersecuritycouncil.org.uk/careers-learning/qualifications/

University of Cambridge. Computer laboratory. Cambridge Cybercrime Centre. Retrieved from: https://www.cambridgecybercrime.uk/.

РЕЗЮМЕ

Ящук Ольга. Кибербезопасность: сравнительные аспекты профессиональной деятельности в контексте подготовки кадров в Украине и Великобритании.

Тенденции технологической эволюции цифрового общества обуславливают запрос на профессии, являющиеся залогом защищенности граждан в нестабильных условиях. Вопрос обеспечения рынка труда квалифицированными специалистами в киберсфере – приоритет государственной политики, требующий совершенствования образовательной базы для их подготовки. В статье отражена сущность терминов, определяющих специфику принадлежности к деятельности в области кибербезопасности. Проанализированы факторы востребованности и аспекты профессиональной деятельности киберспециалистов в Украине и Великобритании. Обоснована гуманитарная составляющая оптимизации подготовки кадров для кибербезопасности.

Ключевые слова: *кибербезопасность, специалист по кибербезопасности, киберпространство, профессиональная деятельность, профессия, подготовка, университет, развитие, аспект, современный.*

SUMMARY

Yashchuk Olga. Cyber security: comparative aspects of professional activity in the context of training specialists in Ukraine and Great Britain.

Nowadays the question of sustainability of cyberspace as virtual electronic environment, which, given intensive development of modern science and introduction of innovative technologies is a global dimension of digitally transformed information and communication activities of people in many areas, becomes relevant. Solving the problems of ensuring resilience of cyberspace to interference – from malicious manipulation with personal data to critical infrastructure failures (banks, power system, manufacturing) on a global scale falls within the competence of cyber security professionals. The analysis of the aspects that form the concept of training and regulate the content of professional activities in the field of cyber security shows that in this area there is a wide range of issues that require careful study in the comparative plane of socio-economic, professional, educational, pedagogical realities, problems, tendencies, ideas, values within Ukrainian and British experience practice. The aim of our study is to engage in development of a holistic paradigm

for training cyber security specialists against the background of current societal demands and global challenges that transform people's needs in the context of digitalization of professional activities. The trends of technological evolution of digital society determine the formation of demand for professions, which are the key to protection of citizens in unstable conditions. In the context of current threats and challenges, the issue of providing labor market with skilled specialists in the field of cybersecurity is a priority of public policy, which requires improving the educational base for their training. The article highlights the essence of terms that define the specifics of belonging to the activities in the field of cyber security. Demand factors and aspects of professional activity of cyber security specialists in Ukraine and Great Britain have been analyzed. The humanitarian component of optimization of training for cyber security industry has been highlighted. The direction of further research has been characterized, a significant part of which is the comparative context of foreign language training of cyber security professionals in view of global dimension of cyber security policy, and thus the need to exchange professional knowledge and establish partnerships with international organizations, companies and institutions interested in expanding cyber security policy throughout the world.

Key words: *cyber security, cyber security specialist, cyberspace, professional activity, profession, training, university, development, aspect, modern.*