УДК 35.088.6:[004:007:351.86] (477)

Арсенович Леонід

ORCID iD: 0000-0001-7081-2838
E-mail: arsen-leon@ukr.net

УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ФОРМУВАННЯ СИСТЕМИ ПІДГОТОВКИ КАДРІВ У СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ ДЕРЖАВНО-ПРИВАТНОЇ ВЗАЄМОДІЇ

doi.org/10.33269/2618-0065-2022-1(11)-6-27

Анотація. Проаналізовано проблемні питання щодо функціонування системи підготовки кадрів і підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки. Наведено статистичні дані щодо підготовки фахівців у сфері кібербезпеки, які узагальнено за результатами вивчення практичних аспектів кіберосвіти, а також численних інформаційних та аналітичних документів сучасних аналітиків й експертів. Розглянуто результати досліджень сучасних науковців щодо оптимізації фахової підготовки майбутніх фахівців з кібербезпеки, а також тенденцій та проблем функціонування ІТ-галузі, що вказують на невідповідність базової професійної освіти ІТ-фахівців вимогам інноваційної економіки. Розглянуто основні напрями Положення про організаційно-технічну модель кіберзахисту, засади якого спрямовані на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів щодо мінімізації вразливості комунікаційних систем, формування спроможностей суб'єктів забезпечення кібербезпеки, а також на створення умов для розвитку державно-приватної взаємодії, у тому числі у сфері кіберосвіти. Розглянуто повноваження суб'єктів забезпечення кібербезпеки стосовно організації та проведення кібернавчань, а також сил кіберзахисту щодо участі у розробленні програм і методик їх проведення, сценаріїв реагування на кіберзагрози та проведення заходів щодо протидії кіберзагрозам. Розроблено та розкрито складові освітньої карти розвитку фахівця у сфері кібербезпеки щодо поетапної сертифікації фахівців з кібербезпеки, які безпосередньо здійснюють організаційні, правові, інженерно-технічні заходи, а також заходи криптографічного та технічного захисту інформації, спрямовані на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості та надійності функціонування комунікаційних і технологічних систем. Запропоновані наявні можливості й гарантії, що надаються у зв'язку із впровадженням освітньої карти розвитку фахівця у сфері кібербезпеки у службову діяльність, а також можливі освітні ініціативи, що надає освітня карта розвитку фахівця у сфері кібербезпеки в контексті впровадження організаційно-технічної моделі кіберзахисту.

Ключові слова: інформаційні технології; кібербезпека; освітня карта; підготовка кадрів, система підготовки; фахівець із кібербезпеки.

Постановка проблеми. Науково-технічний прогрес докорінно змінив сучасне суспільство: нині інформаційні технології відіграють чи не найважливішу роль у розвитку країн і визначенні рівня життя населення. За останні десятиліття інформація стала настільки потужним фактором розвитку суспільства, що призвела до утворення нового інформаційного укладу, який сприяє внутрішньодержавній і світовій інтеграції та реінтеграції. Україна сьогодні впевнено стала на шлях упровадження нових технологій. Протягом останніх десятиліть, зокрема останні шість років в умовах масштабної гібридної агресії проти України, швидкий розвиток і всеохопливе впровадження сучасних інформаційних технологій, формування й розвиток всесвітнього кіберпростору призвело до формування нового спектра ризиків і загроз у сферах національної безпеки та оборони, які розповсюджуються в кіберпросторі та (або) через кіберпростір. Кібернетичні загрози охоплюють усі базові сфери суспільної та громадської діяльності (політичну, безпекову, правову, економічну, інфраструктурну, соціальну тощо), загрозливо впливаючи на складові сектору безпеки та оборони України, основних суб'єктів національної системи кібербезпеки та на органи державної влади України загалом.

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

Аналіз останніх досліджень і публікацій. Наукові напрацювання вчених і практиків засвідчують, що професійна підготовка фахівців у сфері кібербезпеки є одним із напрямів державної політики у сферах національної безпеки та оборони, без якого є неможливими захищене передавання інформації і відповідно науково-технічний та соціально-економічний розвиток країни. Проблеми професійного розвитку фахівців з кібербезпеки є малодослідженими. Так, І. Діордіца досліджує питання стандартизації підготовки фахівців з кібербезпеки та

здійснює аналіз стану підготовки фахівців у сфері кібернетичної безпеки станом на 2015–2016 роки [1; 2]. С. Мельник визначає концептуальні основи організації професійної підготовки майбутніх фахівців з кібербезпеки у вищих навчальних закладах (далі – ЗВО) [3]. В. Бурячка, І. Пархомея, М. Степанова та В. Толубка вивчають проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «Інформаційні технології» [4]. Окремим аспектам вивчення зарубіжного досвіду щодо підготовки фахівців ІТ-підрозділів, проблемам із упровадження освітніх інновацій у вищих навчальних закладах країн світу, підготовки майбутніх фахівців із кібербезпеки присвячені праці І. Артьомова [5], М. Бендаса, О. Бондаренка [6], Л. Гаєвської [7], В. Маркова [8], О. Маркової [9], Н. Павлик [10] та інших.

Попри велику кількість фундаментальних і прикладних робіт, які стосуються актуальних питань підготовки ІТ-фахівців, питанням підготовки кадрів у сфері кібербезпеки в умовах державно-приватної взаємодії приділено мало уваги, що й зумовило актуальність дослідження.

Мета статті – розгляд теоретичних підходів до удосконалення механізмів формування системи підготовки кадрів у сфері кібербезпеки в умовах державно-приватної взаємодії.

Методи дослідження. Для реалізації визначеної мети використано комплекс взаємодоповнюваних загальнонаукових і спеціальних методів дослідження, зокрема: системний метод для дослідження організації підготовки фахівців у сфері кібербезпеки як цілісної множини елементів у сукупності відношень і зв’язків між ними; метод аналізу застосовується на всіх етапах дослідження з метою комплексного вивчення засад підготовки фахівців у сфері кібербезпеки; порівняльний метод – під час вивчення питань підготовки фахівців у сфері кібербезпеки; метод узагальнення та аналогії – на всіх етапах дослідження під час зіставлення теорії та практики у сфері підготовки фахівців із кібербезпеки.

Виклад основного матеріалу. Відповідно до чинного законодавства України заходи із забезпечення кібербезпеки у межах своєї компетенції безпосередньо здійснюють державні

суб'єкти (міністерства й інші центральні органи виконавчої влади, місцеві державні адміністрації, правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності, Збройні Сили України, інші військові формування, утворені відповідно до закону, Національний банк України, підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури), а також інші складові кібербезпеки, які відносяться до недержавних суб'єктів кібербезпеки (підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, суб'єкти господарювання, громадяни України та об'єднання громадян), що провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [11].

Видами діяльності у сфері кібербезпеки є: кіберзахист, кібероборона, протидія кібершпигунству (кібертероризму, кіберзлочинності), кібердипломатія та кіберрозвідка, а також відповідна координація діяльності за цими видами. Зазначена діяльність спрямована на захист суспільства, держави, інформаційних технологій, а також на нейтралізацію різних видів кіберзагроз у кіберпросторі.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», нормативно-правових актів Президента України (Стратегія національної безпеки України (Указ Президента України від 14 вересня 2020 р. № 392/2020) та Стратегія кібербезпеки України (Указ Президента України від 26 серпня 2021 р. № 447/2021)) органи й підрозділи як державних, так і недержавних суб'єктів кібербезпеки, забезпечують захист життєво важливих інтересів людини й громадянина, суспільства та держави, національні інтереси України у кіберпросторі, а також здійснюють основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Одним із таких напрямів, який є стрижневим у всій сфері кібербезпеки, є створення системи підготовки кадрів і підвищення компетентності фахівців різних сфер діяльності із зазначених питань, який застосовується шляхом державно-

приватної взаємодії, а отже безпосередньо стосується як державної, так і приватної кібербезпеки.

Нині можна констатувати проблему відсутності єдиної методології в системі підготовки кадрів у сфері кібербезпеки для всіх фахівців. Відсутність єдиних керівних документів, методичного забезпечення навчання, розбіжність у поглядах на мету, завдання та зміст підготовки з питань кібербезпеки знижують ефективність та якість підготовки кіберфахівців для всієї країни загалом. Крім того, рівень кіберосвіти в Україні має ризики до стрімкого послаблення через недостатню цифрову грамотність населення, представників державного сектора та бізнесових кіл. Також спостерігається певне гальмування процесів цифрових перетворень у країні через: неусвідомлення цифрових навичок і цифрової грамотності як у суспільстві, так і в органах державної влади; невідповідність рівня підготовки людського капіталу з питань цифрових навичок вимогам цифрової економіки та суспільства; відсутність нормативної бази та затвердженого стандарту цифрових компетентностей, їх дескрипторів та описів щодо кожної окремої галузі за сферами економічної діяльності та основними професійними групами; неузгодженість вимог до рівня володіння цифровими компетентностями різних категорій працівників, брак єдиних обґрунтованих затверджених вимог до цифрової компетентності в професійних стандартах і посадових обов'язках різних категорій працівників.

Означене підтверджують статистичні дані. Так, протягом останніх двох – трьох років державні та приватні ЗВО, що здійснюють підготовку фахівців за спеціальністю 125 «Кібербезпека» галузі знань «Інформаційні технології», щороку в середньому випускають 1400 дипломованих кіберфахівців (близько 900 бакалаврів й 500 магістрів), 70 % яких у подальшому працюють в органах і підрозділах недержавних суб'єктів кібербезпеки [12, с. 223], що є суттєвим освітнім дисбалансом у сфері кібербезпеки. Експерти також зазначають, що протягом навчання більшість студентів ІТ-сфери в Україні отримує лише 60–70 % необхідних знань, тоді як їхні закордонні колеги здобувають близько 90 %. Це означає, що, за винятком окремих передових ЗВО країни, система освіти у сфері

інформаційних технологій відчутно відстає від потреб ринкової економіки країни та світу [13, с. 386].

Крім цього, у навчальних планах центрів післядипломної освіти, які здійснюють підвищення кваліфікації працівників органів державної влади, органів місцевого самоврядування, державних підприємств, установ і організацій, тематика щодо вивчення ІТ-технологій, або зовсім відсутня, або їй виділяється всього декілька годин на весь навчальний рік. Своєю чергою ЗВО (51 заклад із 160), які мають відповідну ліцензію на підвищення кваліфікації з питань кібербезпеки та ІТ-технологій, забезпечують такі освітні заходи у переважній більшості на платній основі, що, наприклад, через зменшене фінансування держорганів унеможливлює професійний розвиток з питань кібернетичної безпеки особового складу органів (підрозділів) державної кібербезпеки у повному обсязі (наприклад: затверджено кошторисні призначення на навчання особового складу Держспецзв'язку (більш ніж 5 тис. співробітників) у 2020 році становлять 500 тис. грн). При цьому на сучасному етапі розвитку освіти серед базових парадигм щодо підготовки кадрів як для всього сектору економіки, так і для сектору безпеки та оборони України, є компетентнісна парадигма, яка спрямована на формування у майбутніх фахівців різноманітних, у тому числі й професійних компетенцій [14, с. 106]. Крім того, безпека національного кіберпростору багато в чому залежить від загального рівня кіберосвіти населення, тобто його обізнаності у сфері безпечного користування Інтернетом і новітніми інформаційними технологіями, який на поточний момент є низьким.

Необхідність подальшої розбудови системи підготовки кадрів у сфері кібернетичної безпеки підкреслюють також і сучасні науковці, які вже протягом п'яти років, з моменту затвердження першої редакції Стратегії кібербезпеки України (Указ Президента України від 15 березня 2016 р. № 96/2016), сигналізують і нагадують у наукових статтях і доповідях про пріоритетність і нагальність розвитку державної та приватної кіберосвіти. Так, зокрема, Ю. Даник (начальник Інституту інформаційних технологій Національного університету оборони України) та О. Корнейко (президент громадської організації

«Українська академія кібербезпеки») розкривають передумови, етапи становлення та наявний стан системи підготовки в Україні фахівців у сфері кібербезпеки, аналізують основні поняття у професійно-компетентнісному підході підготовки фахівців з кібербезпеки, а також пропонують основні положення методології розбудови цілісної системи підвищення кіберосвіченості населення та підготовки фахівців з питань кібербезпеки для сектору безпеки та оборони України [14, с. 105].

С. Мельник, С. Воскобойніков і Д. Ступак обґрунтовують оптимізацію фахової підготовки майбутніх фахівців з кібербезпеки на основі інноваційної педагогіки та інтегрованого підходу в системі реалізації ключових компетенцій безпеки в інформаційному суспільстві. Специфіка фахової підготовки й формування професійної компетентності майбутніх фахівців з кібербезпеки зумовлює застосування інтегрованого підходу, що базується на міжпредметних зв'язках фундаментальних і фахових навчальних дисциплін, та ефективного розподілу навчальних модулів у системі професійної підготовки з урахуванням модернізаційних освітніх змін, педагогічної інноватики та застосуванні інноваційних освітніх технологій для формування комплексної готовності до реалізації фахових компетенцій з кібербезпеки [15, с. 125].

Основні тенденції та проблеми функціонування ІТ-галузі, зокрема основні причини невідповідності базової професійної освіти ІТ-фахівців вимогам інноваційної економіки розглядав і доцент кафедри міжнародної економіки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Н. Тимошенко, який, проаналізувавши наукові праці, присвячені вивченню особливостей функціонування підприємств ІТ-галузі, зробив висновок, що серед основних причин невідповідності базової професійної освіти кіберфахівців вимогам інноваційної економіки є такі: недостатньо висока кваліфікація викладачів та низький рівень фінансування ЗВО; неадекватність змісту освітніх програм професійної підготовки ІТ-фахівців сучасним вимогам роботодавців і змінам кон'юнктури ринку праці; знання у сфері інформаційних технологій дуже швидко змінюються та

оновлюються, а навчання у ЗВО не встигає за темпами цих змін; відсутність досвіду практичної роботи, виключно теоретичні знання про специфіку функціонування та особливості кіберсфери [13, с. 386]. Доступність, рівень та якість освіти, поряд з такими показниками, як величина ВВП на душу населення та тривалість життя, є одним із трьох прийнятих у міжнародній практиці показників індексу розвитку людського потенціалу в щорічно зорієнтованій оцінці ООН, що характеризує якість життя у світі [16, с. 1].

Зазначені вище дослідження ще раз підтверджують, що система підготовки кадрів у сфері кібербезпеки має враховувати вимоги ринку праці й відповідати загальносвітовим критеріям якості. Цього потребує інформаційне суспільство, що характеризується активним поширенням нових цифрових технологій, розвитком конкуренції у сфері кіберосвіти та зростанням її ролі.

Про необхідність подальшої розбудови системи підготовки кадрів у сфері кібербезпеки свідчать також нещодавно прийняті Урядом нормативно-правові акти, що спрямовані на забезпечення функціонування національної системи кібербезпеки. Так, у грудні 2021 року затверджено Положення про організаційно-технічну модель кіберзахисту (постанова Кабінету Міністрів України від 29 грудня 2021 р. № 1426 [17]), засади якого спрямовані на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів щодо мінімізації вразливості комунікаційних систем, формування спроможностей суб'єктів забезпечення кібербезпеки, а також створення умов для розвитку державно-приватної взаємодії, у тому числі у сфері кіберосвіти. Організаційно-технічна модель кіберзахисту має створити умови для об'єднання зусиль суб'єктів забезпечення кібербезпеки з метою безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави, зокрема через реалізацію заходів, спрямованих на захист національних інформаційних ресурсів і кіберзахист об'єктів критичної інформаційної інфраструктури, для забезпечення їх кіберстійкості, стабільного функціонування інформаційної інфраструктури державного та приватного секторів економіки.

У положеннях цього акта ще раз наголошується на певній кількості повноважень суб'єктів забезпечення кібербезпеки, серед яких необхідно виділити проведення регулярних навчань щодо попередження та реагування на кіберзагрози й кіберінциденти, відновлення після кібератак, організацію та проведення кібернавчань, розроблення відповідних програм і методик, сценаріїв реагування на кіберзагрози, проведення заходів щодо протидії кіберзагрозам і з кібергігієни. Крім цього, у повноваженнях сил кіберзахисту (урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, інші команди реагування на комп'ютерні надзвичайні події, підрозділи (групи, команди, служби) захисту інформації, підприємства, установи та організації незалежно від форми власності, які провадять діяльність та/або надають послуги, пов'язані з кіберзахистом) також передбачено взяття участі у проведенні кібернавчань, розробленні програм і методик їх проведення, сценаріїв реагування на кіберзагрози та проведення заходів щодо протидії кіберзагрозам і з кібергігієни.

У процесі реалізації зазначених питань необхідно також використовувати досвід роботи ЗВО за кордоном, який є не менш вагомим під час організації відповідних освітніх заходів. Наприклад, у складі Департаменту внутрішньої безпеки США сформовано відповідний відділ освіти та підвищення освіченості з питань кібербезпеки, яким за останні роки відпрацьовано та прийнято ряд документів як щодо підготовки професіоналів з кібербезпеки, так і загальної кіберосвіченості населення США. Серед них насамперед такі: Національна програма підвищення освіченості з питань кібербезпеки, мета якої полягає в сприянні індивідуальній кібернетичній стійкості та освіченості населення з питань кібербезпеки, розумінні кіберзагроз і простих дій щодо їх нейтралізації; Національна програма розвитку професіоналізму та розвитку персоналу, мета якої полягає в сприянні щодо підготовки фахівців з кібербезпеки, які володіють необхідними знаннями, навичками та здатні захистити інтереси нації від наявних та імовірних проблем у всіх складових кібербезпеки; Національна програма освіти та тренінгу в сфері кібербезпеки, мета якої – розширити підготовку професіоналів з кібербезпеки за рахунок створення динамічної освітньої

системи, здатної підготувати нове покоління співробітників з кібербезпеки, які будуть здатні до захисту від наявних і майбутніх кіберзагроз [14, с. 106].

Ще одним наочним фактом забезпечення кіберосвіченості та впровадження цифрових технологій є приклад Великобританії, яка стала першою з країн «Великої сімки», зробивши інформатику обов'язковим предметом початкової школи. Завдання, яке поставлене викладачам, є дуже амбітним: учні повинні навчитися писати й налагоджувати комп'ютерні програми до семи років. Таким чином, Уряд країни надає педагогам можливість виявляти таланти дітей в ранньому віці й вдосконалювати вміння та майстерність учнів.

Необхідно зазначити й про наявність проблемних питань, які існують як у країнах Європи, так і у світі загалом. Нині наявний дефіцит фахівців з кібербезпеки, оскільки IT-ринок є глобальним, високотехнологічним і висококонкурентним. Тенденції перевищення попиту над пропозицією на IT-спеціалістів спостерігаються в багатьох країнах. Так, дослідження міжнародної некомерційної організації ISC, яка спеціалізується на сертифікації фахівців з інформаційної безпеки, показало, що питання власної кібербезпеки та захисту інформації викликає найбільше занепокоєння у представників бізнесу. У дослідженні взяли участь 1500 представників IT-галузі з різних країн. Майже половина респондентів (49 %) планують у найближчий рік найняти більше фахівців для захисту своїх даних і мереж, тоді як 39 % планують залишити все як є. Опитування показало, що найбільший дефіцит фахівців з кібербезпеки – у Тихоокеанському регіоні, куди входять США і Китай (2,15 млн). У Європі – 498 тис. вакансій у цій сфері, в Африці та на Близькому Сході – 142 тис., у Латинській Америці – 136 тис. [18]. Означене підкреслює зростання попиту на IT-спеціалістів як у Європі, так і в усьому світі. Водночас вимоги роботодавців до IT-спеціалістів також нестримно зростають. Компанії потребують високоякісних творчих професіоналів, які є компетентними у технічному плані, здатними працювати у швидкозмінних умовах і постійно розвиватися та самовдосконалюватися, а також мають високий рівень соціальної та комунікативної компетентності.

Враховуючи необхідність створення системи підготовки кадрів і підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки, а також підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, що є вимогами Закону України «Про основні засади забезпечення кібербезпеки України», автором дослідження розроблено освітню карту розвитку фахівця у сфері кібербезпеки (рис. 1), подальше впровадження якої у освітній процес органів і підрозділів державної та приватної кібербезпеки стане справжньою реалізацією у службову діяльність організаційно-технічної моделі кіберзахисту, а також принципу «навчання впродовж життя» для тих фахівців, які безпосередньо забезпечують запобігання й нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі. Запропонована освітня карта є одним із ключових інструментів отримання фахівцями кібернетичної безпеки професійних компетентностей і засобом підвищення їх кваліфікації. Карта встановлює залежність між навичками людей, які безпосередньо забезпечують кібербезпеку держави, і успіхом (результатом) того чи іншого продукту, матеріалу тощо на ринку інформаційних технологій. Проєкт, що пропонується, передбачає поетапне формування і розвиток ключових (базових, основних) та предметних компетентностей особистості, результатом якого буде формування загальної професійної компетентності фахівця із кібербезпеки, що є сукупністю ключових компетентностей ІТ-фахівця та інтегрованою характеристикою особистості. Освітня карта встановлює покрокове освоєння сфери кібербезпеки шляхом послідовного накопичення практичних знань і підтвердження їх рівня отриманням відповідного сертифіката, починаючи від сертифікованого користувача комп'ютера та закінчуючи службовою особою захисту даних.

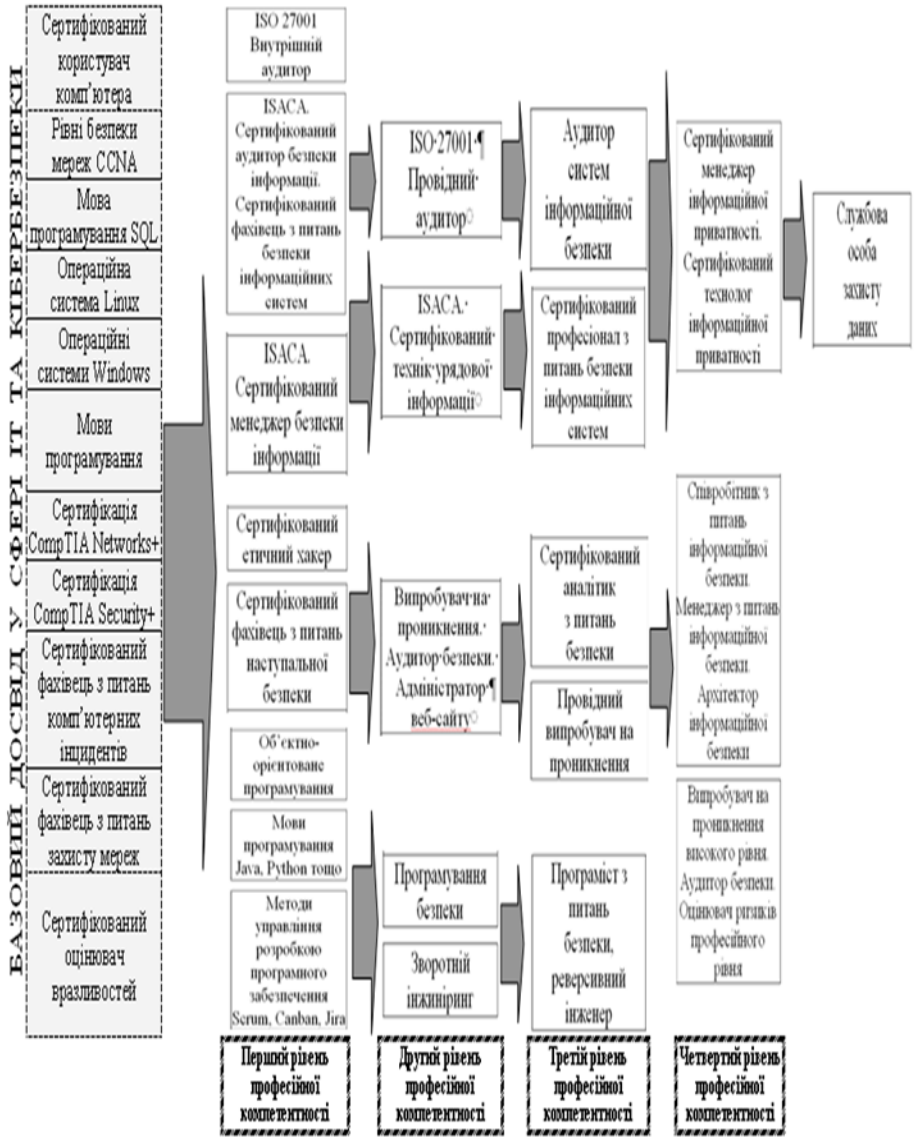

Рисунок 1 – Освітня карта розвитку фахівця у сфері кібербезпеки

Джерело: розроблено автором

Крім цього, проєкт освітньої карти розвитку фахівця у сфері кібербезпеки встановлює чотири рівня професійної компетентності, які за своїм змістом відповідають здобутому професійному рівню.

Знання першого рівня професійної компетентності закладають основу наступних рівнів компетентностей, а також підґрунтя архітектури та основ формування ландшафту кібербезпеки. Причому компетентності щодо знань основ безпеки інформації та програмування повинні бути головним спільним елементом, що пов'язує всі компетентності воєдино.

До другого рівня професійної компетентності належать компетентності щодо уразливостей, характерних для кіберпростору, та способів і засобів використання таких уразливостей у разі застосування різних схем проникнення в інформаційні системи та формування деструктивних векторів нападу. Розуміння характеру таких уразливостей – невід'ємний компонент ризику і принципів зниження його рівня.

Професійні компетентності третього рівня полягають у розумінні ключових принципів національної політики у сфері кібербезпеки в контексті міжнародних стандартів і рекомендованого досвіду, а також порівнянні їх із різними прикладами національних принципів.

Своєю чергою до четвертого рівня професійної компетентності можна віднести компетентності у сфері управління кібербезпекою на національному рівні. Це насамперед компетентності щодо розуміння методів ефективного управління кібербезпекою та рівнем національної готовності у сфері кібербезпеки в узгодженні з контекстом оцінок ризиків.

Отже, запровадження освітньої карти розвитку фахівця у сфері кібербезпеки у службову діяльність спеціалістів, які безпосередньо забезпечують безпеку кібернетичного простору, надасть такі можливості та гарантії:

– конкурентоспроможність під час прийому на роботу, в тому числі в міжнародну компанію. Це пов'язано з тим, що сертифікація кіберфахівців популярна, їй довіряють у багатьох країнах світу, що, безперечно, додає певні переваги для кандидата на посаду;

– кар'єрне зростання і підвищення зарплати. Якщо знання фахівця підтверджені сертифікатом високого рівня, то у керівництва більше довіри до такого співробітника, що надає

можливість працювати над складнішими й цікавішими проєктами;

– систематизацію знань, яка під час підготовки до чергової сертифікації впорядкує розрізнені теоретичні та практичні знання, заповнить прогалини, а також допоможе поглибити професійні компетентності й навички;

– розвиток навичок та експертизи, які, зокрема, підтверджуються виконаними завданнями або публічними виступами на профільних конференціях.

Запропонований проєкт освітньої карти розвитку фахівця у сфері кібербезпеки в контексті впровадження організаційно-технічної моделі кіберзахисту можна використовувати для:

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

– створення більш деталізованих (професійних) освітніх програм у сфері кібербезпеки;

– проведення опитування, тестування, сертифікації тощо;

– системного збору статистичних даних щодо рівня володіння цифровими компетентностями окремих категорій працівників;

– розробки або внесення доповнень і змін у професійні стандарти та стандарти вищої освіти.

Упровадження освітньої карти розвитку фахівця у сфері кібербезпеки у загальну систему підготовки, перепідготовки та підвищення кваліфікації надасть змогу:

– створити сучасну цілісну й гнучку систему професійного розвитку;

– забезпечити якість та безперервність набуття досвіду шляхом підвищення кваліфікації та самоосвіти;

– створити належні умови для реалізації права на професійне зростання;

– створити умови для конкуренції серед співробітників;

– забезпечити розвиток професійної компетентності.

Крім очевидних конкурентних переваг, є й інші позитивні результати сертифікації, що надають керівнику певну користь, серед яких: володіння загальноприйнятою термінологією (учасники тієї чи іншої команди говорять «однією мовою», що

унеможливлює виникнення проблем через нерозуміння один одного), а також можливість оцінити підлеглого на предмет сильних і слабких професійних знань.

Одним із найбільш значущих доказів глибини знань, фактичного досвіду роботи в проєктах, практичних навичок, міжнародних стандартів, технологій, підходів і методологій є проходження та отримання міжнародних сертифікатів. Навчання й сертифікація забезпечує безперервний процес профільного розвитку будь-якого фахівця. Розуміння безперервності та необхідності цих процесів давно лягло в основу внутрішньокорпоративних програм мотивації та розвитку персоналу в більшості світових корпорацій і міжнародних організацій і, як ми бачимо, за останні декілька років стає системною практикою українських роботодавців у сфері кібербезпеки.

Слід відзначити, що нині вже здійснено перший крок у створенні платформи для «мозкового штурму» та механізму для державно-приватного партнерства у сфері кібербезпеки. Так, у жовтні 2020 року Держспецзв'язку разом з Міністерством цифрової трансформації, Радою національної безпеки та оборони України та Службою безпеки України започаткували роботу Експертної ради з інформаційної та кібербезпеки, яка має об'єднати фахівців з державних органів, комерційного сектору та науковців, щоб посилити національну систему кібербезпеки України, у тому числі у напрямі удосконалення системи підготовки кадрів. Планується, що саме Експертна рада стане синергією зусиль однодумців, формуватиме нові ідеї, проєкти, рішення у сфері забезпечення кібербезпеки та кіберосвіті, які необхідно буде втілювати у подальшому на практиці [19].

Враховуючи зазначене, можливими шляхами вдосконалення системи підготовки кадрів у сфері кібербезпеки в умовах державно-приватної взаємодії є:

– запровадження у структурах основних суб'єктів національної системи кібербезпеки окремих підрозділів (секторів, відділів, управлінь), що будуть опікуватися питаннями підготовки та підвищення кваліфікації особового складу з питань кібербезпеки;

– розроблення відповідного механізму щодо організації та впровадження проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, та стосовно визначення потреби на підвищення кваліфікації фахівців із кібербезпеки, представників бізнесових кіл і пересічних громадян;

– організація й проведення конференцій, семінарів, форумів, засідань, круглих столів, тренінгів, навчань з питань інформаційної безпеки, кібербезпеки, кіберзахисту та захисту інформації в кіберпросторі на базі Центрів підвищення кваліфікації з інформаційних технологій, роботу яких необхідно організувати за територіальним принципом.

Нині в Україні система підготовки кадрів у сфері кібербезпеки та кіберосвіта загалом перебувають у трансформаційному стані. Існують поодинокі стохастичні явища, але будь-якої комплексної системності практично немає. Закон України «Про основні засади забезпечення кібербезпеки України» та затверджена Урядом організаційно-технічна модель кіберзахисту жодним чином цього не вирішують, залишаючи осторонь ключові проблеми забезпечення й контролю якості та визнання освіти у сфері кібербезпеки. Не існує офіційної статистики з цих питань, відсутні спеціальні концепції та освітні програми. Отже, для України вкрай важливо найближчим часом вжити дієвих заходів для подолання відставання у цій сфері.

Зрештою, варто погодитись, що в сучасному світі підготовка кадрів з кібербезпеки не може обмежуватися лише отриманням вищої освіти у ЗВО за відповідною спеціальністю. Для збереження належної конкурентоспроможності та професійного рівня цим фахівцям необхідно перманентно підвищувати свою кваліфікацію на засадах «концепції безперервної освіти» («освіти протягом життя»), множинність форм і методів якої відкриває ще один перспективний напрям для міжгалузевого кібербезпекового державно-приватного партнерства. Можливі декілька варіантів роботи в цьому напрямі, серед яких перепідготовка в рамках післядипломної освіти фахівців у споріднених з кібернетичною безпекою спеціальностях, застосування нелінійної схеми підготовки

фахівців, використання потенційних можливостей неформальної освіти для підвищення кваліфікації фахівців-практиків через проведення кібертренінгів, семінарів, міжнародних стажувань тощо [20, с. 62].

Висновки та напрями подальших досліджень. Критично важливим є забезпечення належного рівня обізнаності персоналу компаній та установ у питаннях кібербезпеки, спільними зусиллями приватних і державних суб'єктів. Форми кібербезпекового державно-приватного партнерства тут можуть бути різноманітними: спільні семінари, тренінги, онлайн курси, залучення науково-аналітичних і консалтингових компаній усіх форм власності й багато іншого. Крім того, необхідними є регулярні тестування (навчання) на проникнення, моделювання загроз, грамотність поведінки працівників / користувачів у мережі (дотримання елементарних правил онлайнової безпеки, стійкість до спроб фішингу тощо).

Навчання протягом життя виходить на чільні позиції, у світових освітніх процесах диктується базовими тенденціями сучасного розвитку людства. Такий підхід дасть змогу кардинально змінити систему підготовки кадрів у сфері кібербезпеки, адже донині здебільшого вона зорієнтована на запити минулого. Сучасна ж економіка потребує кадрів, готових працювати в умовах конкуренції, тобто в інноваційній економіці. Використання й подальше впровадження освітньої карти розвитку фахівця у сфері кібербезпеки для потреб державної та приватної кібербезпеки стане ефективним інструментом навчання, який надасть можливість рухатися власною освітньою траєкторією та розширить коло навчальних задач і збагатить їх сучасним змістом. Практика засвідчує, що ніяка теорія не буде реалізована в освітній діяльності, якщо для її впровадження не буде розроблений відповідний алгоритм. Отже, надалі вектор досліджень у сфері кіберосвіти необхідно спрямовувати на створення освітньої медіатехнології як цілісної системи підготовки кадрів у сфері кібербезпеки в умовах розвитку цифрового суспільства України.

Список використаних джерел

1. Діордіца І. Освітні стандарти підготовки фахівців із кібербезпеки. *Национальный юридический журнал: теория и практика*. 2017. Вип. 1. С. 50–53.
2. Діордіца І. Стан підготовки фахівців у сфері кібербезпеки. *Visegrad Journal on Human Rights*. 2016. Вип. 6/1. С. 59–65.
3. Мельник С. Концептуальні основи організації професійної підготовки майбутніх фахівців з кібербезпеки. *Педагогічні науки: теорія, історія, інноваційні технології*. 2016. № 10. С. 79–88.
4. Бурячок В. Л. Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «Інформаційні технології». *Сучасний захист інформації*. 2016. № 2. С. 4–9.
5. Артьомов І. В., Студеняк І. П., Головач Й. Й., Гусь А. В. Інновації у вищій освіті: вітчизняний і зарубіжний досвід : навчальний посібник. Ужгород : ПП «АУТДОР-ШАРК», 2015. 360 с.
6. Бендас Ю. М., Бондаренко О. В. Проблеми підготовки ІТ-спеціалістів у Європі. *Моделювання економіки : проблеми, тенденції, досвід* : тези доп. VIII міжнар. наук.-метод. конф., 28–29 вересня 2017 р. Львів, 2017. С. 129–130.
7. Гаєвська Л. А. Досвід Європейського Союзу щодо формування й реалізації освітньої політики як головного важеля соціально-економічного розвитку країн. *Вісник післядипломної освіти. (Серія : Управління та адміністрування)*. 2017. Вип. 4–5. С. 9–22.
8. Марков В. В. Особливості впровадження зарубіжного досвіду боротьби з кіберзлочинністю в навчальний процес. *Науковий вісник Міжнародного гуманітарного університету. (Серія : Юриспруденція)*. 2014. Вип. 12. С. 105–107.
9. Маркова О. М. Моделі використання хмарних технологій у підготовці ІТ-фахівців. *Науковий часопис НПУ імені М.П. Драгоманова. (Серія : Комп'ютерно-орієнтовані системи навчання)*. 2016. № 18. С. 85–94.
10. Павлик Н.П. Зарубіжний досвід організації неформальної освіти. *Наукові записки Ніжинського державного університету ім. Миколи Гоголя. (Серія : Психолого-педагогічні науки)*. 2016. № 1. С. 264–273.
11. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення : 16.01.2022).
12. Арсенович Л. А. Кіберосвіта в умовах цифровізації публічного управління. *Цифрова трансформація публічного управління : монографія* / Карпенко О. В., Малий І. Й., Муравицька Г. В. та ін. Київ : НАДУ, 2020. С. 168–228.
13. Тимошенко Н. Ю. Проблеми та перспективи розвитку ІТ-індустрії в Україні. *Економіка та суспільство*. 2018. Вип. 17. С. 384–388.
14. Даник Ю. Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України. *Information Technology and Security* . 2018. Vol. 6. Iss. 2. P. 105–123.

15. Мельник С. Оптимізація фахової підготовки майбутніх фахівців з кібербезпеки на основі інноваційної педагогіки та інтегрованого підходу в системі реалізації ключових компетенцій безпеки в інформаційному суспільстві. *Витоки педагогічної майстерності. (Серія : Педагогічні науки)*. 2018. Вип. 21. С. 125–129.
16. Куценко В. І. Перспективи розвитку системи підготовки кадрів : пошук альтернативи. *Ефективна економіка*. 2011. № 1.
17. Про затвердження Положення про організаційно-технічну модель кіберзахисту : постанова Кабінету Міністрів України від 29 грудня 2021 р. № 1426. URL : https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text (дата звернення : 16.01.2022).
18. Фахівець із кібербезпеки є однією з найоплачуваніших та найдефіцитніших IT-спеціальностей – дослідження. *Співтовариство Happy Monday :* вебсайт. URL : https://happymonday.ua/ru/fahivec-iz-kiberbezpeky-je-odnijeju-z-najoplachuvanishyh-ta-najdeficytnishyh-it-specialnostej/ (дата звернення : 16.01.2022).
19. Держспецзв'язку започаткувала роботу Експертної ради з інформаційної та кібербезпеки. *Детектор медіа : веб-сайт.* URL : https://detector.media/infospace/article/181312/2020-10-06-derzhspetszvyazku-zapochatkuvala-robotu-ekspertnoi-rady-z-informatsiynoi-ta-kiberbezpeky/ (дата звернення : 16.01.2022).
20. Державно-приватне партнерство у сфері кібербезпеки : міжнародний досвід та можливості для України. *Аналітична доповідь* / Дубов Д. та ін.; Національний інститут стратегічних досліджень. Київ : 2018. 84 с.

References

1. Diorditsa, I. (2017). Osvitni standarty pidhotovky fakhivtsiv iz kiberbezpeky [Educational standards for training cybersecurity professionals]. *Natsyonalnyi yurydycheskyi zhurnal: teoryia i praktyka*, *1*, 50–53 [in Ukrainian].
2. Diorditsa, I. (2016). Stan pidhotovky fakhivtsiv u sferi kiberbezpeky [The state of training of specialists in the field of cybersecurity]. *Visegrad Journal on Human Rights, 6/1*, 59–65 [in Ukrainian].
3. Melnyk, S. (2016). Kontseptualni osnovy orhanizatsii profesiinoi pidhotovky maibutnikh fakhivtsiv iz kiberbezpeky [Conceptual bases of organization of professional training of future cybersecurity specialists]. *Pedahohichni nauky: teoriia, istoriia, innovatsiini tekhnolohii*, *10*, 79–88 [in Ukrainian].
4. Buriachok, V. L. (2016). Problemni pytannia ta aktualni zavdannia pidhotovky fakhivtsiv z kibernetychnoi bezpeky haluzi znan «Informatsiini tekhnolohii» [Problematic issues and current tasks of training specialists in cyber security in the field of knowledge «Information Technology»], *Suchasnyi zakhyst informatsii*, *2*, 4–9 [in Ukrainian].
5. Artomov, I. V., Studeniak, I. P., Holovach, Y. Y. & Hus, A. V. (2015). Innovatsii u vyshchii osviti: vitchyznianyi i zarubizhnyi dosvid [Innovations in higher education: domestic and foreign experience]. Uzhhorod: PP «AUTDOR-ShARK» [in Ukrainian].

6. Bendas, Y. M. & Bondarenko, O. V. (2017), Problemy pidhotovky IT-spetsialistiv u Yevropi [Problems of training IT specialists in Europe], *Modeliuvannia ekonomiky: problemy, tendentsii, dosvid*: tezy dopovidei VIII Mizhnarodnoi naukovo-metodychnoi konferentsii [Modeling of economy: problems, tendencies, experience: abstracts of reports of the VIII International scientific and methodical conference]. Lviv [in Ukrainian].
7. Haievska, L. A. (2017). Dosvid Yevropeiskoho Soiuzu shshodo formuvannia y realizatsii osvitnoi polityky yak holovnoho vazhelia sotsialno-ekonomichnoho rozvytku krain [The experience of the European Union in the formation and implementation of educational policy as the main lever of socio-economic development]. *Visnyk pisliadyplomnoi osvity. (Seriia: Upravlinnia ta administruvannia)*, *4–5*, 9–22 [in Ukrainian].
8. Markov, V. V. (2014), Osoblyvosti vprovadzhennia zarubizhnoho dosvidu borot'by z kiberzlochynnistiu v navchalnyi protses [Features of the introduction of foreign experience in combating cybercrime in the educational process]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: Yurysprudentsiia*, *12(1)*, 105–107 [in Ukrainian].
9. Markova, O. M. (2016). Modeli vykorystannia khmarnykh tekhnolohii u pidhotovtsi IT-fakhivtsiv [Models of using cloud technologies in the training of IT specialists]. *Naukovyi chasopys NPU imeni M. P. Drahomanova. (Seriia 2: Kompiuterno-oriientovani systemy navchannia)*, *18*, 85–94 [in Ukrainian].
10. Pavlyk, N. P. (2016). Zarubizhnyi dosvid orhanizatsii neformalnoi osvity [Foreign experience in the organization of non-formal education in Ukrainian]. *Naukovi zapysky Nizhynskoho derzhavnoho universytetu im. Mykoly Hoholia. (Psykholoho-pedahohichni nauky)*, *1*, 264–273 [in Ukrainian].
11. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» vid 05 zhovtnia 2017 r. № 2163-VIII [Law of Ukraine «On the basic principles of cybersecurity in Ukraine»]. (n.d.). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].
12. Arsenovych, L. A. (2020). Kiberosvita v umovakh tsyfrovizatsii publichnoho upravlinnia. [Cyberworld in the context of digitalization of public administration]. Karpenko, O.V., Malyi, I.Y., Muravytska, H. V. ta in. / *Tsyfrova transformatsiia publichnoho upravlinnia – Digital transformation of public administration* : monohrafaia. Kyiv, NADU [in Ukrainian].
13. Tymoshenko, N. Y. (2018). Problemy ta perspektyvy rozvytku IT-industrii v Ukraini [Problems and prospects of development of the IT industry in Ukraine]. *Ekonomika ta suspilstvo*, *17*, 384–388 [in Ukrainian].
14. Danyk, Y. (2018), Osnovy metodolohii formuvannia kiberkompetentsii u fakhivtsiv sektoru bezpeky i oborony Ukrainy [Fundamentals of the methodology of formation of cybercompetences of specialists in the security and defense sector of Ukraine]. *Information Technology and Security*, *6*, *2*, 105–123 [in Ukrainian].
15. Melnyk, S. (2018). Optymizatsiia fakhovoi pidhotovky maibutnikh fakhivtsiv z kiberbezpeky na osnovi innovatsiinoi pedahohiky ta intehrovanoho pidkhodu v systemi realizatsii kliuchovykh kompetentsii bezpeky v informatsiinomu suspilstvi [Optimization of professional training of future cybersecurity

specialists on the basis of innovative pedagogy and integrated approach in the system of implementation of key security competencies in the information society]. *Vytoky pedahohichnoi maisternosti. (Seriia: Pedahohichni nauky)*, *21*, 125–129 [in Ukrainian].

16. Kutsenko, V. I. (2011). Perspektyvy rozvytku systemy pidhotovky kadriv: poshuk alternatyvy [Prospects for the development of the training system : finding an alternative]. *Efektyvna ekonomika*, *1* [in Ukrainian].
17. Postanova Kabinetu Ministriv Ukrainy «Pro zatverdzhennia Polozhennia pro orhanizatsiino-tekhnichnu model kiberzakhystu» [On approval of the Regulation on the organizational and technical model of cybersecurity]. Retrieved from https://zakon.rada.gov.ua/laws/show/ 1426-2021-%D0%BF#Text [in Ukrainian].
18. Fakhivets iz kiberbezpeky ye odniieiu z naioplachuvanishykh ta naidefitsytnishykh IT-spetsialnostei – doslidzhennia. Spivtovarystvo Happy Monday : vebsait (2022) [The cybersecurity specialist is one of the highest paid and most scarce IT specialties – research. Happy Monday community : Web site]. Retrieved from https://happymonday.ua/ru/fahivec-iz-kiberbezpeky-je-odnijeju-z-najoplachuvanishyh-ta-najdeficytnishyh-it-specialnostej/ [in Ukrainian].
19. Derzhspetszviazku zapochatkuvala robotu Ekspertnoi rady z informatsiinoi ta kiberbezpeky (2022). [The State Special Communications Service has launched the work of the Expert Council on Information and CyberSecurity]. *Detektor media : veb-sait.* Retrieved from https://detector.media/infospace/article/181312/2020-10-06-derzhspetszvyazku-zapochatkuvala-robotu-ekspertnoi-rady-z-informatsiynoi-ta-kiberbezpeky/ [in Ukrainian].
20. Dubov, D. (2018). Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy. Analitychna dopovid [Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine. Analytical report]. Natsionalnyi instytut stratehichnykh doslidzhen. Kyiv [in Ukrainian].

IMPROVING THE MECHANISMS FOR FORMING A SYSTEM OF TRAINING IN THE FIELD OF CYBERSECURITY IN TERMS OF PUBLIC-PRIVATE INTERACTION

Arsenovych Leonid

Abstract. Problematic issues related to the functioning of the training system and increasing the competence of specialists in various fields of activity on cybersecurity are analyzed. Statistics on the training of specialists in the field of cybersecurity are presented, which are summarized based on the results of studying the practical aspects of cybersecurity, as well as numerous information and analytical documents of modern analysts and experts. The results of research of modern scientists on the optimization of professional training of future specialists in cybersecurity, as well as trends and problems of the IT industry, indicating the inconsistency of basic professional education of IT professionals to the requirements of innovative economy. The main directions of the Regulation on the organizational and technical model of cyber defense are considered. private interaction, including in the field of cyber education. The powers of cybersecurity actors to organize and conduct cyber exercises, as well as cyber defense forces to participate in the development of programs and methods of their implementation, scenarios for responding to cyber threats and measures to combat cyber threats are considered. Developed and disclosed components of the educational map of cybersecurity specialist on the phased certification of cybersecurity professionals who directly implement organizational, legal, engineering and technical measures, as well as cryptographic and technical protection of information aimed at preventing cyber incidents, detection and protection against cyber attacks, elimination of their consequences, restoration of sustainability and reliability of functioning of communication and technological systems. The available opportunities and guarantees provided in connection with the implementation of the educational card of cybersecurity specialist in the service, as well as possible educational initiatives provided by the educational card of cybersecurity specialist in the context of implementing organizational and technical model of cybersecurity.

Keywords: information technologies; cybersecurity; educational card; training, training system; cybersecurity specialist.