ДЕЯКІ ПИТАННЯ УДОСКОНАЛЕННЯ ДЕРЖАВНО-ПРИВАТНОЇ ВЗАЄМОДІЇ У СФЕРІ КІБЕРОСВІТИ

SOME ISSUES OF IMPROVING PUBLIC-PRIVATE COOPERATION IN CYBEREDUCATION

УДК 35.088.6:[004:007:351.86] (477)
DOI https://doi.org/10.32782/pma2663-5240-2022.31.4

Арсенович Л.А.
д. філос. з публ. упр. та адміністр., заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом Адміністрація Держспецзв'язку

Розвиток партнерських відносин між державою та бізнесом на теперішній час відіграє вагому роль у підвищенні не тільки ефективного функціонування підприємств, закладів та установ, а й соціально-економічного розвитку країни в цілому. Завдяки такому розвитку з'являється можливість залучення в державний сектор економіки додаткових ресурсів, іншими словами – інвестицій. Такі відносини сприяють підняттю ефективності використання наявних ресурсів, розподілу ризиків між державним і приватним сектором та їх мінімізації завдяки об'єднанню ресурсів та потенціалів держави та бізнесу.

Глобалізація та швидкі зміни навколишнього середовища вимагають пошуку нових методів і механізмів взаємодії не лише між національними економіками на макрорівні, а й між учасниками ринкових відносин всередині держави – на мікрорівні. Одним із таких механізмів співпраці є розвиток державно-приватної взаємодії.

У статті розглянуто механізм реалізації державно-приватної взаємодії у сфері кіберосвіти, метою якого є забезпечення співробітництва між державою та приватним сектором шляхом створення дієвої та ефективної системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки, кіберзахисту, кібероборони.

Проаналізовано склад суб'єктів державно-освітньої та приватно-освітньої кібербезпеки, здійснено аналіз алгоритму реалізації механізму державно-приватної взаємодії у сфері кіберосвіти, визначено його переваги в процесі впровадження. Сформульовано шляхи удосконалення державно-приватної взаємодії у сфері кіберосвіти, які направлені на впровадження освітніх інновацій та посилення їх ефективності, створення комплексної системи практичного навчання, удосконалення законодавчої бази, що регулює державно-приватну взаємодію, та посилення ресурсної спроможності національної системи кібербезпеки України шляхом розроблення Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України механізму державно-приватного замовлення на підготовку і підвищення кваліфікації фахівців із кібербезпеки.

Ключові слова: *державно-приватна взаємодія, кібербезпека, кіберосвіта, професійна підготовка, система підготовки кадрів, фахівці із кібербезпеки.*

To develop partnership relations between the state and business is now tangible for encouraging not only the effective operation of companies and institutions, but also the social and economic development of the country as a whole. This development allows attracting additional funds, in other words – investments, to the public sector of economy. Such relations contribute to the increase of efficiency in using the available funds, to distribution of risks between the public and private sectors, and to minimization of these risks due to bringing together the funds and potentials of the state and business.

Globalization and rapid environment changes require to seek new methods and ways of interaction not only between national economies at the macro level, but also between the participants of market relations within the state – at the micro level. One of such ways of interaction is the development of public-private cooperation.

The article analyzes the way of implementing public-private cooperation in cybereducation, which intends to ensure cooperation between the state and the private sector by coming up with an effective personnel training system and by increasing the competence of specialists in a variety of cybersecurity, cyberprotection and cyberdefense issues.

Analysis has been made to study the composition of the public education and private education cybersecurity units, to examine the algorithm for implementing the pattern of public-private cooperation in cybereducation, and to identify the advantages of this algorithm during its implementation. Ways to improve the public-private cooperation in cybereducation have been outlined, which aim to implement educational innovations and increase their effectiveness, create a comprehensive system of practical training, improve the legislative framework that regulates the public-private cooperation, and strengthen the resource capacity of Ukraine's national cybersecurity system with the help of a mechanism of public-private procurement for professional and advanced professional training of cybersecurity specialists as developed by the National Coordination Center for Cybersecurity at the National Security and Defense Council of Ukraine.

Key words: *public-private cooperation, cybersecurity, cybereducation, professional training, personnel training system, cybersecurity specialists.*

Постановка проблеми у загальному вигляді. В умовах розбудови цифрового світу та розвитку інформаційних технологій особливого значення набувають проблеми професійної підготовки спеціалістів IT-сфери, і перш за все фахівців із кібербезпеки.

Зовнішні та внутрішні загрози у безпековому середовищі України актуалізують потребу підвищення рівня професійної компетенції фахівців, які в умовах протидії збройній агресії російської федерації опікуються питаннями кібербезпеки та кіберзахисту державних інформаційних ресурсів.

Система підготовки кадрів у будь-якій сфері діяльності завжди буде унікальною. На конфігурацію та функціонування такої системи впливає цілий комплекс чинників: від особливостей законодавства до розподілу повноважень

між державними органами або підрозділами всередині органу, від менталітету та рівня освіти співробітників (населення) до їх комп'ютерної грамотності, від соціальної відповідальності до розвитку державно-приватної взаємодії у цій сфері тощо. При цьому комплексний характер завдань, пов'язаних зі створенням такої системи, вимагає забезпечення потреб у навчанні в широкому діапазоні цільових аудиторій, створення можливостей як для розповсюдження серед співробітників базових понять знань (підвищення інформованості), так і отримання додаткової вищої освіти.

У контексті проведення освітніх реформ у всіх сферах діяльності українського суспільства, співробітництво між державою та приватним сектором шляхом створення дієвої та ефективної системи підготовки кадрів та підвищення компетентності фахівців кібербезпеки, кіберзахисту та кібероборони набуває особливої актуальності та потребує окремої уваги.

Аналіз останніх досліджень і публікацій. Необхідність подальшої розбудови системи підготовки кадрів у сфері кібернетичної безпеки шляхом удосконалення державно-приватної взаємодії підкреслюють як іноземні так і сучасні науковці, які з моменту затвердження другої редакції Стратегії кібербезпеки України сигналізують і нагадують про це у наукових статтях і доповідях.

Так, науковці кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ Рязанцева І.М. та Тулупов В.В. у своїй статті зазначають, що гарантувати ефективну протидію кібернетичним загрозам в Україні може лише застосування комплексних підходів до забезпечення інформаційної безпеки, у тому числі шляхом активного співробітництва між державами і приватним безпековим сектором, безпековими установами та приватними компаніями, задіяними у сфері інформаційно-комунікаційних технологій [1, с. 143].

Інший науковець Прав Р.Ю. у своєму дослідженні в діяльності громадських інститутів – учасників державно-приватного партнерства у сфері кібербезпеки виділяє, у тому числі, такий напрямок як підготовка фахівців. На думку науковця, підготовка фахівців повинна спрямовуватися на надання допомоги у підвищенні кваліфікації співробітників органів державної влади, фахівців-практиків, а також у підготовці наукових і науково-технічних кадрів, обдарованої молоді, виявленні і підтримці талановитих дослідників і спеціалістів-практиків, сприянні творчого зростання молодих фахівців і науковців [2, с. 147].

Герасимюк К.Х., доцент кафедри управління та адміністрування Комунального закладу вищої освіти «Вінницька академія безперервної освіти», описуючи у своїй науковій статті механізми державного управління кібер- та інформаційною безпекою, зазначає про розробку Міносвіти та Мінцифри відповідної концепції трансформації ІТ-освіти в Україні, акцент якої робиться саме на потребах ринку ІТ-індустрії в приватній сфері та на підвищенні професійного рівня фахівців такої сфери [3, с. 38].

Водночас слід зазначити, що питання державно-приватної взаємодії у сфері кіберосвіти в контексті реалізації Стратегії кібербезпеки України та інших нормативно-правових актів залишилося поза увагою комплексних наукових досліджень, що потребує окремої уваги та подальшої розвідки.

Виділення невирішених раніше частин загальної проблеми. Серед механізмів системи освіти України сучасні науковці виділяють механізми удосконалення розвитку освіти (нормативно-правовий, організаційно-функціональний, кадрово-мотиваційний) та інтегровані механізми розвитку освіти (стратегічного фінансування, міжнародного співробітництва, науково-освітньої локалізації), які при комплексному застосуванні формують державну освітню політику. Інструментами реалізації вищезазначених механізмів визнано засоби, прямі і непрямі форми, методи та прийоми, використовуючи які держава послідовно і систематично впливає на кон'юнктуру ринку освітніх послуг і діяльність закладів вищої освіти з метою підтримки оптимальних організаційних, соціальних, педагогічних, правових, кадрових, матеріально-фінансових та інших умов їх розвитку, забезпечення високоякісних освітніх послуг, рівного доступу до освіти, інтеграції української освітньої сфери у європейський простір [4].

Враховуючи наявність нормативно-правової бази, яка хоча і перебуває на етапі становлення, мережу державних і приватних закладів освіти сфери кібербезпеки, які у зв'язку із впровадженням цифрових технологій мають тенденцію до збільшення, суттєве розширення кола учасників освітньої діяльності у сфері кібербезпеки, а також те, що механізми та інструменти системи освіти України, які мають як теоретичне, так і практичне значення, можуть так само застосовуватися і в системі підготовки кадрів у сфері кібербезпеки, слід констатувати, що система, яка досліджується, заснована відповідно до чинного законодавства та перебуває на початковому шляху її розбудови.

Мета статті. Метою статті є вивчення питання щодо подальшого удосконалення державно-приватної взаємодії у сфері кіберосвіти.

Виклад основного матеріалу. Державно-приватна взаємодія є важливою ланкою партнерства між державою та бізнесом, що пов'язує їх інтереси і дозволяє ефективно та дієво реалізовувати пріоритетні, соціально значущі проєкти. Державно-приватна взаємодія стимулює залучення інвестицій у реальний сектор економіки та сприяє розвитку ринків капіталу, товарів та послуг, інноваційних галузей промисловості. Механізми державно-приватної взаємодії використовують практично у всіх галузях економіки.

Поняття державно-приватної взаємодії можна тлумачити як в широкому так і у вузькому значеннях. У широкому розумінні державно-приватна взаємодія – це система відносин держави (уряду) та приватної (комерційної) сфери, яка широко використовується як інструмент національного, міжнародного, регіонального (міського), економічного або соціального розвитку. У вузькому розумінні державно-приватна взаємодія – це відповідні проєкти, що запроваджуються державними органами спільно із приватними компаніями на об'єктах національної (державної) та муніципальної (приватної) власності.

До ознак державно-приватної взаємодії відносять: забезпечення вищих техніко-економічних показників ефективності діяльності; довготривалість відносин (від 5 до 50 років); передачу приватному партнеру частини ризиків; внесення приватним партнером інвестицій в об'єкти партнерства із легальних джерел. Крім того, до ключових ознак державно-приватної взаємодії прийнято відносити конкурентний спосіб відбору та фільтрації партнерів, а успіх реалізації проєкту за технологіями державно-приватної взаємодії залежить від прозорості проведеного конкурсу, оскільки тільки такий спосіб забезпечує вибір найбільш економічно вигідного проєкту та надійного партнера [5, с. 221].

Передбачається, що взаємодія між державою і приватним сектором повинна будуватися на принципах: законності, «здорової» конкуренції, прозорості, підзвітності, зрозумілості і передбачуваності, економічної а також фінансової сталості, врахування відповідної специфіки, гнучкості та рівності.

Формування державно-приватної взаємодії має відповідати умовам нестабільної економіки та ґрунтуватися на таких методологічних засадах:

– партнерство має відповідати цілям розвитку економіки країни та її суб'єктів;

– партнерство має бути підпорядковане вирішенню не лише поточних, а й стратегічних завдань розвитку відповідної сфери економіки країни загалом та її суб'єктів окремо;

– дотримання рівності інтересів сторін та свободи вибору дій;

– невтручання держави у сферу відповідальності приватного партнера;

– конкурентність та відповідальність за виконання умов контракту [6, с. 107-108].

Відповідно до законодавчих актів та нормативно-правових актів Президента України органи і підрозділи як державних, так і недержавних суб'єктів кібербезпеки, забезпечують захист життєво важливих інтересів людини і громадянина, суспільства та держави, національні інтереси України у кіберпросторі, а також здійснюють основні цілі, напрями та принципи державної політики у сфері кібербезпеки. І одним із таких напрямів, який є стрижневим у всій сфері кібербезпеки, є застосування державно-приватної взаємодії, яка реалізовується, у тому числі, шляхом розбудови кіберосвіти, а саме напрямом розроблення і впровадження освітніх заходів у сфері кібербезпеки, кіберзахисту та кібероборони.

Так, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [7] державно-приватна взаємодія у сфері кібербезпеки здійснюється, у тому числі, шляхом створення системи підготовки кадрів, підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки, підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

Крім цього, згідно Указу Президента України від 26 серпня 2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [8] Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить посилення національної кіберготовності та кіберзахисту, у тому числі, шляхом проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів.

Зазначені акти ще раз підкреслюють необхідність подальшого вдосконалення кібернетичної освіти у тісній співпраці із складовими приватної (комерційної) кібербезпеки, що надасть змогу забезпечувати підготовку, перепідготовку та підвищення кваліфікації в обсязі, необхідному для задоволення потреб держави, у тому числі в умовах воєнного стану.

На сьогодні, враховуючи думки та дослідження сучасних науковців, можна констатувати проблему відсутності єдиної методології в системі підготовки кадрів у сфері кібербезпеки для всіх фахівців – як на державному, так і на приватному рівнях. Відсутність єдиних керівних документів, методичного забезпечення навчання, розбіжність у поглядах на мету, завдання та зміст підготовки з питань кібербезпеки знижує ефективність та якість підготовки кіберфахівців для всієї країни в цілому. Крім того, рівень кіберосвіти в Україні має ризики до стрімкого послаблення через недостатню цифрову грамотність населення, представників державного сектора та бізнес кіл.

Ці тези підтверджують статистичні дані, які узагальнено за результатами вивчення практичних аспектів кіберосвіти, а також численні інформаційні та аналітичні документи сучасних аналітиків і експертів. Так, протягом останніх двох – трьох років державні та приватні заклади вищої освіти, що здійснюють підготовку фахівців за спеціальністю 125 «Кібербезпека» галузі знань «Інформаційні технології», щороку в середньому випускають 1400 дипломованих кіберфахівців (близько 900 бакалаврів та 500 магістрів), 70% яких у подальшому працюють в органах і підрозділах недержавних суб'єктів кібербезпеки [9, 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 вишів країни система освіти у сфері інформаційних технологій відчутно відстає від потреб ринкової економіки країни та світу [10, с. 386].

Враховуючи зазначене, з метою розвитку державно-приватної взаємодії у сфері кіберосвіти, необхідним є удосконалення реалізації відповідного механізму, що можна зробити шляхом удосконалення законодавства, вивчення міжнародного досвіду та запозичення кращих практик (рис. 1).

Розроблений проєкт – це механізм створений для зацікавленості приватного сектору в розвитку кіберосвіти, стимулювання співпраці між науковим і освітнім секторами економіки, підтримки державних і недержавних суб'єктів кібербезпеки, надання допомоги у створенні державної політики та плануванні освітніх кібернетичних ініціатив, сприяння трансферу технологій, формування освітніх та інноваційних кіберкластерів, а також для спільного усвідомлення і визначення ключових понять та складових цифрової компетентності.

Зазначений механізм спрямований на впровадження нових інформаційних та освітніх технологій, застосування прогресивних форм організації освітнього процесу та активних методів навчання, а також сучасних навчально-методичних матеріалів, які в сукупності є основою для всебічного розвитку людини та добробуту населення в цілому.

Сферу кіберосвіти України формують складові державної кібербезпеки (Національний координаційний центр кібербезпеки при РНБО України, суб'єкти національної системи кібербезпеки та Мінцифри), державно-освітньої (академічної) кібербезпеки (державні заклади вищої освіти) та приватно-освітньої (комерційно-освітньої) кібербезпеки (ІТ-школи (навчальні центри) та приватні заклади вищої освіти).

При цьому ключову роль у побудові ефективної кібернетичної освіти повинен відігравати Національний координаційний центр кібербезпеки при РНБО України, одними із основних завдань якого є здійснення аналізу стану забезпечення кадрами національної системи кібербезпеки, підготовка пропозицій щодо її удосконалення, а також участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів у сфері забезпечення кібербезпеки, розроблення відповідних методичних документів і рекомендацій [11].

Основу державної кібербезпеки складають основні суб'єкти національної системи кібербезпеки: Держспецзв'язку, Нацполіція, СБ України, Міноборони, Генеральний штаб ЗС України, розвідувальні органи та Нацбанк. Для потреб зазначених органів сформовані відповідні заклади освіти, які в тій чи іншій мірі опікуються питаннями кібербезпеки, а саме: в Держспецзв'язку – Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ імені Ігоря Сікорського»; для потреб Нацполіції – кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, яка здійснює підготовку кваліфікованих фахівців для підрозділів Нацполіції; в СБ України – Національна академія СБ України; для потреб ЗС України – Харківський національний університет Повітряних сил імені Івана Кожедуба та Військовий інститут телекомунікацій та інформатизації імені Героїв Крут.

Мінцифри в свою чергу відповідно до покладених на нього завдань (постанова Кабінету Міністрів України від 18 вересня 2019 року № 856) бере участь у формуванні державної політики цифровізації освіти та розробленні професійних стандартів з питань цифрової грамотності.

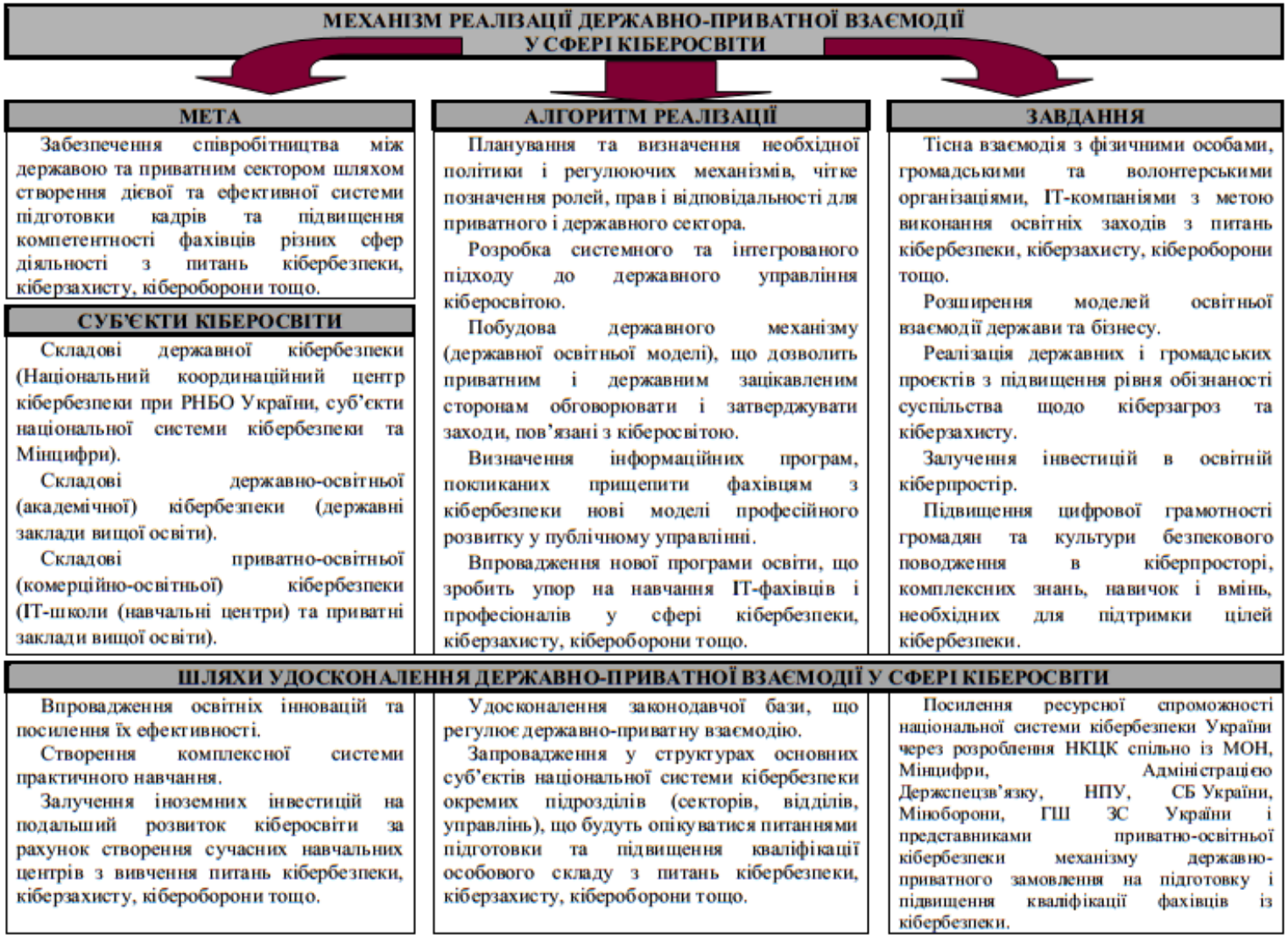

Рис. 1. Механізм реалізації державно-приватної взаємодії у сфері кіберосвіти

Розробка автора

До основи державно-освітньої та приватно-освітньої кібербезпеки відносяться:

– 160 закладів вищої освіти, які здійснюють підготовку бакалаврів та магістрів за спеціальностями галузі знань «Інформаційні технології», з яких 123 заклади вищої освіти є державними (76,7%), а 37 закладів вищої освіти – здійснюють підготовку у приватному порядку (23,3%);

– 56 державних та 3 приватних закладів вищої освіти, що здійснюють підготовку докторів філософії та докторів наук за спеціальностями галузі знань «Інформаційні технології»;

– 51 заклад вищої освіти, що організовує підвищення кваліфікації фахівців за спеціальностями галузі знань «Інформаційні технології» та з питань інформаційних технологій і кібербезпеки;

– 133 IT-школи (навчальні центри), які на сьогодні здійснюють комплексну підготовку і розвиток фахівців з інформаційних технологій та кібербезпеки, а також звичайних громадян, які виявили бажання стати IT-спеціалістами;

– 62 навчальні IT-школи, які здійснюють навчання дітей та підлітків програмуванню, а також створенню власних проєктів у сфері IT-технологій та кібербезпеки.

Крім цього до складу приватно-освітньої кібербезпеки відносяться профільні бізнес-асоціації, регіональні об'єднання (кластери), приватні освітні проєкти, інноваційні парки, технологічні хаби, масштабні індустріальні події, професіональні формальні та неформальні спільноти. Кожен з цих елементів має свої пріоритети та вектори роботи, що в результаті створює позитивні умови для розвитку кіберосвіти.

Процес кіберосвіти та створення в Україні дієвої та ефективної системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки, кіберзахисту та кібероборони необхідно розглядати, виходячи в першу чергу, з реалій та можливостей. Звісно, не можна не враховувати як позитивний, так і негативний досвід провідних країн світу, у яких вже впроваджені та функціонують аналогічні системи. Тому при аналізі алгоритму реалізації механізму державно-приватної взаємодії необхідно робити особливий акцент, який вказує на необхідність:

– розроблення відповідних змін до чинного законодавства, що у подальшому забезпечить визначення цифрової освіти (навичок) та цифрових компетентностей у всіх сферах суспільного життя;

– правового регулювання з питань формування державної політики у сфері розвитку цифрових навичок та відповідних компетентностей всіх громадян;

– впровадження координації дій серед складових державно-освітньої та приватно-освітньої кібербезпеки щодо підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки, кіберзахисту та кібероборони;

– підвищення рівня цифрових навичок та компетентностей в державі, а також рівня конкурентоспроможності країни щодо розвитку кіберосвіти;

– створення певних індикаторів для контролю (моніторингу) стану розвитку цифрових навичок та компетентностей;

– прискорення всіх освітніх процесів у сфері кібербезпеки, кіберзахисту, кібероборони в Україні;

– підвищення конкурентоспроможності співробітників сектору безпеки і оборони України, а також інших громадян шляхом оволодіння новими цифровими навичками та компетентностями.

Разом з тим виконання завдань, які визначені в рамках реалізації державно-приватної взаємодії у сфері кіберосвіти, надали би змогу:

– підвищити рівень доступності до державних послуг для громадян похилого віку, осіб з інвалідністю, малозабезпечених сімей, інших вразливих груп населення;

– суттєво зменшити ризики виникнення небезпек під час користування Інтернетом;

– визначити систему та опис складових цифрової компетентності (рамки цифрової компетентності), а також вимог до рівня володіння цифровими навичками та цифровими компетентностями різних категорій працівників, зокрема в професійних стандартах [12].

Наступною відправною точкою в удосконаленні державно-приватної взаємодії у сфері кіберосвіти є негайна потреба у розробленні стратегічного бачення у сфері кіберосвіти, та затвердженні відповідних нормативно-правових документів урядового рівня, спрямованих на підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки, кіберзахисту, кібероборони тощо.

Впровадження освітніх інновацій, посилення їх ефективності а також створення комплексної системи практичного навчання нададуть змогу:

– створити сучасну цілісну та 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 [13, с. 104].

Створення сучасних навчальних центрів з вивчення питань кібербезпеки, кіберзахисту, кібероборони зможуть забезпечити:

– гранти та стипендії для студентів IT-спеціальностей;

– професійну сертифікацію та можливість тестування студентів на відповідність професійним IT-стандартам;

– матеріальну підтримку та працевлаштування випускників.

Разом з тим, 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, кіберзахисту, кібероборони надасть можливість:

– вдосконалити професійну підготовку шляхом поглиблення і розширення професійних знань, умінь і навичок;

– набути кіберзахисниками досвіду виконання додаткових завдань та обов'язків у межах отриманої спеціальності;

– підвищувати рівень професійних знань, удосконалити свою майстерність;

– закріпити й удосконалити особисті практичні уміння і навички, необхідні для якісного та ефективного виконання службових обов'язків;

– оновити, розширити і формувати нові професійні знання у галузі знань «Інформаційні технології»;

– вивчити сучасні методи управління, ознайомитись з досягненнями науки і техніки та перспективами їх розвитку;

– розроблювати пропозиції щодо удосконалення і впровадження у практику найкращих досягнень науки і техніки у галузі знань «Інформаційні технології».

У свою чергу посилення ресурсної спроможності національної системи кібербезпеки України через розроблення Національним координаційним центром кібербезпеки при РНБО України (спільно із Міносвіти, Мінцифри, Адміністрацією Держспецзв'язку, Нацполіцією, СБ України, Міноборони, ГШ ЗС України і представниками приватно-освітньої кібербезпеки) механізму державно-приватного замовлення на підготовку і підвищення кваліфікації фахівців із кібербезпеки надав би змогу:

– забезпечувати розвиток державних і недержавних суб'єктів кібербезпеки за рахунок впровадження освітніх інновацій та посилення їх ефективності;

– підвищити загальну культуру відносин між державною і приватною кібербезпекою за допомогою створення комплексної системи практичного навчання;

– вирішувати проблеми зайнятості населення та залучати іноземні інвестиції на подальший розвиток кіберосвіти за рахунок створення сучасних навчальних центрів з вивчення питань кібербезпеки.

На сьогодні в Україні система підготовки кадрів у сфері кібербезпеки та кіберосвіта в цілому перебувають у трансформаційному стані. Існують поодинокі стохастичні явища, але будь-яка комплексна системність практично відсутня. Закон України «Про основні засади забезпечення кібербезпеки України» жодним чином не вирішує цієї проблеми, залишаючи осторонь ключові проблеми забезпечення і контролю якості та визнання освіти у сфері кібербезпеки. Не існує офіційної статистики з цих питань, відсутні спеціальні концепції та освітні програми. Тому для України вкрай важливо найближчим часом вжити дієві заходи для подолання відставання у цій сфері.

Висновки. Забезпеченню якісної підготовки фахівців у сфері кібербезпеки має сприяти інтеграція закладів вищої освіти, академічних і галузевих секторів науки. У цьому контексті особливого значення має набути впровадження у діяльність закладів освіти інноваційних технологій на кшталт віртуальних лабораторій. Адже нині кіберосвіта характеризується недостатнім рівнем інноваційної активності. Цьому певною мірою сприяє і те, що, власне, в науці, яка нині поділяється на академічну, галузеву та вишівську, на жаль, існує незбалансованість її зусиль на розвиток та впровадження нових організаційних форм, які відповідають логіці ринкових відносин, у тому числі у сфері кіберосвіти. Подолання цих недоліків сприятиме інтеграції кібернетичної освіти, залученню роботодавців до підготовки IT-фахівців, прискоренню формування конкурентоспроможної головної продуктивної сили суспільства.

Навчання протягом життя виходить на чільні позиції у світових освітніх процесах – це диктується базовими тенденціями сучасного розвитку людства. Такий підхід, на наш погляд, дозволить кардинально змінити систему підготовки кадрів у сфері кібербезпеки. Адже до цього часу, на жаль, у переважній більшості вона зорієнтована на запити минулого. Сучасна ж економіка потребує кадрів, готових працювати в умовах конкуренції, тобто в інноваційній економіці.

Слід відзначити, що на теперішній час вже здійснено перший крок у створенні платформи для «мозкового штурму» і механізму для державно-приватної взаємодії в сфері кібербезпеки. Так, у жовтні 2020 року Держспецзв'язку разом із Міністерством цифрової трансформації, Радою національної безпеки та оборони України та Службою безпеки України започатковано роботу Експертної ради з інформаційної та кібербезпеки, яка має об'єднати фахівців з державних органів, комерційного сектора та науковців, щоб посилити національну систему кібербезпеки України, у тому числі в напрямі удосконалення системи підготовки кадрів. Планується, що саме Експертна рада стане синергією зусиль однодумців, формуватиме нові ідеї, проєкти, рішення в сфері забезпечення кібербезпеки та кіберосвіті, які необхідно буде втілювати у подальшому на практиці [14].

ЛІТЕРАТУРА:

1. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки. *Право і Безпека.* 2014. Вип. № 2. С. 140-144.

2. Прав Р. Ю. Роль механізму державно-приватного партнерства у розвитку кібербезпеки України на сучасному етапі. *Інвестиції: практика та досвід.* 2019. Вип. № 21. С. 143-150.

3. Герасимюк К. Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. *Економіка, управління та адміністрування.* 2021. Вип. № 3. С. 36-40.

4. Якайтіс І. Б. Механізми державного управління інноваційним розвитком вищої освіти в Україні : автореф. дис. на здобуття наук. ступеня канд. наук. з держ. упр. : 25.00.02. Івано-Франківськ, 2018. 22 с.

5. Губанова Т. Державно-приватне партнерство у сфері освіти і науки в Україні: нормативно-правова характеристика. *Підприємництво, господарство і право.* 2019. Вип. № 6. С. 220-224.

6. Шевчук О. А. Державно-приватне партнерство в сфері інноваційного розвитку : дис. ... д-ра філософ. у галузі публ. управлін. та адміністрував. : 281 / Державний університет – Житом. політех. Житомир, 2021. 175 с.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жов. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 21.10.2022).

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 21.10.2022).

9. Арсенович Л. А. Кіберосвіта в умовах цифровізації публічного управління. Цифрова трансформація публічного управління : кол. моногр. / О. В. Карпенко, І. Й. Малий, Г. В. Муравицька та ін. Київ : НАДУ, 2020. 256 с. С. 168-228.

10. Тимошенко Н. Ю. Проблеми та перспективи розвитку IT-індустрії в Україні. *Економіка та суспільство.* 2018. Вип. № 17. С. 384-388.

11. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07 черв. 2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення: 21.10.2022).

12. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : розпорядження Кабінету Міністрів України від 03 бер. 2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text (дата звернення: 21.10.2022).

13. Арсенович Л. А. Модель професійного розвитку фахівця з кібербезпеки (на прикладі Державної служби спеціального зв'язку та захисту інформації України). *Вісн. НАДУ. Серія «Державне управління».* 2019. Вип. № 4 (95). С. 98–104.

14. Держспецзв'язку започаткувала роботу Експертної ради з інформаційної та кібербезпеки : веб-сайт. URL: https://detector.media/infospace/article/181312/2020-10-06-derzhspetszvyazku-zapochatkuvala-robotu-ekspertnoi-rady-z-informatsiynoi-ta-kiberbezpeky/ (дата звернення: 21.10.2022).