Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Категорія «Б», Наказ Міністерства освіти і науки України від 28.12.2019 №1643)
www.dy.nayka.com.ua | № 2 2021 р. | 25.02.2021

DOI: 10.32702/2307-2156-2021.2.2

УДК 327.7:061.

О. В. Євсюкова,
д. держ. упр., доцент кафедри публічного управління та публічної служби,
Національна академія державного управління при Президентові України
ORCID ID: 0000-0002-1299-6955

ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

O. Evsyukova
Doctor of Science in Public Administration, Associate Professor, Associate Professor of the Department of Public Governance and Public Service, National Academy of Public Administration under the President of Ukraine

FEATURES OF TRAINING OF SPECIALISTS IN THE FIELD OF CYBER SECURITY: CURRENT CHALLENGES AND PROSPECTS

У статті обґрунтовано актуальність осмислення кібербезпеки держави, як однієї з найважливіших галузей трансформаційного, цифрового суспільства. Визначено об'єктивну необхідність функціонування системи підготовки фахівців у сфері кібербезпеки, що обумовлена зростанням кіберзлочинності та кіберзагроз у сучасному світі. Проаналізовані теоретичні аспекти щодо формування системи професійної підготовки фахівців із кібербезпеки, визначено особливості та перспективи її функціонування в умовах сьогодення. Охарактеризовано американський досвід підготовки фахівців із кібербезпеки на базі навчальних закладів США, що мають світове визнання у цій сфері. Акцентовано увагу на питаннях стандартизації підготовки зі спеціальності 125 "Кібербезпека" та на фахових компетенціях фахівців у сфері кібербезпеки. підготовка висококваліфікованих кадрів з кібербезпеки для органів публічної влади залишається ключовим елементом повноцінної життєдіяльності держави. Зроблено висновок, що належне функціонування системи підготовки фахівців у сфері кібербезпеки формування обумовлене необхідністю у покращенні кібербезпеки, яка є надзвичайно важливою для забезпечення довіри людей до інновацій, взаємозв'язку та автоматизації, отримання переваг від них, а також для захисту основних прав і свобод, зокрема права на приватність та захист персональних даних, а також свободу вираження поглядів та інформації.

The article substantiates the relevance of understanding the cybersecurity of the state as one of the most important branches of a transformational, digital society. Due to the extremely widespread use of modern information and communication technologies in all spheres of its existence, society has become vulnerable to cyber influences, which are increasingly becoming an effective tool to achieve the goal of non-violent control and management of infrastructure, state enterprises and individual citizens. associations.
In view of the above, the main idea of the article is to determine the features of the system of training in the field of cybersecurity, taking into account the objective need and prospects for its operation in modern conditions.

The specified objective necessity of functioning of the system of training of specialists in the field of cybersecurity, which is caused by the growth of cybercrime and cyberthreats in the modern world, is determined. Theoretical aspects of the formation of the system of professional training of specialists in cybersecurity are analyzed, the features and prospects of its functioning in today's conditions are determined. The American experience of training cybersecurity specialists on the basis of US educational institutions with world recognition in this field is described. Emphasis is placed on the issues of standardization of training in the specialty 125 "Cybersecurity" and on the professional competencies of specialists in the field of cybersecurity. training of highly qualified cybersecurity personnel for public authorities remains a key element of the full functioning of the state.

It is concluded that the proper functioning of the training system in the field of cybersecurity is due to the need to improve cybersecurity, which is extremely important to ensure people's confidence in innovation, communication and automation, benefit from them, and to protect fundamental rights and freedoms, in particular the right to privacy and protection of personal data, as well as freedom of expression and information.

It is stated that cybersecurity is: an objective necessity for network communication and the global and open Internet, which should be the basis for the transformation of the economy and society in the 2020s; is an important tool for international security and the stability and development of economies, democracies and societies around the world. Accordingly, public authorities, businesses and citizens must use digital tools responsibly, taking all necessary security measures.

Ключові слова: *цифрове суспільство; інформаційно-комунікаційні технології; інформаційна безпека; кібербезпека; система підготовки фахівців у сфері кібербезпеки.*

Key words: *digital society; information and communication technologies; information security; cybersecurity; system of training specialists in the field of cybersecurity.*

Постановка проблеми. За умов сьогодення, демократичні принципи управління державою не викликають сумніву у громадян України, але нагальним завданням науки державного управління та практики публічного адміністрування залишається переосмислення значення держави, як головного суб'єкта-виконавця у реалізації інтересів і задоволенні потреб суспільства. Новий поштовх розвитку демократії за допомогою інформаційно-комунікативних технологій, на думку багатьох практиків-управлінців, форматує діалог держави та суспільства, влади та громадян у новому ракурсі, наближуючи її до ідеальної демократії, при цьому держава набуває сервісних ознак, суспільство перетворюється в "smart"-спільноту, а влада є якісно новим засобом вирішення публічних справ в інтересах усієї країни шляхом залучення якомога більшої кількістю громадян до даного процесу. На сучасному етапі розвитку науки й техніки кібербезпека кожної розвинутої держави перетворюється на одну з найважливіших галузей високотехнологічного суспільства. Унаслідок надзвичайно широкого використання сучасних інформаційних-комунікативних технологій у всіх сферах свого існування суспільство стало вразливим від кібернетичних впливів, які все частіше стають ефективним інструментом для досягнення мети несилового контролю та управління як об'єктами інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об'єднаннями. Потоки інформації, що передаються, зберігаються й обробляються в кіберпросторі, постійно збільшуються, що вимагає їх належного захисту від несанкціонованого доступу зі злочинною метою. Тому посилення кібербезпеки є надзвичайно важливим для забезпечення довіри людей до інновацій, взаємозв'язку та автоматизації, отримання переваг від них, а також для захисту основних прав і свобод, зокрема права на приватність та захист персональних даних, а також свободу вираження поглядів та інформації [16].

Безперечним є той факт, що в умовах подальшого розвитку високотехнологічного суспільства потреба у фахівцях із кібербезпеки буде постійно зростати.

Аналіз останніх досліджень і публікацій. Існує значна кількість досліджень, що стосуються обраної тематики представленої публікації. Мова йде про наукові праці: Л. Арсеновича (щодо специфіки формування системи підготовки фахівців у сфері кібербезпеки органів публічної влади тощо); Б. Бистрової, Ю. Савчук (щодо формування концептуальних засад професійної підготовки фахівців із кібербезпеки та удосконалення чинного законодавства, що регулює сферу інформаційної та кібернетичної безпеки, використання кращих практик зарубіжного досвіду у вказаному напрямі тощо); І. Діордиці (щодо формування системи забезпечення кібербезпеки, сутнісного визначення кіберзлочинності, правововового регулювання кібертероризму тощо); О. Криворучка, І. Костюка (щодо стратегування безпеки інформації); Л. Рудник (щодо інформаційної безпеки та кібербезпеки, як складових елементів національної безпеки тощо). При цьому наукова проблематика у сфері кібербезпеки досить ґрунтовно висвітлюється в наукових розробках таких вчених, як: В. Богуш, В. Бурячок, С. Воскобойніков, Т. Запорожець, О. Карпенко, І. Кулик, С. Мельник та ін.

Невирішені частини проблеми. Незважаючи на досить вагомі фундаментальні напрацювання науковців за вказаним напрямом, все ще залишаються далекими від завершення наукові дослідження щодо: формування та функціонування системи підготовки фахівців у сфері кібербезпеки органів публічної влади в Україні; розробки освітньо-професійних програм "Професійна кібербезпека (за спеціалізаціями)" для підготовки вузькопрофільних фахівців із кібербезпеки та захисту інформації; полемічності в обговоренні проблематики формування фахових компетентностей та стандартизації процесу підготовки фахівців зі спеціальності 125 "Кібербезпека" тощо, які і перебувають в епіцентрі серйозних наукових дискусій.

Формулювання мети статті. З огляду на зазначене, головна ідея статті полягає у визначенні особливостей системи підготовки фахівців у сфері кібербезпеки з врахуванням об'єктивної необхідності та перспектив її функціонування в сучасних умовах.

Виклад основного матеріалу. У процесі активного розвитку інтернету та соціальних мереж у суспільстві, починають здійснюватися зміни глобального інформаційного простору, як елементи глобальної мережевої структури людства. Подія, яка відбулася на Женевському всесвітньому саміті в грудні 2003 р., що був присвячений питанням інформаційного суспільства, сприяла підписанню лідерами більшості світових країн таких стратегічних документів, як: "Декларація принципів" та "План дій", в яких визначено основні напрямки розвитку інформаційного суспільства на всіх рівнях, а також визнана необхідність модернізації та реалізації національних стратегій впровадження інформаційно-комунікативних технологій у сферу публічного управління.

Ураховуючи вище зазначене, цілком слушною є думка Л.І. Рудник, яка зазначає, що в умовах наукового-технічного та технологічного прогресу інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки та визначається складною взаємодією багатьох факторів, серед яких провідне місце займає "фактор людини" [14]. Вітчизняна дослідниця вдало зазначає, що людина є основним носієм і користувачем інформації, вона є основним суб'єктом і об'єктом інформаційної боротьби, а також основним творцем і користувачем комп'ютерних систем і мереж та/або телекомунікаційних мереж і, саме тому, вона є основним суб'єктом і об'єктом кіберборотьби. Кіберпростір, кібернетичні ресурси, комп'ютерно-системна й мережева інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Інформаційна безпека й кібербезпека є невід'ємними складовими кожної зі сфер національної безпеки і, водночас, інформаційна безпека та кібербезпека є важливими самостійними складовими процесу забезпечення національної безпеки [14].

Прикметним у даному контексті є аналіз наукових праць І.В. Діордіци, які присвячені багатьом аспектам формування державної політики кібербезпеки, зокрема: аналізу нормативно-правових засад у сфері безпеки з виокремленням тих норм, які безпосередньо стосуються державної політики кібербезпеки, визначення основних напрямів державної політики кібербезпеки і її основне призначення, які постійно змінюються, потребують швидкого реагування, прийняття відповідних рішень та запровадження необхідних дієвих заходів щодо. Варто погодитися з автором, що сучасне українське суспільство у процесі трансформації до кібернетичного суспільства [4, с.118-119; 5 с.112].

На думку вказаного науковця, державну політику кібербезпеки варто розуміти як діяльність держави в кібернетичній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства (кібернетичного суспільства) на основі розвитку єдиного кібернетичного простору цілісної, інформаційно розвиненої держави та її інтеграції у світовий кібернетичний простір з урахуванням збереження національної ідентичності, реалізації національних інтересів за гарантування кібернетичної безпеки на внутрішньодержавному та міжнародному рівнях. І.В. Діордіца вважає, що основною метою державної політики кібербезпеки є управління реальними та потенційними кіберзагрозами і небезпеками для створення необхідних умов для задоволення кібернетичних потреб людини і громадянина, а також реалізації національних інтересів у зазначеній сфері [4, с.120]

Українські науковці – О.В. Криворучко та І.В. Костюк вказують на те, що посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом найбільш вразливим до кіберзагроз. Нині у сучасному інформаційному суспільстві комп'ютерні злочини стали характерною ознакою сьогодення. Розріняють різні категорії комп'ютерних злочинців: "хакери", "кракери", "пірати", "шкідники". Злочини, що утворюються злочинними угрупуваннями з використанням інформаційних технологій: кібертероризм, загроза фізичної розправи, дитяча порнографія, "відмивання" грошей, крадіжка грошей з банківських рахунків, шахрайські операції з пластиковими платіжними картками, розповсюдження інформації про наркотики через Інтернет [10]. Слушною є точка зору науковців щодо необхідності розробки стратегії захисту інформації з чітким визначенням її змістовних елементів, а саме: мети, критеріїв, принципів, процедур на засадах яких варто створити надійну систему захисту. На основі концепції безпеки інформації необхідно розробити вказану стратегію та архітектуру системи захисту інформації і, відповідно – політику безпеки інформації.

Інформація, як сукупність знань про фактичні дані і залежності між ними, стала стратегічним ресурсом, основою для прийняття будь-якого рішення. В інформаційних системах, які створюються в органах державної влади і у комерційних структурах, циркулює інформація, що містить секретні відомості про досягнутий потенціал в області економіки, оборони, науки і техніки, конфіденційні відомості про управлінську, господарську, комерційну, фінансову й іншу діяльність. Відповідно захист інформації – складна, наукомістка і багатогранна проблема в умовах упровадження сучасних інформаційних технологій, створення розподілених обчислювальних систем і мереж зв'язку, що набуває особливої гостроти [10].

Зазначимо, що сьогодні у будь-якому суспільстві справедливою є теза: “хто володіє інформацією, той володіє світом”. Володіння інформацією робить індивіда більш адаптованим до навколишнього середовища, створює відчуття захищеності (найчастіше мінливе відчуття). Проте інформаційне (у вищезазначеному контексті – кібернетичне) суспільство вже досить швидко перетворюється на суспільство знань, у якому “хто володіє знаннями, той володіє світом”. Принципово, що поняття “знання” не тотожне поняттю “інформація”, воно включає більш широкий когнітивний спектр: розуміння, засвоєння, володіння як уміння застосувати інформацію та ін. Однак суспільство знань разом із величезним перспективами характеризується наявністю нових проблем. Припускаючи, що обсяг загальної інформації, що зростає, можливо встановити певні “захисні фільтри”, хоча ситуація з виборчим процесом 2019 р. кардинально заперечує це твердження. Але виникає питання як опанувати постійно зростаючим обсягом не просто інформації, а знань, якими повинен оволодіти державний службовець, щоб бути успішним, конкурентним на ринку праці. У такому разі виникає потреба не в традиційній освіті, а у впровадженні перспективного освітнього процесу на засадах використання інноваційних технологій управління знаннями. Когнітивна стратегія інформування спрямована на виокремлення з інформаційного потоку актуальної інформації та опрацювання її за допомогою порівняння з цільовими і мотиваційними, вираженими в образно-емоційній формі, з когнітивними ймовірними припущеннями особистості [11].

Як зазначає Т. В. Запорожець, бурхливий розвиток сучасного суспільства детермінований стрімким збільшенням та динамічністю росту різноманітної інформації. Ці дані усе складніше піддаються формальній структуризації, відтак так стандартні бази даних та сховища інформації потребують значних змін в методах роботи з ними та вимагають не лише автоматизації процесів їх обробки та аналізу, а й інтелектуалізації інформаційних та організаційних процесів, побудови та запровадження ефективних інтелектуальних технологій [7, с. 52].

Однак сучасні науковці звертають увагу на існування так званої межі новизни (нових факторів і ідей), які людина може засвоїти за певний період часу. Це її адаптативний рівень сприйняття. Тому проблеми, пов’язані з необхідністю інтелектуалізації інформаційних і організаційних процесів, інтенсифікації інтелектуальної діяльності фахівців-управлінців, вимагають негайного вирішення [9, с. 49].

На підтвердження вказаному, науковий інтерес становлять праці вітчизняної дослідниці Б. Бистрової, яка досліджуючи американський досвід у сфері кібербезпеки зазначає, що розповсюдження інформаційних засобів відкриває можливість для розвитку особистості, актуалізує вивчення змін у свідомості людини в постіндустріальному суспільстві США, у якому формується потреба якісного кадрового забезпечення галузей [2]. “Проведений вказаною дослідницею змістовний аналіз Національної стратегії досягнення безпеки в кіберпросторі (National Strategy to Secure Cyberspace) у США”, дозволив виокремити п’ять пріоритетів діяльності США в ІТ-галузі, та кібербезпеки країни [17]. Мова йде про таки напрями як: становлення і розвиток національної системи реагування на події в сфері інформаційної безпеки; реалізація комплексної системи заходів щодо зменшення загроз інформаційній безпеці; забезпечення підготовки фахівців у сфері комп’ютерної безпеки й забезпечення відповідального ставлення всього населення країни до питань захисту ІТ-систем; забезпечення захисту інформаційних систем, що мають відношення до державних органів; розвиток різних форм кооперації (у тому числі й міжнародної) у сфері забезпечення інформаційної безпеки [2]. Відповідно до пріоритетного напряму – забезпечення підготовки фахівців у сфері комп’ютерної безпеки й забезпечення відповідального ставлення всього населення країни до питань захисту ІТ-систем, Б. Бистрова зазначає, що дії американського суспільства націлені на забезпечення підготовки фахівців у сфері комп’ютерної безпеки й забезпечення відповідального ставлення всього населення країни до національної безпеки. Розвиток відповідального ставлення до ІТ-систем та підготовка кадрів у цій сфері передбачає, що джерелом багатьох вразливостей є недостатньо відповідальне ставлення деяких користувачів, системних адміністраторів і розробників інформаційних систем до питань захисту інформації, їх недостатня поінформованість у цій сфері. Для забезпечення кіберзахисту держави “Національна стратегія досягнення безпеки в кіберпросторі” передбачає реалізацію таких основних заходів: просування багатосторонньої загальнонаціональної програми з інформування та розвитку відповідального ставлення громадян країни до забезпечення безпеки тих інформаційних систем, до яких вони мають будь-який доступ; заохочення створення програм підготовки фахівців, які забезпечили б задоволення потреби в професіоналах; підвищення ефективності існуючих програм підготовки фахівців із кібербезпеки; підтримку зусиль приватних компаній щодо створення, поширення й забезпечення загального визнання сертифікаційних програм у сфері інформаційної безпеки [2].

Підготовка фахівців з кібербезпеки у США ґрунтується на оволодінні сучасними інформаційними технологіями, фундаментальними та прикладними науковими дисциплінами, що дозволяє одержувати високий рівень теоретичного та практичного навчання. Проведений аналіз дозволяє стверджувати, що США приділяють велику увагу посиленню національної безпеки, захисту цивільних прав та інтересів бізнесу тому, що науковий, технічний, військовий, фінансовий потенціал та потенціал високих технологій США є національним надбанням американського народу, що потребує захисту на державному рівні. Концентрація найбільших фінансових компаній, науково-дослідницьких установ та корпорацій, які суттєво впливають на фінансову стабільність і економічний розвиток країни, на створення та розвиток важливих технологічних процесів підсилюють значимість управління кібербезпекою в США [2].

Показовим є те, що до сукупності кращих світових навчальних закладів у галузі кібербезпеки належать, саме американські вищі навчальні заклади, такі як (табл.1) : Каліфорнійський державний університет Сан-Бернардіно, штат Каліфорнія, (США) [18]; Університет Карнегі-Меллона, Піттсбург, штат Пенсильванія (США) [19]; Університет Джорджа Вашингтона, округ Колумбія (США) [23]; Університет Індіани Блумінгтон, штат

Індіана, (США) [20]; Канзаський державний університет Манхеттен, штат Канзас (США) [21]; Університет штату Пенсильванія, штат Пенсильванія (США) [22]; Глобальний кампус Університету Меріленда, Адельфі, штат Меріленд (США) [26]; Техаський університет в Сан-Антоніо, штат Техас (США) [24].

Таблиця 1.
Навчальні заклади США, що здійснюють підготовку фахівців у сфері кібербезпеки*

№ з/п	Назва навчального закладу	Перелік програм з кібербезпеки
1.	Каліфорнійський державний університет Сан-Бернардіно, *(California State University SANBERNARDINO)*	Функціонує Центр кібербезпеки (CSUSB), де пропонують кращі програми у сфері кібербезпеки (MBA – Фокус кібербезпеки; публічне управління та кібербезпека; національні дослідження у сфері кібербезпеки; інформаційні системи і технології BS та кібербезпека; криміналістика – кіберзлочинність та кібербезпека тощо).
2.	Університет Карнегі-Меллона *(Carnegie Mellon University)*	Функціонує Інститут безпеки та конфіденційності, що пропонує магістерські програми з кібербезпеки (інформаційні технології та проєктування конфіденційності; інформаційна безпека і управління; забезпечення інформаційної безпеки тощо).
3.	Університет Джорджа Вашингтона *(The George Washington University)*	Функціонує Інститут досліджень в галузі кібербезпеки і конфеденційності у структурі Школи інженерних та прикладних наук, фахівці якого залучені до розробки кращих у світі програм з кібербезпеки (кібербезпека у сфері комп'ютерних наук; стратегування кібербезпеки і управління інформацією; політика кібербезпеки і відповідності; національна безпека і право США; професійні дослідження у галузі кібербезпеки тощо).
4.	Університет Індіани, Блумінгтон *(Indiana University BLOOMINGTON)*	Функціонує Центр прикладних досліджень у сфері кібербезпеки (CACR), де пропонують магістерські програми з кібербезпеки (світовий виконавчий майстер ділового адміністрування з концентрацією у кібербезпеці; кібербезпека у сфері комп'ютерних наук; стратегування кібербезпеки і управління інформацією; політика кібербезпеки і відповідності; національна безпека і право США; професійні дослідження у галузі кібербезпеки тощо).
5.	Канзаський державний університет *(Kansas State University)*	Функціонує Центр інформації та системного забезпечення (CISA) разом з Національним центром академічних досягнень у дослідженнях в області кібербезпеки, що пропонують одну з кращих програм кібербезпеки у світі (інформатика Cyber Security BS; магістр програмної інженерії; бакалавр у галузі комп'ютерних наук).
6.	Університет штату Пенсильванія *(Penn State College of Information Sciences and Technology)*	Представлено широкий спектр якісних програм для студентів і аспірантів з кібербезпеки (магістр професійних досліджень в галузі інформаційних наук – кібербезпека і забезпечення інформації; бакалавр з безпеки і аналізу ризиків – опція інформаційної безпеки та кібербезпеки; магістр професійних досліджень в галузі національної безпеки – спеціалізація інформаційна безпека і криміналістика тощо).
7.	Глобальний кампус Університету Меріленда *(University of Maryl and Global Campus Formerly UMUC)*	Має репутацію як однієї з найкращих шкіл кібербезпеки у світі, пропонує програми для студентів і аспірантів (управління та політика кібербезпеки (магістерська програма та програма бакалаврату); комп'ютерні мережі та кібербезпека (програма бакалаврату); розробка програмного забезпечення та безпеки (програма бакалаврату); цифрова криміналістика і кібер-розслідування (магістерська програма); інформаційні технології за спеціальністю інформаційне забезпечення (магістерська програма тощо).
8.	Техаський університет в Сан-Антоніо *(The University of Texas at San Antonio (UTSA))*	Функціонують такі дослідницькі центри, як: Центр забезпечення і безпеки інфраструктури, Інститут кібербезпеки і Кібер-центр безпеки і аналітики які забезпечують реалізацію навчальних програм (ділове адміністрування у галузі інформаційних систем; інформаційні технології та кібербезпека тощо).

**Джерело: [18,19,20,21,22,23,24,25].*

Інша дослідниця О.В. Матвійчук-Юдіна використовує досвід американських науковців у дослідженні особливостей основного підходу до формування професійних або фахових компетентностей з навчальної дисципліни "Комп'ютерна графіка" для бакалаврів спеціальності "Кібербезпека" за індустріальною моделлю США, а також з врахуванням тенденції в українському суспільстві – появи різних сфер з використання та надання послуг з комп'ютерної графіки. Вибудовуючи свою теоретичну позицію, О. В. Матвійчук-Юдіна здійснила порівняльний аналіз компетентностей згідно світової системи стандартизації ISO 9001:2015 та освітньо-професійного стандарту – Індустріальної Моделі Кібербезпеки США, оскільки вказаний стандарт має свій перелік компетентностей для фахівців сектору індустрії кібербезпеки [12, с. 95]. Вітчизняна система освіти, на думку дослідниці, надає рекомендації щодо словосполучень: "здатність виконувати", "забезпечувати" тощо. Світова система та її форма перекладу українською мовою встановлює такі приклади визначення

компетентностей, як: “можливість або вміння продемонструвати”, “розуміти теорію та термінологію”, “розуміти та ефективно використовувати”, “бути здатним” тощо. Тому авторка пропонує свою форму перекладу та тлумачення компетентностей [12, с. 94].

Дослідниця Ю. Савчук здійснила пошук шляхів удосконалення професійної підготовки фахівців із кібербезпеці та захисту інформації через призму чинного законадавства Заслуговує на увагу узагальнення вітчизняної дослідниці щодо доцільності виокремлення різних спеціалізацій профілю “Кібербезпека”, удосконалення освітніх програм та стандартів щодо підготовки фахівців з досліджуваного профілю, формування нової парадигми професійної підготовки, здійснення підбору найбільш доцільних технологій та методів навчання фахівців з кібербезпеки та захисту інформації а також формування метасередовища їх освітньої діяльності. Слушною є точка зору Ю. Савчук організацію системи підготовки фахівців із кібербезпеки у військовій, банківській, енергетичній, правовій, економічній, сільськогосподарській, освітній сфері, бізнесі, логістиці, промисловості, енергетиці, журналістиці, аудиті [15].

Зазначимо, що підготовка фахівців з управління інформаційною та кібернетичною безпекою має базуватися на урахуванні різних категорій кібербезпеки, зокрема, як:

- мережева кібербезпека (захист комп’ютерів від зловмисників, шкідливих програм;
- безпека додатків (захист програмного забезпечення і пристроїв від кіберзагроз;
- інформаційна безпека (захист цілісності і конфеденційності данних під час їх зберігання чи передачі);
- аварійна безпека і безперервність бізнесу (реагування на аварійні ситуації в області кібербезпеки, які призводять до втрати операцій або даних);
- операційна безпека (забезпечення обробки і захист даних).

Велика увага дослідженню основних аспектів формування системи підготовки фахівців у сфері кібербезпеки органів публічної влади в умовах глобалізації приділяється Л. Арсеновичем, який зазначає, що між вимогами ринку праці та практичними результатами освітньої діяльності вищих навчальних закладів утворився відчутний розрив, що призводить до численних нарікань з боку споживачів освітніх послуг і роботодавців, зокрема на відсутність умінь та навичок практичної роботи за обраним напрямом або спеціальністю, знань сучасних технологій і, як наслідок, зростання часу адаптації випускників на первинних посадах, ускладнення працевлаштування й зниження престижу вищої освіти загалом. Загалом викликає занепокоєння складових сектору безпеки і оборони України питання щодо підготовки фахівців у сфері кібербезпеки галузі знань “Інформаційні технології”. Вказане лише підтверджує тезу про те, що ситуація з організацією практичної підготовки фахівців з кібербезпеки для органів публічної влади у вищих закладах освіти вимагає суттєвого удосконалення [1].

Зазначимо, що сьогодні на порядку денному країн Європейського Союзу теж значної актуальності набуває питання щодо наявності “кваліфікованої робочої сили європейського співтовариства”. Так у Стратегії кібербезпеки Європейського Союзу на цифрове десятиліття, оприлюдненої для світової спільноти шляхом спільного повідомлення Європейського Парламенту та ради зазначено, що зусилля країн Європейського Союзу щодо підвищення кваліфікації робочої сили, розвитку, залучення, збереження найкращих талантів у галузі кібербезпеки та інвестування у дослідження й інновації світового класу становлять важливий компонент загального захисту від кіберзагроз. Це галузь із величезним потенціалом. Отже, особлива увага повинна бути приділена розвитку, залученню та збереженню різноманітних талантів у вказаній сфері. Переглянутий План дій щодо цифрової освіти підвищить рівень обізнаності щодо кібербезпеки серед людей, особливо дітей та молоді та організацій. Це також сприятиме участі жінок у таких сферах як наука, технології, техніка та математика (STEM) та підвищенню кваліфікації та перекваліфікації робочих місць в ІКТ у галузі цифрових навичок. Крім того, Комісія спільно з Управлінням інтелектуальної власності Європейського Союзу (ENISA), державами-членами та приватним сектором розроблятиме інструменти підвищення обізнаності та настанови для підвищення стійкості підприємств ЄС проти крадіжок інтелектуальної власності, що здійснюються за допомогою кіберінструментів. Освіта, зокрема професійна освіта та професійно-технічна підготовка, обізнаність та навчання, також повинна підвищувати кібербезпеку та навички кіберзахисту в європейських країнах. Із цією метою відповідні актори ЄС, такі як ENISA, Європейське оборонне агентство (EDA), Європейський коледж безпеки та оборони (ESDC) повинні віднайти різноманітні способи досягнення синергії у власній діяльності у напрямі співпраці [16].

Не підлягає сумніву управлінська аксіома, що компетентності (навички, знання та здатність) забезпечують ефективність надання всього комплексу послуг в державі, у т.ч. і електронних (цифрових). У вказаному аспекті потрібною компетентністю є орієнтація на обслуговування громадянина як клієнта, тобто як здатність скоригувати власну діяльність для забезпечення відповідного розуміння та задоволення його потреб, а також здатність пропонувати відповідні довгострокові рішення із доданою цінністю [6, с. 39]. Беззаперечно, що професійна компетентність має певну структуру, що включає компоненти, пов’язані із здатністю особистості (фахівця) вирішувати необхідні проблеми в певній сфері професійної діяльності.

У даному контексті вважаємо за доцільне згадати зміст Національного стандарту України ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT, п. 7.2. де мова йде про компетентність організації (що варто враховувати і тоді коли ми орієнтуємося на функціонування органів публічної влади). Зокрема, організація повинна а) визначити необхідну компетентність особи (осіб), яка(-і) під її контролем виконує(-ють) роботу, що впливає на дієвість і результативність системи управління якістю; б) забезпечувати впевненість у тому, що компетентність цих осіб ґрунтується на належних освіті, професійній підготовленості чи досвіді; в) там, де застосовано, вживати заходів для набуття необхідної компетентності та оцінювати результативність ужитих заходів; г) зберігати належну задокументовану інформацію як доказ компетентності [13].

Відповідно до практичних навичок, які мають бути притаманні державним службовцям вцілому і особливо у сфері кібербезпеки (за основу взято класифікацію National Standards for Civics; The National Assessment for Educational Progress (NAEP) in Civics: The National Council of Social Studies standards for Civics), варто віднести: здатність критично мислити; приймати інформовані, відповідальні рішення; аналізувати інформацію; оцінювати інформацію; обговорювати проблеми та розглядати різні погляди; визнавати роль упередженості, точки зору та контексту, а також оцінювати цінність джерела; вивчати актуальні проблеми та події; формулювати питання на основі інформації; використовувати ефективні стратегії для пошуку інформації; узагальнювати інформацію в усній, письмовій та графічній формах; співпрацювати з іншими для досягнення спільної мети; забезпечувати лідерство; вирішувати проблеми; вести ефективний та раціональний диспут [18].

Сьогодні вже зрозуміло, що для визначення, діагностики та дослідження проблем, які стосуються як діяльності органів публічних влади, так і осіб, що їх очолюють у сфері кібербезпеки, здатності передбачати проблеми, які стосуються життєдіяльності та безпеки держави, необхідні відповідна кваліфікація та вміння. Щодо останніх, то особливо необхідними є вміння: думати, аналізувати інформацію, приймати відповідні рішення та діяти, тобто реалізовувати рішення, які відповідають потребам та вимогам громадян. Так, канадський дослідник П. Браун визначає перелік вимог до професійних якостей політика, але, на нашу думку, їх типологізацію варто застосувати і до вимог якостей фахівця з кібербезпеки. Зазначені вимоги, а саме: щодо знань, організаційних вмінь, технічних навичок, інтелектуальних здібностей та особистих якостей розроблені для використання в системі управління людськими ресурсами (відбір, навчання, просування по службі тощо) [4]. Залежно від специфіки діяльності органу публічної влади вказані автором вимоги здатні видозмінюватися та трансформуватися, а знання та вміння залежать, передусім від рівня, специфіки і типу управлінської діяльності.

Таким чином, повертаючись до формування фундаментальних компетенцій (які мають базуватися на відповідних академічних компетенціях, знаннях технологій та навичках користувача) фахівця кібербезпеки в органах публічної влади варто вважати наступні:

- демонстрація вільного використання принципів функціонування інформаційних технологій та кібербезпеки;
- реалізація практичних навиків користувачів комп'ютерною технікою і програмного забезпечення;
- репродукування і маніпулювання інформаційним текстом та зображеннями, володіння практикою візуалізації;
- демонстрація здатності конструювати знання нелінійною навігацією через області академічного знання (наприклад: аналіз контексту або графіки через Інтернет чи через інші медіа (комунікаційні) середовища;
- демонстрація здатності критично оцінити текстові або графічні характеристики цифрових ЗМІ, їх соціальні контексти і тенденції, спрямованість, а також економічне й культурне значення;
- демонстрація вільного використання методів візуалізації або графічного подання загальних даних;
- вміння оцінити якість, доречність, повноцінність, ефективність, і адекватність інформації і безпосередньо джерела інформації для певної мети або політики організації (у тому числі повноваження і своєчасність інформації);
- демонстрація здатності аналізувати (порівняння, контраст, підсумок), інтерпретувати і висвітлювати інформацію від багатьох джерел, яка зібрана з використанням інструментів якісного менеджменту з умов подальшого розвитку організації:
- вміння забезпечувати захист інформаційних ресурсів і баз даних;
- вміння забезпечувати висвітлення інформаційних потоків даних тощо.

Висновки та перспективи подальших досліджень. Отже, підготовка висококваліфікованих кадрів з кібербезпеки для органів публічної влади залишається ключовим елементом повноцінної життєдіяльності держави. Цей процес обумовлений необхідністю у покращенні кібербезпеки, яка є надзвичайно важливою для забезпечення довіри людей до інновацій, взаємозв'язку та автоматизації, отримання переваг від них, а також для захисту основних прав і свобод, зокрема права на приватність та захист персональних даних, а також свободу вираження поглядів та інформації. Кібербезпека є: необхідністю для мережевого зв'язку та глобального і відкритого Інтернету, який повинен бути основою трансформації економіки та суспільства у 2020-х рр; виступає важливим інструментом для міжнародної безпеки та стабільності і розвитку економік, демократій та суспільств у всьому світі. Відповідно, органи публічної влади, бізнес-структури, інституції громадянського суспільства та громадяни в цілому повинні використовувати цифрові інструменти відповідально, вживаючи усіх необхідних заходів безпеки. Кібербезпека та цифрова гігієна повинні бути основою цифрової трансформації повсякденної діяльності не тільки державних службовців, але й кожного громадянина зокрема. Вказане лише актуалізує нагальну потребу у формуванні системи підготовки професійних, кваліфікованих, компетентних фахівців у сфері інформаційної та кібернетичної безпеки, які розуміються на різноманітті правових, управлінських, економічних аспектах захисту інформації, володіють як загально-академічними, так і специфічними знаннями, а також, відповідними практичними навичками.

Резюмуючи вищевикладене, зауважимо, що сучасні уявлення про ефективний розвиток системи підготовки фахівців у сфері кібербезпеки, успішно апробованого не тільки в США, але і у багатьох європейських країнах світу, виступають у даному дослідженні тією концептуальною базою, яка має надавати поштовх до розробки інноваційних механізмів функціонування цілісної системи підготовки фахівців у сфері кібербезпеки в Україні. Вказане визначає перспективи наших подальших наукових досліджень.

Список використаних джерел.

1. Арсенович, Л. (2018), "Формування системи підготовки фахівців у сфері кібербезпеки органів публічної влади в умовах глобалізації", *Публічне управління в умовах глобалізації* [Public administration in the context of globalization], Міжнародна студентська наукова конференція [International student scientific conference], ВАПН-NSG Київ, Україна, 07.12.2018 р, available at:https://internconferences.io.ua/s2640916/arsenovich_leonid.07.12.2018r._za_red._v.bebika.k._vapn-nsg (Accessed 30 Jan 2021).

2. Бистрова, Б. (2017), "Основні поняття досягнення та концептуальні засади професійної підготовки фахівців із кібербеспеки", *Педагогічні науки: теорія, історія, інноваційні технології,* vol. 8. pp. 58–70.

3. Браун, П. (2000) "Портрет ідеального аналітика", available at: http: //learnet.ge.ca/eng/lrncentr/competencise (Accessed 28 Jan 2021).

4. Діордіца, І. В. (2017), "Напрями державної політики кібербезпеки", *Прикарпатський юридичний вісник*, vol. 3. pp. 116–122.

5. Діордіца, І. В. (2017), "Система забезпечення кібербезпеки : сутність та призначення", *Підприємництво, господарство і право*, vol. 7. pp. 109–116.

6. Євсюкова, О. В. (2018), "Професійна відповідальність як показник сервісної діяльності органів публічної влади". *Публічне врядування в Україні: стан, виклики та перспективи розвитку* [Public governance in Ukraine: state, challenges and prospects of development], Всеукр. наук-практич. конф. за міжн.участю [All-Ukrainian scientific-practical conference with international participation], КиЇв, Україна, НАДУ, 25 травня 2018 р, pp. 38 – 40.

7. Запорожець, Т. В. (2019), "Інтелектуальні технології та системи штучного інтелекту для підтримки прийняття управлінських рішень", *Інституціоналізація публічного управління в умовах євроінтеграційних та глобалізаційних викликів* [Institutionalization of public administration in Ukraine in the context of European integration and globalization challenges], Всеукр. наук-практич. конф. за міжн.участю [All-Ukrainian scientific-practical conference with international participation], КиЇв, Україна, НАДУ, 24 травня 2019 р, pp. 52– 54.

8. Карпенко, О. В. (2018), "Цифрові трансформації комунікативного управління: глобальні здобутки, тенденції розвитку та актуальні загрози". *Інституціоналізація публічного управління в Україні в умовах євроінтеграційних та глобалізаційних викликів* [Institutionalization of public administration in Ukraine in the context of European integration and globalization challenges], Всеукр. наук-практич. конф. за міжн.участю [All-Ukrainian scientific-practical conference with international participation], КиЇв, Україна, НАДУ, 24 травня 2019 р, pp. 38 – 40.

9. Конотопцев, О. (2014) "Використання інформаційно-комунікаційних технологій в процесі надання адміністративних послуг", available at: http://fmd.kh.ua/news/vikoristannya-informatsijnokomunikatsijnih-tehnologij-v-protsesi-nadannya-administrativnih-poslug.html (Accessed 28 Jan 2021).

10. Криворучко, О.В., Костюк, І.В., (2020) "Стратегія безпеки інформації" *Кібергігієна. Кібербезпека. Безпека держави*, available at: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf (Accessed 28 Jan 2021).

11. Лутчин, Т. М. (2018) "Професіоналізм державних службовців як умова ефективної діяльності органів державної влади", available at: http://kds.org.ua/blog/lutchin-tm-tvorcha-robota-profesionalizm-derzhavnih-sluzhbovtsiv-yak-umova-efektivnoi-diyalnost, (Accessed 30 Jan 2021).

12. Матвійчук-Юдіна, О. В. (2017), "Ключові компетентності фахівців спеціальності "Кібербезпека" з предмету "Комп'ютерна графіка" згідно індустріальної моделі промисловості"", *Вісник Житомирського державного університету імені Івана Франка,* vol. 4 (90). pp. 93–98.

13. Національний стандарт України ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT) Система управління якістю, available at: khoda.gov.ua/image/catalog/files/%209001.pdf (Accessed 30 Jan 2021).

14. Рудник, Л. І. (2015), "Право на доступ до інформації", Науковий ступінь кандидата юридичних наук, адміністративне право і процес, Національний університет біоресурсів і природокористування України, Київ, Україна.

15. Савчук, Ю. Є. (2017), "Формування соціально-професійної мобільності майбутніх викладачів інформатики в процесі магістерської підготовки", Науковий ступінь кандидата педагогічних наук, теорія та методика професійної освіти, Луцький національний технічний університет, Луцьк, Україна.

16. Стратегія кібербезпеки ЄС на цифрове десятиліття (2020), available at: http://bit.ly/3ag55OJ м (Accessed 28 Jan 2021).

17. National Strategy to Cyberspace Secure – US-CERT, available at: https://www.us-cert.gov/sites/.cyberspace_strategy (Accessed 28 Jan 2021).

18. The official site of California State University, San Bernardino (2021), available at: http://www.csusb.edu (Accessed 30 Jan 2021).

19. The official site of Carnegie Mellon University (2021), available at: https://www.cmu.edu/ (Accessed 30 Jan 2021).

20. The official site of Indiana University BLOOMINGTON (2021), available at: https://www.indiana.edu/ (Accessed 30 Jan 2021).

21. The official site of Kansas State University (2021), available at: https://www.k-state.edu/ (Accessed 30 Jan 2021).

22. The official site of Penn State College of Information Sciences and Technology (2021), available at: https://ist.psu.edu/ (Accessed 30 Jan 2021).

23. The official site of The George Washington University (2021), available at: https://www.gwu.edu/ (Accessed 30 Jan 2021).

24. The official site of The University of Texas at San Antonio (UTSA) (2021), available at: https://www.utsa.edu/ (Accessed 30 Jan 2021).

25. The official site of United Nations Educational, Scientific and Cultural Organization (2021), available at: https://en.unesco.org/ (Accessed 30 Jan 2021).

26. The official site of University of Maryl and Global Campus Formerly UMUC (2021), available at: https://www.umgc.edu/index.cfm (Accessed 30 Jan 2021).

References.

1. Arsenovych L. (2018), "Formation of a system of training specialists in the field of cybersecurity of public authorities in the context of globalization", *Publichne upravlinnia v umovakh hlobalizatsii. Mizhnarodna studentska naukova konferentsiia* [Public administration in the context of globalization. International student scientific conference], VAPN-NSG, Kyiv, Ukraine, available at: https://internconferences.io.ua/s2640916/arsenovich_leonid.__07.12.2018r._za_red._v.bebika.k._vapn-nsg (Accessed 30 Jun 2021).

2. Bystrova, B. (2017), "Basic concepts of achievement and conceptual principles of professional training of cybersecurity specialists", *Pedahohichni nauky: teoriia, istoriia, innovatsiini tekhnolohii* , vol. 8. pp. 58–70.

3. Braun, P. (2000), "Portrait of a perfect analyst", available at: http: //learnet.ge.ca/eng/lrncentr/competencise (Accessed 28 Jun 2021).

4. Diorditsa, I. V. (2017), "Directions of state cybersecurity policy", *Prykarpatskyi yurydychnyi visnyk*, vol. 3. pp. 116–122.

5 Diorditsa, I. V. (2017), "Cybersecurity system: essence and purpose", *Pidpryiemnytstvo, hospodarstvo i pravo*, vol. 7. pp. 109–116.

6. Ievsiukova, O. V. (2018), "Professional responsibility as an indicator of service activity of public authorities". *Publichne vriaduvannia v Ukraini: stan, vyklyky ta perspektyvy rozvytku. Vseukr. nauk-praktych. konf. za mizhn.uchastiu* [Public governance in Ukraine: state, challenges and prospects of development. All-Ukrainian scientific-practical conference with international participation], NADU, KyIv, Ukraine, pp. 38 – 40.

7. Zaporozhets, T. V. (2019), "Intelligent technologies and artificial intelligence systems to support management decisions", *Instytutsionalizatsiia publichnoho upravlinnia v umovakh yevrointehratsiinykh ta hlobalizatsiinykh vyklykiv. Vseukr. nauk-praktych. konf. za mizhn.uchastiu* [Institutionalization of public administration in Ukraine in the context of European integration and globalization challenges. All-Ukrainian scientific-practical conference with international participation], KyIv, Ukraine, NADU, pp. 52– 54.

8. Karpenko, O. V. (2018), "Digital transformations of communicative management: global achievements, development trends and current threats", *Instytutsionalizatsiia publichnoho upravlinnia v umovakh yevrointehratsiinykh ta hlobalizatsiinykh vyklykiv. Vseukr. nauk-praktych. konf. za mizhn.uchastiu* [Institutionalization of public administration in Ukraine in the context of European integration and globalization challenges. All-Ukrainian scientific-practical conference with international participation], KyIv, Ukraine, NADU, pp. 38 – 40.

9. Konotoptsev, O. (2014), "Use of information and communication technologies in the process of providing administrative services", available at: http://fmd.kh.ua/news/vikoristannyainformatsijnokomunikatsijnihtehnologijvprotsesinadannyaadministrativnihposlug.html (Accessed 28 Jan 2021).

10. Kryvoruchko, O. V. and Kostiuk, I. V., (2020), "Information security strategy", *Kiberhihiiena. Kiberbezpeka. Bezpeka derzhavy,* available at: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf (Accessed 28 Jan 2021).

11. Lutchyn, T. M., (2018), "Professionalism of civil servants as a condition for effective activity of public authorities", available at: http://kds.org.ua/blog/lutchin-tm-tvorcha-robota-profesionalizm-derzhavnih-sluzhbovtsiv-yak-umova-efektivnoi-diyalnost (Accessed 30 Jan 2021).

12. Matviichuk-Yudina, O.V. (2017), "Key competencies of Cybersecurity specialists in Computer Graphics", *Visnyk Zhytomyrskoho derzhavnoho universytetu imeni Ivana Franka,* vol. 4 (90), pp. 93–98.

13. Ukrainian Research and Training Center of Standardization, Certification and Quality (2016), "National standard of Ukraine DSTU ISO 9001: 2015 (ISO 9001: 2015, IDT) Quality management system", available at: khoda.gov.ua/image/catalog/files/%209001.pdf (Accessed 30 Jan 2021).

14. Rudnyk, L. I. (2015), "The Concept of Information Human Rights", Abstract of Ph.D. dissertation, Administrative law and process, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine.

15. Savchuk, Y. Y. (2017), "Formation of social and professional mobility of future computer science teachers in the process of master's training", Abstract of Ph.D. dissertation, Theory and Methods of Vocational Education, Lutsk National Technical University, Lutsk, Ukraine.

16. EU (2020), "EU Cyber Security Strategy for the Digital Decade", available at: http://bit.ly/3ag55OJm (Accessed 28 Jan 2021).

17. US-CERT (2020), "National Strategy to Cyberspace Secure", available at: https://www.us-cert.gov/sites/.../cyberspace_strategy (Accessed 28 Jan 2021).

18. The official site of California State University, San Bernardino (2021), available at: http://www.csusb.edu (Accessed 30 Jan 2021).
19. The official site of Carnegie Mellon University (2021), available at: https://www.cmu.edu/ (Accessed 30 Jan 2021).
20. The official site of Indiana University BLOOMINGTON (2021), available at: https://www.indiana.edu/ (Accessed 30 Jan 2021).
21. The official site of Kansas State University (2021), available at: https://www.k-state.edu/ (Accessed 30 Jan 2021).
22. The official site of Penn State College of Information Sciences and Technology (2021), available at: https://ist.psu.edu/ (Accessed 30 Jan 2021).
23. The official site of The George Washington University (2021), available at: https://www.gwu.edu/ (Accessed 30 Jan 2021).
24. The official site of The University of Texas at San Antonio (UTSA) (2021), available at: https://www.utsa.edu/ (Accessed 30 Jan 2021).
25. The official site of United Nations Educational, Scientific and Cultural Organization (2021), available at: https://en.unesco.org/ (Accessed 30 Jan 2021).
26. The official site of University of Maryl and Global Campus Formerly UMUC (2021), available at: https://www.umgc.edu/index.cfm (Accessed 30 Jan 2021).

Стаття надійшла до редакції 01.02.2021 р.