CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI: 10.20535/2411-1031.2018.6.2.153495
УДК 004.056::378.016

ЮРІЙ ДАНИК
ОЛЕКСАНДР КОРНЕЙКО

ОСНОВИ МЕТОДОЛОГІЇ ФОРМУВАННЯ КІБЕРКОМПЕТЕНЦІЙ У ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Проведено аналіз наявних в провідних країнах світу (США, Великобританія, Канада, Федеративна Республіка Німеччина, Республіка Польща) систем підготовки військових фахівців з кібербезпеки для сфер національної безпеки та оборони, а також рівня освіченості населення з питань кібербезпеки. Наведені дані щодо основних військових закладів освіти цих країн, де успішно готуються військові фахівці з кібербезпеки, а також навчальних програм, що пропонуються Департаментом внутрішньої безпеки США (Department of Homeland Security) для проведення навчання дітей в системі дошкільної та шкільної освіти, їх батьків, вчителів тощо. Приведені дані щодо системи та програм підготовки бакалаврів з кібербезпеки в закладах освіти США. Проаналізовані передумови, етапи становлення та існуючий стан системи підготовки в Україні фахівців у сфері кібербезпеки. Встановлено, що формування компетенцій з основ кібербезпеки, у тих хто навчається у закладах вищої освіти сектору безпеки і оборони України, не достатньо враховано у стандартах освіти випускників. Здійснено аналіз основних понять в професійно-компетентнісному підході підготовки фахівців з кібербезпеки. Запропоновані основні положення методології розбудови цілісної системи підвищення кіберосвіченості населення та підготовки фахівців з питань кібербезпеки для сектору безпеки і оборони України. Доведено, що освіченість населення з питань кібербезпеки в Україні необхідно починати ще з дошкільного навчання та запровадити сталу систему шкільної кіберосвіти, що надасть можливість більш якісно підготувати дитину до дорослого життя в сучасному високотехнологічному суспільстві. Уточнені вимоги до навчання з питань кібербезпеки в закладах вищої освіти. Відповідно до кращого зарубіжного досвіду запропоновано основні зусилля в підготовці фахівців із кібербезпеки для сектору безпеки і оборони зосередити на інтеграції наукового, науково-педагогічного та матеріально-технічного потенціалів на єдиній базі, шляхом формування військового закладу вищої освіти (закладу вищої освіти із специфічними умовами навчання) нового типу у вигляді інтегрованого навчально-наукового та дослідно-випробувального комплексу.

Ключові слова: сектор безпеки і оборони, кібербезпека, кіберосвіта, кіберкомпетентність, заклад вищої освіти, військовий заклад вищої освіти.

Вступ і постановка задачі на дослідження. На протязі останніх десятиліть стрімкий розвиток та масове впровадження сучасних інформаційних технологій призвело до формування нового спектру ризиків і загроз у сферах національної безпеки і оборони держави, які реалізуються в кіберпросторі та (або) через кіберпростір [1]. Кіберзагрози охоплюють всі базові сфери суспільної діяльності (політичну, воєнну, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну, технологічну тощо), загрозливо впливаючи на всі складові сектору безпеки і оборони України (надалі – СБОУ) [2].

Відповідно до чинного законодавства до складу СБОУ входять органи державної влади, військові формування, правоохоронні та розвідувальні органи, державні органи спеціального призначення, Апарат Ради національної безпеки і оборони України (надалі – РНБОУ) тощо, що беруть участь у формуванні та реалізації завдань із забезпечення

національної безпеки і оборони України. Закон [2] також визначає, що до складу СБОУ відносяться громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки України.

Отже, хоча переважна більшість майбутніх фахівців з кібербезпеки для СБОУ після закінчення навчання у закладах вищої освіти (надалі – ЗВО) буде проходити подальшу службу в якості військовослужбовців і осіб, які мають спеціальні звання, але деяка частка таких фахівців буде працювати в якості державних службовців та цивільних фахівців в підрозділах державних органів, підприємств оборонно-промислового комплексу, в організаціях та установах державного та приватного сектору, що опікуються питаннями кібербезпеки й інформатизації та будуть брати участь в забезпеченні безпеки кіберпростору України та її кібероборони. Крім того, безпека національного кіберпростору багато в чому залежить від загального рівня кіберосвіти населення – тобто його обізнаності в сфері безпечного користування Інтернетом та інформаційними технологіями.

Тому питання підготовки сучасних фахівців з кібербезпеки для органів та формувань, що входять до складу СБОУ, а також забезпечення загальної кіберосвіти широких верств населення, є одним із найбільш пріоритетних завдань, що визначені нормативно-правовими актами у сфері забезпечення кібербезпеки, як однієї із важливих складових сфер національної безпеки і оборони України [3] - [7].

При цьому на сучасному етапі розвитку освіти серед базових парадигм щодо підготовки кадрів як для всього сектору економіки, так і для СБОУ, є компетентнісна парадигма, яка спрямована на формування у майбутніх фахівців різноманітних, у тому числі й професійних компетенцій [8], [9].

Таким чином, ***мета роботи*** полягає в проведенні аналізу відомих результатів та подальшого дослідження щодо формування загальної методології впровадження професійно-компетентнісного підходу до підготовки кадрів із кібербезпеки для СБОУ та підвищення рівня загальної кіберосвіченості населення.

Досягнення поставленої мети роботи потребує проведення наступних досліджень та вирішення таких завдань: здійснення аналізу існуючих систем підготовки фахівців з кібербезпеки у провідних країнах світу в контексті впровадження їх досвіду в Україні; здійснення аналізу передумов та існуючого стану системи підготовки фахівців з питань кібербезпеки в Україні, а також наявного рівня кіберосвіченості населення; здійснення аналізу щодо основних понять в професійно-компетентнісному підході підготовки фахівців з кібербезпеки; здійснення розробки основних положень методології професійно-компетентнісної підготовки фахівців з питань кібербезпеки для СБОУ.

Виклад основного матеріалу дослідження. Як було зазначено вище, важливим аспектом формування системи освіти фахівців з питань кібербезпеки для СБОУ та загальної кіберосвідченості населення є вивчення та дослідження досвіду провідних країн світу, насамперед, США.

Питанням забезпечення кіберосвідченості всіх верств населення в США приділяють першочергової уваги на всіх рівнях системи освіти.

Для забезпечення узгодженого функціонування цієї системи для безумовного досягнення визначених цілей, у складі Департаменту внутрішньої безпеки США (Department of Homeland Security – DHS) 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, розумінню кіберзагроз та 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 існуючих та

виникаючих проблем у всіх складових кібербезпеки; Національна програма освіти та тренінгу в сфері кібербезпеки (National Cybersecurity Education and Training Program – NCTEP), 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 існуючих та майбутніх кіберзагроз [10].

У своєму виступі 8 червня 2017 року представник DHS Ноэль Кайл зазначив: "Щоб ліквідувати розрив між зростаючою потребою у фахівцях з кібербезпеки та системою підготовки кваліфікованого персоналу, вкрай важливо, щоб всі спільноти – галузеві організації, федеральні агентства і академічні заклади, – з'єднались та сформували комплексний підхід до координації зусиль у галузі освіти, навчання та працевлаштування фахівців з кібербезпеки" [11].

Реалізуючи це, в американських ЗВО здобуття освітнього рівня "бакалавр" зі спеціальності "Кібербезпека" можливе за такими моделями навчання: модель 4-річного безперервного навчання, як правило, в одному ЗВО (вищий коледж / університет / професійна школа); модель "2+2", яка можлива в різних ЗВО (молодший коледж / технічна школа + вищий коледж / університет / вища професійна школа) [12].

Всі програми підготовки бакалаврів в американських ЗВО розраховані на чотири роки навчання, після чого присуджується ступінь бакалавра комп'ютерних наук у сфері кібербезпеки. В [12] проаналізовані навчальні програми 45 ЗВО з 25 штатів США щодо підготовки фахівців у сфері кібербезпеки. Показано, що вагома кількість предметів являють собою обов'язкові курси навчання, які є спеціалізованими. Наприклад, основними обов'язковими дисциплінами є: інформаційна безпека, розслідування комп'ютерних інцидентів, управління інформаційною безпекою, міжмережеві екрани і виявлення вторгнень, безпека бездротових мереж, IT-аудит тощо. Існують й дисципліни за власним вибором студента, що значно підвищує їх захопленість та зацікавленість змістом навчання. Але студенти можуть самостійно вибрати лише невелику кількість дисциплін (3–4) за вибором, спрямованих на засвоєння додаткових знань та навичок в обраній галузі підготовки, наприклад: соціальні аспекти інформаційної безпеки, дані і інтелектуальний аналіз, безпека розподілених баз даних, безпека електронної комерції, політика інформаційної безпеки, прикладна криптографія, практичні питання безпеки, спеціальні питання інформаційної безпеки, незалежні дослідження. Виходячи з цього, очевидно, що в американській системі вищої освіти в підготовці фахівців у сфері кібербезпеки дотримуються широкого профілю їх спеціалізації [12].

У рамках програми NCTEP урядова організація DHS пропонує кілька безкоштовних курсів позавузівського навчання для підтримки освіти з питань кібербезпеки [10]. При цьому для вчителів молодших, середніх та старших класів передбачені не тільки відповідні тренінги, а й надання для використання відповідних навчальних матеріалів з кібербезпеки. Для державних службовців сформовані програми і здійснюється безкоштовне навчання та підвищення кваліфікації з кібербезпеки.

В США окрема увага приділяється питанням кіберосвіти населення ще у дошкільному і молодшому шкільному віці. Так, наприклад, у рамках програми NCTEP пропонується ряд розваг та комп'ютерних ігор для дітей, що формують їх кіберосвіченість: "Kids Com Jr."; "Cyber Spacers"; "FBI – безпечний он-лайн серфінг"; ігри серії "Net smartz Teens"; кросворди та шаради "Crypto Kids"; "PBS – Cyber Chase"; Інтернет-академія "Webonauts"; навчальний курс "AT & T – земля безпеки"; програма постійно діючої навчальної лабораторії – "Навчайтесь у професора Гарфилда: Cyber bullying" [10].

Програмою NCTEP для батьків також пропонується ряд курсів: семінар "Net Smartz" – батьки та опікуни; "On Guard Online" – тільки для батьків; "I Keep Safe" – батьки; "Будьте у безпеці в Інтернеті – навчайте он-лайн безпеці"; "Будь кращім – звертайся до дитячої он-лайн безпеки"; "Net Cetera" – спілкування з дітьми про правила поведінки в мережі; "Безпечне підключення – поради та рекомендації з безпеки"; навчальна гра "Net Safe – мир

Гектора"; "Cyber smart!"; курс відділу послуг карного правосуддя – "Безпека в Інтернеті"; курс Центру безпеки родини компанії Google; "Kids Health" – чиста безпека; "Наша любов – діти США"; курс відділу із захисту прав споживачів у Нью-Йорку – "Поради з безпеки в Інтернеті"; курс сімейного ресурсного центру Norton; "ProtectKids.com"; курс "Безпечні діти"; курс "Припиніть залякування зараз! Що можуть зробити дорослі?"; курс Міністерства юстиції США – "Безпека в Інтернеті" [10].

Все це надає змогу реалізувати комплексний підхід у побудові в США системи підготовки фахівців з кібербезпеки.

Особливого значення в зарубіжних країнах питання кіберосвіти мають для сектору їх національної безпеки і, особливо, оборони [1], [13]. Адже, ефективність застосування військ (сил) оснащених сучасними високотехнологічними засобами озброєння та військової техніки, в найбільшому ступені залежить від якості підготовки особового складу з питань сучасних інформаційних технологій, кібербезпеки і кібероборони [1]. В усіх військових ЗВО Міністерства оборони (надалі – МО) США та інших країн членів НАТО питання забезпечення інформаційної та кібернетичної безпеки вивчаються всіма тими, хто в них навчається.

Так, наприклад, питання кібербезпеки і кібероборони, в частині що стосується, вивчаються в таких видових військових закладах вищої освіти США: Військова академія Армії США у Вест-Пойнті (US Militari Academi, West Point, NY, 16.03.1802) – у коледжі електронних та комп'ютерних систем (Department of Electrical Engineering and Computer Science), центрі інформаційних технологій і операцій (Information Technology and Operations Center) у складі якого є лабораторія досліджень і аналізу інформаційної війни (The Information Warfare Analysis and Research Laboratory (IWAR)); Академія Військово-повітряних Сил в Колорадо-Спрінгс (United States Air Force Academy, Колорадо); Академія Військово-морських Сил в Анаполісі (Меріленд) [1].

Питання з кібербезпеки і кібероборони також вивчаються в інших військових закладах вищої освіти США: Технологічний університет ВПС (Air Force Institute of Technology, Wright-Patterson AFB, Ohio) – на факультеті інформаційної безпеки та Військово-космічних сил; Університет інформаційних технологій (Universiti of information Technologi, Fort Gordon, GA); Університет національної оборони (National Defense University) – на факультеті інформаційних та кібернетичних наук (College of Information and Cyberspace); коледж інформаційного менеджменту (Information Resources Management College-School of Information Warfare and Strategy at NDU, Fort McNair, Washington, D.C.); командно-штабний коледж – на факультеті інформаційно-психологічних операцій (The Joint Forces Staff College, Norfolk, VA); в видових навчально-дослідницьких центрах: Air Force Information Warfare Center (AFIWC), Neelis Air Force Base, 1.07.1953; Fleet Information Warfare Center (FIWC), Norfolk, 4.11.2005; Space Information Warfare Center (SIWC), Schriever Air Force Base, Colorado, 8.12.1993 та інші; в військових ЗВО з підготовки фахівців кібербезпеки гуманітарного профілю: Військовий інститут іноземних мов ЗС США (Defense Language Institute, Monterey); Центр і школа спеціальних методів війни імені Дж. Ф. Кеннеді (Форт-Брег); школа підготовки спеціалістів засобів масової інформації МО США [1].

Як видно з приведено вище, мережа підготовки фахівців в США досить розвинута. Але навіть при таких масштабах, на думку американських експертів, у США відчувається недостача фахівців у сфері кібербезпеки [14].

На відміну від США, зважаючи на значно меншу чисельність збройних сил, в інших країнах членах блоку НАТО (Великобританія, Федеративна Республіка Німеччина, Республіка Польща тощо) ефективність вирішення зазначених вище задач щодо підготовки військових фахівців з кібербезпеки і кібероборони досягається шляхом формування та забезпечення функціонування інтегрованих навчально-наукових, дослідно-випробувальних комплексів (дослідницьких військових технологічних університетів, високотехнологічних оборонних кластерів), які здійснюють на єдиній базі освітню і наукову діяльність за високотехнологічними напрямами.

Наприклад, така інтеграція військової освіти і науки за високотехнологічними напрямами успішно реалізована в Республіці Польщі: у Військовій академії (Akademia sztuki wojennej) на факультеті інформаційної безпеки (The Faculty of Information Security) та центрі імітаційного моделювання та військових ігор (War Games and Simulation Centre); у Військово-технічній академії імені Ярослава Домбровского (Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego) [15], [16].

Так само в ФРН у Мюнхенському університеті Бундесвера (Universität der Bundeswehr München) на факультеті застосування кібернетичних та інформаційних систем (Fakultät Einsatz, Cyber und Informationsraum) командно-штабного коледжу (Führungsakademie der Bundeswehr) зосереджені разом різні спеціальності з підготовки військових фахівців у сфері кібербезпеки, інформаційних технологій і військової інженерії [17].

Підготовка фахівців у сфері кібербезпеки в Великобританії здійснюється в Академії оборони (The Defence Academy of the United Kingdom) – у технологічній школі (Technology School) на базі центру імітаційного моделювання (Defence Simulation Centre), школи кібернетичної оборони (Defence Cyber School) [18].

Підготовка фахівців у сфері кібербезпеки і кібероборони в Канаді здійснюється у Королівському військовому коледжі (Royal Military College of Canada) – на окремому факультеті, що має у складі кафедру електронної та комп'ютерної інженерії (Department of Electrical and Computer Engineering) та кафедру математичних та комп'ютерних наук (Department of Mathematics and Computer Science), де безпосередньо вивчаються зазначені питання [19].

Таким чином, у провідних країнах світу, особливо в США, сектор безпеки і оборони має розгалужену систему підготовки фахівців у сфері кібербезпеки, а всі верстви населення мають можливість отримати відповідну кіберосвіту. У більшості європейських країн за рахунок інтеграції високотехнологічних напрямів підготовки військових фахівців та наукових досліджень в єдиному навчальному закладі та на єдиній навчально-тренувальній базі забезпечується позбавлення їх дубляжу і розпорошення зусиль при вирішенні однотипних завдань, раціональне використання та економію ресурсів і кадрового потенціалу, полігонної, матеріально-технічної бази, ефективне виконання замовлень на підготовку (перепідготовку) фахівців і здійснення наукових досліджень для усіх міністерств і відомств сектору безпеки і оборони держави в рамках єдиних стандартів освіти.

Розглянемо передумови, існуючий стан підготовки в Україні фахівців у сфері кібербезпеки та наявні тенденції його покращення.

До обрання Україною в 1991 році незалежності планова підготовка фахівців у сфері захисту інформації в інфокомунікаційних системах (тоді ще не було сталого поняття "кібербезпека") на території колишньої УРСР велась фактично виключно в вищих військових закладах освіти, де за державним замовленням та за так званими "закритими" навчальними програмами дозовано готували офіцерські кадри у цій сфері, насамперед, для Збройних Сил та КДБ [20].

У 1990-х роках закрита до того освітня сфера щодо захисту інформації в інформаційно-комунікаційних системах стає доступною для більшості закладів вищої освіти України у зв'язку з тим, що в так званому "Переліку-1994" [21] у напрямі 0924 "Телекомунікації з'явилася спеціальність "Захист інформації у телекомунікаційних системах", а у напрямі 0915 "Комп'ютерна інженерія" – спеціальність "Захист інформації в комп'ютерних системах" для кваліфікаційних рівнів молодшого спеціаліста і спеціаліста [22].

Наступний "Перелік-1997" [23] містив вже не дві спеціальності, а два напрями підготовки 1601 "Інформаційна безпека" та 1602 "Національна безпека", які розширили набір спеціальностей щодо захисту інформації для освітньо-кваліфікаційних рівнів бакалавра, спеціаліста та магістра [22]. Так, в напрямі підготовки 1601 "Інформаційна безпека" з'явилися спеціальності 160101 та 160102 "Захист інформації з обмеженим доступом та автоматизація її обробки", що відповідали технічному та гуманітарному аспектам захисту

інформації, 160103 “Системи захисту інформації від несанкціонованого доступу”, 160104 “Адміністративній менеджмент в системах захисту інформації з обмеженим доступом”, 160105 “Захист інформації в комп'ютерних системах і мережах” (рис. 1) [22, 24]. При цьому, для підготовки виключно військових фахівців для СБОУ була також введена спеціальність 092482 “Безпека інформації в спеціальних телекомунікаційних системах”, а в напрямі 1602 “Національна безпека” буда введена спеціальність 160203 “Організація захисту інформації з обмеженим доступом” для органів державної безпеки [25].

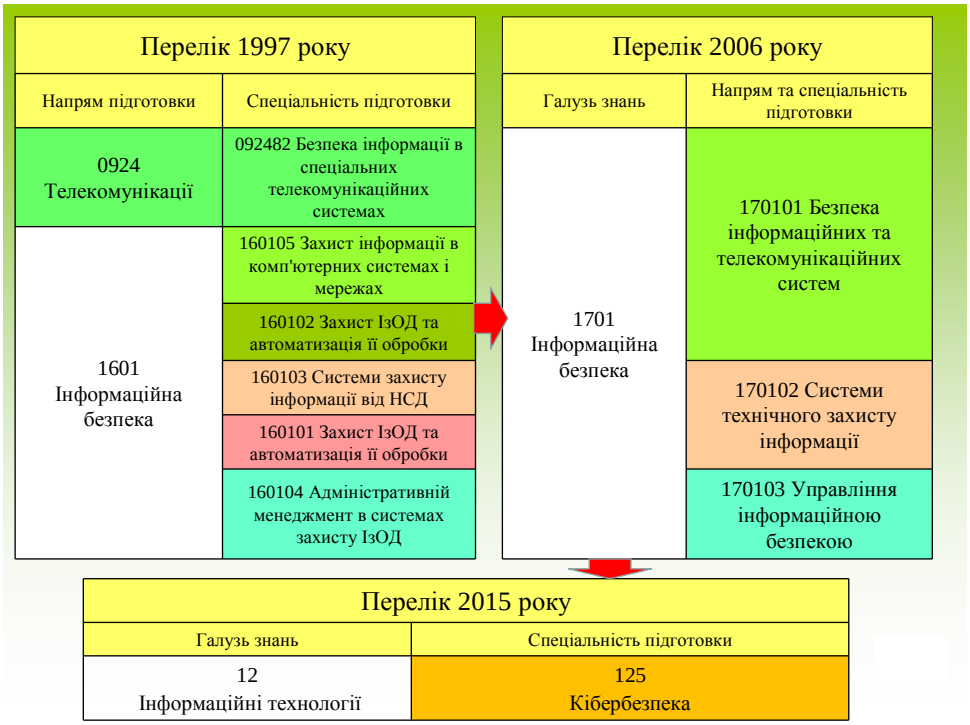

Рисунок 1 – Трансформація спеціальностей вищої освіти в сфері захисту інформації та інформаційної безпеки в сферу кібербезпеки

Прийнятий у 2006 році так званий “Перелік-2006” [26] зберіг існуючі підходи щодо підготовки фахівців із захисту інформації за двома галузями 1601 “Військові науки” і 1701 “Інформаційна безпека” [22]. При цьому галузь знань 1701 “Інформаційна безпека” містила три базових бакалаврата: 6.170101 “Безпека інформаційних і комунікаційних систем”; 6.170102 “Системи технічного захисту інформації”; 6.170103 “Управління інформаційною безпекою” (див. рис. 1), а галузь знань 1601 “Військові науки” містила відповідні спеціальності виключно щодо підготовки військових фахівців у сфері захисту інформації та забезпечення інформаційної безпеки [27].

За даними [22] підготовку фахівців з вищою освітою у галузі знань “Інформаційна безпека” на освітньому рівні “бакалавр” здійснювали на той час 28 вітчизняних ЗВО.

Пізніше, у 2010 році, відповідним нормативно-правовим актом [28] був уточнений перелік спеціальностей для фахівців освітніх рівнів “спеціаліст” і “магістр”. Цим переліком не тільки вводились відповідні спеціальності з підготовки спеціалістів та магістрів в галузі знань 1701 “Інформаційна безпека” (170101 “Безпека інформаційних і комунікаційних систем”, 170102 “Безпека державних інформаційних ресурсів”, 170103 “Системи технічного захисту інформації, автоматизація її обробки”, 170104 “Управління інформаційною безпекою”, 170105 “Адміністративний менеджмент у сфері захисту інформації”), що фактично відповідали існуючим на той час в Україні з “Переліку-1997” спеціальностям, але й в галузі знань 0403 “Системні науки та кібернетика” запроваджувала нову спеціальність 04030104 “Криптологія” щодо підготовки математиків у сфері криптографії та криптоаналізу.

Але вже на початку 2000-х років в зарубіжних країнах в нормативно-правових актах щодо захисту їх інфокомунікаційного (кібернетичного) простору та на міжнародному рівні (наприклад, в документах Європейського Союзу та організації Міжнародного Союзу Електрозв'язку ITU, що діє при ООН) все частіше став застосовуватись новий термін "кібербезпека" (англ. Cyber Security), що охоплював всі можливі аспекти захисту кіберпростору (технічний, фізико-математичний, правовий, адміністративний тощо) [1], [24], [29], [30].

У 2011 році в Україні вперше на офіційному рівні (в документі [31], затвердженому відповідною постановою Кабінету Міністрів України) також використаний термін "кібербезпека" хоча законодавчого тлумачення він тоді ще не отримав. Упродовж 2012-2015 років термін "кібербезпека@ все частіше став застосовуватись в нормативно-правових актах України [32]. У ці роки відповідно до рішень РНБОУ Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) також розпочинається підготовка проектів концептуальних документів у сфері кібербезпеки України – відповідної Стратегії [3] та профільного Закону [4].

Тому не дивно, що при формуванні Міністерством освіти і науки (далі – МОН) України в 2015 році нового "Переліку-2015" [33], який значно скорочував число галузей та спеціальностей підготовки фахівців з вищою освітою й узгоджував наявні в державі спеціальності підготовки фахівців з міжнародних досвідом, було запроваджено нову освітню спеціальність 125 "Кібербезпека" в галузі знань 12 "Інформаційні технології". На думку МОН України ця нова спеціальність повинна була інтегрувати в себе всі наявні здобутки та спеціальності щодо забезпечення захисту інформації, безпечного користування інформаційними технологіями, забезпечення інформаційної безпеки тощо.

На даний час за цією спеціальністю йде підготовка фахівців з вищою освітою в 53 вітчизняних ЗВО відповідно до затвердженого МОН України стандарту вищої освіти [34]. Крім цивільних ЗВО підготовка фахівців у сфері кібербезпеки (за спеціальністю 125 "Кібербезпека" та споріднених спеціалізацій інших спеціальностей) для державних органів і формувань СБОУ ведеться також в військових ЗВО (ЗВО зі специфічними умовами навчання), що підпорядковані або знаходяться в сфері управління МО України, Генерального штабу Збройних Сил України, Міністерства внутрішніх справ України, Адміністрації Держспецзв'язку, Служби безпеки України, Державної служби України з надзвичайних ситуацій, Державної прикордонної служби України, розвідувальних органів України тощо.

Але можна констатувати проблему відсутності єдиної методології в системі підготовки фахівців з питань кібербезпеки та загальної кіберосвіти для всіх фахівців СБОУ [1], [24], [29]. Відсутність єдиних керівних документів, методичного забезпечення навчання, розбіжність у поглядах на мету, завдання та зміст підготовки з питань кібербезпеки в військових ЗВО і ЗВО зі специфічними умовами навчання знижує ефективність та якість підготовки фахівців для СБОУ в цілому. Особливо яскраво це проявилося з початком повномасштабної "гібридної війни" проти України, в якій основне протиборство відбувається в інформаційному та кібернетичному просторах.

Крім того, ряд досліджень вітчизняних науковців, наприклад [35], [36], зазначають, що зазначена вище позиція МОН України щодо введення лише однієї спеціальності "Кібербезпека" замість цілої галузі знань "Інформаційна безпека" є неприпустимою для деяких сфер СБОУ, оскільки поняття "Кібербезпека" та "Інформаційна безпека" є спорідненими, проте не тотожними. Предметна сфера інформаційної безпеки включає в себе більш широкий спектр питань, в тому числі щодо забезпечення позитивного іміджу держави на міжнародному рівні, інформаційних прав і свобод її громадян, інформаційного суверенітету, інформаційно-психологічного протиборства, здійснення правоохоронної та контррозвідувальної діяльності з цих питань тощо. В [30] зазначається, що прикладна галузь "Кібербезпека" є інтегрованою з поняттями "Захист додатків", "Мережева безпека",

“Інтернет-безпека”, базується на понятті “Безпека критичної інформаційної інфраструктури та забезпечує поняття “Інформаційна безпека” (див. рис. 2).

Тому з метою забезпечення зазначеного вище кола питань саме у сфері інформаційної безпеки держави, що покладені законодавством на Службу безпеки України, в 2017 році в “Переліку-2015” в галузі знань 25 “Військова освіта, національна безпека, безпека державного кордону” постановою Кабінету Міністрів України [37] була введена нова спеціальність 256 “Національна безпека (за окремими сферами забезпечення і видами діяльності)”.

Хоча, як це показано вище, на даний час в Україні система підготовки в ЗВО фахівців з кібербезпеки вже достатньо складалася, але в системі дошкільної, шкільної, професійної (професійно-технічної), фахової передвищої і післядипломної освіти впровадження кіберосвіти для широких верств населення знаходиться фактично лише на початковому етапі. Лише за ініціативою деякої невеликої кількості українських та міжнародних громадських організацій (далі – ГО), що опікуються в Україні питаннями кіберосвіти (наприклад, ГО “Українська академія кібербезпеки”, Київське відділення міжнародної ГО “ISACA), комерційних тренінгових центрів (наприклад, Академія CISCO, IT Education Academy) в останні роки організовані та проводяться відповідні навчальні курси, але більшість з них лише розрахована на школярів старшої школи, студентів ЗВО та фахівців з вищою технічною освітою.

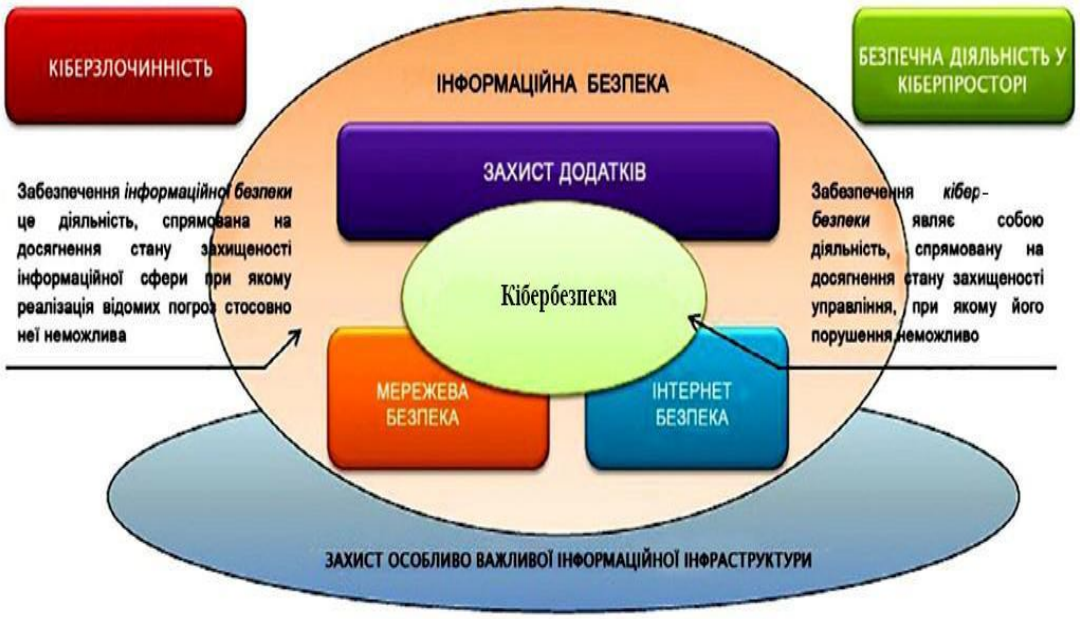

Рис. 2. Прикладна галузь інформаційної та кібербезпеки [30]

Отже, наявна в Україні система підготовки фахівців у сфері кібербезпеки для СБОУ та здійснення кіберосвіти широких верств населення України потребує подальшого вдосконалення.

Відповідно до поставлених завдань дослідження, визначимося щодо основних понять в професійно-компетентнісному підході до підготовки фахівців з кібербезпеки. На рис. 3 показано, яким чином на законодавчому рівні визначено поняття “компетентність” [38].

Як видно на рис. 3, компетентність є характеристикою професіоналізму особистості, яка володіє сукупністю високорозвинених компетенцій. Компетентний фахівець відрізняється від просто кваліфікованого тим, що він: реалізує у своїй роботі професійні знання, уміння та навички; завжди саморозвивається та виходить за межі своєї спеціальності, вважає свою професію великою цінністю [38]. Отже, компетентність більш повно розкриває аспекти професійних здатностей та умінь людини, допомагає фахівцеві ефективно вирішувати різноманітні завдання, що стосуються його професійної діяльності [8], [38].

Рисунок 3 – Нормативні підходи до розуміння компетентності [38]

Найбільшого поширення в українській науковій літературі щодо освіти набуло визначення поняття “професійна компетентність” як сукупність знань й умінь, необхідних для ефективної професійної діяльності: вміння аналізувати, передбачати наслідки професійної діяльності, використовувати інформацію тощо [8], [38].

В [39] зазначено, що “професійні компетенції – це ті компетенції (загально-професійні; спеціалізовано-професійні), які можуть мати узагальнений характер, притаманний професіоналу (фахівцю) взагалі або з певного класу (підкласу, групи) професій, а також визначаються вимогами конкретних галузевих освітніх стандартів або (у разі їх відсутності) експертним шляхом за пропозиціями відповідних робочих груп на основі європейських аналогів та кваліфікаційною характеристикою професії працівника”.

Отже, “професійна компетентність”– це готовність і здатність випускника ЗВО доцільно діяти у відповідності з вимогами справи (сфери професійної діяльності), методично організовано і самостійно розв'язувати завдання і проблеми, а також оцінювати результати своєї діяльності [8]. При цьому, враховуючи, що кібербезпека пов’язана, насамперед, з сучасними інформаційними технологіями, в подальшому можна врахувати результати досліджень [40], які показали особливості розвитку професійної компетентності майбутніх фахівців комп’ютерного профілю.

І наостанок, коротко визначимось щодо загальної методології вдосконалення кіберосвіченості населення, здійснення подальшої розбудови системи підготовки фахівців у сфері кібербезпеки, в тому числі для СБОУ, та формування в них необхідних професійних компетенцій.

Пропонується структурувати підготовку з питань кібербезпеки за наступними рівнями освіти, що прийняті в державі відповідно до Закону [41].

Перший етап підготовки кіберосвідченості доцільно розпочати на рівні дошкільної освіти. Саме у цьому віці людина починає сприймати цифрові пристрої, як частину свого життя. Тому особливо важливим на цьому етапі життя сформувати у дитини основні базові елементи елементарної кібергігієни, правильне сприйняття на рівні інстинктів меж безпеки і загроз при використанні електронних гаджетів та інших продуктів інформаційних технологій. В ігровій формі та у вигляді коміксів тощо, потрібно надати розуміння відповіді на питання: "Що не можна робити з електронними (інфокомунікаційними) девайсами і чому?". Важливу роль у цьому процесі повинна відігравати синергія спільних зусиль дітей, батьків, вихователів, методик та інструментів навчання. Інструменти навчання дітей на цьому етапі: ігри, які формують основи он-лайн безпеки, у тому числі комп’ютерні; заняття у групах; спілкування з батьками та вихователями; наочні посібники у вигляді плакатів, малюнків та інше. Окреме важливе місце у вихованні дітей дошкільного віку з питань кібербезпеки повинна займати підготовленість батьків та вихователів у цій сфері. Для практичної реалізації першого (дошкільного) етапу навчання з питань кібербезпеки, доцільно ввести до варіативної частини державного стандарту дошкільної освіти навчальний курс

“Елементарна кібергігієна”, який повинен розроблятися фахівцями в галузі дошкільної освіти у тісній співпраці з фахівцями всіх напрямів кібербезпеки.

Другим етапом підготовки з питань кібербезпеки повинна стати підготовка у шкільному віці. При цьому її також можливо розділити на декілька курсів за етапами шкільної освіти: початкова освіта, базова та профільна середня освіта.

Для початкової освіти підготовка з питань кібербезпеки повинна стати продовженням дошкільної підготовки на більш високому рівні уявлення – наприклад, курс “Кібергігієна та початкова кібербезпека”. Одночасно доцільно почати надавати знання та формувати первинні навички правильного та безпечного користування простими інфокомунікаційними системами та програмним забезпеченням, що встановлене на гаджетах (девайсах) школярів.

Для базової та профільної середньої освіти вважається за доцільне включити питання кібербезпеки у самостійну дисципліну “Початкова кібербезпека” та сформувати компетенції з безпечного користування електронними пристроями, мережами, програмним забезпеченням, паролями, поштою, електронними рахунками, безпечної поведінки при користування соціальними мережами, захисту особистих даних, запобігання порушень міжнародного та національного законодавства з питань кібербезпеки та інші питання. Ще одним завданням старшої школи є формування правильної уяви про можливу для учня майбутню професію фахівця з кібербезпеки, виявити здібних та надати їм поштовх до подальшого професійного розвитку.

Наступним, третім етапом підготовки з питань кібербезпеки, є підготовка фахівців у ЗВО, які умовно можливо розділити на 4 групи. Перша група, це ЗВО, які здійснюють підготовку у галузях знань, що охоплюють гуманітарні, природничі та інші науки, не пов’язані з поглибленим вивченням цифрових та інформаційних технологій. Друга група, це ЗВО, які здійснюють підготовку фахівців технічних галузей з поглибленим вивченням сучасних цифрових технологій, які будуть працювати на об’єктах критичної (з точки зору кіберзагроз) інфраструктури держави. До таких фахівців можливо віднести працівників енергетичного сектору (у тому числі і атомної енергетики), транспортної інфраструктури та інших. Третя група, це ЗВО, що здійснюють підготовку фахівців, тісно пов'язаних з фаховим використанням інфокомунікаційних технологій, за спеціальностями в галузях знань 12 “Інформаційні технології” (за винятком спеціальності 125 “Кібербезпека”), 15 “Автоматизація та приладобудування” та 17 “Електроніка та телекомунікації". Четверту групу складають ЗВО, які безпосередньо готують фахівців з кібербезпеки за спеціальністю 125 “Кібербезпека”.

Аналіз державних (галузевих) стандартів та навчальних планів підготовки ЗВО першої та другої груп показав, що серед компетенцій випускника є вміння використовувати інформаційні технології під час вирішення завдань за профілем підготовки. Одночасно, встановлено повну відсутність у змісті навчання ЗВО першої групи питань з кібербезпеки, тому вважається необхідним доповнити зміст навчання їх випускників базовим курсом “Основи кібербезпеки”. Передбачається, що випускники ЗВО другої групи будуть експлуатувати об’єкти з потужними інфокомунікаційними складовими, у тому числі критичної інфраструктури. Тому вважається за доцільне ввести до державних та професійних стандартів їх підготовки компетентності випускника за напрямком кібербезпеки. Для їх формування доцільно викладати базовий загальний курс “Основи кібербезпеки” для спеціальностей всіх галузей знань та відповідні спеціалізовані курси за напрямками майбутньої діяльності. Наприклад, “Основи кібербезпеки в сфері енергетики”, “Основи кібербезпеки в сфері транспорту”, “Основи кібербезпеки в банківській сфері. Такий підхід дозволить гідно відповісти викликам часу на фоні подальшої глобалізації та інформатизації суспільства, коли інформаційні технології стають засобом виробництва практично для кожної професії.

Підготовка фахівців третьої групи ЗВО повинна відрізнятися більш ґрунтовними знаннями у сфері кібербезпеки порівняно з фахівцями перших двох груп ЗВО. Для

формування єдиних поглядів на питання кібербезпеки потрібно передбачити у нормативній частині підготовки загальний курс "Основи кібербезпеки" для всіх, хто навчається, та у варіативній частині – спеціалізовані курси за профілем обраних спеціальностей і спеціалізацій.

Основну змістовну частину навчального плану для фахівців четвертої групи ЗВО, де безпосередньо готуються фахівців з кібербезпеки, повинні складати органічно пов'язані між собою дисципліни з кібербезпеки та інфокомунікаційних технологій. Без глибокого розуміння сутності сучасних високих, в тому числі інформаційних та телекомунікаційних технологій підготовка фахівця в сфері кібербезпеки неможлива. Тому необхідно підготовку фахівця, яка притаманна четвертої групи ЗВО, розширити спеціалізованими курсами за складовими кібербезпеки. Змістом навчання, для тих хто навчається, повинні бути, наприклад, наступні питання: кіберпростір та загрози в кіберсфері; міжнародні та національні організації з кібербезпеки; стандарти з кібербезпеки; управління кібербезпекою тощо. Важливим є впровадження єдиного навчально-методичного забезпечення, що розроблено з врахуванням найкращих світових практик та гармонізовано з термінологію країн-членів ЄС та НАТО, дозволить уникнути розбіжностей у термінології та поглядах на зміст питань кібербезпеки, сформувати однакове розуміння проблем забезпечення кібербезпеки, уніфікацію і стандартизацію підготовки з провідними країнами світу, можливість ефективно співпрацювати в єдиному інформаційному і кібер- просторах.

До окремої групи ЗВО, випускникам яких вкрай необхідні знання в сфері кібербезпеки, необхідно віднести ЗВО сектору безпеки і оборони України.

Так, на тактичному та оперативно-тактичному рівнях підготовки фахівців доцільно ввести розподіл на підготовку фахівців за високотехнологічними напрямами та підготовку всіх інших фахівців. Таким чином, створюються умови щоб фахівці, які не мають технічної освіти, отримали більш повне уявлення про технологічні аспекти кібербезпеки й у достатній мірі розумілися щодо особливостей реалізації політики кібербезпеки, як у сферах національної безпеки і оборони, так і на міжнародному рівні, а фахівці з високотехнологічних напрямів отримали повні і всебічні сучасні знання з усіх сфер кібербезпеки (кібероборони, кіберрозвідки, кіберзахисту, протидії кіберзлочинам тощо – за сферами компетенції ЗВО та суб'єкта СБОУ) з врахуванням кращих практик країн членів ЄС та НАТО.

Доцільно доповнити нормативну частину навчання базовим курсом (дисципліною, модулем у дисципліні) "Основи кібербезпеки" з урахуванням подальшого посадового призначення випускника. Особливої уваги слід приділяти практичній складовій підготовки на розробленому, наближеному до реального, тактичному або оперативному фоні із використанням відповідних кіберполігонів та засобів дистанційного проведення кібернавчань.

Відповідно до розглянутого вище світового досвіду, основні зусилля на цих рівнях підготовки фахівців за високотехнологічними напрямами СБОУ необхідно зосередити на інтеграції наукового, науково-педагогічного та матеріально-технічного потенціалів на єдиній базі, шляхом формування військового ЗВО (ЗВО із специфічними умовами навчання) нового типу у вигляді інтегрованого навчально-наукового та дослідно-випробувального комплексу (дослідницького університету, високотехнологічних оборонних кластерів тощо) для комплексного проведення наукових досліджень та підготовки фахівців за високотехнологічними галузями, спеціальностями і спеціалізаціями.

Окремим питанням, що потребує подальшого більш поглибленого вивчення, є розробка методології щодо підготовки фахівців зі знаннями в галузі кібербезпеки для різних сфер СБОУ на оперативно-стратегічному рівні їх підготовки (рівні вищого державного управління у відповідній сфері діяльності). Автори навмисно не наводять відповідні рекомендації з цієї проблематики, так як вважають за доцільне викласти їх в окремій статті.

Нарешті четвертим рівнем підготовки фахівців для СБОУ повинна бути постійно діюча система курсової (післядипломної) підготовки, що буде виконувати функції підтримуючої та тренувальної системи між розглянутими вище рівнями підготовки. Для її повноцінного функціонування необхідне: постійні зібрання, аналіз, систематизація та впровадження в зміст курсів з питань кібербезпеки всіх основних досягнень і інновацій в цій сфері; створення баз даних та відповідних веб-порталів, з яких можливо отримати доступ до спеціалізованих тренінгових курсів; постійний моніторинг контенту з питань кібербезпеки, виявлення нових загроз і ризиків в кіберсфері та реакція на них у вигляді спеціально розроблених навчальних курсів. Важливе місце під час реалізації курсової підготовки буде мати можливість здійснення дистанційного навчання.

Висновки. В умовах стрімкого розвитку інформаційних технологій, запропонована у статті методологія формування кіберкомпетенцій у фахівців, представляє собою комплексне та гнучке рішення проблемного питання освіченості суспільства та особистості з питань кібербезпеки. Освіту з питань кібербезпеки необхідно починати вже з дошкільного навчання, що знизить ризики для дітей на етапі їх формування як особистості, а запровадження системи шкільної кіберосвіти надасть можливість більш якісно підготувати дитину до дорослого життя, життя в сучасному високотехнологічному цифровому суспільстві. Впровадження запропонованих змін для системи вищої освіти буде мати системний характер та підвищить конкурентну спроможність випускника на ринку праці. Запропонована методологія для підготовки фахівців СБОУ дозволить сформувати та підтримувати їх компетентності у відповідних сферах кібербезпеки (відповідно до призначення того чи іншого суб'єкта СБОУ) для виконання завдань за призначенням в умовах сучасних "гібридних" впливів та війн.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Ю. Г. Даник, та Р. В. Грищук *Основи кібернетичної безпеки*. Житомир, Україна: ЖНАЕУ, 2016.

[2] Верховна Рада України. (2018, Черв. 21). *Закон № 2469-VIII. Про національну безпеку України*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/2469-19.

[3] Президент України. (2016, Бер. 15). *Указ № 96/2016. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/96/2016.

[4] Верховна Рада України. (2017, Жовт. 5). *Закон № 2163-VIII. Про основні засади кібербезпеки України*. [Електронний ресурс]. Доступно: http://zakon.rada. gov.ua/laws/show/2163-19.

[5] Кабінет Міністрів України. (2016, Черв. 24). *Розпорядження № 440-р. Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/440-2016-%D1%80.

[6] Кабінет Міністрів України. (2017, Бер. 10). *Розпорядження № 155-р. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/155-2017-%D1%80.

[7] Кабінет Міністрів України. (2018, Лип. 11). *Розпорядження № 481-р. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/481-2018-%D1%80.

[8] Н.П. Степанець, "Компетентнісна парадигма в підготовці кадрів", *Проблеми сучасної педагогічної освіти. Сер.: Педагогіка і психологія: Зб. статей*, вип. 39, ч. 3, с. 262-271, 2013.

[9] Г. Гапоненко, "Професійна компетентність фахівців сектору безпеки і оборони", *Вісник Національної академії Державної прикордонної служби України. Серія: Педагогіка*, вип. 2, 2017. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/ UJRN/Vnadped_2017_2_10.

[10] Official website of the Department of Homeland Security: cybersecurity. [Online]. Available: https://www.dhs.gov/topic/cybersecurity.
[11] Boosting the Cyberworkforce. [Online]. Available: http://www.govtech.com/data/ Boosting-the-Cyberworkforce.html.
[12] Б. В. Бистрова, "Особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ США", *Вісник Черкаського університету*, вип. 6, с. 15-18, 2017.
[13] Ю.Г. Даник та Ю.М. Супрунов, "Особливості формування системи кібернетичної безпеки України в контексті розвитку системи кібернетичної безпеки провідних країн світу", *Труди Національно університету оборони України*, № 7 (106), с. 5-21, 2011.
[14] Досвід США в розслідуванні комп'ютерних злочинів. [Електронний ресурс]. Доступно: http://www.crime-research.org/news/2002/09/1103.htm.
[15] Akademia sztuki wojennej. [Online]. Available: http://www.akademia.mil.pl.
[16] Wojskowa Akademia Techniczna. [Online]. Available: http://www.wat.edu.pl.
[17] Universität der Bundeswehr München. [Online]. Available: https://www.unibw.de/home.
[18] The Defence Academy of the United Kingdom. [Online]. Available: https://www.da.mod.uk.
[19] Royal Military College of Canada. [Online]. Available: https://www.rmc-cmr.ca/en.
[20] О. М. Богданов, О. Г. Додонов, О. В. Корнейко, В. В. Мохор та В. О. Хорошко, "Проблеми становлення національної системи підготовки кадрів в області інформаційної безпеки", *Захист інформації*, вип. 2 (7), с. 66-70, 2001.
[21] Кабінет Міністрів України. (1994, Трав. 18). *Постанова № 325. Про перелік напрямів підготовки фахівців з вищою освітою за професійним спрямуванням, спеціальностей різних кваліфікаційних рівнів та робітничих професій*. [Електронний ресурс]. Доступно: http://search.ligazakon.ua/l_doc2.nsf/link1/KP940325.html.
[22] С. Р. Красильников, "Розробка освітньо-професійної програми підготовки фахівців спеціальності "кібербезпека" на компетентнісній основі", *Herald of Khmelnytskyi national university*, iss. 3, pp. 82-86, 2016.
[23] Кабінет Міністрів України. (1997, Трав. 24). *Постанова № 507. Про перелік напрямів та спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за відповідними освітньо-кваліфікаційними рівнями*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/507-97-%D0%BF.
[24] О. В. Корнейко та О. П. Смольянінов, "27 років незалежності України: здобутки та успіхи в сфері захисту інформації та кіберпростору України", на наук. практ. конф. *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2018): збірник тез наукових доповідей*, Миколаїв, 2018, с. 47-48.
[25] А. В. Корнейко, И. В. Васюков, та В. М. Зинченко, "Особенности подготовки в Украине специалистов для органов государственного управления по обеспечению информационной безопасности и противодействия киберпреступлениям", на *наук. практ. конф. Проблеми котррозвідувального захисту економічної безпеки держави*, Харків, 2004, с. 17-29.
[26] Кабінет Міністрів України. (2006, Груд. 13). *Постанова № 1719. Про перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/1719-2006-%D0%BF.
[27] А.В. Корнейко, "Современное состояние подготовки специалистов в Украине в области защиты информации и обеспечения безопасности информационно-телекоммуникационных систем", на *III міжд. наук. практ. конф. Безопасность современных информационных и телекоммуникационных систем*, Київ, 2006, с. 28.
[28] Кабінет Міністрів України. (2010, Серп. 7). *Постанова № 787. Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра*. Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/787-2010-%D0%BF.

[29] Ю. Г. Даник, та Ю. М. Супрунов, "Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України", *Збірник наукових праць ЖВІ НАУ "Інформаційні системи"*, вип. 5, с. 5-22, 2011.

[30] В. Л. Бурячок, та В. М. Богуш, "Рекомендації щодо розробки та реалізації моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки", *Захист інформації*, том 20, №2, с. 72-78, 2018.

[31] Кабінет Міністрів України. (2011, Серп. 31). *Постанова № 914. Порядок використання коштів, передбачених у державному бюджеті для здійснення заходів щодо підтримки реалізації державної політики у сфері транспорту*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/914-2011-%D0%BF.

[32] Верховна Рада України. *Портал "Законодавство"*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws.

[33] Кабінет Міністрів України. (2015, Квіт. 29). *Постанова № 266. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF.

[34] Міністерство освіти і науки України. (2018, Жовт. 4). *Наказ № 1074. Про затвердження стандарту вищої освіти за спеціальністю 125 "Кібербезпека" для першого (бакалаврського) рівня вищої освіти*. [Електронний ресурс]. Доступно: https://mon.gov.ua/storage/app/uploads/public/5bb/626/1a8/5bb6261a84776166409164.pdf.

[35] І. Діордиця, "Кваліфікаційні вимоги до фахівців із кібербезпеки", *Підприємництво, господарство і право*, № 2, с. 215-219, 2017.

[36] С. М. Мамченко, "Проблеми підготовки фахівців із забезпечення інформаційної безпеки на сучасному етапі реформування системи вищої освіти України", на *наук. практ. конф. Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2017, с. 19-21.

[37] Кабінет Міністрів України. (2017, Лют. 1). *Постанова № 53. Про внесення змін до постанови Кабінету Міністрів України від 29 квітня 2015 р. № 266*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/53-2017-%D0%BF.

[38] І.І. Смагін, Структура професійної компетентності педагога: нормативно-функціональний підхід. [Електронний ресурс]. Доступно: https://www.narodnaosvita.kiev.ua/?page_id=5001.

[39] Методичні рекомендації щодо розроблення стандартів вищої освіти [Електронний ресурс]. Доступно: https://mon.gov.ua/storage/app/media/vishcha-osvita/rekomendatsii-1648.pdf.

[40] О. Й. Карабін, "Розвиток професійної компетентності майбутніх фахівців комп'ютерного профілю як педагогічна проблема" [Електронний ресурс]. Доступно: http://naukajournal.org/index.php/naukajournal/article/view/76/92.

[41] Верховна Рада України. (2017, Вер. 5). *Закон України № 2145-VIII. Про освіту*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/2145-19.

Стаття надійшла до редакції 25 вересня 2018 року.

REFERENCES

[1] Yu. G. Danyk, and R. V. Hrushchuk, *The basics of cybernetic security*. Zhytomyr, Ukraine: Zhytomyr National Agroecological University, 2016.

[2] Verkhovna Rada of Ukraine. (2018, June 21). *Law no. 2469-VIII. On National Security of Ukraine* [Online]. Available: http://zakon.rada.gov.ua/ laws/show/ 2469-19.

[3] President of Ukraine. (2016, Mar. 15). *Decree no. 96/2016. On the decision of the Council of National Security and Defense of Ukraine dated January 27, 2016 "On the Strategy of Cyber Security of Ukraine*" [Online]. Available: http://zakon.rada.gov.ua/laws/show/96/ 2016.

[4] Verkhovna Rada of Ukraine. (2017, Oct. 5). *Law no. 2163-VIII. About the Basic Principles of Cyber Security of Ukraine*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/2163-19.

[5] Cabinet of Ministers of Ukraine. (2016, June 24). *Regulation no. 40-r. On Approval of the Action Plan for 2017 on the Implementation of the Cyber Security Strategy of Ukraine*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/440-2016-%D1%80.

[6] Cabinet of Ministers of Ukraine. (2017, Mar. 11). *Regulation no. 155-r. On Approval of the Action Plan for 2017 on the Implementation of the Cyber Security Strategy of Ukraine*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/155-2017-%D1%80.

[7] Cabinet of Ministers of Ukraine. (2018, Yuly 11). *Regulation no. 481-r. On Approval of the Action Plan for 2018 on the Implementation of the Cyber Security Strategy of Ukraine*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/481-2018-%D1%80.

[8] N.P. Stepanets, "Competency paradigm in training staff", *Problems of modern pedagogical education. Ser. Pedagogy and Psychology: Coll. articles*, no. 39, part 3, pp. 262-271, 2013.

[9] G. Gaponenko, "Professional competence of specialists in the security and defense sector", *Bulletin of the National Academy of the State Border Guard Service of Ukraine. Series: Pedagogy*, вип. 2, 2017. [Online]. Available: http://nbuv.gov.ua/UJRN/Vnadped_2017_2_10.

[10] Official website of the Department of Homeland Security: cybersecurity. [Online]. Available: https://www.dhs.gov/topic/cybersecurity.

[11] Boosting the Cyberworkforce. [Online]. Available: http://www.govtech.com/data/Boosting-the-Cyberworkforce.html.

[12] B. V. Bystrova, "Features of the formation of a system of professional training for future bachelors of cyber security in US universities", *Bulletin of Cherkasy University*, no. 6, pp. 15-18, 2017.

[13] Yu. G. Danyk, and Yu. M. Suprunov, "Features of the formation of the system of cybernetic security of Ukraine in the context of the development of the system of cybernetic security of the leading countries of the world", in *Proc. of the National University of Defense of Ukraine*, no 7 (106), pp. 5-21, 2011.

[14] US Experience in Computer Crime Investigation. [Online]. Available: http://www.crime-research.org/news/2002/09/1103.htm.

[15] Akademia sztuki wojennej. [Online]. Available: http://www.akademia.mil.pl.

[16] Wojskowa Akademia Techniczna. [Online]. Available: http://www.wat.edu.pl.

[17] Universität der Bundeswehr München. [Online]. Available: https://www.unibw.de/home.

[18] The Defence Academy of the United Kingdom. [Online]. Available: https://www.da.mod.uk.

[19] Royal Military College of Canada. [Online]. Available: https://www.rmc-cmr.ca/en.

[20] O. M. Bohdanov, O. G. Dodonov, O. V. Korneiko, V. V. Mokhor, and V. O. Khoroshko, "Problems of formation of the national system of personnel training in the field of information security", *Information protection*, no. 2 (7), pp. 66-70, 2001.

[21] Cabinet of Ministers of Ukraine. (1994, May. 18). *Regulation no.* 325. *About the list of directions of training of specialists with higher education according to professional direction, specialties of different qualification levels and working professions*. [Online]. Available: http://search.ligazakon.ua/l_doc2.nsf/link1/KP940325.html.

[22] S. R. Krasylnykov, "Development of an educational professional program of training specialists in the specialty "cybersecurity" on a competent basis", *Herald of Khmelnytskyi national university*, vol. 3, pp. 82-86, 2016.

[23] Cabinet of Ministers of Ukraine. (1997, May 24). *Regulation no. 507. About the list of directions and specialties, which are carried out training of specialists in higher educational institutions at the relevant educational-qualification levels*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/507-97-%D0%BF.

[24] O. V. Korneiko, and O. P. Smolianinov, "27 years of independence of Ukraine: achievements and acknowledgment in the field of information security and cyberspace of Ukraine", in *Proc. of sciences practice conf. Status and improvement of security of information and telecommunication systems (SITS'2018)*, Mykolayiv, 2018, pp. 47-48.

[25] O. V. Korneiko, I. V. Vasiucov, and V. M. Zinchenko, "Features of training in Ukraine for government agencies to provide information security and countering cybercrime", in *Proc. sciences practice conf. Problems of the Counter-Intelligence Protection of the Economic Security of the State*, Kharkiv, 2004, pp. 17-29.

[26] Cabinet of Ministers of Ukraine. (2006, Dec. 13). *Regulation no. 1719. About the list of areas for which specialists are trained in higher education institutions at the educational and qualification level of the bachelor's degree*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/1719-2006-%D0%BF.

[27] O. V. Korneiko, "The current state of training specialists in Ukraine in the field of information security and security of information and telecommunication systems", in *Proc. III International science practice conf. Security of modern information and telecommunication systems*, Kyiv, 2006, p. 28.

[28] Cabinet of Ministers of Ukraine. (2010, Aug. 7). *Regulation no. 787. About the approval of the list of specialties, which are carried out training of specialists in higher educational institutions for educational and qualification levels of specialist and master*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/787-2010-%D0%BF.

[29] Yu. G. Danyk, and Yu. M. Suprunov, "Some approaches to the formation of a system of training for the system of cybernetic security of Ukraine", *Collection of scientific works of Zhytomyr Military Institute of the National Aviation University "Information systems"*, no. 5, pp. 5-22, 2011.

[30] V. L. Buriachok, and B. M. Bogush, "Recommendations for the development and implementation of a model of professional competences in the field of training for the national cyber security system", *Information protection*, vol. 20, no. 2, pp. 72-78, 2018.

[31] Cabinet of Ministers of Ukraine. (2011, Aug. 31). *Regulation no. 914. The procedure for using funds provided for in the state budget to implement measures to support the implementation of state policy in the field of transport*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/914-2011-%D0%BF.

[32] Verkhovna Rada of Ukraine. The portal "Legislation". [Online]. Available: http://zakon.rada.gov.ua/laws.

[33] Cabinet of Ministers of Ukraine. (2015, Apr. 29). *Regulation no. 266. On Approval of the List of Fields of Knowledge and Specialties under which Higher Education Institutions are Prepared*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF.

[34] Ministry of Education and Science of Ukraine. (2018, Oct. 4). *Order no. 1074. On approval of the standard of higher education by specialty 125 "Cyber Security" for the first (Bachelor) level of higher education*. [Online]. Available: https://mon.gov.ua/storage/app/uploads/public/5bb/626/1a8/5bb6261a84776166409164.pdf.

[35] I. Diordytsia, "Qualification requirements for cyber security specialists", *Entrepreneurship, economy and law*, no. 2, pp. 215-219, 2017.

[36] S. M. Mamchenko, "Problems of training specialists in providing information security at the current stage of reforming the system of higher education in Ukraine", in *Proc. of scien. pract. conf. Actual problems of information security management of the state*, Kyiv, 2017, pp. 19-21.

[37] Cabinet of Ministers of Ukraine. (2017, Feb. 1). *Regulation no. 53. On Amendments to the Resolution of the Cabinet of Ministers of Ukraine dated April 29, 2015, № 266*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/53-2017-D0%BF.

[38] I. I. Smahin, *The structure of the professional competence of the teacher: the normative-functional approach* [Online]. Available: https://www.narodnaosvita.kiev.ua/?page_id =5001.

[39] *Methodical recommendations for the development of higher education standards* [Online]. Available: https://mon.gov.ua/storage/app/media/vishcha-osvita/rekomendatsii-1648.pdf.

[40] O. Y. Karavin, *Development of professional competence of future specialists of the computer profile as a pedagogical problem*. [Online]. Available: http://naukajournal. org/index.php/naukajournal/article/view/76/92.

[41] Verkhovna Rada of Ukraine. (2017, Sept. 5). *Law of Ukraine no. 2145-VIII. About education*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/2145-19.

ЮРИЙ ДАНИК,
АЛЕКСАНДР КОРНЕЙКО

ОСНОВЫ МЕТОДОЛОГИИ ФОРМИРОВАНИЯ КИБЕРКОМПЕТЕНЦИЙ У СПЕЦИАЛИСТОВ СЕКТОРА БЕЗОПАСНОСТИ И ОБОРОНЫ УКРАИНЫ

Проведен анализ существующих систем подготовки военных специалистов по вопросам кибербезопасности для сфер национальной безопасности и обороны в ряде ведущих стран мира (США, Великобритания, Канада, Федеративная Республика Германия, Республика Польша), а также уровня образованности их населения по вопросам кибербезопасности. Приведены данные об основных учебных заведениях этих стран, где успешно готовятся военные специалисты в сфере кибербезопасности, а также учебных программ, которые предлагаются Департаментом внутренней безопасности США (Department of Homeland Security) для проведения обучения детей в системе дошкольного и школьного образования, их родителей, учителей и др. Приведены данные о системе и программах подготовки бакалавров по кибербезопасности в высших учебных заведениях США. Проанализированы предпосылки, этапы становления и существующее состояние системы подготовки в Украине специалистов по кибербезопасности. Определено, что в стандартах подготовки военных специалистов в высших учебных заведениях сектора безопасности и обороны Украины не достаточно учтены их компетенции по основам кибербезопасности. Осуществлен анализ основных понятий в профессионально-компетентностном подходе к подготовке специалистов по кибербезопасности. Предложены основные положения методологии развития целостной системы повышения киберобразованности населения и подготовки специалистов по вопросам кибербезопасности для сектора безопасности и обороны Украины. Показано, что повышать образованность населения в вопросах кибербезопасности в Украине необходимо начинать уже с дошкольного обучения, а также ввести постоянную систему школьного киберобразования, что позволит более качественно подготовить ребенка к взрослой жизни в современном высокотехнологическом обществе. Уточнены требования к обучению по вопросам кибербезопасности в высших учебных заведениях. В соответствии с лучшим зарубежным опытом предложено основные усилия в подготовке специалистов по кибербезопасности для сектора безопасности и обороны сосредоточить на интеграции научного, научно-педагогического и материально-технического потенциалов на единой базе, путем формирования военно-учебных заведений (высших учебных заведений со специфическими условиями обучения) нового типа в виде интегрированного учебно-научного и опытно-испытательного комплекса.

Ключевые слова: сектор безопасности и обороны, кибербезопасность, киберобразование, киберкомпетентность, высшее учебное заведение, высшее военно-учебное заведение.

YURII DANYK,
OLEKSANDR KORNEIKO

FUNDAMENTALS METHODOLOGY OF FORMATION CYBER COMPETENCES AT SECURITY SECTOR EXPERTS AND UKRAINE DEFENSE

The analysis of the existing systems of training military specialists in cybersecurity issues for the national security and defense spheres in a number of leading countries of the world (USA, UK, Canada, Germany, Poland) was conducted. An analysis of the cybersecurity education system of the US population was also conducted. Data is provided about main educational institutions in these countries where military cybersecurity experts are successfully trained, as well as the training programs offered by the US Department of Homeland Security to train children in the system of pre-school and school education, their parents, teachers and other. The data shows system and programs for the preparation of cybersecurity bachelors in higher educational institutions of the United States. Analyzed the prerequisites, stages of formation and the current state of the training system in Ukraine of cybersecurity specialists. It was determined that the standards for training military specialists in higher education institutions of the security and defense sector of Ukraine did not sufficiently take into account their competence in the cybersecurity basics. The analysis of the basic concepts in the professional-competence approach to the training of cybersecurity specialists has been carried out. The main provisions of the methodology for the development of an integrated system of improving cyber-education of the population and training of specialists in cybersecurity issues for the security and defense sector of Ukraine are proposed. It has been shown that raising the level of population education in cybersecurity issues in Ukraine should begin with pre-school education, as well as introduce a permanent school cyber-education system, which will make it possible to better prepare a child for adulthood in a modern high-tech society. Clarified requirements for cybersecurity education in higher education. In accordance with the best foreign experience, it was suggested that the main efforts in training cybersecurity experts for the security and defense sector should be focused on integrating the scientific, pedagogical and material-technical potentials on a single basis, by forming higher military schools (higher education institutions with specific learning conditions) a new type in the form of an integrated teaching and research and experimental test complex.

Keywords: security and defense sector, cyber security, cyber education, cyber competence, higher educational institution, higher military schools.

Юрій Григорович Даник, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, начальник інституту інформаційних технологій, Національний університет оборони України, Київ, Україна.

ORCID: 0000-0001-6990-8656.

E-mail: zhvinau@ukr.net.

Олександр Васильович Корнейко, кандидат технічних наук, професор, завідувач кафедри інформаційних технологій та кібербезпеки, Національна академія внутрішніх справ, Президент громадської організації "Українська академія кібербезпеки", Київ, Україна.

ORCID: 0000-0002-1882-9680.

E-mail: alex_korneiko@meta.ua

Юрий Григорьевич Даник, доктор технических наук, профессор, Заслуженный деятель науки и техники Украины, Лауреат Государственной премии Украины в области науки и техники, начальник института информационных технологий, Национальный университет обороны Украины, Киев, Украина.

Александр Васильевич Корнейко, кандидат технических наук, профессор, заведующий кафедрой информационных технологий и кибербезопасности, Национальная академия внутренних дел, Президент общественной организации “Украинская академия кибербезопасности”, Киев, Украина.

Yuriy Danyk, doctor of technical sciences, professor, honored science and technology worker of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, chief of Information technologies institute, National defense universityof Ukraine, Kyiv, Ukraine.

Oleksandr Korneiko, candidate of technical sciences, professor, head of the department of Information technologies and cyber security, National Academy of Internal Affairs, President of NGO "Ukrainian Academy of Cyber Security", Kyiv, Ukraine.