DOI 10.33099/2618-1614-2018-5-4-35-42
УДК 371(378)

В. М. Телелим,
доктор військових наук, професор, професор кафедри стратегії національної безпеки та оборони Національного університету оборони України імені Івана Черняховського,
Ю. Г. Даник,
доктор технічних наук, професор, начальник інституту інформаційних технологій Національного університету оборони України імені Івана Черняховського, генарал-майор,
А. О. Зінченко,
доктор технічних наук, доцент, начальник кафедри зв'язку та автоматизованих систем управління Національного університету оборони України імені Івана Черняховського, полковник

Кіберосвіта у сфері оборони

У статті проведено аналіз формування та розвитку систем кіберосвіти секторів безпеки і оборони провідних країн світу й України. Установлено, що формування компетенцій з основ кібербезпеки у тих, хто навчається в закладах вищої освіти сектору безпеки і оборони України, недостатньо враховане у стандартах освіти випускників. Доведено, що в сучасних умовах знання з кібербезпеки в тих, хто навчається, повинні формуватися в рамках базових курсів для всіх галузей знань, спеціальностей та спеціалізацій підготовки. Це питання потребує постійного уточнення, відповідно до змін та розвитку, що відбуваються в цій сфері. Для систематизації та вдосконалення підготовки у сфері кібербезпеки сектору безпеки і оборони Україні авторами запропонований варіант організації підготовки фахівців з питань кібербезпеки у сфері оборони в закладах вищої освіти сектора безпеки і оборони України. Запропонована та практично апробована цілісна, послідовна, взаємопов'язана та безперервна система підготовки з питань кібербезпеки та кібероборони на тактичному, оперативному і стратегічному рівнях підготовки та зміст навчання для її реалізації.

Ключові слова: національна безпека і оборона, кіберпростір, кіберзагрози, кібербезпека, кібероборона, кіберосвіта, заклад вищої освіти.

Постановка проблеми. Упродовж останніх десятиліть відбувається бурхливий розвиток інформаційних технологій (ІТ). За сучасних умов ефективне виконання функцій фахівцями практично всіх галузей неможливе без застосування кіберінфокомунікаційних технологій. Особливо це характерно для воєнної сфери. Унаслідок революційного розвитку високих технологій та глобальної інформатизації практично всі засоби озброєння та військової техніки (ОВТ) містять електронні та інформаційні компоненти, бойові дії плануються та відбуваються в єдиному інформаційному просторі за кіберінформаційними циклами та кіберциклічними технологіями. Основою для здійснення ефективного управління військами та зброєю стали інноваційні локальні та глобальні кібернетичні системи: системи автоматизації, автоматизовані системи управління (АСУ), комплекси оперативного управління силами та засобами, системи управління зброєю. Інтенсивно розвиваються, впроваджуються та застосовуються технічні системи (засоби) розвідки, робототехнічні (безпілотні, безекіпажні) системи (комплекси) повітряного, наземного і морського (надводного, підводного) базування. Виник і став об'єктивною загальновизнаною реальністю принципово новий, штучний простір – кіберпростір (КП), який одразу став середовищем як різноманітної корисної діяльності людства, так і злочинності, тероризму, протистояння і боротьби між державами, державними та недержавними акторами, включаючи воєнні та інші конфлікти, фактичного кіберінформаційного протиборства «всіх проти всіх». Якщо у світі на даний час ще до певної міри зберігаються стратегічний баланс, система противаг і міжнародних угод у сфері звичайних озброєнь та зброї масового ураження, то питання паритету в КП залишається відкритим і проблемним.

Основною характеристикою КП є те, що він пропонує середовище, що складається з багатьох учасників, здатних впливати один на одного як у ньому, так і через нього. Уряди провідних країн світу (ПКС) відносять взаємопов'язані ІТ і взаємозалежну мережу інфраструктур інформаційних технологій КП до національної критичної інфраструктури. Кібернетичні загрози (КЗ) охоплюють усі базові сфери суспільної діяльності: політичну, воєнну, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну, когнітивну, технологічну тощо. При цьому для кожної з них є як спільні вразливості, так і свої специфічні, притаманні лише конкретній сфері загрози, які постійно розвиваються, урізноманітнюються та ускладнюються, а в разі своєї реалізації викликають ланцюгові реакції та супроводжуються синергетичними деструктивними наслідками. При цьому відбувається зміна традиційних форм і способів ведення протиборства.

У щорічному звіті Генерального секретаря НАТО Єнса Столтенберга за 2016 р. зазначалося: «Ще однією галузю, що викликає стурбованість, але в якій НАТО також

досягла відчутного поступу, є КБ. Протягом 2016 року НАТО довелося реагувати в середньому на 500 спроб кібернападів на місяць, що становить збільшення їх кількості на 60% порівняно із 2015 роком. Фахівці НАТО гарантують захист мереж Альянсу в цілодобовому режимі, а на Варшавському саміті держави – члени Альянсу взяли на себе зобов'язання у галузі КБ, згідно з яким вони розвиватимуть найширший перелік засобів в галузі КБ» [1]. Такий курс був підтверджений на конференції голів оборонних відомств країн Північної Європи та їхніх союзників з питань стримування російської агресії, що відбулася 7 вересня 2018 р. в Осло під керівництвом міністра оборони Норвегії адмірала Хаакона Брун-Хансена. Тому розв'язання проблеми забезпечення КБ у сучасних умовах і особливо на перспективу викликала гостру потребу у високопрофесійних фахівцях з питань КБ та володіння базовими знаннями із забезпечення КБ фахівцями всіх галузей знань, спеціальностей та спеціалізацій. Забезпечення захисту від: втручання в роботу інформаційних систем державних і комерційних структур; витоку і викривлення даних, крадіжки інформації з електронних засобів; порушення нормального функціонування систем управління державних, приватних структур та об'єктів критичної інфраструктури, інфокомунікаційних мереж та систем управління військами (силами) і засобами (зброєю); здійснення інформаційних, психологічних і когнітивних впливів на соціум; маніпулювання репутацією ключових осіб держави та сектора безпеки і оборони (СБО) держави за допомогою соціальних мереж та електронних ЗМІ; і багато іншого, пов'язаного з деструктивними діями у КП та через КП стало реальною необхідністю на всіх рівнях – від простого громадянина до держави в цілому.

Найбільших успіхів у підготовці фахівців з КБ та кібероборони (КО) у світі досягли США, Ізраїль, Японія, РФ, КНР та країни – члени блоку НАТО. Невід'ємною складовою забезпечення КБ і КО будь-якої держави є питання розбудови системи кіберосвіти. Вони знайшли своє відображення в роботах Дж. Треглія, М. Делія, Ш. Костігана, Дж. Маршалла, Дж. Антонакос, М. Корби, Р. Гоеля, Е. Херда, К. Камінскі, Н. Кайла, Д. Момота, М. Хеннессі, С. Найта, Д. Керигана-Кайру, Ф. Ларка, К. Палларіса, Д. Педера Багге, Р. Росса, Д. Романа, Н. Спину, Т. Тагарєва, Р. Тейлора та Д. Вана. Проте проведений аналіз відомих публікацій, на жаль, свідчить про відсутність єдиних поглядів на систему, зміст і методологію навчання фахівців з КБ та КО. Аналіз наукових публікацій вітчизняних авторів (В. Л. Бурячок, В. О. Хорошко, В. С. Толюпа, М. М. Присяжнюк, Є. І. Цифра, І. Діордіца, Б. В. Бистрова, В. Богуш, С. Мельник [2–7]) із цих питань установив аналогічну відсутність єдиної раціональної системи, змісту та методології підготовки фахівців з КБ, особливо для сектору безпеки та оборони України (СБОУ).

Має місце також недостатнє розуміння і сприйняття особливостей та масштабів систем кібернетичної безпеки ПКС, що розгортаються в останні 5–10 років, їх складу і завдань, змісту діяльності військових і цивільних фахівців у цій сфері, термінологічна та нормативно-правова невизначеність щодо понять КП, КЗ, КБ, КО тощо. У цьому контексті можна стверджувати, що аналіз проблем нормативно-правового, організаційного та кадрового забезпечення розвитку систем кібернетичної безпеки є актуальним для створення в Україні національної системи КБ і КО та потребує ретельного і творчого врахування світового досвіду, національних реалій та особливостей.

Проведена у процесі комплексного огляду СБОУ у 2016 р. оцінка стану воєнної безпеки держави, а також набутий досвід участі Збройних Сил України (ЗСУ) в антитерористичній операції виявили щиру існуючих та потенційних загроз у кібернетичній сфері, зокрема: низьку ефективність систем оперативного (бойового) управління, зв'язку, розвідки та спостереження; неспроможність ефективно реагувати на зростаючу кількість і потужність кібератак та протистояти кіберзлочинності [8]. Для нейтралізації таких загроз Стратегічним оборонним бюлетенем України до кінця 2020 р. передбачене досягнення оперативних цілей 1.4 (створення ефективної системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR)) та 1.5 (удосконалення системи кібербезпеки та захисту інформації). Результатом досягнення оперативних цілей буде сформований єдиний кібернетичний простір ЗСУ та реалізована в ньому система КБ та КО.

Для унормування питань створення національної системи кібербезпеки України та розподілу повноважень між суб'єктами КБ і КО України були розроблені й уведенні в дію «Стратегія кібербезпеки України» та Закон України «Про основні засади забезпечення кібербезпеки України» [9, 10].

Цими документами на Міністерство оборони України (МОУ) та Генеральний штаб (ГШ) ЗСУ покладені завдання «відповідно до компетенції здійснювати заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони), здійснювати військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки КП та спільного захисту від кіберзагроз; впроваджувати заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану» [10]. У прикінцевих положеннях Закону [10] внесені зміни до статті 3 «Підготовка держави до оборони» Закону України «Про оборону України». Її доповнено абзацом: «Здійснення заходів з кібернетичної оборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройної агресії». Другу частину статті 4 викладено в новій редакції: «На підставі відповідного рішення Президента України, Збройні Сили України разом з іншими військовими формуваннями розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі» [11].

Для нарощування спроможностей СБОУ щодо КБ і КО широко використовуються інструменти міжнародного співробітництва між Україною та НАТО. Для допомоги Україні з боку НАТО у 2014–2015 рр. створений Цільовий трастовий фонд з метою надання допомоги в галузі КБ і КО [12]. Ідеться про обмін досвідом, отримання спеціалізованого програмного забезпечення і технологій, найкращих світових практик, проведення спільних навчань з питань КЗ і КО, новітнє обладнання для запобігання кібератакам і виявлення їхніх джерел у сфері кіберзахисту інформаційно-комунікаційних систем.

Покладені на МОУ та ГШ ЗСУ завдання потребують розробки в стислі терміни теоретичних і прикладних основ та практичних заходів КБ і КО держави в усіх їх аспектах, які повинні органічно інтегруватися до системи військової освіти і науки України. Надалі вони стануть базою для розробки відомчих нормативних документів з КБ та КО. Одночасно з розробкою теоретичних основ КБ і КО України потребує вдосконалення й нарощування система підготовки фахівців СБОУ з КБ і КО.

При розробці методології кіберосвіти СБОУ необхідно враховувати низку особливостей, притаманних сучасним ІТ: швидку зміну поколінь інформаційно-телекомунікаційних технологій; постійне зростання можливостей впливу на складові кібернетичних систем та об'єкти критичної інформаційної інфраструктури; необхідність постійного оновлення знань з питань КБ; різні рівні здатності і готовності до навчання тих, хто навчається; особливості курсу КБ; велику кількість специфічних складових КБ і КО тощо.

Існуючий стан справ і спонукав авторів до розробки та апробації системи, змістовних і методологічних основ освіти фахівців СБОУ з питань КБ та КО.

Метою статті є формування системи, змісту й методології навчання фахівців з КБ та КО в закладах вищої освіти СБОУ.

Досягнення поставленої мети потребувало дослідження та вирішення таких завдань: здійснення аналізу існуючих систем підготовки фахівців з КБ і КО в провідних країнах світу в контексті КБ і КО України; здійснення аналізу існуючого стану системи і методології підготовки фахівців з питань кібербезпеки та кібероборони СБОУ; здійснення розробки системи, змісту й методології підготовки фахівців з питань КБ та КО для СБОУ.

Важливим аспектом формування системи освіти фахівців з питань КБ і КО є вивчення та дослідження досвіду ПКС, насамперед США, де питанням підготовки фахівців КБ приділяється надзвичайна увага. Так, у складі Департаменту внутрішньої безпеки (Department of Homeland Security's (DHS)) США сформований відділ освіти та підвищення освіченості з питань КБ і КО [13]. Завданнями відділу є формування єдиної державної політики, системи та методології підготовки фахівців з КБ і КО.

Питання інформаційної та кібернетичної безпеки вивчаються тими, хто навчається, в усіх військових навчальних закладах Міністерства оборони США та інших країн – членів НАТО, передусім у видових закладах вищої освіти: у Військовій академії армії США у Вест-Пойнті (US Military Academy, West Point, NY) – на кафедрі електронної інженерії та комп'ютерних наук (Department of Electrical Engineering and Computer Science); в Академії військово-повітряних сил у Колорадо-Спрінгс (United States Air Force Academy, Колорадо); Академії військово-морських сил в Анаполісі (Меріленд).

Ці питання вивчаються і в інших військових закладах вищої освіти, таких як Технологічний інститут військово-повітряних сил (Air Force Institute of Technology, Wright-Patterson AFB, Огайо), Університет національної оборони (National Defense University) – коледж інформаційних та кібернетичних наук (College of Information and Cyberspace).

На відміну від США, зважаючи на значно меншу чисельність збройних сил, в інших країнах – членах блоку НАТО (Великій Британії, Федеративній Республіці Німеччина, Республіці Польща тощо) ефективність розв'язання зазначених проблем досягається шляхом формування та забезпечення функціонування інтегрованих навчально-наукових, дослідно-випробувальних комплексів (високотехнологічних оборонних кластерів), які здійснюють на єдиній базі освітню й наукову діяльність за високотехнологічними напрямами. Наприклад:

1. Республіка Польща. На оперативному і стратегічному рівнях – у Військовій академії (War Studies University (Akademia sztuki wojennej)). На тактичному рівні фахівців усіх високотехнологічних галузей, спеціальностей і спеціалізацій для всіх видів збройних сил готують у Військово-технічній академії (Військовому університеті технологій) імені Ярослава Домбровського (Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego)

2. Канада. Королівський військовий коледж Канади (Royal Military College of Canada) має окремий факультет, який веде шість напрямів підготовки: хімічної, цивільної, комп'ютерної, електронної, повітряної та технічної інженерії. Факультет має у своєму складі кафедри електронної та комп'ютерної інженерії, математичних і комп'ютерних наук (Department of Electrical and Computer Engineering, Department of Mathematics and Computer Science) [14].

3. Федеративна Республіка Німеччина. В Академії Бундесверу в Гамбурзі (Führungsakademie der Bundeswehr) функціонує факультет оперативного планування, територіальної оборони, логістики, цивільно-військового співробітництва, застосування кібернетичних та інформаційних систем (Fakultät Einsatz, CIR, SKB).

4. Велика Британія. У складі Академії оборони Об'єднаного Королівства (The Defense Academy of the United Kingdom) створені Технологічна школа (Technology School), яка містить у своєму складі Центр імітаційного моделювання (Defense Simulation Centre) та Школу кібернетичної оборони (Defense Cyber School).

Найбільш удало, на нашу думку, інтеграція військової освіти та науки за високотехнологічними напрямами реалізована у Військовому університеті технологій (Республіка Польща), де на одній базі зосереджені всі високотехнологічні спеціальності та спеціалізації підготовки військових фахівців (кафедри: національної безпеки, електроніки і телекомунікацій, енергетики, технічної фізики, геодезії та картографії, інформатики, інженерії безпеки, інженерії матеріалів, криптології та кібербезпеки, авіації й космонавтики, механіки і машинобудування, механотроніки, управління тощо) та підрозділи наукових досліджень із цих питань [15]. Те саме реалізоване в Університеті Бундесвера в Мюнхені (ФРН) (спеціальності: електротехніка та інформаційні технології, комп'ютерні науки, аерокосмічна інженерія, менеджмент інформаційних систем, математична інженерія, політологія та соціальні науки, розвиток людських ресурсів, медіа-менеджмент, дослідження міжнародної безпеки, економіко-організаційні науки, інженерна справа та екологія, інженерна психологія, комп'ютерні технології та комунікаційні технології, машинобудування, комп'ютерна техніка, державне управління, оборонна інженерія) [16]. За рахунок інтеграції високотехнологічних напрямів підготовки фахівців і наукових досліджень у єдиному навчальному закладі та на єдиній базі у ПКС забезпечують 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 всіх міністерств і відомств СБО держави в рамках єдиних стандартів. У подібних єдиних для держави високотехнологічних військових навчально-науково-випробувальних центрах зосереджена підготовка фахівців для СБО в більшості країн – членів НАТО та інших ПКС.

Особливістю підготовки фахівців СБОУ є трирівнева (тактичний, оперативний і стратегічний рівні) система підготовки. Це відповідає загальноприйнятим у світі підходам до підготовки фахівців СБО.

При цьому на тактичному рівні вища освіта надається у видових навчальних закладах Сухопутних Військ (Національній академії сухопутних військ імені гетьмана Петра Сагайдачного (м. Львів), Військовій академії (м. Одеса), Харківському інституті танкових військ Національного технічного університету «Харківський політехнічний університет» (м. Харків) – які разом є певним аналогом Академії сухопутних військ США (Вест Пойнт), Вищої офіцерської школи сухопутних військ Республіка Польща (м. Вроцлав)), Повітряних Сил (Харківському національному університеті Повітряних Сил імені Івана Кожедуба – аналогу Академії повітряних сил США (Форт Брагге), Вищої офіцерської школи військово-повітряних сил Республіки Польща (м. Демблін)), Військово-Морських Сил (Інституті Військово-Морських Сил Національного університету «Одеська морська академія» – аналогу Військово-морської академії США (Анаполіс), Академії військово-морських сил Республіки Польща (м. Гдиня)).

Фахівців з високотехнологічних напрямів (радіоелектроніки, ІТ, військової кібернетики, геоінформаційних систем, зв'язку тощо) готують у міжвидових інститутах (Житомирському військовому інституті імені С. П. Корольова, Військовому інституті телекомунікації та інформатизації імені Героїв Крут, Військовому інституті Київського національного університету імені Тараса Шевченка, які разом можна розглядати як певний аналог Університету Бундесвера в Мюнхені (ФРН), Військового університету технологій (Військової технічної академії імені Ярослава Домбровського (Республіка Польща)).

Аналіз питань підготовки фахівців кібербезпеки СБОУ в закладах вищої освіти, що підпорядковані МОУ, Генеральному штабу ЗСУ, Міністерству внутрішніх справ України, Службі безпеки України, Державній службі спеціального зв'язку та захисту інформації України тощо, на жаль, висвітлив аналогічну (так само, як і в цивільних закладах вищої освіти) проблему відсутності єдиної методології та сформованої системи підготовки фахівців з питань КБ та загальної кіберосвіти. Відсутність єдиних керівних документів, методичного забезпечення навчання, розбіжність у поглядах на мету, завдання та зміст підготовки з питань КБ у військових вищих навчальних закладах (ВВНЗ) знижує ефективність і якість підготовки фахівців для СБОУ загалом. Особливо яскраво це проявилося з початком повномасштабної «гібридної війни» проти України, в якій значна частка протиборства сторін відбувається в інформаційному та кібернетичному просторах.

З метою реалізації комплексного та гнучкого підходу до підготовки фахівців КБ і КО авторами були розроблені та апробовані система підготовки фахівців СБОУ з питань КБ і КО (*рис. 1*) та зміст навчання для її реалізації в навчальних планах закладів вищої освіти СБОУ.

Авторами доведено доцільність розподілу підготовки фахівців із цих питань за високотехнологічними та всіма іншими спеціальностями і спеціалізаціями на тактичному та оперативному рівнях. Це, у свою чергу, дасть змогу створити умови, щоб фахівці, які не мають технічної освіти, отримали повніше уявлення про технологічні аспекти КБ і достатньою мірою розумілися на особливостях реалізації політики КБ як у сфері оборони держави, так і на національному та міжнародному рівнях, а фахівці з високотехнологічних напрямів отримали повні й усебічні сучасні знання з питань КБ і КО, їх організації та управління ними у сфері оборони з урахуванням кращих практик країн – членів НАТО.

Основна особливість підготовки фахівців тактичного рівня – це навчання здобувачів вищої освіти за високотехнологічними напрямами поза межами основної для військових галузі знань 25 – «Воєнні науки, національна безпека, безпека державного кордону». Причиною цього

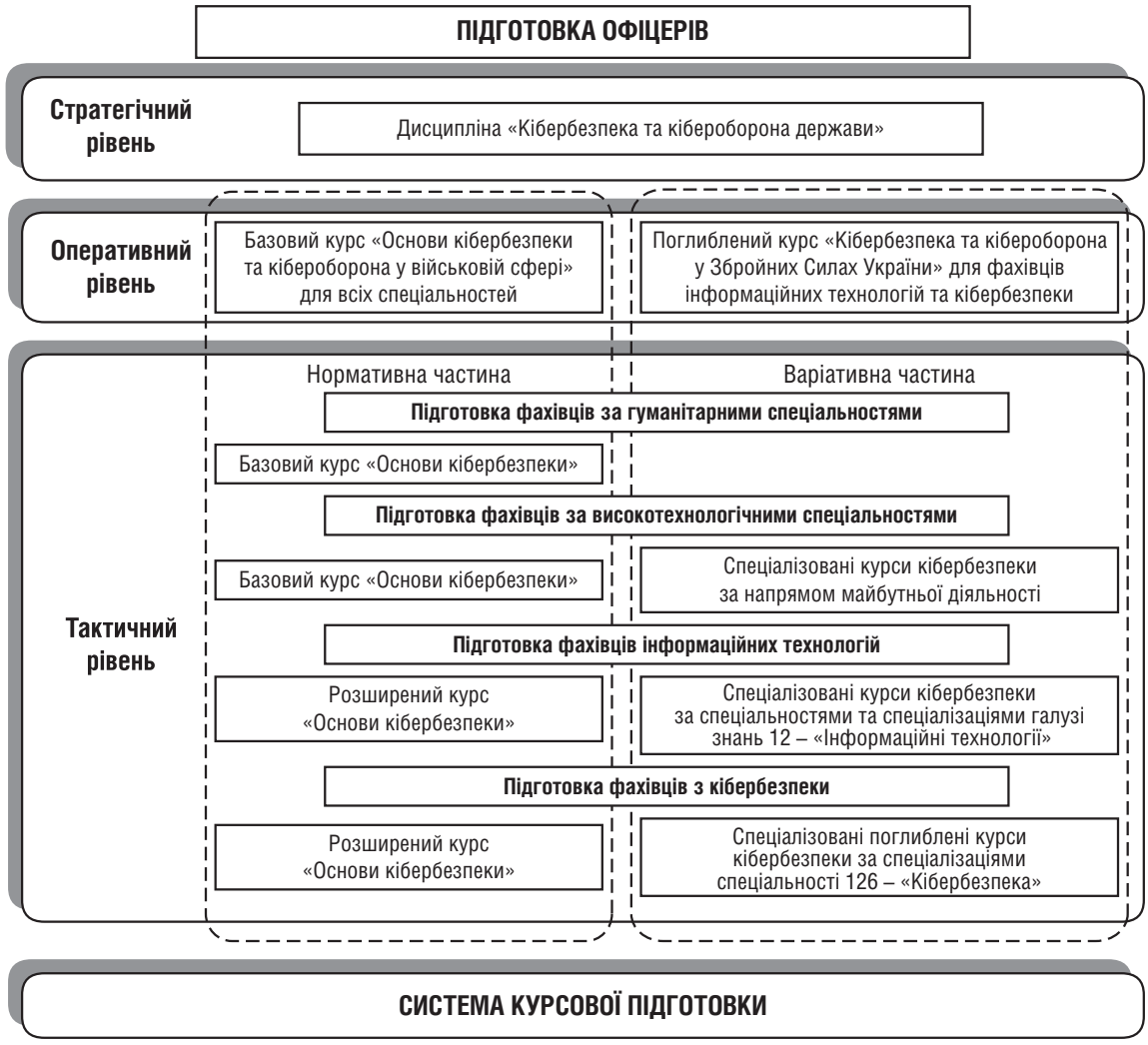

Рис. 1. Система підготовки фахівців СБОУ з питань КБ і КО

є відсутність у переліку спеціальностей 25-ї галузі знань інформаційної складової [17]. Базовими для тактичного рівня є галузі 12 – «Інформаційні технології», 15 – «Автоматизація та приладобудування», 17 – «Електроніка та телекомунікації» та ін. Тому об'єктивна необхідність уведення в нормативну частину загального базового курсу з питань КБ та у варіативну частину спеціалізованих курсів з КБ за складовими КБ для підготовки майбутніх фахівців СБОУ за високотехнологічними спеціальностями та спеціалізаціями всіх галузей знань не викликає сумніву. Змістом навчання мають бути навчальні дисципліни або блоки навчальних дисциплін, які охоплюють питання: кібернетика, КП та його особливості, загрози і ризики в кібернетичній сфері, основи інформаційної та кібер- безпеки і кібероборони, технологічні, соціотехнічні, інформаційні та інші аспекти КБ і КО, особливості організації та стандарти у сфері КБ і КО у світі та в Україні, управління КБ у сфері національної безпеки та оборони.

Розуміння тими, хто навчається, питань виникнення і формування КП, його структурних компонентів, архітектури та особливостей, дасть змогу зрозуміти й засвоїти, в чому полягає феномен і парадигма КБ, закласти основи знань для всього подальшого вивчення питань КБ. При цьому особлива увага приділяється основам методології аналізу загроз і ризиків у галузі інформаційної та кібербезпеки, вивченню типових підходів до оцінювання їх забезпечення, в тому числі заснованих на управлінні ризиками. Окремим блоком вивчаються питання функціонування й архітектури глобального Інтернету, мережевих інфраструктур держав, а також управління мережами, стандарти мережевих та інформаційних технологій, проектування та експлуатації мереж. Методичні основи та практика проведення аналізу загроз, ризиків і вразливостей є базовими для формування навичок розробки стратегії та архітектури КБ, запобігання, обмеження й нейтралізації відомих і невідомих уразливостей та загроз, управління кібернетичними ризиками з метою їх

зниження. Огляд уразливостей, характерних для КП, форм, способів і засобів використання таких уразливостей, вивчення основного спектра різноманітних сценаріїв і технологій кіберрозвідки, кіберзахисту або активного впливу (несанкціонованого проникнення, отримання інформації, зміни алгоритмів діяльності тощо) сформує в тих, хто навчається, вміння оцінювати ризики деструктивних впливів, у тому числі пов'язаних з використанням мобільних девайсів (гаджетів), інших технологій і систем, пов'язаних з мобільністю, і забезпечувати зниження їх рівня.

Важливою складовою підготовки фахівців з питань КБ і КО є вивчення ними світового й вітчизняного досвіду створення і розвитку систем КБ та їхніх складових, вирішення питань забезпечення КБ на різних етапах її становлення, розподілу сфер відповідальності, задач, функцій, організації взаємодії з питань КБ і КО між складовими національної безпеки та оборони, міжнародних і національних стандартів у галузі КБ, особливостей формування національної політики з КБ, найкращих світових практик у вирішенні зазначених питань і тенденцій їх розвитку, загальної системи та структури міжнародних і національних організацій у сфері КБ, їхніх завдань, організаційної структури, повноважень, функцій, розподілу повноважень між ними, організації та характеру взаємодії з національними організаціями з КБ, міжнародних та національних правових аспектів забезпечення КБ та відповідальності за здійснення деструктивних впливів у КП та їхні наслідки.

Підготовка фахівців за високотехнологічними напрямами, фахівців КБ та всіх інших військових фахівців з наведених вище базових питань КБ відрізняється лише шириною та глибиною їх подання.

Компетентності з питань КБ, необхідні для виконання завдань за посадами випускниками ВВНЗ – фахівцями з КБ і КО, закладатимуться при вивченні питань управління КБ у сфері оборони в рамках варіативних дисциплін. На основі базових питань КБ, попередньо засвоєних тими, хто навчається, здійснюється їх підготовка до виконання завдань за посадою командира підрозділу військової частини КБ або офіцера з КБ органу військового управління. Для цього вони ознайомлюються з основними КЗ у воєнній сфері, відомчими нормативними актами з питань КБ і КО, змістом, завданнями та складовими частинами КО, силами та засобами КО, формами та способами бойового застосування підрозділів кібервійськ і вимогами до їхніх спроможностей, досвідом їх підготовки та застосування, у тому числі за прикладами ПКС, методами роботи посадових осіб і методиками планування застосування підрозділів КБ у мирний час, в особливий період та за умов воєнного стану, усвідомлюють розподіл повноважень з питань КБ і КО між суб'єктами забезпечення КБ і КО, засвоюють особливості підготовки і проведення навчань з КО, аудиту й оцінювання КБ на рівні окремої військової частини та органу військового управління.

Особливу увагу варто приділити практичній складовій підготовки фахівців КБ тактичного рівня на розробленому, наближеному до реального, тактичному або оперативному фоні з використанням кіберполігонів та засобів дистанційного проведення кібернавчань. Актуальною є розробка комплексних тактичних задач (комплексних методичних тактичних задач) для практичної підготовки фахівців КБ. Змістом задач буде вивчення методів роботи посадових осіб (командира підрозділу) військової частини КБ, організація та бойове застосування підрозділів КБ. В основу задач доцільно покласти алгоритм планування за стандартами НАТО TLP та MDMP (*military decision-making process*), а групові вправи поєднувати з практичними заняттями для відпрацювання практичних питань, у тому числі з використанням кіберполігонів. Подальше нарощування циклу розглянутих питань надасть можливість сформувати зміст навчання для підготовки фахівця з КБ тактичного рівня з необхідними компетенціями.

На підставі вивчення досвіду розбудови систем забезпечення КБ у провідних країнах світу, досвіду ведення бойових дій на сході України та протистояння у КП України є можливим реалізувати варіант побудови системи КБ України, подібний до кращих практик країн – членів НАТО. Виконання завдань, визначених у Стратегічному оборонному бюлетені України [8], передбачає побудову такої системи. Водночас потребує вдосконалення й систематизації система підготовки військових фахівців з КБ від тактичного до стратегічного рівнів.

На жаль, при аналізі стандартів підготовки фахівців тактичного рівня СБОУ всіх галузей знань, спеціальностей та спеціалізацій (крім високотехнологічних) установлена наявність лише компетенції щодо застосування ІТ за профілем діяльності та повна відсутність компетенцій випускника з питань КБ і КО. Таким чином, виникає потреба доповнити нормативну частину навчання базовим курсом (дисципліною, блоком у дисципліні) основ КБ з урахуванням подальшого посадового призначення випускників. Змістом їхнього навчання мають стати питання кібернетики, КП та його особливостей, загроз і ризиків у кібернетичній сфері, основ інформаційної безпеки, КБ і КО, технологічних, соціотехнічних, інформаційних та інших аспектів КБ і КО, основних заходів КБ під час виконання обов'язків за посадою.

Наступними рівнями підготовки є оперативний і стратегічний. Фахівці з КБ та КО, які отримали освіту цих рівнів, повинні отримати знання та бути здатними практично здійснювати:

- формування та реалізацію державної політики з питань інформаційної безпеки, КБ та КО;
- формування та реалізацію політики МОУ та ЗСУ щодо дій у КП;
- виконання заходів зі створення та розвитку інформаційних систем та ресурсів у ЗСУ;
- координацію дій суб'єктів інформаційної безпеки, КБ та КО МОУ та ЗСУ;

• розробку стандартів підготовки фахівців з інформаційної безпеки, КБ та КО;

• організацію взаємодії та проведення заходів (у тому числі щодо підготовки держави до КО) зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами з питань КБ і КО;

• організацію та підтримку взаємодію із системою відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT);

• планування та узгоджене управління діяльністю суб'єктів у КП за єдиним замислом і планом, контроль та координацію їхніх дій;

• моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у КП та ефективності дій системи КБ і КО, виявлення вразливостей в інформаційних та кіберсистемах своїх і противника;

• планування, організацію та координацію розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій у КП (Cyberspace Operation) та кібероперацій (Cyber Operation);

• організацію та координацію кібернетичних, електронних, мережевих, інформаційних, когнітивних і психологічних дій у КП (включаючи соціальні мережі).

Особливістю підготовки фахівців оперативного рівня на цей час, у тому числі фахівців з КБ, які закінчили ВВНЗ за галуззю знань 12 – «Інформаційні технології» та спеціальністю 125 – «Кібербезпека», є їх підготовка в межах галузі знань 25 – «Воєнні науки, національна безпека, безпека державного кордону». Спеціальність «Кібербезпека» в цій галузі знань відсутня. Найбільш споріднена підготовка здійснюється за спеціалізацією «Управління інформаційною безпекою у військовій сфері» в межах спеціальності 254 – «Забезпечення військ (сил)», де проводиться підготовка всіх спеціалізацій за напрямом ІТ [17]. Такий підхід не є раціональним для формування фахівця ІТ оперативного рівня. Доцільно інтегрувати підготовку в межах окремої спеціальності з подальшим поділом на спеціалізації.

Аналіз професійних стандартів та освітньо-професійних програм усіх спеціальностей та спеціалізацій офіцера оперативного рівня показав наявність компетенції з володіння ІТ під час вирішення професійних завдань. При цьому в компетенціях цілковито відсутні згадки про питання КБ і КО. За сучасних умов таке нехтування питаннями КБ і КО не є прийнятним і потребує виправлення. Це викликає необхідність введення базового курсу основ КБ у військовій сфері для всіх спеціальностей та поглибленого курсу для фахівців ІТ та КБ (*рис. 1*).

Для базового курсу основ КБ у військовій сфері змістом навчання варто передбачити питання національного та відомчого законодавства у сфері КБ і КО держави, склад сил та засобів КБ і КО, їхні завдання, можливості, форми та способи застосування, основи планування, підготовки та проведення кібернетичної операції ЗСУ, організації системи КБ у військових частинах та органах військового управління.

Для фахівців ІТ та КБ доцільно запропонувати поглиблений курс КБ у сфері безпеки і оборони за спеціалізаціями з урахуванням подальшого посадового призначення, а змістом їхнього навчання визначити:

• вивчення міжнародних та відомчих стандартів у сфері КБ та КО;

• зміст, завдання, форми організації КО держави;

• критичну кібер- та інформаційну інфраструктуру держави;

• структуру та принципи управління глобальною мережею Інтернет, телекомунікаційними мережами, соціальними мережами;

• склад сил і засобів КБ та КО держави, їхні завдання, можливості;

• основи підготовки та ведення КО держави та кібернетичної операції ЗСУ;

• форми та способи застосування військових частин і підрозділів КБ під час здійснення КО держави, кібернетичної та інших операцій ЗСУ та угруповань військ;

• методи роботи посадових осіб з КБ органів військового управління, командирів військових частин та установ КБ під час виконання завдань у мирний час, в особливий період та за умов воєнного стану.

Наступним, третім рівнем, є стратегічний рівень підготовки (*рис. 1*), особливістю якого є підготовка фахівців усіх родів, видів військ та відомств у межах галузі знань 07 – «Управління та адміністрування» спеціальності 074 – «Публічне управління та адміністрування» та спеціалізації «Управління у воєнній сфері» у Національному університеті оборони України імені Івана Черняховського. Такий підхід дає можливість досягти якісної міжвидової та міжвідомчої підготовки вищих керівників СБОУ, сформувати єдину систему поглядів на питання національної безпеки і оборони держави, у тому числі на питання КБ і КО держави.

Проведений аналіз стандартів підготовки фахівців стратегічного рівня підготовки також показав відсутність компетенції випускника з питань КБ і КО держави, у зв'язку із чим вважаємо за необхідне доповнити нею перелік компетенцій випускника. Для реалізації зазначеної компетенції слухачі повинні засвоїти зміст дисципліни «Кібербезпека та кібероборона держави», змістом якої має бути:

• вивчення основ забезпечення КБ та КО держави;

• склад сил і засобів КБ та КО СБОУ, їхні завдання, можливості, форми та способи застосування;

• основи підготовки і ведення КО держави та спеціальних операцій у КП;

• методи роботи посадових осіб під час підготовки і ведення КО держави та спеціальних операцій у КП;

• аудит і оцінювання стану КБ на державному рівні.

Важливим інструментом підготовки фахівців з КБ оперативного та стратегічного рівнів є впровадження

системи комплексних тактичних та оперативних задач із відпрацювання питань підготовки та бойового застосування військових частин та органів військового управління КБ та КО. Ці задачі повинні бути розроблені на загальному оперативному і стратегічному фоні, що використовується в Національному університеті оборони України імені Івана Черняховського, та інтегровані в загальний зміст навчання. Наступним кроком практичної підготовки є впровадження у ВВНЗ та органах військового управління системи комплексних командно-штабних і тактико-спеціальних навчань з питань КБ і КО. Подібні навчання є найбільш доцільним і раціональним способом отримання практичного досвіду застосування сил та засобів КБ і КО держави.

Четвертим етапом підготовки є постійно діюча система курсової підготовки (*рис. 1*). Вона виконуватиме функції підтримуючої та тренувальної системи між рівнями підготовки. Безумовно, її повноцінне функціонування потребуватиме постійного збирання, аналізу, систематизації та впровадження у зміст курсів з питань КБ усіх основних досягнень та інновацій у цій сфері, створення баз даних і сайту, з якого можливо отримати доступ до спеціалізованих курсів, постійного моніторингу контенту з питань КБ, виявлення нових загроз і ризиків та реакції на них у вигляді спеціально розроблених курсів. Важливе місце під час реалізації курсової підготовки буде мати можливість дистанційного навчання.

Висновки. В умовах виконання завдань, визначених МОУ та ЗСУ Стратегічним оборонним бюлетенем України, запропонована система освіти з питань КБ і КО являє собою комплексне та гнучке рішення проблемного питання підготовки фахівців для всіх складових СБОУ. Підготовка фахівців ґрунтується на знаннях, отриманих під час здобуття середньої освіти, і нарощуватиметься під час навчання у ВВНЗ до рівня, необхідного для виконання завдань за призначенням. Її впровадження дасть змогу досягти єдності поглядів на застосування складових СБОУ та сумісності між ними. Запропонована система для підготовки фахівців СБОУ дасть можливість сформувати й підтримувати актуальність компетентності випускників з питань КБ і КО для виконання завдань за призначенням упродовж усього терміну служби в умовах перенесення бойових дій в інформаційний та КП.

Питання, що розглядаються в статті, є важливими і потребують конструктивного діалогу між усіма причетними до них фахівцями військових університетів, академій та інститутів МОУ, інших військових формувань, правоохоронних органів України з метою вдосконалення та розвитку підготовки військових фахівців з питань КБ і КО, формування єдиного сучасного змісту їхнього навчання, який відповідає реаліям сьогодення і налаштований на майбутнє.

Перелік літератури

1. Щорічний звіт Генерального секретаря НАТО за 2016 рік / NATO Public Diplomacy Division / 1110 Brussels – Belgium [Електронний ресурс]. – Режим доступу : https://ukraine-nato.mfa.gov.ua/ua/inform-center/nato-activities/shhorichnij-zvit-generalynogo-sekretarya-nato-za-2016-rik/.

2. *Присяжнюк М. М., Цифра Є. І.* Особливості забезпечення кібербезпеки / М. М. Присяжнюк , Є. І. Цифра // Реєстрація, зберігання та обробка даних. – 2017. – Т. 19. – № 2. – С. 61–68.

3. *Діордіца І.* Кваліфікаційні вимоги до компетенцій фахівців із кібербезпеки / І. Діордіца // Підприємництво, господарство і право. – 2017. – № 2. – С. 215-219.

4. *Бистрова Б. В.* Особливості формування системи професійної підготовки бакалаврів з кібербезпеки у ВНЗ США / Б. В. Бистрова // Вісник Черкаського університету. – 2017. – № 6. – С. 15–18.

5. *Бурячок В., Богуш В.* Рекомендації щодо розробки та запровадження профілю навчання «Кібернетична безпека» в Україні / В. Бурячок, В. Богуш // Інформаційна безпека. – 2014. – № 2 (20). – С. 126-131.

6. *Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа В. С.* Інформаційна та кібербезпека: соціотехнічний аспект / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, В. С. Толюпа . – К. : ДУТ, 2015. – 288 с.

7. *Мельник С.* Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки / С. Мельник // Педагогічні науки: теорія, історія, інноваційні технології. – 2016. – № 10 (64). – С. 79-88.

8. Указ Президента України № 240/2016 «Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України» від 6 червня 2016 р.

9. Указ Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 р.

10. Закон України Про основні засади забезпечення кібербезпеки України // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.

11. Закон України «Про оборону України» // Відомості Верховної Ради України. – 1992. – № 9. – Ст. 106.

12. Україна ефективно співпрацює з НАТО у галузі кібербезпеки – Президент [Електронний ресурс]. – Режим доступу : http://www.mil.gov.ua/news/2017/07/10/ukraina-efektivno-spivpraczyue-z-nato-u-galuzi-kiberbezpeki---prezident/.

13. Cybersecurity Education & Career Development [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/topic/cybersecurity-education-career-development (дата звернення – 03.11.2018).

14. Royal Military College of Canada [Електронний ресурс]. – Режим доступу : https://www.rmc-cmr.ca/en (дата звернення – 27.04.2018).

15. Військова Технічна Академія імені Ярослава Домбровського [Електронний ресурс]. – Режим доступу : http://www.wat.edu.pl. (дата звернення – 27.04.2018).

16. Universität der Bundeswehr M?nchen [Електронний ресурс]. – Режим доступу : https://www.unibw.de/home (дата звернення – 27.04.2018).

17. Постанова Кабінету Міністрів України № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29 квітня 2015 р.