УДК 371 (378)

Юрій Даник,
доктор технічних наук, професор,
ORCID ID 0000 0001 6990 865
Андрій Зінченко,
доктор технічних наук, доцент,
ORCID ID 0000 0002 4734 3401
Національний університет оборони України
імені Івана Черняховського

КІБЕРОСВІТА ТА ЇЇ ОСОБЛИВОСТІ

У статті проведено аналіз формування та розвитку кіберосвіти в Україні та у світі. Доведено, що в сучасних умовах знання з кібербезпеки у тих хто навчається повинні формуватися в рамках базових курсів всіх без винятку навчальних закладів, а не тільки спеціалізованих за ІТ та кібер- напрямами. Для систематизації та удосконалення підготовки у сфері кібербезпеки авторами розроблено варіант реалізації організації системи освіти з питань кібербезпеки. Він охоплює всі рівні освіти від дошкільної та середньої до вищої та післядипломної. Для закладів освіти сектору безпеки та оборони запропоновані і практично апробовані цілісна, послідовна, взаємопов'язана та безперервна система підготовки з питань кібербезпеки та кібероборони та зміст навчання для її реалізації. При цьому передбачається поетапне та безперервне формування, у тих хто навчається, необхідних у сучасному суспільстві знань і компетенцій з питань кібербезпеки.

Ключові слова: *національна безпека і оборона; кіберзагрози; кібербезпека; кібероборона; кіберосвіта; освіта; заклад вищої освіти.*

Постановка проблеми. На протязі останніх десятиліть суспільство знаходиться у стані революційних змін і перетворень в інформаційній сфері. Стрімкий розвиток та масове впровадження продуктів сучасних інформаційних технологій (ІТ) призвело до формування нового спектру ризиків і загроз національній безпеці і обороні держав, які реалізуються у кіберпросторі та (або) через кіберпростір (КП). КП вже став офіційно визнаним п'ятим (додатково до чотирьох природних: суходільного, морського повітряного та космічного) простором, що штучно сформувався та фактично перетворився на окрему сферу різноманітної діяльності людства, протистояння і боротьби між державами, державними та недержавними акторами, включаючи воєнні та інші конфлікти і збройне протиборство.

Перше офіційне визначення КП було дано військовими експертами США в настанові КНШ 2006 року "Інформаційні операції": "Кіберпростір – сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), що використовують широкий діапазон електромагнітного спектра частот для прийому, передачі, обробки, зберігання, перетворення і обміну інформацією, і пов'язана з ними інформаційна інфраструктура ЗС США". За визначенням Чіпа Морнінгстара і Ф. Рендалла Фермера, КП визначається скоріше соціальними взаємодіями, а не його технічною реалізацією [1]. На їхню

думку, обчислювальне середовище в КП є доповненням каналу зв'язку між реальними людьми. Основною характеристикою КП є те, що він пропонує середовище, що складається з багатьох учасників, здатних впливати один на одного. Уряди провідних країн світу відносять взаємопов'язані ІТ і взаємозалежну мережу інфраструктур інформаційних технологій КП до національної критичної інфраструктури. Кібернетичні загрози (КЗ) охоплюють всі базові сфери суспільної діяльності: політичну, воєнну, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну, технологічну тощо. При цьому для кожної з них є як спільні вразливості так і свої особливості, які так само як і загрози знаходяться у постійному розвитку. Тому вирішення проблеми забезпечення кібербезпеки (КБ) у сучасних умовах і особливо на перспективу викликала гостру потребу у високопрофесійних фахівцях з питань КБ. Актуальність ефективного вирішення проблеми загальної кіберосвіти населення та підготовки професіональних фахівців з питань КБ постійно зростає.

Аналіз досліджень і публікацій. Директор Національної розвідки США, Дэн Куат, назвав КБ своїм "найбільшим клопотом", який випередив зброю масового ураження та тероризм. Журнал Cyber Education, що видається Cyber Innovation Center США, констатує: "Сьогодні наша країна наражається на нестачу робітників у сфері КБ. Фактично, у нас більш 380 000 робочих місць у сфері КБ. Їх кількість зросте до 1 мільйона у 2020 році. Нестача кваліфікованих фахівців у галузі КБ представляє великий ризик не тільки для національній безпеки, але і для нашої економічної безпеки. Для того щоб зберегти наше місце, у якості світового лідера, США повинні сьогодні вирішити проблему кібернетичної робочої сили".

Найбільш інтенсивно в цій сфері діють КНР, Ізраїль, Японія, РФ, США та країни-члени НАТО. Питання кіберосвіти є невід'ємною складовою забезпечення кібербезпеки і кібероборони (КО) будь-якої держави. Вони знайшли своє відображення в роботах Дж. Треглія, М. Делія, Ш. Костігана, Дж. Маршалла, Дж. Антонакоса, М. Корби, Р. Гоэля, Э. Херда, К. Камински, Н. Кайла, Д. Момота, М. Хеннесси, С. Найта, Д. Керигана-Кайру, Ф. Ларка, К. Палляриса, Д. Педера Багге, Р. Росса, Д. Романа, Н. Спину, Т. Тагарева, Р. Тейлора и Д. Вана. Але, як свідчить проведений аналіз відомих публікацій, єдина система, методологія та зміст навчання з питань підготовки фахівців у галузі КБ і загальної кіберосвіти досі не сформувалися.

Також при розробці методології освіти в галузі КБ необхідно враховувати ряд особливостей притаманних сучасним ІТ: швидка зміна електронних, кібернетичних та інфокомунікаційних технологій; постійне зростання можливостей впливу на складові кібернетичних систем; необхідність постійного оновлення знань з питань КБ; різні рівні здатності та готовності до навчання, тих хто навчається, у тому числі і дистанційного; особливості курсу КБ; велика кількість специфічних складових КБ. Це спонукало авторів до дослідження шляхів удосконалення теоретичних основ

КБ, а до розробки та апробації методологічних основ освіти за напрямком КБ, як комплексного та безперервного процесу.

Метою статті є формування системи, змісту та методології навчання питанням кібербезпеки (кіберосвіти) у закладах освіти України.

Методи дослідження – аналіз; синтез; класифікація та систематизація теоретичних даних; конкретизація теоретичного та практичного знання, щодо підготовки фахівців з КБ та КО; індукція та дедукція; порівняльний аналіз отриманих теоретичних матеріалів.

Виклад основного матеріалу. Важливим аспектом формування системи освіти фахівців з питань КБ є вивчення та дослідження міжнародного досвіду провідних країн світу (ПКС), у першу чергу США, де питанням підготовки фахівців КБ та загальної кіберосвіти населення приділяється надзвичайна увага. Так у складі Департаменту внутрішньої безпеки (Department of Homeland Security's (DHS)) США сформовано відділ освіти та підвищення освіченості з питань КБ [2]. Яким відпрацьовано та прийнято ряд документів:

1. Національна програма підвищення освіченості з питань КБ. Мета програми – сприяти індивідуальній кібернетичній стійкості та освіченості населення з питань КБ, розумінню КЗ та простих дій щодо їх нейтралізації.

2. Національна програма розвитку професіоналізму та розвитку персоналу. Мета програми – сприяти підготовці фахівців з КБ, які володіють необхідними знаннями, навичками та здатні захистити інтереси нації від існуючих та виникаючих проблем у всіх складових КБ.

3. Національна програма освіти та тренінгу у галузі КБ (National Cybersecurity Education and Training Program (NCTEP)). Мета програми – розширити підготовку професіоналів КБ за рахунок створення динамічної освітньої системи, здатної підготувати нове покоління співробітників КБ, які будуть здатні до захисту від існуючих та майбутніх КЗ.

У своєму виступі представник DHS Ноэль Кайл 8 червня 2017 року зазначив: “Щоб ліквідувати розрив між зростаючою потребою у фахівцях з КБ та системою підготовки кваліфікованого персоналу, вкрай важливо, щоб всі спільноти – галузеві організації, федеральні агентства і академічні заклади – з’єднались та прийняли комплексний підхід до координації зусиль у галузі освіти, навчання та працевлаштування фахівців КБ” [3]. DHS веде навчальний каталог розроблених навчальних курсів з вивчення питань КБ за всю країну. Також вирішуються питання розробки єдиної термінології, ведеться повний список задач КБ, знань, навичок та компетенцій необхідних для вирішення цих задач [3]. Це надає змогу реалізувати комплексний підхід у побудові системи підготовки фахівців КБ з єдиним центром управління.

Особливого значення питання кіберосвіти має для сектору безпеки і оборони (СБО) держави. Ефективність застосування військ (сил) оснащених сучасними високотехнологічними засобами озброєння та військової техніки (ОВТ), в найбільшому ступені залежить від якості підготовки особового складу з питань КБ і КО та супроводжується відповідним удосконаленням і розвитком системи військової освіти і науки провідних країн світу (ПКС)

саме з цих питань. Взагалі, експлуатація зразків та комплексів ОВТ, які є кібер-вразливими, мають високу вартість та вирішують особливо важливі завдання особовим складом, який не має необхідного рівня і якості підготовки та не володіє знаннями стосовно сучасних загроз ним, особливо у кіберсфері, не дозволяє ефективно їх застосовувати. При цьому, дуже часто у зв'язку з непрофесійними діями персоналу такі комплекси (засоби) виходять з ладу. Тобто завдання не виконуються і держава несе значні збитки. Тому, в багатьох країнах світу вбачають недостатню якість підготовки військових кадрів, які повинні виконувати завдання з управління військами (силами) і засобами (військова кібернетика) та забезпечити їх раціональне застосування у війнах і збройних конфліктах сьогодення та майбутнього в умовах інтенсивного здійснення деструктивних кібервпливів, однією із основних загроз національній безпеці у сфері оборони.

В ПКС (США, Великобританія, Федеративна Республіка Німеччина, Республіка Польща, тощо) ефективність вирішення зазначених проблем 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 у Військовому університеті технологій (Республіка Польща), де на одній базі зосереджені всі високотехнологічні галузі, спеціальності і спеціалізації підготовки військових фахівців (факультети: національної безпеки, кібербезпеки і криптології, інформатики, електроніки та телекомунікацій, авіації і космонавтики, енергетики, технічної фізики, геодезії і картографії, інженерії безпеки, інженерії матеріалів, механіки і машинобудування, мехатроніки, управління тощо) та наукових досліджень за цими напрямами [4]. Теж саме реалізовано 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) та в аналогічних навчальних закладах інших країн-членів НАТО [5, 6]. За рахунок такої інтеграції забезпечують позбавлення 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 та оборони держави в рамках єдиних стандартів. В них зосереджена

підготовка всіх фахівців, які виконують свої функції в кіберпросторі або через кіберпростір.

Проведений аналіз публікацій вітчизняних авторів (Бурячок В.Л., Хорошко В. О., Присяжнюк М. М., Цифра Є. І., Діордиця І., Бистрова Б. В., Богуш В., Мельник С., основним змістом робіт, яких є спроба окреслити кваліфікаційні вимоги до фахівців із КБ), та державного стандарту підготовки фахівців за спеціальністю 125 – "Кібербезпека", дозволив встановити, що єдина раціональна система та методологія підготовки фахівців з КБ в Україні досі остаточно не сформовані [7 – 10]. Крім того, світова практика показує, що в сучасних умовах необхідно переходити від підготовки фахівців з питань КБ у рамках закладу вищої освіти (ЗВО) до підготовки кожного громадянина (особистості) з цих питань на протязі всього життя.

Автори пропонують структурувати підготовку з питань КБ за етапами або рівнями освіти прийнятими у державі (Рис. 1). Перший етап розпочинається на рівні дошкільної освіти. Саме у цьому віці людина починає сприймати електронні 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, у вигляді коміксів, тощо, потрібно надати розуміння відповіді на питання: "Що і чому не можна робити з електронними (інфокомунікаційними) девайсами?". 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 КБ повинна займати підготовка батьків та вихователів. Для цього доцільно використовувати різні он-лайн та дистанційні курси навчання. Наприклад, у рамках програми NCTEP пропонується ряд розваг та комп'ютерних ігор для дітей [2].

Для практичної реалізації першого (дошкільного) етапу навчання з питань КБ, доцільно ввести до варіативної дисципліни "Комп'ютерна грамота" [11] курс "Елементарна кібергігієна", який повинен розроблятися фахівцями у галузі дошкільної освіти у тісній співпраці з фахівцями всіх напрямів КБ.

Другим етапом підготовки з питань КБ є підготовка у шкільному віці. При цьому її можливо розділити на декілька курсів за рівнями шкільної освіти: початкова середня освіта, базова середня освіта та старша школа. На цей час, як показав аналіз діючих державних стандартів та програм навчання середньої школи з дисципліни "Інформатика", питання КБ в них не згадуються взагалі [11]. Для початкової середньої освіти підготовка з питань

КБ повинна стати продовженням дошкільної підготовки на більш високому рівні уявлення (курс “Кібергігієна та початкова КБ”). Одночасно доцільно почати надавати знання та формувати первинні навички правильного та безпечного користування простими інформаційними (інфокомунікаційними) системами та програмним забезпеченням встановленим на гаджетах (девайсах).

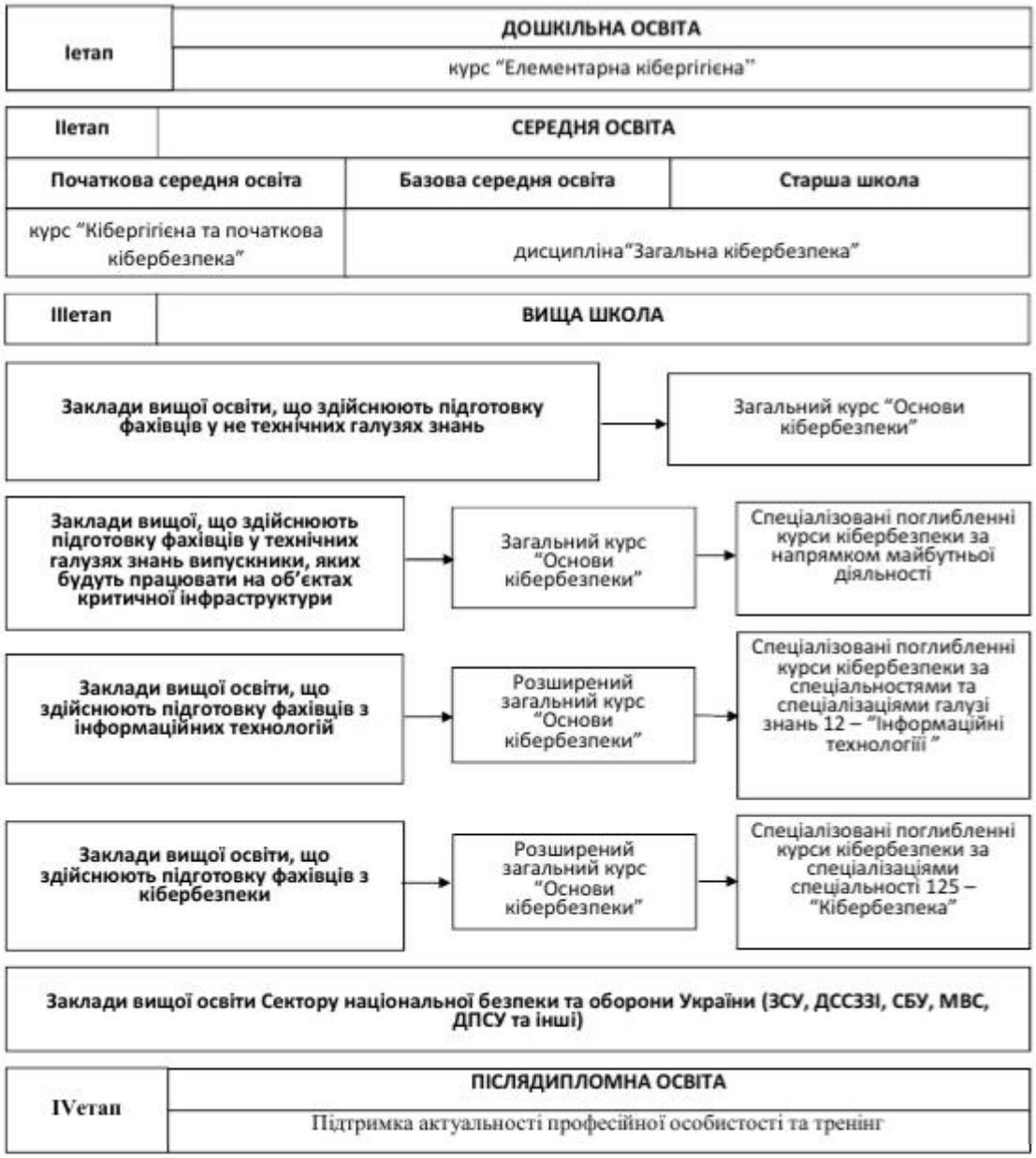

Рис. 1 Система кіберосвіти України.

Для базової середньої освіти та старшої школи вважається за доцільне включити питання КБ у самостійну дисципліну “Загальна КБ” 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 КБ та інші питання. Ще одним

завданням старшої школи є формування правильної уяви про можливу для учня майбутню професію фахівця з КБ, виявлення здібних та надання їм поштовху до розвитку.

Наступним, третім етапом підготовки з питань КБ, є підготовка фахівців у ЗВО. ЗВО умовно можливо розділити на 4 групи. Перша група, це заклади які здійснюють підготовку у галузях знань, що охоплюють гуманітарні, природничі та інші науки, не пов'язані з поглибленим вивченням ІТ. Друга група, це ЗВО, які здійснюють підготовку фахівців технічних галузей з поглибленим вивченням ІТ, які будуть працювати на об'єктах критичної (з точки зору КЗ) інфраструктури держави. Третя група, це ЗВО, які здійснюють підготовку фахівців у галузі знань 12 – "Інформаційні технології", за винятком спеціальності 125 – "Кібербезпека". Четверту групу складають ЗВО, які готують фахівців з КБ за спеціальністю 125 – "Кібербезпека".

Аналіз державних стандартів і навчальних планів підготовки ЗВО першої та другої груп показав, що серед компетенцій випускника є вміння використовувати ІТ під час вирішення завдань за профілем підготовки. Одночасно, встановлено повну відсутність у змісті навчання питань КБ. Вважається необхідним доповнити зміст навчання випускників першої групи ЗВО базовим курсом "Основи КБ". Передбачається, що випускники ЗВО, які відносяться до другої групи, будуть працювати на підприємствах та організаціях різних сфер економіки. Значний відсоток із них працюватиме на об'єктах, які відносяться до критичної інфраструктури держави у важливих для національної безпеки сферах: енергетика, машинобудування, транспорт, економіка, паливно-енергетичний комплекс та інші. Вони будуть експлуатувати об'єкти з потужними кіберінфокомунікаційними складовими, у тому числі з критичною кібер-інформаційною інфраструктурою. Тому вважається за доцільне ввести до державних та професійних стандартів їх підготовки компетентності випускника за напрямком КБ. Для їх формування доцільно викладати базовий загальний курс основ КБ для спеціальностей всіх галузей знань та спеціалізовані курси за напрямками майбутньої діяльності. Наприклад, "КБ в сфері енергетики", "КБ в сфері транспорту", "КБ в сфері інфраструктури", "КБ в сфері економіки", "КБ в банківській сфері", "КБ соціальних та соціотехнічних систем" та інші. Такий підхід дозволить гідно відповісти викликам часу на фоні подальшої глобалізації та інформатизації суспільства, коли ІТ стають засобом виробництва практично для кожної професії.

Наступна група ЗВО здійснює підготовку у галузях знань: 12 – "Інформаційні технології"; 15 – "Автоматизація та приладобудування"; 17 – "Електроніка та телекомунікації". Підготовка цих фахівців повинна відрізнятися більш ґрунтовними знаннями порівняно з фахівцями інших галузей знань. Для формування єдиних поглядів на питання КБ потрібно передбачити загальний курс основ КБ для всіх хто навчається у нормативній частині підготовки та спеціалізовані курси за спеціальностями і

спеціалізаціями у варіативній частині. Впровадження єдиного нормативного курсу з методичним забезпеченням, яке розроблено із врахуванням найкращих світових практик та гармонізовано з термінологію країн-членів ЄС та НАТО, дозволяє уникнути розбіжностей у термінології і поглядах на зміст питань КБ, сформувати однакове розуміння проблем забезпечення КБ, уніфікацію і стандартизацію підготовки з провідними країнами світу, можливість ефективно співпрацювати в єдиному інформаційному і кібер-просторах.

Четверта група ЗВО безпосередньо готує фахівців з КБ. Основну змістовну частину навчального плану для таких фахівців повинні складати органічно пов'язані між собою дисципліни з КБ та інфокомунікаційних технології. Без глибокого розуміння сутності сучасних високих, в тому числі і інформаційно-телекомунікаційних технологій, підготовка фахівця у галузі КБ неможлива. Тому необхідно підготовку фахівця, яка притаманна 3 групі ЗВО, розширити спеціалізованими курсами за складовими КБ. Змістом навчання для тих, хто навчається, повинні бути питання: загальна кібернетика, КП та основи КБ; загрози у кіберсфері; міжнародні і національні організації з КБ, принципи і стандарти з КБ; управління КБ.

До окремої групи можливо віднести ЗВО сектору безпеки і оборони України (СБОУ). Їм притаманні ознаки всіх попередніх груп, але є і специфічні особливості, наприклад, підготовка фахівців СБОУ в рамках трирівневої (тактичний, оперативний та стратегічний рівні) системи підготовки.

Аналіз питань підготовки фахівців кібербезпеки СБОУ висвітлив аналогічну (так само, як і в цивільних ЗВО) проблему відсутності єдиної методології та сформованої системи підготовки фахівців з питань КБ і загальної кіберосвіти всіх військових фахівців. Відсутність єдиних керівних документів, методичного забезпечення навчання, розбіжність у поглядах на мету, завдання і зміст підготовки з питань КБ у ВВНЗ знижує ефективність та якість підготовки фахівців для СБОУ в цілому. Особливо яскраво це проявилося з початком "гібрідної війни" проти України, в якій значна частка протиборства відбувається в інформаційному, когнітивному та кібернетичному просторах.

З метою реалізації комплексного і гнучкого підходу до підготовки фахівців КБ і КО були розроблені та апробовані система підготовки фахівців СБОУ з питань КБ (Рис. 2) і зміст навчання для її реалізації у навчальних планах закладів вищої освіти СБОУ.

На тактичному і оперативному рівнях 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 КБ і у достатній мірі розумілися щодо особливостей реалізації політики КБ, як у сфері оборони держави, так і на національному і міжнародному рівнях, а фахівці з високотехнологічних напрямів отримали повні і всебічні сучасні

знання з питань КБ і КО, їх організації і управління ними в сфері оборони з врахуванням кращих практик країн-членів НАТО.

Для всіх високотехнологічних спеціальностей і спеціалізацій підготовки фахівців тактичного рівня доцільно ввести у нормативну частину базовий курс з питань КБ та у варіативну частину спеціалізовані курси з КБ за складовими КБ. Для цього у зміст навчання вводяться навчальні дисципліни або блоки навчальних дисциплін, які охоплюють питання: загальної та військової кібернетики, кіберпростір та його особливості, загрози і ризики у кібернетичній сфері; основи інформаційної-, КБ і КО, 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 в сфері безпеки та оборони.

Розуміння тими хто навчається питань виникнення і формування КП, його структурних компонентів, архітектури та особливостей, дозволяє зрозуміти і засвоїти в чому полягає феномен і парадигма КБ, закласти основи знань для всього подальшого вивчення питань КБ. При цьому, розглядаються основи методології аналізу ризиків в області інформаційної та кібер- безпеки і вивчаються типові підходи до оцінки їх забезпечення, в тому числі ті, що засновані на управлінні ризиками. Окремим блоком подаються питання функціонування і 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 уразливостей є базовими для формування навичок розробки стратегії та архітектури КБ, запобігання, обмеження та нейтралізації відомих і невідомих уразливостей та загроз, управління кібернетичними ризиками з метою їх зниження. Огляд уразливостей, характерних для КП, форм, способів, засобів використання таких уразливостей, основний спектр різноманітних сценаріїв та технологій кіберрозвідки, кіберзахисту або активного впливу (несанкціонованого проникнення, отримання інформації, зміни алгоритмів діяльності тощо) сформує у тих хто навчається вміння оцінювати ризики деструктивних впливів, в тому числі і пов'язаних з використанням мобільних девайсів (гаджетів), іншими технологіями і системами, що пов’язані з мобільністю.

Важливою складовою підготовки фахівців з питань КБ є вивчення ними: світового і вітчизняного досвіду створення і розвитку систем КБ та їх 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 та національних стандартів у галузі КБ; особливості формування національної політики з КБ, найкращих світових практик у вирішенні зазначених питань та тенденцій їх розвитку; загальної системи та структури міжнародних і національних організацій у сфері КБ, їх завдання, організаційна структура, повноваження, задачі, функції, розподіл

повноважень між ними; організація та характер взаємодії з національними організаціями з КБ; міжнародні та національні правові аспекти забезпечення КБ та відповідальності за здійснення деструктивних впливів у кібернетичному просторі та їх наслідки.

Підготовка фахівців за високотехнологічними напрямами, фахівців КБ та всіх інших військових фахівців з вищенаведених базових питань КБ відрізняється лише шириною та глибиною їх подання, але охоплює їх всі без винятку.

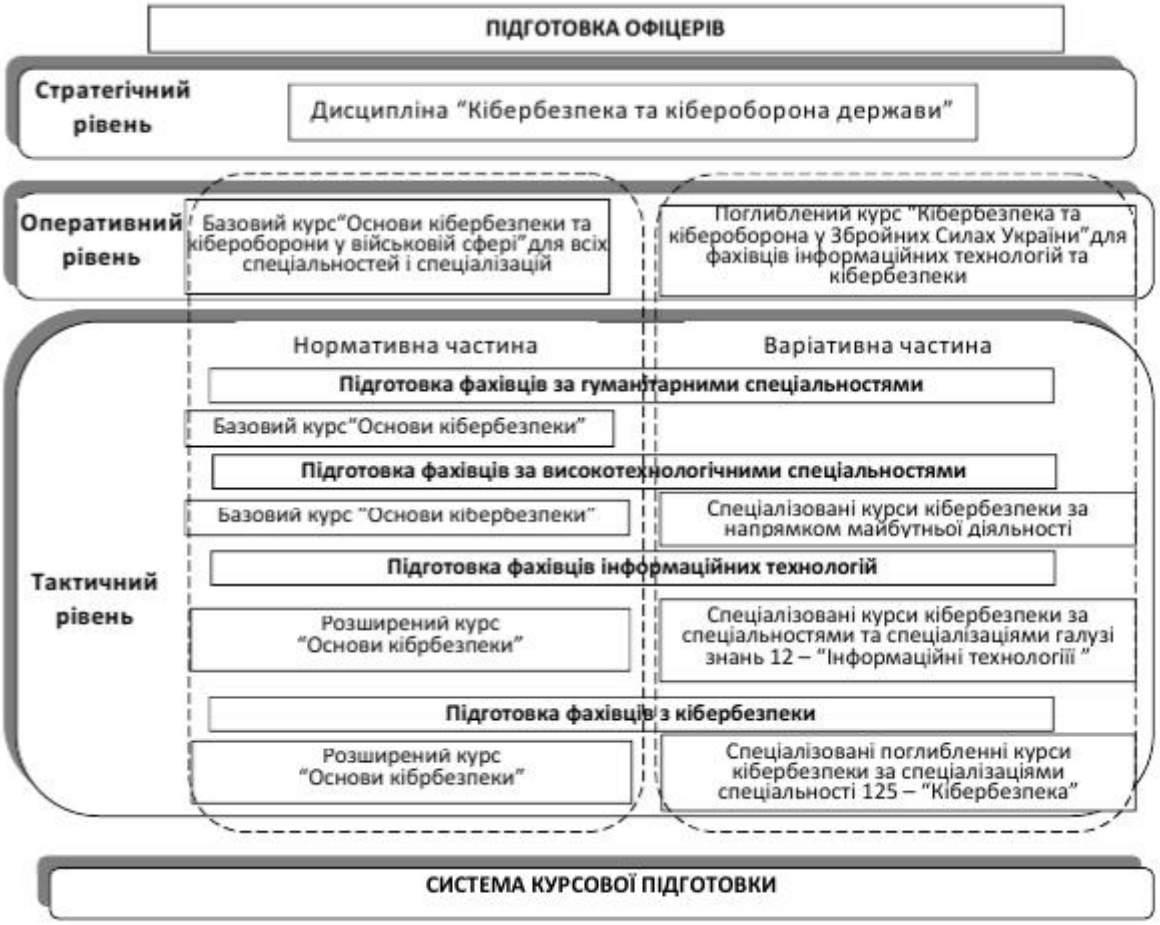

Рис. 2 Система підготовки фахівців СБОУ з питань КБ і КО.

Компетентності з питань КБ, необхідні для виконання завдань за посадами випускниками ВВНЗ – фахівцями з КБ, будуть закладатися при вивченні питань управління КБ у сфері оборони у рамках варіативних дисциплін. На основі попередньо засвоєних тими хто навчається базових питань КБ здійснюється їх підготовка до виконання завдань за посадою командира підрозділу військової частини КБ або офіцера з КБ органу військового управління. Для цього вони вивчають основні КЗ у воєнній сфері, відомчі нормативні акти з питань КБ і КО, змістом, завданнями та складовими частинами КО, силами та засобами КО, формами і способами бойового застосування підрозділів кібервійськ та вимогами до їх спроможностей, досвідом їх підготовки і застосування, у тому числі за прикладами ПКС, методами роботи посадових осіб та методиками планування застосування підрозділів кібернетичного захисту у мирний час і в

особливий період, усвідомлюють розподіл повноважень з питань КБ і КО між суб'єктами забезпечення КБ, засвоюють особливості підготовки і проведення навчань з КО, аудиту та оцінки КБ на рівні військової частини та органу військового управління.

На підставі визначених в Стратегічному оборонному бюлетені України [12] пріоритетних напрямів розвитку Збройних Сил (ЗС) України з урахуванням досвіду бойових дій на сході України та кращих світових практик у зв'язку з відсутністю раціональної, чітко структурованої системи підготовки військових кадрів за високотехнологічними напрямами від тактичного до стратегічного рівня доцільно реалізувати варіант подібний до кращих практик країн-членів НАТО.

Відповідно світовому досвіду основні зусилля на тактичному рівні для підготовки фахівців за високотехнологічними напрямами необхідно зосередити на інтеграції наукового, науково-педагогічного та матеріально-технічного потенціалів на єдиній базі, шляхом формування об'єднаного ВВНЗ для комплексного проведення наукових досліджень та підготовки фахівців за високотехнологічними галузями, спеціальностями, спеціалізаціями. А саме: інформаційної та КБ, технічних видів розвідки, радіоелектронної боротьби, захисту інформації, криптології, космічних систем, автоматизованої обробки розвідувальної інформації, інформаційно-аналітичної роботи, інформаційно-психологічної протидії, автоматизованих систем управління, систем оперативного управління силами та засобами, інформаційно-комунікаційних систем, геоінформаційних систем, експлуатації та бойового застосування робототехнічних (безпілотних, безекіпажних) систем (комплексів) і комплексів боротьби з ними, спеціальної метрології, енергетики, квантово-оптичних систем, впровадження квантових і нанотехнологій та штучного інтелекту у військовій сфері, зброї, побудованої на нетрадиційних і новітніх принципах тощо. Це дозволить: запобігти дублюванню функцій різними структурами; забезпечити раціональне використання фінансів, кадрових та інших ресурсів; підвищити якість підготовки фахівців з високотехнологічних напрямків для всіх видів ЗС і інших міністерств і відомств СНБОУ; суттєво підвищити ефективність здійснення досліджень, розробки, створення, випробування і застосування інноваційних високотехнологічних систем (зразків) ОВТ.

З цією метою, відповідно досвіду ПКС, такий єдиний, інтегрований дослідницький ВВНЗ у своєму складі повинен мати: освітню складову за високотехнологічними напрямами; потужну систему воєнно-наукових досліджень з науково-організаційною структурою; навчально-наукову, дослідницьку та випробувальну бази (науково-дослідно-випробувальний комплекс високих оборонних технологій) зі стаціонарними та мобільними зразками ОВТ, командними пунктами та лабораторіями; експериментально-бойові підрозділи високотехнологічної спрямованості, які відпрацьовують основи застосування інноваційних високотехнологічних засобів з дослідженням їх бойової ефективності та спроможностей, визначенням

перспективних зразків і напрямів їх подальшого розвитку. Такий інтегрований дослідницький ВВНЗ у сфері високих оборонних технологій, в першу чергу, має концентрувати свою діяльність на дослідженні: концепцій, стратегій, проблем і особливостей війн сучасності (4GW, гібридних війн тощо) та тих, які прогнозуються, технологій їх ведення, своєчасного виявлення гібридних впливів у всіх сферах і протидії їм, а також подолання їх наслідків; високотехнологічних аспектів превентивної оборони, як виду стратегічних дій в сучасних умовах [13]; проблем виявлення деструктивних інформаційних, психологічних та когнітивних впливів на військовослужбовців і цивільне населення та протидії ним; методів підвищення психофізичної стійкості та психологічної готовності військовослужбовців до виконання бойових завдань в умовах сучасної (гібридної) війни та профілактики формування у них постравматичних стресових розладів; проблем забезпечення інформаційної (інформаційно-психологічної) та КБ держави з урахуванням особливостей гібридних війн; проблем формування та розвитку стратегічних комунікацій; проблем розвитку та застосування технічних систем розвідки; проблем розробки і застосування засобів радіоелектронного подавлення та ведення радіоелектронної боротьби; проблем створення та бойового застосування систем оперативного управління силами і засобами та автоматизованих систем управління зброєю, систем типу “C2-C5 X…X” (C2, C3, C4ISR тощо); проблем формування, підготовки, високотехнологічного оснащення, забезпечення та застосування ССО; проблем розвитку та застосування когнітивних технологій в інтересах оборони; проблем розвитку та застосування нано- та квантових технологій в інтересах оборони; проблем розвитку та застосування штучного інтелекту в інтересах оборони; проблем застосування космічних систем в інтересах оборони; проблем створення захищених робототехнічних систем (комплексів) (безпілотних авіаційних комплексів, робототехнічних комплексів наземного і морського базування) та їх бойового застосування; проблем боротьби з робототехнічними комплексами противника (безпілотними літальними апаратами (дронами), робототехнічними комплексами наземного і морського базування тощо) [14, 15]; проблем організації та проведення наукових досліджень та випробувань в сфері високих оборонних технологій і підготовки висококваліфікованих військових фахівців для цієї сфери.

Аналіз стандартів підготовки фахівців тактичного рівня СБОУ всіх галузей знань, спеціальностей та спеціалізацій (крім високотехнологічних спеціальностей та спеціалізацій) виявив наявність компетенцій щодо застосування інформаційних технологій за профілем діяльності та повну відсутність компетенцій випускника з питань КБ і КО. Доцільно доповнити нормативну частину навчання базовим курсом (дисципліною, блоком у дисципліні) основ КБ з урахуванням подальшого посадового призначення випускника. Змістом навчання будуть питання: загальна і військова кібернетика, КП та його особливості, загрози і ризики у кібернетичній сфері,

основи інформаційної безпеки, КБ і КО, технологічні, соціо-технічні, інформаційні та інші аспекти КБ і КБ, основні заходи кіберзахисту під час виконання обов'язків за посадою.

Наступними рівнями підготовки є оперативний та стратегічний рівні. Відповідно до світових тенденцій розвитку технологій, ОВТ та воєнного мистецтва всі офіцери, які отримують освіту оперативного та стратегічного рівнів незалежно від галузей, спеціальностей, спеціалізацій підготовки, повинні набути компетенції та володіти знаннями щодо: стану та тенденцій розвитку високих та інформаційних технологій і їх застосування в сфері оборони; інформаційно-аналітичної діяльності в сфері оборони (яка відіграє визначальну роль в арміях країн-членів НАТО) та імітаційного моделювання; організації застосування автоматизованих систем управління військами (силами) (АСУВ(с)) та систем типу C4ISR; організації та застосування технічних систем моніторингу (розвідки) операційного (бойового) простору в інтересах військ (сил); застосування сучасних геоінформаційних технологій та систем в інтересах військ (сил); скритого управління військами та комплексної протидії технічним розвідкам; основ інформаційної безпеки держави у воєнній сфері та захисту інформації; основ КБ у воєнній сфері та КБ; стратегічних комунікацій в сфері оборони.

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, КБ та КО; формування та реалізацію політики МО України та ЗС України щодо дій у КП; виконання заходів зі створення та розвитку інформаційних систем та ресурсів у ЗС України; координацію дій суб'єктів інформаційної, кібер- безпеки та кібероборони МО та ЗС України; розробку стандартів підготовки фахівців з інформаційної, КБ та КО; організацію взаємодії та проведення заходів (в т.ч. щодо підготовки держави до КО) зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами з питань КБ і КО; організовувати та підтримувати взаємодію з 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 їх дій; моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у КП та ефективності дій системи КБ і КО, виявлення уразливостей в інформаційних та кібер- системах своїх і противника; планування, організацію та координацію розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій в КП (Cyberspace Operation) та кібероперацій (Cyber Operation); організацію та координацію кібернетичних, електронних, мережевих, інформаційних, когнітивних і психологічних дій у КП (включаючи соціальні мережі).

Це викликає необхідність введення базового курсу основ КБ і КО у військовій сфері для всіх спеціальностей та поглиблений курс для фахівців ІТ і КБ (Рис. 2). Для базового курсу основ КБ у військовій сфері змістом

навчання будуть питання національного та відомчого законодавства у сфері КБ і КО держави, склад сил та засобів КБ і КО, їх завдання, можливості, форми і способи застосування, основи планування, підготовки та проведення кібернетичної операції ЗС України, організація системи КБ у військових частинах і 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. Змістом навчання буде: вивчення міжнародних та відомчих стандартів у сфері КБ і КО; зміст, завдання, форми організації КО держави; критична кібер- та інформаційна інфраструктура держави; структура і принципи управління глобальною мережею Інтернет, телекомунікаційними мережами, соціальними мережами; склад сил і засобів КБ та КО держави, їх завдання, можливості; основи підготовки і ведення КО держави та кібернетичної операції ЗС України; форми та способи застосування військових частин і підрозділів КБ під час здійснення КО держави, кібернетичної та інших операцій ЗС України і 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 і за воєнного стану.

У слухачів стратегічного рівня необхідно сформувати єдину систему поглядів на питання КБ і КО держави та їх вирішення відповідно до вимог законодавства [16, 17]. Для реалізації цього слухачі повинні засвоїти наступні питання: основи забезпечення КБ і КО держави; склад сил та засобів КБ і КО СБОУ, їх 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 та оцінка стану КБ на державному рівні.

Останнім етапом підготовки є постійно діюча система курсової підготовки (Рис. 1, 2). Вона буде виконувати функції підтримуючої та тренувальної системи між рівнями підготовки. Для її повноцінного функціонування необхідне постійні зібрання, аналіз, систематизація та впровадження в зміст курсів з питань КБ всіх основних досягнень і інновацій в цій сфері, створення баз даних і сайту з якого можливо отримати доступ до спеціалізованих курсів, постійний моніторинг контенту з питань КБ, виявлення нових загроз і ризиків та реакція на них у вигляді спеціально розроблених курсів. Важливе місце під час реалізації курсової підготовки буде мати можливість здійснення дистанційного навчання.

Висновки та перспективи подальших досліджень. Запропонована система освіти з питань КБ представляє собою комплексне і гнучке рішення проблемного питання освіченості суспільства та особистості з питань КБ. Освіта з питань КБ буде починатися з дошкільного навчання та знизить ризики для дітей на етапі їх формування як особистості. Запровадження системи для шкільної освіти наддасть можливість більш якісно підготувати дитину до дорослого життя, життя в високотехнологічному, інформаційному

суспільстві. Впровадження запропонованих змін для системи вищої освіти буде мати системний характер та підвищить конкурентну спроможність випускника на ринку праці. Запропонована система для підготовки фахівців СБОУ дозволить сформувати і підтримувати компетентності випускників з питань КБ і КО для виконання завдань за призначенням в умовах перенесення бойових дій в інформаційний та кібернетичний простір.

Ми не претендуємо "на істину в останній інстанції" та відкриті для обговорення і дискусії з нашими колегами-освітянами військових університетів, академій та інститутів ЗС України, інших військових формувань та правоохоронних органів України з метою удосконалення та розвитку підготовки військових фахівців з питань КБ та КО, формування єдиного сучасного, який відповідає реаліям сьогодення і налаштованого на майбутнє, змісту навчання.

ЛІТЕРАТУРА

1. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки : монографія. Житомир : ЖНАЕУ, 2016. 636 с.
2. Освіта та кар'єра в галузі кібернетики. URL: https://www.dhs.gov/topic/cybersecurity-education-career-development.
3. Daniel Castro. Boosting the Cyberworkforce. *Gavernment Tehnologi*. 2018. URL: https://www.us-ert.gov/sites/default/files/cmd_files/FNR_CGB_MTG_AprilWebenar.pdf.
4. Військова Технічна Академія імені Ярослава Домбровського. URL: https://www.wat.edu.pl.
5. Королівський військовий коледж Канади. URL: https://www.rmc-cmr.ca/en.
6. Universität der Bundeswehr München. URL: https://www.unibw.de/home.
7. Діордиця І. Кваліфікаційні вимоги до фахівців із кібербезпеки. *Підприємництво, господарство і право*. 2017. № 2. С. 215–219.
8. Бистрова Б. В. Особливості формування системи професійної підготовки бакалаврів з кібербезпеки у ВНЗ США. *Вісник Черкаського університету*. 2017. № 6. С. 15–18.
9. Бурячок В., Богуш В. Рекомендації щодо розробки та запровадження профілю навчання "Кібернетична безпека" в Україні. *Інформаційна безпека*. 2014. № 2(20). С. 126–131.
10. Мельник С. Концептуальні основи підготовки майбутніх фахівців з кібернетичної безпеки. *Педагогічні науки: теорія, історія, інноваційні технології*. 2016. № 10(64). С. 79–88.
11. Освітні програми загальної середньої освіти. URL: https://mon.gov.ua/ua/osvita/zagalna-serednya-osvita/navchalni-programi.
12. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 06.06.2016 р. № 240/2016. URL: https://www.president.gov.ua/documents/2402016-20137.
13. Даник Ю. Г., Телелим В. М., Чмельов В. О. Превентивна оборона як вид стратегічних дій. *Наука і оборона*. 2008. № 4. С. 34–41.
14. Даник Ю. Г., Телелим В. М., Радецький В. Г. Питання трансформації оборонних структур держави та удосконалення системи військової освіти. *Наука і оборона*. 2009. № 1. С. 15–19.
15. Даник Ю. Г., Супрунов Ю. М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України. Проблеми створення, випробування та експлуатації складних інформаційних систем. *Збірник наукових праць*. Житомир : ЖВІНАУ. 2011. № 5. С. 5–22.

16. Про основні засади кібербезпеки України : Закон України. *Відомості Верховної Ради України*. 2017. № 45. Ст.403.

17. Про оборону України : Закон України. *Відомості Верховної Ради України*. 2017. № 45. Ст.403.

REFERENCES

1. Danik Y.G., Grishchuk R.V. Osnovy kibernetychnoyi bespeky [Fundamentals of Cybernetic Security] : Monograph. Zhytomyr : ZNAMEU, 2016. 636 p. (in Ukrainian).

2. Osvita ta kar'yera v haluzi kibernetyky [Cybersecurity Education & Career Development]. URL: https://www.dhs.gov/topic/cybersecurity-education-career-development. (in Ukrainian).

3. Daniel Castro. Boosting the Cyber workforce. *Government Technology*. 2018. URL: https://www.us-ert.gov/sites/default/files/cmd_files/FNR_CGB_MTG_AprilWebenar.pdf.

4. Viys'kova Tekhnichna Akademiya imeni Yaroslava Dombrovs'koho [Military Technical Academy named after Yaroslav Dombrovsky]. URL: https://www.wat.edu.pl. (in Ukrainian).

5. Korolivs'kyy viys'kovyy koledzh Kanady [Royal Military College of Canada]. URL: https://www.rmc-cmr.ca/en. (in Ukrainian).

6. Unyversytet Bundesvera Myunkhen [Universität der Bundeswehr München]. URL: https://www.unibw.de/home. (in Ukrainian).

7. Dioritsa I. Kvalifikatsiyni vymohy do fakhivtsiv iz kiberbezpeky [Qualification Requirements for Cybersecurity Specialists]. *Entrepreneurship, Economy and Law*. 2017. № 2. P. 215–219. (in Ukrainian).

8. Bystrova B.V. Osoblyvosti formuvannya systemy profesiynoyi pidhotovky bakalavriv z kiberbezpeky u VNZ SSHA [Features of the formation of the system of professional training of bachelors of cybersecurity in US universities]. *Bulletin of the Cherkasy University*. 2017. № 6. P. 15–18. (in Ukrainian).

9. Buryachok V., Bogush V. Rekomendatsiyi shchodo rozrobky ta zaprovadzhennya profilyu navchannya "Kibernetichna bezpeka" v Ukrayini [Recommendations for the development and implementation of the profile of training "Cybernetics Security" in Ukraine]. *Information Security*. 2014. № 2 (20). P. 126–131. (in Ukrainian).

10. Melnik S. Kontseptual'ni osnovy pidhotovky maybutnikh fakhivtsiv z kibernetychnoyi bezpeky [Conceptual Fundamentals for the Training of Future Cybernetics Specialists]. *Pedagogical Sciences: Theory, History, Innovative Technologies*. 2016. № 10 (64). P. 79–88. (in Ukrainian).

11. Osvitni prohramy zahal'noyi seredn'oyi osvity [Educational programs of general secondary education]. URL: https://mon.gov.ua/ua/osvita/zagalna-serednya-osvita/navchalni-programi. (in Ukrainian).

12. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 20 travnya 2016 roku "Pro stratehichnyy oboronnyy byuleten' Ukrayiny" [About the decision of the National Security and Defense Council of Ukraine dated 20 May 2016 "About the Strategic Defense Bulletin of Ukraine"] : Decree of the President of Ukraine dated June 6, 2016. № 240/2016. URL: https://www.president.gov.ua/documents/2402016-20137. (in Ukrainian).

13. Danik Y.G., Teleim V.M., Chmelov V.O. Preventyvna oborona yak vyd stratehichnykh diy [Preventive defense as a form of strategic actions]. *Science and defense*. 2008. №4. P. 34–41. (in Ukrainian).

14. Danik Y.G., Teleim V.M., Radetsky V.G. Pytannya transformatsiyi oboronnykh struktur derzhavy ta udoskonalennya systemy viys'kovoyi osvity [Questions of Transformation of State Defense Structures and Improvement of the System of Military Education]. *Science and defense*. 2009. №1. P. 15–16. (in Ukrainian).

15. Danik Y. G., Suprunov Yu. M. Deyaki pidkhody do formuvannya systemy pidhotovky kadriv dlya systemy kibernetychnoyi bezpeky Ukrayiny. Problemy stvorennya, vyprobuvannya

ta ekspluatatsiyi skladnykh informatsiynykh system [Some approaches to the formation of a system of training for the system of cybernetic security of Ukraine. Problems of creation, testing and operation of complex information systems]. *A collection of scientific works*. Zhytomyr : ZhVINAU. 2011. №5. P. 5–22. (in Ukrainian).

16. Pro osnovni zasady kiberbezpeky Ukrayiny [About the Basic Principles of Cybersecurity of Ukraine] : The Law of Ukraine. *Information from the Verkhovna Rada of Ukraine*. 2017. № 45. art. 403. (in Ukrainian).

17. Pro oboronu Ukrayiny [About the Defense of Ukraine] : The Law of Ukraine. *Information from the Verkhovna Rada of Ukraine*. 2017. № 45. art. 403. (in Ukrainian).

РЕЗЮМЕ

Юрий Даник,
доктор технических наук, профессор,
Андрей Зинченко,
доктор технических наук, доцент
Национальный университет обороны Украины
имени Ивана Черняховского

Киберобразование и его особенности

В статье проведено анализ формирования и развития киберобразования в Украине и в мире. Доказано, что в современных условиях знания по кибербезопасности у обучаемых должны формироваться в рамках базовых курсов всех без исключения учреждений образования, а не только специализированных на IT и кибер- направлениях. Для систематизации и усовершенствования подготовки в сфере кибербезопасности авторами разработано вариант реализации организации системы образования по вопросам кибербезопасности. Он включает все уровни образования от школьной до высшей и последипломной. Для сектора безопасности и обороны Украины предложены и практически апробированы целостная, последовательная, взаимосвязанная и беспрерывная система подготовки по вопросам кибербезопасности и кибероборони, а также содержание обучения для ее реализации.

Ключевые слова: *национальная безопасность и оборона; киберугрозы; кибербезопасность; кибероборона; киберобразование; образование; учреждение высшего образования.*

SUMMARY

Yuri Danik
Doctor of technical sciences, Professor
Andrey Zinchenko
Doctor of Technical Sciences, Associate Professor
National Defense University of Ukraine
named by Ivan Chernyakhovskyi

Cyber Education and its features

Abstract. Introduction. *The article analyzes the formation and development of cyber education in Ukraine and in the world. The problematic issues of the formation of the system, content and methodologies of cyber-education in Ukraine are revealed. An option for implementing an integrated and continuous education system on cybersecurity has been developed.*

Purpose. *Formation of a methodology, system and content of training on cybersecurity issues (cyber education) in educational institutions of Ukraine.*

Methods. *Theoretical analysis, synthesis, comparison, generalization and forecasting*

Results. *To systematize and improve training in cybersecurity, the authors developed an option for implementing an education system on cybersecurity. It includes all levels of education from school to higher and postgraduate. At the same time, a gradual and continuous formation of knowledge and competence in cybersecurity necessary for the modern information society is envisaged. Particular attention is paid to the formation of these knowledge and competences in higher education institutions of the security and defense sector of Ukraine. An integral, consistent, interconnected and continuous system of training in cyber security and cyber defense at the tactical, operational and strategic levels of training, as well as the content of training for their implementation, has been proposed and practically tested.*

Conclusion. *The proposed system of education on cybersecurity is a comprehensive and flexible solution to the problem question of educating the society and personality on cybersecurity directions. Education on cybersecurity will begin with pre-school education and reduce the risks for children at the stage of their formation as a person. The proposed system for training specialists of the National Security and Defense Sector of Ukraine will enable the formation and support of graduates' competence in cybersecurity and cyber defense for the purpose of performing assigned tasks in the context of the transfer of hostilities to information and cybernetic space.*

Key words: *national security and defense; cyber threats; cybersecurity; cyber defense; cyber-attacks; education; institution of higher education.*