РОЗДІЛ ІІ. ПРОБЛЕМИ ПОРІВНЯЛЬНОЇ ПЕДАГОГІКИ

УДК 378.14(73): 004.056.5 (045)

Богдана Бистрова
Національний авіаційний університет
м. Київ
ORCID ID 0000-0003-1313-8300
DOI 10.24139/2312-5993/2017.08/058-070

ОСНОВНІ ПОНЯТТЯ ДОСЛІДЖЕННЯ ТА КОНЦЕПТУАЛЬНІ ЗАСАДИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ.

Мета статті – публікація результатів дослідження щодо стану процесу професійної підготовки фахівців із кібербезпеки у США. Застосовано теоретичні методи дослідження педагогічних праць. У статті обґрунтовано концептуальні засади підготовки фахівців із кібербезпеки та схарактеризовано нормативно-правові засади щодо галузей знань і спеціальностей, за якими у США здійснюються підготовка й підвищення кваліфікації фахівців із кібербезпеки. Описано виділені ключові терміни та подано їх тлумачення з метою конкретизації й уточнення їх сутнісних значень. Практичне значення дослідження полягає у формуванні уяви про концептуальні засади та термінологічне наповнення навчальних програм з підготовки фахівців із кібербезпеки, які є предметом наших подальших наукових розвідок.

Ключові слова: *ІТ-галузь, кіберзагрози, кібератака, кіберпростір, кіберзахист, інформаційна безпека, кібербезпека, кібербезпекова політика, фахівець із кібербезпеки, концептуальні засади.*

Постановка проблеми. На сучасному етапі розвитку науки й техніки кібербезпека кожної розвинутої держави перетворюється на одну з найважливіших галузей високотехнологічного суспільства. Унаслідок надзвичайно широкого використання сучасних інформаційних технологій у всіх сферах свого існування суспільство стало вразливим від кібернетичних впливів, які все частіше стають ефективним інструментом для досягнення мети несилового контролю та управління як об’єктами інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об’єднаннями. Потоки інформації, що передаються, зберігаються й обробляються в кіберпросторі, постійно збільшуються, що вимагає їх належного захисту від несанкціонованого доступу зі злочинною метою. Безперечним є той факт, що в умовах подальшого розвитку високотехнологічного суспільства потреба у фахівцях із кібербезпеки буде постійно зростати.

Аналіз актуальних досліджень У контексті наукового пошуку вагоме значення мали праці відомих вітчизняних та зарубіжних учених щодо дослідження сучасних процесів глобалізації, інформатизації суспільства, сучасних напрямів підготовки фахівців із кібербезпеки (Г. Глотова, С. Дорогунцов, П. Дракер, І. Діордіц, Д. Дубов, М. Кастельс, К. Мей, Р. Роберт, П. Саух, А. Чернов Р. Шаран та ін.). Проблеми професійної підготовки фахівців за кордоном знайшли висвітлення в дослідженнях вітчизняних науковців з

проблем порівняльної професійної педагогіки Н. Бідюк, А. Глузман, Т. Десятова, В. Коваленко, О. Коваленко, Т. Коржинської, Т. Кошманової, Н. Ничкало, Н. Пазюра, Н. Пацевко, Л. Пуховської, А. Сбруєвої, Н. Собчак, Б. Шуневича та ін. Особливості формування змісту навчання, професійних компетенцій, організаційних форм і технологій професійної підготовки педагогічного персоналу розкрито у працях В. Байденка, Л. Морської, Г. Терещука, В. Чайки, С. Щеннікова та ін. Основні положення порівняльної педагогіки, теорії і методики професійної освіти (О. Алексеєва, О. Арсентьєва, В. Зубик, Л. Зубик, І. Козубовська, Т. Кошманов, Н. Ничкало, Н. Пазюра, І. Пододіменко, В. Поліщук).

Мета статті – публікація результатів дослідження щодо стану процесу професійної підготовки фахівців із кібербезпеки у США, обґрунтувавши концептуальні засади підготовки та схарактеризувавши нормативно-правові засади ІТ-галузі, за якими у США здійснюються підготовка й підвищення кваліфікації фахівців ІТ-галузі з кібербезпеки. Виділити та описати ключові терміни, подати їх тлумачення з метою конкретизації та уточнення їх сутнісних значень; сформувати уяву про концептуальні засади та термінологічне наповнення навчальних програм з підготовки фахівців із кібербезпеки.

Методи дослідження. Застосовано теоретичні методи дослідження педагогічних праць – моніторинг, аналіз, синтез, порівняння та узагальнення наукових, навчально-методичних джерел щодо вивчення концептуальних засад та термінологічне наповнення навчальних програм з підготовки фахівців із кібербезпеки США та вивчення праць за темою вітчизняних і зарубіжних науковців, офіційних і нормативних документів

Виклад основного матеріалу. У сучасних умовах наукового-технічного та технологічного прогресу інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки та визначається складною взаємодією багатьох факторів, серед яких провідне місце займає «фактор людини». Людина є основним носієм і користувачем інформації, вона є основним суб’єктом і об’єктом інформаційної боротьби. Людина є основним творцем і користувачем комп’ютерних систем і мереж (КСМ) та/або телекомунікаційних мереж (ТКМ), саме тому вона є основним суб’єктом і об’єктом кіберборотьби. Кіберпростір, кібернетичні ресурси, комп’ютерно-системна й мережева інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Інформаційна безпека й кібербезпека є невід’ємними складовими кожної зі сфер національної безпеки і водночас ІБ та кібербезпека є важливими самостійними складовими процесу забезпечення національної безпеки [1].

На думку американського дослідника теорії мережевого суспільства професора Каліфорнійського університету Мануеля Кастельса, ядром комунікаційної організації сучасного суспільства є не сама інформація, а

мережева логіка, яка наповнює інформацію якістю та функціями, що системно перетворюють усі основні сфери життєдіяльності людей. Нова комунікаційна система радикально трансформує основні виміри людського життя. У цьому контексті доступ до Інтернету є одним із критеріїв, за яким країни поділяються на високорозвинені та слаборозвинені. Термін «digital divide» (цифрова нерівність) було вперше вжито Білом Клінтоном у 1998 році, який порівняв телекомунікацію з епохою розширення «медіа кордонів» [12].

На рис 1.1 зображено чотирьохкомпонентну структуру Інформації та взаємозв'язок між чотирма її складовими, які з метою безпечного зберігання та передачі інформації повинні знаходитись у рівновазі між собою.

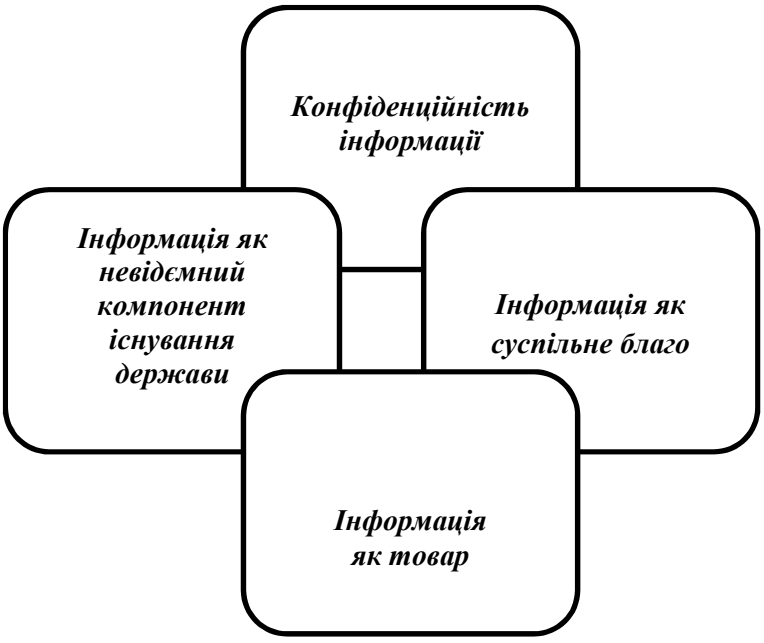

Рис. 1.1. Чотири складові інформації та взаємозв'язок між ними.

Як можна бачити, основними інформаційними компонентами є інформація як невід'ємний компонент існування будь якої держави, інформація як товар, інформація як суспільне благо та конфіденційність інформації. Для досягнення та збереження цієї рівноваги необхідне забезпечення інформаційної та загальної безпеки людини, суспільства, держави з метою протидії тенденціям значного зростання проявів кіберзлочинності й військово-політичного протистояння в кіберпросторі, які в деяких випадках мають ознаки кібервійни, навіть із людськими жертвами. Питання захисту інформаційних активів, що обробляються, зберігаються та передаються в кіберпросторі, а також питання інформаційно-психологічного протиборства повинні вирішувати фахівці з кібербезпеки. Як зазначено в роботі «Кібервійна в перспективі: російська агресія проти України» [2], виданої центром компетенцій НАТО з кіберзахисту – «кібератака» включає не тільки інформаційну війну, але також цифрову пропаганду, DoS-компанії, дефейси web-сайтів, виток

інформації внаслідок атак активістів, а також використання шкідливого програмного забезпечення для шпигунства.

У контексті нашого дослідження необхідно виділити ключові терміни з метою конкретизації та уточнення їх сутнісних значень*: «ІТ-галузь», «кіберзагрози», «кібератака», «кіберпростір», «кіберзахист», «інформаційна безпека», «кібербезпека», «кібербезпекова політика», «ризики», «фахівець з кібербезпеки».* Це допоможе сформувати уяву про термінологічне наповнення навчальних програм з підготовки фахівців із кібербезпеки. Експерти ЮНЕСКО дають визначення *«ІТ-галузі»,* як сукупності обчислювальної техніки, її прикладних програм, а також методів її взаємодії з людьми і промисловим обладнанням. Наступне тлумачення доповнює це визначення: *«ІТ-галузь»* – це сукупність методів, виробничих і програмно-технологічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує збирання, зберігання, обробку, висновок і поширення інформації. Інформаційні технології призначені для зниження трудомісткості процесів використання інформаційних ресурсів.

Термін *«кіберпростір»* означає простір, під яким пропонується розглядати сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах і пов'язаній з ними інфраструктурі, разом із об'єктами, що підпадають під їх контроль та управління.

Важливим для нашого дослідження є термін «кібербезпека». У Великому тлумачному словнику української мови терміни *«кібер»* або *«кібернетичний»* трактуються як такий, що походить від терміну *«кібернетика»,* який створено та працює на основі принципів та методів кібернетики [3, 308]. А термін «безпека» описує стан, коли кому та/або чому-небудь ніщо не загрожує, тобто характеризує відсутність небезпеки [3, 106]. Аргументом щодо даного твердження виступає етимологічне тлумачення двох складових даної правової категорії – кібер та безпека. Дане тлумачення є досить звуженим та не розкриває основної сутності поняття.

Визначення терміну «кібербезпеки» базується на визначенні терміну *«кіберпростір*». На базі порівняння всіх основних просторів «землі», «моря», «повітря», «космосу» як джерел суперництва та могутності, американський фахівець з питань Інтернет-безпеки, пов'язаних із забезпеченням стабільності та стійкості системи доменних імен, а також корпоративної програми безпеки, безперервності та управління ризиками Інтернет-корпорації з присвоєння імен та номерів – ICANN (Internet Corporation for Assigned Names and Numbers) Г. Реттрей (Gregory J. Rattray) доводить, що «кіберпростір» дійсно є новим п'ятим простором як джерело могутності. Як правило, могутність зростає у випадку контролю над ключовими аспектами операційного середовища. Нездатність же отримати доступ до таких аспектів чи неможливість управляти ними може

призвести до обмеження кола політичних, дипломатичних, економічних, військових та інформаційних аспектів могутності» [19].

За тлумаченням ITU (International Telecommunication Union – Міжнародного телекомунікаційного союзу) використовується категорія *«кіберсередовище»*, яке вносить плутанину через тотожність із терміном *«кіберпростір».* Кіберпростір можна розглядати як локальне комунікативне середовище, у випадку функціонування засобу комп'ютерної техніки (КТ), що не підключено до мережі та/або розосереджене середовище, у випадку підключення КТ до локальної та/або глобальної мережі передачі даних (Інтернет) [8]. Отже, термін *«кіберпростір»,* з нашої точки зору, актуальніший для використання в контексті дослідження.

Підґрунтям запровадження терміну «кібербезпека» стало розуміння необхідності вирішення проблеми нейтралізації або мінімізації сукупності кіберзагрози. З технологічної точки зору кібербезпека є складовою частиною інформаційної безпеки, оскільки сутність загроз, методів, засобів і заходів є однаковою та кібербезпека стосується лише кіберпростору. З іншої точки зору термін «Кібербезпека» розглядається як окремий випадок інформаційної безпеки, введення якого обумовлене використанням комп'ютерних систем і мереж (КСМ) та/або телекомунікаційних мереж (ТКМ). «*Кібербезпека» як* безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує, передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам [5, 7]. Аналіз основних факторів, що негативно впливають на функціонування комп'ютерних систем і мереж та/або телекомунікаційних мереж показав, що існує низка чинників, які спричиняють ризики кіберзагрози їх функціонуванню та потребу їх захищеності від кібератак.

У наукових колах чітко дано пояснення терміну *«кібернетична загроза (кіберзагроза)»* – це назва протиправних дій суб'єктів правових відносин ІТ-галузі і назва наявних та/або потенційно можливих явищ і чинників, що створюють небезпеку інтересам людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури [13]. Ми погоджуємося, що таке тлумачення є завершеним обґрунтуванням терміну «*кіберзагроза».*

Наступним ключовим терміном, який належить до компонентів об'єкту нашого дослідження є термін *«кібератака»* як посилений наступ різних кодів і програм на адресу певних користувачів, що як результат несе велику шкоду. Адже атаки, частіше всього, спрямовані на установи та організації, та завдають серйозної шкоди їх діяльності, з довготривалими негативними за своїми результатами наслідками. Крім іншого, існує трактовка терміну «кібербезпека» як стану систем, за яким

нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [4]. Ми підтримуємо думку І. В. Діордіца про те, що дана дефініція є недосконалою через відсутність пояснення, стан якої саме системи мається на увазі [5].

На Рис. 1.1 зображено основні чинники негативного впливу на КСМ та/або ТКМ. До факторів впливу на комп'ютерні системи й мережі та/або телекомунікаційні мережі, що можуть спричиняти ризики та загрози кібератак, відносять неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання й порушення цілісності, конфіденційності та доступності інформації [4].

Рис 1.1. Чинники негативного впливу на комп'ютерні системи та телекомунікаційні мережі.

Міжнародний телекомунікаційний союз у рекомендаціях (International Telecommunication Union Regulations) визначає термін кібербезпека як набір засобів, стратегій, принципів забезпечення безпеки, а також керівні принципи, підходи до управління ризиками, певні заходи й технології, професійна підготовка і практичний досвід, які можуть бути використані для захисту кіберсередовища, інформаційних ресурсів організації та користувача [14]. Важливим, на нашу думку, є те, що професійна підготовка визначається як одна зі складових кібербезпеки, без якої неможлива захищена передача інформації. Ключовою категорією дефініції «кібербезпеки» є «інформація», як основний об'єкт інформаційних відносин, що належать до єдиного кіберпростору. Розуміння необхідності вирішення проблеми нейтралізації

або мінімізації сукупності загроз дало підґрунтя запровадження даного терміну «Кібербезпека». Отже, якщо інформаційна безпека – це стан безпеки інформації, зазвичай організації чи компанії, у тому числі в ІТ-системах, то кібербезпека – це стан захищеності ІТ-систем, тобто обладнання та програм.

Проведений нами аналіз різних точок зору щодо тлумачення цього поняття лише підсилює розуміння того, що кібербезпека має статус самостійної складової національної безпеки. *З нашої точки зору «кібербезпека»* – це комплексна система заходів із боку держави: щодо гарантій стану захищеності людини як основного творця й користувача мережевої логіки (КСМ та ТКМ), як основного суб'єкту і об'єкту кіберзахисту та ІТ-систем, тобто обладнання та програмного забезпечення; запобігання, мінімізації можливості ризиків, спричиненої шкоди та усунення кібератак та створення педагогічних умов підготовки фахівців/професіоналів із кібербезпеки, шляхом забезпечення ефективного навчання та необхідної матеріально-технічної бази для підготовки конкурентоспроможних на ринку праці фахівців із кібербезпеки.

У контексті нашого дослідження необхідно звернутись до терміну «фахівець із кібербезпеки», тому що він є основним суб'єктом і об'єктом кіберборотьби та кіберзахисту. На думку І. Діордіца, «вживаючи термінологічне сполучення *«фахівець із кібербезпеки»* у широкому розумінні, щоб іменувати так осіб, які за родом своєї професійної діяльності можуть використовувати спеціальні знання для попередження потенційних загроз, викриття, нейтралізації або мінімізації наслідків протиправної поведінки правопорушників у комп'ютерному просторі» [6].

Незважаючи на поширене хибне уявлення щодо подібності сфери діяльності та компетенції спеціалістів із кібербезпеки та інформаційної безпеки вони є відмінними. Підтвердженням думки про необхідність розмежування сфери їхньої діяльності та компетенції є спосіб їх сертифікації. У світі існує низка самостійних сертифікацій фахівців з кібербезпеки та ІБ. Найпоширеніші та найбільш популярні сертифікації для фахівців із кібербезпеки: CEH (Certified Ethical Hacker); CISSP (Certified Information System Security Professional); CCSP (Cisco Certified Security Professional) та із інформаційної безпеки: CISA (Certified Information Systems Auditor);

ISO 27001 Lead Implementer; ISO 27001 Lead Auditor [15].

Важливим для нашого дослідження є термін «*кібербезпекова політика»,* як політика надання гарантії національної безпеки у сфері кіберпростору. У формуванні кібербезпекової політики, що має на меті продемонструвати аудиторії як у США, так і на міжнародному рівні серйозність намірів американського керівництва у сфері кібербезпеки, центральну роль відведено Білому Дому. На долю адміністрації Б. Обами припав процес формування, організації та кадрового забезпечення реалізації кібербезпекової політики США. Важливим питанням

кібербезпекової політики американського інформаційного суспільства стало інтенсивне насичення всіх його сфер життєдіяльності висококваліфікованими кадрами.

Проведений аналіз дозволяє стверджувати, що США приділяють велику увагу посиленню національної безпеки, захисту цивільних прав та інтересів бізнесу тому, що науковий, технічний, військовий, фінансовий потенціал та потенціал високих технологій Сполучених штатів Америки є національним надбанням американського народу, що потребує захисту на державному рівні. Концентрація найбільших фінансових компаній, науково-дослідницьких установ та корпорацій, які суттєво впливають на фінансову стабільність і економічний розвиток країни, на створення та розвиток важливих технологічних процесів підсилюють значимість управління кібербезпекою в США. Зауважимо, що однією з особливостей явища кібербезпеки є її бінарний характер. Кібербезпека є елементом національної безпеки і водночас є явищем глобалізованим, оскільки інформаційний простір не має кордонів, тому злочини в цій сфері здебільшого кваліфікуються як транснаціональні [17].

Нормативно-правові засади здійснення підготовки й підвищення кваліфікації фахівців із кібербезпеки у США розробляються на національному рівні урядом країни. Вважається, що в США вперше термін «кібербезпека» було запропоновано в середині 1990-х років, коли уряд зацікавився проблемою і почав її досліджувати. Саме директива адміністрації Президента Білла Клінтона Presidential Decision Directive 63 (PDD 63) «Захист критично важливої інфраструктури» від 22 травня 1998 року започаткувала цілеспрямовану регулярну організаційну діяльність в ІТ- галузі на національному рівні. Цей документ лежить в основі підписаного у 2000 році президентом Клінтоном «Загальнонаціонального плану захисту інформаційних систем». У ньому сформульовані основні напрями діяльності країни й усього суспільства щодо забезпечення кібербезпеки як складової ІБ.

Національну політику країни в цій сфері формує Агентство національної безпеки, а першочергові питання розв’язуються, як правило, на рівні Ради національної та внутрішньої безпеки країни. При цьому кібернетичний захист розглядається АНБ як забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в інформаційно-комунікаційних системах. Крім того, сучасна політика інформаційної безпеки США пов’язана з концепціями інформаційного протиборства і пріоритетами співробітництва у форматі «інформаційної парадигми», що передбачає інформаційно-технологічні переваги держави, здатні зберегти досягнуту в докризовий період стабільність і забезпечити посткризовий розвиток, зробити перебіг соціальних конфліктів більш прогнозованим, запобігти суперечностям у суспільстві [10, 18].

У відповідності до «Національної стратегії досягнення безпеки в кіберпросторі» (National Strategy to Secure Cyberspace), яка означила п'ять пріоритетів діяльності США в ІТ-галузі, та кібербезпеки країни зокрема і розкрила сутність основних завдань у межах цих пріоритетних напрямів на середньострокову й довгострокову перспективу.

Розглянемо основний зміст цих пріоритетних напрямів: *напрям 1* – становлення і розвиток національної системи реагування на події в сфері інформаційної безпеки; *напрям 2* – реалізація комплексної системи заходів щодо зменшення загроз інформаційній безпеці; *напрям 3* – забезпечення підготовки фахівців у сфері комп'ютерної безпеки й забезпечення відповідального ставлення всього населення країни до питань захисту ІТ-систем; *напрям 4* – забезпечення захисту інформаційних систем, що мають відношення до державних органів; *напрям 5* – розвиток різних форм кооперації (у тому числі й міжнародної) у сфері забезпечення інформаційної безпеки [16]. Відповідно до Пріоритетного напряму 3, дії американського суспільства націлені на забезпечення підготовки фахівців у сфері комп'ютерної безпеки й забезпечення відповідального ставлення всього населення країни до національної безпеки. Розвиток відповідального ставлення до ІТ-систем та підготовка кадрів у цій сфері передбачає, що джерелом багатьох вразливостей є недостатньо відповідальне ставлення деяких користувачів, системних адміністраторів і розробників інформаційних систем до питань захисту інформації, їх недостатня поінформованість у цій сфері. Для забезпечення кіберзахисту держави «Національна стратегія досягнення безпеки в кіберпросторі» передбачає реалізацію таких основних заходів: просування багатосторонньої загальнонаціональної програми з інформування та розвитку відповідального ставлення громадян країни до забезпечення безпеки тих інформаційних систем, до яких вони мають будь-який доступ; заохочення створення програм підготовки фахівців, які забезпечили б задоволення потреби в професіоналах; підвищення ефективності існуючих програм підготовки фахівців із кібербезпеки; підтримку зусиль приватних компаній щодо створення, поширення й забезпечення загального визнання сертифікаційних програм у сфері інформаційної безпеки.

Зауважимо, що в контексті підготовки фахівців із кібербезпеки у США є необхідним упровадження «неперервної освіти», яка входить у науковий обіг та стає невід'ємним компонентом освітніх реформ. Неперервна освіта є процесом, що складається з двох послідовних етапів: базової вищої освіти, у формі підготовчого навчання, яке передує професійній підготовці та післядипломна освіта – що відбувається паралельно з практичною діяльністю. Післядипломна освіта «сьогодні вирішує важливу соціальну, економічну, культурну проблему: сприяє розвиткові професійної культури, професіоналізму збільшує

конкурентоспроможність та здатність забезпечити якісну підготовку майбутніх спеціалістів для будь-якої галузі суспільного життя [9].

Фактично «Національна стратегія досягнення безпеки в кіберпросторі» і стала керівництвом до дії державної влади за стратегічними напрямами розвитку цієї галузі. Як наслідок, відбувається модернізація структури державних органів, які забезпечують ІТ-галузь фахівцями зі спеціальності кібербезпеки в країні. Втілення в життя стратегії досягнення ІБ та кібербезпеки за основними державними пріоритетами в цій області є офіційною загальнонаціональною кібербезпековою політикою США [16].

У зв'язку з цим доцільно зазначити, що розповсюдження інформаційних засобів відкриває можливість для розвитку особистості, актуалізує вивчення змін у свідомості людини в постіндустріальному суспільстві США, у якому формується потреба якісного кадрового забезпечення галузей. Глибока зміна особистісних характеристик людини – це процес, властивий сучасному етапу інформатизації суспільного життя у США. Найбільш радикальні гіпотези припускають виникнення нового біологічного виду людини, головною рисою якої є інформаційна потреба. Зусилля, яких повинен докладати професіонал, щоб бути конкурентоспроможним на ринку праці, спонукають його до саморозвитку, самовдосконалення, самоосвіти. У США кібербезпека та інші сфери інформаційної діяльності забезпечують зайнятість 2/3 працездатного населення, а решта працює у виробництві, яке перебуває в залежності від інформації. Структурний перерозподіл зайнятості населення відбувається в бік інформаційної сфери діяльності, сфери захисту інформації та кіберпростору.

Висновки. Проведений аналіз дозволив сформувати уяву про концептуальні засади професійної підготовки фахівців із кібербезпеки. Конкретизовано та уточнено сутнісне значення термінологічного наповнення навчальних програм із підготовки фахівців із кібербезпеки. Також охарактеризовано нормативно-правові засади щодо галузей знань і спеціальностей, за якими у США здійснюються підготовка й підвищення кваліфікації фахівців із кібербезпеки. Виділено чотирьохкомпонентну структуру інформаційної складової як одного з найважливіших елементів забезпечення національної безпеки та підкреслено наявність взаємозв'язку між чотирма її складовими, які з метою безпечного зберігання та передачі інформації повинні знаходитись у рівновазі між собою.

Перспективи подальших наукових розвідок. Предметом наших подальших наукових розвідок є соціально-економічні та політичні передумови становлення системи підготовки фахівців з кібербезпеки в нових умовах життя XXI століття.

ЛІТЕРАТУРА

1. Рудник, Л. І. (2015). *Право на доступ до інформації* (дис. … канд. юрид. наук: 12.00.07) Київ (Rudnyk, L. I. (2015). *The Concept of Information Human Rights* (PhD Thesis). Kyiv).

2. Соснін, О. В. (2005). *Державна політика в галузі управління інформаційним ресурсом України* (дис. … д-ра політ. наук: 23.00.02). Одеса (Sosnin, O. V. (2005). *The state politics in the field of information resource management (DSc thesis).* Odesa).

3. Єрошенко, О. (2012). *Великий тлумачний словник сучасної української мови. Донецьк: ТОВ «Глорія Трейд»* (Yeroshenko, O. (2012). *The great dicionary of modern ukrainian language*. Donetsk: LLC "Gloria Trade").

4. Баранов, О. А. *Про тлумачення та визначення поняття «кібербезпека».* Режим доступу: http://www.ippi.org.ua (Baranov, O. A. *Research of the "cybersecurity" term definition*. Retrieved from: http://www.ippi.org.ua)

5. Діордіца, І. В. (2017). Кваліфікаційні вимоги до компетенції фахівців із кібербезпеки. *Інформаційне право, 2,* 215–219 (Diorditsa, I. V. (2017). Qualification requirements for the competence of experts on cybersecurity *Information Law, 2,* 215–219).

6. Діордіца, І. В. (2017). Напрями підготовки та підвищення кваліфікації фахівців із кібербезпеки. *Інформаційне право, 3,* 199–202 (Diorditsa, I. V. (2017). The directions of training and advanced training of specialists in cybersecurity. *Information law, 3,* 199–202).

7. Дубов, Д. В. (2010). Кібербезпекова політика контексті трансформації політики безпеки США за адміністрації Б.Обами. *Політичний менеджмент, 1,* 155–163 (Dubov, D. V. (2010). Cybersecurity in the transformation context of the us security policy under the administration of B. Obama. *Political Management, 1,* 155–163).

8. Зубик, Л. В. (2016). Аналіз структури підготовки бакалаврів з Інформаційних технологій. *Молодь і ринок, 3 (134),* 173–174 (Zubyk, L. V. (2016). The analysis of structure of training of bachelors in information technology. *Youth and Market, 3 (134),* 173–174).

9. Коваленко, О. Ю. (2010). Неперервна педагогічна освіта у США: сучасний стан і перспективи розвитку. *Педагогічні науки: теорія, історія, інноваційні технології, 6 (8),* 127–132 (Kovalenko, O. Yu. (2010*).* Continuous education of teachers in the usa: contemporary condition and the development prospects. *Teaching science: theory, history, innovative technology, 6 (8),* 127–132).

10. Макаренко, Є. А. (2012). Геополітіка и прагматика стратегії зміцнення світового лідерства США у XXI столітті. *Дослідження світової політики*, *4 (61),* 3–12 (Makarenko, Ye. A. (2012). Geopolitics and pragmatics of the strategy of strengthening the world leadership of the USA in the 21st century. *World Policy Study, 4 (61),* 3–12).

11. Ничкало, Н. Г. (2002). *Професійна освіта в зарубіжних країнах*. Черкаси: Вибір (Nychkalo, N. G. (2002*). Professional Education in Foreign Countries.* Cherkasy: Choice).

12. Moore, M. G. (2005). Distance Education: A Systems View. *Belmont CA: Wadsworth Publishers,* 146–151.

13. *Проект Стратегії забезпечення кібернетичної безпеки України*. Режим доступу: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg

The strategy project of providing cybernetic security of Ukraine. Retrieved from: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.

14. *Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. Женева: МСЭ.* (2009). Режим доступу: http://www.itu.int/ITU-T/ipr/. (*Recommendations ITU-T X.1205. Cybersecurity Overview. Geneva: ITU.* (2009). Retrieved from: http://www.itu.int/ITU-T/ipr/).

15. Franscella, J. (2013). *Cybersecurity vs. Cyber Security: When, Why and How to Use the Term.* Retrieved from: http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html.

16. *National Strategy to Cyberspace Secure – US-CERT.* Retrieved from: https://www.us-cert.gov/sites/.../cyberspace_strategy.

17. *NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from: https://ccdcoe.org/sites/default/.

18. *NIST, National Initiative for Cybersecurity Education Strategic Plan*. National Institute of Standards and Technology (2012). Retrieved from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP 800-181.

19. *Strategic Warfare in Cyberspace*, by Gregory J. Rattray. Cambridge, MA. Retrieved from: www.tandfonline.com/doi/abs/.

РЕЗЮМЕ

Быстрова Богдана. Основные понятия исследования и концептуальные основы профессиональной подготовки специалистов по кибербезопасности.

Цель статьи – публикация результатов исследований о состоянии процесса подготовки специалистов по кибербезопасности в Соединенных Штатах. В статье обоснованы концептуальные основы подготовки специалистов по кибербезопасности и охарактеризованы правовые принципы, касающиеся дисциплин и специальностей, для которых Соединенные Штаты провели подготовку и повышение квалификации экспертов по кибербезопасности. Описаны, выделены ключевые термины и представлены их толкования с целью конкретизации и уточнения их сущностных значений. Практическое значение исследования заключается в формировании представления о концептуальных основах и терминологическом наполнении учебных программ по подготовке специалистов по кибербезопасности, которые являются предметом наших дальнейших научных исследований.

Ключевые слова: *ИТ-отрасль, киберугрозы, кибератака, киберпространство, киберзащита, информационная безопасность, кибербезопасность, политика, кибербезопасности специалист по кибербезопасности, концептуальные основы.*

SUMMARY

Bystrova Bogdana. Basic concepts of research and conceptual bases for the cybersecurity specialists training.

The purpose of the article is to present the results of studies due to the training process of specialists in cybersecurity in the United States. The article substantiates the conceptual bases for the training of specialists in cybersecurity and characterizes the legal principles relating to disciplines and specialties for which the United States have lead preparation and upgraded the skills of cybersecurity experts. Key terms have been described, identified and their interpretation with the objective of a concrete definition and specification of their essential values are presented.

The conducted research of American experience of professional training in the field of cybersecurity bachelor's degree will enable to determine the possibilities of its progressive ideas implementation into higher education of Ukraine. In particular: improvement of industry standards for cybersecurity bachelor's degree; providing the information support of Internet resources; development and improvement of the content of curriculum and educational programs for training bachelors of cybersecurity; improvement of the educational and methodological implementation; advanced study of foreign experience. The successful implementation of reasonable opportunities will promote professional training of national experts in the field of cybersecurity, accelerate the process of reforming of the national higher education system, convergence of the international educational standards, and ensure its competitiveness in today's job market.

The successful implementation of reasonable opportunities will promote professional training of the national experts in the field of cybersecurity, accelerate the process of reform

of the national higher education system, convergence of the international educational standards, and ensure its competitiveness in today's job market.

The practical significance of the research is to form an idea of the conceptual bases and terminology of the curriculum for training specialists in cybersecurity, which are the subject of our further research.

Key words: *IT-industry, cyber-threats, cyber-attack, cyberspace, cyber-defense, information security, cybersecurity, cyber-spam policy, cybersecurity specialist, conceptual framework.*

УДК 378.014.6:061.2

Інна Єременко
Сумський державний педагогічний
університет імені А. С. Макаренка
ORCID ID 0000-0001-6323-8444
Аліна Сбруєва
Сумський державний педагогічний
університет імені А. С. Макаренка
ORCID ID 0000-0002-1910-0138
DOI 10.24139/2312-5993/2017.08/070-085

ЕТАПИ РОЗВИТКУЄВРОПЕЙСЬКОГО ВИМІРУ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

У дослідженні висвітлено процеси розвитку наднаціонального (європейського) виміру забезпечення якості вищої освіти (ЗЯВО). На основі аналізу документів ЄС та Болонського процесу виокремлено етапи розвитку досліджуваного феномену: 1) розробка й експериментальна перевірка методології та процедур ЗЯВО; 2) інституалізація; 3) стандартизація; 4) легітимізація. Систематизовано аспекти інтернаціоналізації діяльності агенцій ЗЯВО в сучасних умовах: транскордонна діяльність агенцій ЗЯВО, оцінювання якості спільних освітніх програм університетів різних країн оцінювання якості транскордонної/транснаціональної вищої освіти.

Ключові слова*: якість вищої освіти, забезпечення якості вищої освіти, освітня політика ЄС, Болонський процес, етапи, розвиток.*

Постановка проблеми. Формування Європейського простору вищої освіти (ЄПВО), що є найбільш успішним освітнім проектом початку XXI століття не тільки в європейському, але й у глобальному контексті, має багато-вимірний характер. Вже стали історією процеси структурної трансформації національних систем вищої освіти більшості європейських країн на засадах єдиної європейської моделі «бакалавр-магістр-доктор»; запровадження єдиних норм трудомісткості навчального процесу та можливості трансферу його складових на засадах ECTS, уведення в практику діяльності європейських університетів Рамки кваліфікацій ЄПВО та Додатку до диплома про вищу освіту європейського зразка. Ще одним важливим виміром розбудови ЄПВО є формування європейського виміру забезпечення якості вищої освіти.

Підкреслимо, що шляхи забезпечення якості вищої освіти (ЗЯВО) зазнали в європейському регіоні протягом останніх 30-ти років не менш