

МОДЕРНІЗАЦІЯ ОСВІТНЬОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА»: РЕАЛІЇ ТА ПЕРСПЕКТИВИ

У статті представлені результати порівняльного аналізу освітніх програм вищих навчальних закладів США в галузі кібербезпеки. Висвітлено уявлення про реальний стан справ, отриманих зіставленням організації, технології, змісту і результатів навчання за схожими освітніми програмами при порівнянні підготовки бакалаврів з кібербезпеки в університетах України та США. Основними завданнями на шляху реалізації національної стратегії з кібербезпеки означено наступне: стандартизація, впровадження дуального та змішаного видів навчання, впровадження новітніх технологій у навчальному процесі; мотивація професорсько-викладацької складу. Зроблено акцент на забезпеченні рівноваги між цілями та результатами освіти.

Ключові слова: освітні програми, стратегія кіберзахисту, ІТ, модернізація, кібербезпека, бакалавр, дуальне навчання, стандартизація, змішане навчання.

Постановка проблеми. На сучасному етапі розвитку науки і техніки у кожній розвинутій державі зростає потреба зміцнення кібербезпеки та перетворення її на одну з найважливіших галузей суспільства. Через атаки на критичні інфраструктурні об'єкти, розвиток системи Інтернет речей, 4-у індустріальну революцію, кібератаки, підвищення глобальної нестабільності виникає потреба розвитку галузі кібербезпеки. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим до кібернетичних впливів, тому є потреба несилового контролю та управління як об'єктами критичної інфраструктури, так і окремо взятими громадянами чи їх об'єднаннями. Потіки інформації, що передаються, зберігаються та обробляються в кіберпросторі, постійно зростають, є потреба їх належного захисту від несанкціонованого злочинного доступу. Є актуальною потреба у фахівцях з кібербезпеки і буде ще зростати з подальшим розвитком високотехнологічного суспільства. Якість підготовки фахівців в області кібербезпеки визначається сьогодні рівнем технологічного розвитку країни, проте для відповіді на питання, наскільки ця підготовка відповідає сучасним вимогам, виникла потреба у порівняльному аналізі підготовки фахівців з кібербезпеки в інших країнах. Ми порівняли програми підготовки бакалаврів з кібербезпеки на предмет організації, технології, змісту і результатів навчання за схожими освітніми програмами у вишах України та США.

Аналіз останніх досліджень і публікацій. Детальне порівняння освітніх програм вузів США та України за змістом і вимогами до результатів навчання дозволяє оцінити кожну програму в цілому і рівень викладання окремих ключових дисциплін. Конкретизуємо аналіз, взявши для порівняння програми підготовки бакалаврів за напрямом Cyber Security університету штату Північна Кароліна (NCSU) та програми з кібербезпеки ВНЗ України. В Україні підготовка фахівців у ВНЗ регламентована державними освітніми стандартами і кожні п'ять років підлягає розгляду Акредитаційної комісії України (АКУ). У США державних освітніх стандартів немає, але кожен університет акредитує свої освітні програми в спеціалізованих агентствах, що виставляють однакові вимоги по кожній програмі, і раз у шість років підтверджує акредитацію. За програмою Cyber Security в якості такого агентства виступає Рада з акредитації інженерних наук і техніки (ABET, www.abet.org). Масштаб акредитації (3000 програм) дозволяє говорити про їх уніфікацію. В Україні, починаючи з 2013 року, кібератаки набули нового статусу («кібервійна»), щорічний зріст кібератак складає 40%. Україна не має достатніх ресурсів і кадрового потенціалу для забезпечення гідного протистояння. Кількість сертифікованих спеціалістів з кібербезпеки у світі 108 тис. чоловік, серед них абсолютний лідер США – 71 тис. чоловік, тоді як в Україні – 18 чоловік, це 78 місце у світі. Вивчення наукових здобутків та передового досвіду підготовки бакалаврів з кібербезпеки у США дозволяє визначити завдання та шляхи подальшої модернізації системи підготовки фахівців даної галузі в Україні. [2]

Мета статті полягає в презентації результатів порівняльного аналізу навчального процесу підготовки бакалаврів з

кібербезпеки у ВНЗ США та України, висвітлити результати реалізації національної стратегії України з кібербезпеки про основні перешкоди, шляхи їх подолання та основні завдання системи підготовки фахівців для галузі. Проаналізувати стратегію модернізації освітньої програми за напрямом «кібербезпеки» у ВНЗ України з акцентом на особливому завданні – забезпечення рівноваги між цілями та результатами освіти, внутрішньої гармонії суб'єктів навчання.

Результати дослідження. Для порівняльного аналізу організації і технології навчальних процесів ВНЗ США обрано NCSU (університет штату Північна Кароліна), його інженерний факультет (програма Cyber Security). NCSU стійко займає високі місця в рейтингу Новини США і World Report (2015 рік – 31-е місце з 150). В Україні 30 цивільних ВНЗ готують фахівців за напрямом «кібербезпеки». Щорічно випуск складає 800 бакалаврів, тоді як потреба – 2000 у рік (за розрахунками щодо кількості кібератак). В NCSU готують ІТ-фахівців за однією програмою силами 50 викладачів однієї кафедри, щорічний випуск 1300 студентів і аспірантів. Програма Cyber Security в NCSU і в Україні мають схожу структуру і спрямованість. Серед особливостей NCSU є те, що школярі старших класів можуть записуватися на окремі курси університету, складаючи іспити разом зі студентами, а потім, після вступу, раніше отримані результати їм зараховують. Випускник коледжу, який поступає до NCSU, на отримані результати теж має перезалік. В українських ВНЗ тільки для випускників профільних коледжів і вищів організовується навчання за скороченою програмою (2.5-3 роки) для отримання ступеня бакалавра. У школах США ІТ в більшості штатів (Північна Кароліна у т.ч.) не є обов'язковим предметом, тому на 1-2 курсах вивчається інформатика. В Україні інформатика обов'язковий предмет у школі, і під час вступу на напрям кібербезпеки необхідні результати складання ЗНО з інформатики, ІТ є обов'язковим курсом у подальшому навчанні. У NCSU студент, який бажає стати бакалавром з кібербезпеки, вступає на інженерний факультет та зобов'язаний спочатку вивчити мінімум дисциплін (англійська мова, математика, хімія, фізика, вступ до інженерії) та вибрати основну програму і при цьому додатково обрати скорочену версію іншої програми. В наших вишах студент відразу поступає на конкретний напрям, а опанування іншої освітньої програми теоретично можливе, але зазвичай є винятком. За 4 роки навчання в NCSU за програмою Cyber Security студент для отримання ступеню бакалавра повинен вивчити мінімум 40 односеместрових дисциплін, наприклад в 2015-2016 н. р. серед них було - 23 обов'язкові і 17 за вибором. В Україні за аналогічною програмою студент вивчає 45 дисциплін, за перерахунком на одно семестровий підхід – це 60 обов'язкових та 12 за вибором. Співвідношення загальноосвітніх дисциплін до фахових 1:1. Дисципліни за вибором складають 20%. Аналіз показав, що українські навчальні плани недосконалі своїм нефаховим дисциплінарним наповненням та недостатньою кількістю годин і відсутністю стандартизації дисциплін. Формування складу курсів і тем пов'язане не з потребою ринку і абітурієнтів, а з наявністю кафедр і викладачів. Щодо дисциплін за вибором – то це вибір без вибору. За програмою Cyber Security в NCSU на ступінь бакалавра необхідно набрати мінімум 120

кредитів (1 кредит – 15 аудиторних, лекція триває 75 хв., на 1 аудиторну планується 2-3 години самостійної, аудиторні роботи складають 25%). У ВНЗ України для більшості курсів 1 кредит це 30 аудиторних, лекційна тривалість 90 хв. Переліки дисциплін математичної і професійної підготовки в значній мірі збігаються. Разом з тим кількість аудиторних годин різниться так: 2000 в NCSU проти 2840 в ВНЗ України, що обумовлено майже повною відсутністю в NCSU практичних і лабораторних занять з дисциплін спеціальної підготовки. Співвідношення годин між лекційними і практичними заняттями досліджуваних програм сильно відрізняється. У NCSU домінують лекційні заняття, а по багатьох дисциплінах практичних робіт немає. В Україні співвідношення між лекційним і практичним заняттями приблизно 1:2. Українські студенти виконують значну частину завдань в аудиторії за допомогою викладачів, студенти NCSU виконують їх самостійно в якості домашніх завдань. Студенти NCSU практично не конспектують лекції, оскільки лектор викладає на сайті великий обсяг інформації і рекомендує студентам підручник, якого він буде дотримуватися в своїх лекціях. Українські студенти в основному конспектують лекції, оскільки викладач не пов'язує свій курс з одним підручником і не завжди на сайті достатня кількість навчальних матеріалів. У NCSU немає усних іспитів і форми звітності, аналогічної українському «зараховано». Підсумковий іспит існує для кожної дисципліни і включає завдання трьох типів: з вибірковою відповіддю, відповіддю у вигляді числа або короткого рядка та розгорнутою відповіддю. Тривалість іспиту – 3 години. В Україні велика частина іспитів приймається в усній формі, що містить питання з переліку (відомого студентам). Студенти NCSU найчастіше отримують від викладача на іспит зразки тестів різних рівнів складності. У NCSU з кожної дисципліни на початку семестру оголошується система оцінювання для іспиту. У ВНЗ України іспит не відіграє вирішальної ролі у формуванні оцінки, що є співвідношенням відповіді та результатів з практичних занять у семестрі. В NCSU іспит не можна «перездати», але можливо взяти повторний курс. В Україні все ще практикується перездача іспитів. Навчання в NCSU платне для всіх студентів (деяким вдається отримати підтримку різних фондів). У 2015-16 н.р. для резидентів штату Північна Кароліна повні витрати на навчання за програмою бакалаврату Cyber Security склали близько 20 тис. дол., в Україні відношення бюджетних місць для навчання до контрактних становить 1:1. Досліджувані програми обох країн враховують регламентуючі вимоги до результатів підготовки – Державний освітній стандарт в Україні і для NCSU – це Рада з акредитації інженерних наук і техніки. В обох випадках вимоги стосуються як результатів навчання, так і умов його реалізації, на базі цих вимог створюють розгорнуті освітні програми. На думку дослідників в США «традиційна сертифікація» – це програми навчання на базі 4-річних коледжів з напрямку «освіта», що передбачає підготовку студентів та набуття ними компетентці, що оцінюється через складання іспиту відповідно до вимог штату. [1] В Україні з підготовкою фахівців з кібербезпеки виявлено реальні проблеми: неготовність випускників до задач міжнародних фахових екзаменів та працювати за фахом; відсутність у випускників практичних навичок.[2] Загальна структура підготовки в NCSU і в Україні схожа в обох випадках приблизно однаковий відсоток гуманітарних, математичних, природничо-наукових і фахових дисциплін. Підготовка кадрів в США для галузі передбачає ряд вимог від фахівця по завершенню університетської підготовки, а саме: розуміти важливу термінологію, матеріали, технології; бути спроможним володіти загальними навичками з кібербезпеки; мати

досить високу майстерність з практики у своїй галузі; розуміти систему, проводити моніторинг систем безпеки, застосовуючи міжмережеві екрани та системи виявлення вторгнень; вміти створювати, впроваджувати і контролювати виконання політики безпеки; вміло діяти за планом аварійного відновлення даних для операційних систем, баз даних, мереж, серверів і додатків; професійно проводити дослідження нових продуктів, послуг, протоколів і стандартів для підвищення рівня безпеки; проводити регулярні перевірки на відповідність використання. [6] Основними завданнями удосконалення системи підготовки фахівців з кібербезпеки на етапі реалізації національної стратегії з кібербезпеки є наступне: стандартизувати вимоги до підготовки фахівців; розробити програму навчання у відповідності до практичних потреб галузі та міжнародних сертифікаційних вимог; заохочувати новітні технології навчання; впровадити дуальний та змішаний види навчання; популяризувати спеціальність шляхом заохочення фахівців; забезпечити мотивацію професорсько-викладацького складу. З метою реалізації Стратегії з кібербезпеки України на 2017-18 н.р. намічено ряд перспективних кроків: а) затвердження освітнього стандарту з фаху; б) розробка навчальних матеріалів для 1-2 курсів на платформі дистанційного навчання; в) запуск освітньої програми з вересня 2017 року; г) формування платформи дуальної освіти, залучивши провідні українські та міжнародні компанії; д) розробка навчальних матеріалів для фахових дисциплін 3-4 років навчання; ж) розробка он лайн - платформи тренувань навичок з кіберзахисту для змішаного навчання; з) створення співтовариства викладачів та експертів з кібербезпеки. [4] Модернізація системи вищої освіти з підготовки бакалаврів з кібербезпеки передбачає наступні результати: а) після 2 курсу рівень англійської мови – B2; б) розвиток Soft Skills, які дозволяють бути успішним незалежно від специфіки діяльності (навички переконувати, знаходити підхід до людей, працювати в команді; характеристики: ерудиція, креативне мислення, лідерство; вміння вести переговори, професійно володіти мовою, працювати з інформацією); в) всі підготовчі дисципліни підпорядковані фаховим і викладаються на 1-2 курсах; г) на 3-4 курсах фахова підготовка шляхом дуальної освіти та вільного доступу до онлайн-платформи змішаного виду навчання; [5] д) програма навчання підпорядковується вимогам міжнародних сертифікаційних програм CISSP, ISACA та типовим посадовим інструкціям провідних компаній світу.

Висновки та перспективи подальших досліджень. На сьогодні в рамках державної програми модернізації освітнього стандарту за напрямком «Кібербезпека» розроблено методичні рекомендації з підготовки навчальних матеріалів; сформовано структуру підготовчих дисциплін; розпочата робота з підготовки навчальних планів для 1-2 курсу (2017-19 н.р.) та з підготовки навчальних матеріалів для підготовчих дисциплін; проведено круглий стіл на базі Міністерства освіти і науки України з провідними ВНЗ країни; планується зробити вільний доступ до онлайн-платформи змішаного виду навчання; створити співтовариство викладачів та експертів з кібербезпеки. До проекту вже долучилися 5 ВНЗ, що є критично мало на поточний момент. Зроблено акцент на підвищенні довіри до українських ВНЗ з боку роботодавців та абітурієнтів.

Подальші наукові дослідження плануємо присвятити особливостям дуальної освіти (50% на 50% навчання та стажування) у ВНЗ та конкурентоспроможності України на глобальному ринку кібербезпеки.

Список використаних джерел

1. Пазюра Н.В. Загальна характеристика альтернативної педагогічної освіти в США. / Н.В. Пазюра // Вісник Національного авіаційного університету. Серія: Педагогіка. Психологія: зб.наук.пр. – К.: НАУ, 2015. – С. 92 – 98.
2. Сьомін С.В. Система підготовки кадрів для сил безпеки України: проблеми та перспективи розвитку: аналітична доп. / С.В. Сьомін, О.О. Резнікова; за заг. ред. В.П. Горбуліна. – К.: НІСД, 2016. – 50 с.
3. Chabrow E. Cybersecurity as a Campaign Issue / E. Chabrow / [Електронний ресурс]. – Режим доступу: <http://www.govinfosecurity.com/blogs.php.postID=1161&opg=1>

4. The National Security Strategy of the United States of America – 2015 / [Електронний ресурс]. – Режим доступу: nssarchive.us/national-security-strategy-2015/

5. Rossett A., Vaughan F., Blended learning CEO Epic Group plc, 52 Old Steine, Brighton BN1 1NH, 2003, URL: <http://www.obs.ru/interest/publ/?thread=57>

6. Watson, Cynthia Ann. U.S. national security: a reference handbook. – Santa Barbara, California: ABC-CLIO, 2008. – P. 59.

В статті описані результати порівняльного аналізу освітніх програм ВНЗ США та України, по кибербезпеці. Сопоставлено навчальні програми, що використовуються в процесі підготовки бакалаврів по кибербезпеці на предмет структури, технологій та їх змісту. Зроблено акцент на особливості завдання – забезпечення рівноваги між цілями та результатами освіти. Основними завданнями визначено: стандартизацію, введення дуального та змішаного видів навчання, поощрення новітніх технологій навчання, мотивація професорсько-викладацького складу.

Ключові слова: модернізація, освітні програми, ІТ, стратегія кибербезпеки, стандартизація, бакалавр, дуальне навчання, змішане навчання.

The purpose of this research is to identify the results of the comparative analysis of educational programs of cybersecurity bachelor's degree in the U.S and Ukraine. At the stage of the national strategy implementation on cybersecurity, it was made an emphasis on a specific task - to provide a balance between the objectives and results of education for inner the inner harmony of the study process. We have indicated a number of key tasks, namely: Standardization, implementation compared with dual and mixed types of training, the promotion of new technologies in the educational process; provide the motivation of faculty. We have indicated a number of key tasks, as follows: standardization, implementation of dual and mixed types of training, the promotion of new technologies in the educational process; provide the motivation of department. 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: the improvement of industry standards for Cybersecurity bachelor's degree; providing the information support of Internet resources; development and improvement the content of the curriculum and educational programs for training bachelors of cyber security; improvement of the educational and methodical 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 reform of the national higher education system, convergence of the international educational standards, and ensure its competitiveness in today's job market.

Key words: Higher education, USA, cyber security, development, bachelor, standardization, IT, dual training, mixed training.

УДК378[81'367:811.161.2]

Дружененко Раїса Сергіївна,

кандидат педагогічних наук, доцент,

Київський університет імені Бориса Грінченка, м. Київ

СИСТЕМА ЗНАТЬ ЯК РЕЗУЛЬТАТ ФУНКЦІОНУВАННЯ МЕТОДИЧНОЇ СИСТЕМИ НАВЧАННЯ: ФІЛОСОФСЬКЕ ОСМИСЛЕННЯ ПРОБЛЕМИ

Проаналізовано глибинні філософські позиції в аспекті отримання системи знань у результаті функціонування методичної системи навчання та теорії взаємозалежності ефективної методичної системи й ґрунтовності системних знань; з'ясовано філософські основи розвитку поняття знання як системи, проілюстровано філософське вирішення проблеми причинно-наслідкових відношень у дихотомії «методична система навчання – система знань».

Ключові слова: філософська наукова база, система знань, функціонування методичної системи, система навчання, результат навчальної діяльності.

Постановка проблеми. Широкоаспектність обґрунтування поняття *методична система навчання* в сучасному науковому дискурсі знаходить вияв у ряді досліджень, що підпорядковані вивченню його природи, змісту, будови, основних ознак, властивостей, особливостей існування та розвитку тощо. У фокусі означеної проблеми вивченню підлягає питання отримання системи знань як результату функціонування будь-якої системи, у тому числі й методичної системи навчання.

За нашими спостереженнями, декларовані вченими різних наукових галузей визначення поняття системи набувають, з одного боку, нових специфічних особливостей, адаптованих до особливостей конкретної науки, а з іншого – зберігають фундаментальну філософську основу, адже, за словами українського дослідника А.Цофнаса, «ніяка теорія ні в природознавстві, ні в соціології, ні в гуманітарних науках не обходиться без метафізичних передумов онтологічного і гносеологічного змісту» [10, с. 15], «філософські методи обов'язкові для всіх як директиви» [10, с. 11].

Мета статті. Філософське вчення є базою для розвитку будь-якої наукової проблеми, тому за *метою* маємо аналіз глибинних джерельних позицій в аспекті отримання системи знань у результаті функціонування методичної системи навчання та теорію взаємозалежності ефективної методичної системи й отримання ґрунтовних системних знань. Серед *завдань* – з'ясувати філософські

основи розвитку поняття знання як системи, проілюструвати філософське вирішення проблеми причинно-наслідкових відношень у дихотомії «методична система навчання – система знань».

Аналіз останніх досліджень і публікацій. Науковою базою дослідження послужили філософські погляди на проблеми педагогіки Аристотеля, вчення про систему як інструмент досягнення результату Б.Кеккермана, позиція про взаємозв'язок системи-знаряддя та системи-результату Е.Кондільяка, теорії системи знань філософів епохи Просвітництва (Ф.Бекон, Д.Дідро, Х.Вольф, І.Гердер, К.Гельвецій, П.Гольбах).

Результати дослідження. Поняття будь-якої системи, у тому числі й методичної системи навчання, підпорядковується тривимірному осмисленню: змістовому, структурному, інструментальному. Останній дає можливість розуміння системи як деякого знаряддя у досягненні мети. Маркером досягнення мети є позитивний прогнозований результат. У такому разі методична система виступає як активна, функційна, тобто така, що за основу має процес навчальної діяльності, націлений на результат.

Нагадаємо, що глибоке обґрунтування функційної властивості системи знайшло відображення у наукових розвідках П.Анохіна (1935 р.). Функційність системи дослідник пов'язує із внутрішньою змінованістю її структурних компонентів у часі з метою отримання оптимального результату [1]. Виходячи з цього, функціонування методичної системи навчання можна розглядати як