УДК378.14(73): 004.056.5 (045)

СИСТЕМНИЙ ПІДХІД ДО ОРГАНІЗАЦІЇ ПРОФЕСІЙНОЇ ОСВІТИ В ГАЛУЗІ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ В США

Богдана Бистрова

Національний авіаційний університет (Київ)

Анотація. У статті презентовано результати аналізу з навчальних програм підготовки фахівців в області кібербезпеки вищих навчальних закладів США. Встановлено, що внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим від незначних кібернетичних впливів, які все частіше стають ефективним інструментом на шляху досягнення мети щодо несилового контролю та управління як об'єктами критичної інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об'єднаннями. Найбільш затребуваними є фахівці в області розслідування комп'ютерних інцидентів, інформаційної безпека, комп'ютерної безпека, безпеки комп'ютерних мереж. Для системи вищої освіти США характерна наявність альтернативної освіти з підготовки фахівців. Це говорить про зацікавленість держави у фахівцях суміжних областей підготовки, що знаходить своє відображення у дисциплінах, що вибрані для вивчення.

Ключові слова: *вища освіта в США; кібербезпека, бакалавр, альтернативна освіта, кадрове забезпечення*.

Богдана Быстрова

СИСТЕМНЫЙ ПОДХОД К ОРГАНИЗАЦИИ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ В ОБЛАСТИ ПОДГОТОВКИ БАКАЛАВРОВ ПО КИБЕРБЕЗОПАСНОСТИ В США

Аннотация. В статье описаны результаты анализа образовательных программ высших учебных заведений США, которые предлагают программы подготовки специалистов в области кибербезопасности. Анализ программ подготовки бакалавров показывает, что наиболее востребованными являются расследование компьютерных инцидентов, информационная безопасность, компьютерная безопасность, безопасность компьютерных сетей. Для образования США характерно наличие альтернативных направлений подготовки. Это говорит о заинтересованности в специалистах смежных областей подготовки, что находит свое отражение в наборе дисциплин для изучения.

Ключевые слова: *высшее образование в США; кибербезопасность, бакалавр, кадровое обеспечение.*

Bogdana Bystrova

THE SYSTEM APPROACH TO THE PROFESSIONAL EDUCATION OF BACHELOR'S IN CYBERSECURITY IN THE UNITED STATES

Abstract. The article deals with the peculiarities of the professional training of cyber security bachelor's degree in the U.S. higher education system. The Relevance of this approach is determined by the dynamics of technological advances. Due to the extremely widespread use of modern information technologies in all spheres of its existence, the society has become vulnerable to cyber-attacks, which are increasingly becoming an effective tool towards achieving the objective of non-forcible control and management of critical infrastructure of the State, enterprises, and separately enclosed citizens, their associations. An innovative approach is a methodological platform for research and students' project work, their communication with professional scientific community. The conducted research of American experience of professional training in the field of cyber security 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 Cyber

security bachelor's degree; providing the information support of Internet resources; development and improvement the content of 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 cyber security, 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. In different countries at different periods of education development it was defined some conceptual basis of modern education in the field of information security with the need for further restructuring the education process in cyber security.

It is obvious to meet the need for highly qualified specialists in the field of information security can only be based on the integrated use of all the possibilities of secondary, higher, and the alternative education through certification, using trained personnel in the consortium of international level. Thus, an implementation of the information security doctrine and strategy of information society development in Ukraine is quite a challenge in this industry reform by integrating best practices in US education.

***Key words**: Higher education in the United States; information security, bachelor, staffing.*

Постановка проблеми. На сучасному етапі розвитку науки і техніки кібербезпека кожної розвинутої держави перетворюється на одну з найважливіших галузей високотехнологічного суспільства. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим від незначних кібернетичних впливів, які все частіше стають ефективним інструментом на шляху досягнення мети щодо несилового контролю та управління як

об’єктами критичної інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об’єднаннями. Потоки інформації, що передаються, зберігаються та обробляються в кіберпросторі постійно зростають, що вимагає їх належного захисту від несанкціонованого доступу зі злочинною метою. Тому потреба у фахівцях з кібербезпеки є актуальною і з подальшим розвитком високотехнологічного суспільства буде ще більше зростати.

Аналіз актуальних досліджень. Вивчення наукових здобутків та передового досвіду підготовки бакалаврів з кібербезпеки у США дозволяє визначити завдання та шляхи подальшого удосконалення системи підготовки фахівців даної галузі: наповнення новим змістом навчальних планів та програм; внесення змін, пов’язаних з інтеграцією прогресивного досвіду в освіту України. Існує думка, що особливим завданням є забезпечення рівноваги між цілями та результатами освіти, внутрішньої гармонії суб’єктів навчання.

В університетах США, як і в нашій країні, одним із обов’язкових завдань є акредитація, яка проходить у декілька етапів. Здійснюючи акредитаційний самоаналіз ВНЗ визначає відповідність освітніх послуг визначеним критеріям. На етапі визначення перспективних напрямів розвитку ВНЗ звертається до незалежних експертів, аудиторів академічних послуг, з метою отримання допомоги. Як правило це є люди, які працюють у споріднених спеціальностях в інших навчальних закладах, члени професійних асоціацій, працівники агенцій з академічного аудиту та відділів ліцензування. Проводиться розширений моніторинг системи управління навчальним закладом, всіх рішень, що приймалися та отриманих результатів.

Наступним етапом є аналіз спроможності навчального закладу щодо актуалізації резервів. Вподовж 2-х років через періодичні відвідування університету експертами з метою аналізу щодо змін стану суб’єктів

навчально-виховного процесу та відгуків випускників, працедавців, громадськості про результати наданої освіти та рівень підготовки випускників. Завершальний етап презентує висновки про відповідність показників освітньої діяльності встановленим вимогам з акцентом на поліпшених результатах якісних показників отриманих вході аналізу процесу, який запроваджено у навчальному закладі. «Матеріали акредитаційної справи можуть повертатися на доопрацювання. Експерти, як правило, запрошують додаткову інформацію, коментарі. Цей період триває до року. Слід зазначити, що в американських університетах акредитація займає більше часу і має, на відміну від української реальності, систематичний, планомірний характер протікання, що дозволяє розглядати її як процес спрямований на удосконалення існуючої практики надання освітніх послуг» [1, с. 86].

Аналіз наукових праць показав, що теоретичною основою дослідження стали основні положення порівняльної педагогіки, теорії і методики професійної освіти, а також праці, в яких висвітлено результати досліджень проблем розвитку вищої технічної освіти в різних країнах, зокрема у Росії (Н. Аітов, К. Байчаров, В. Баранов, А. Кірсанов, А. Кочнєв), Білорусії (Л. Акімова, П. Хейфец), США (Т. Георгієва, А. Іванова, Н. Пазюра, В. Параіл, С. Романова, М. Чванова), Німеччині (Н. Абашкіна, Т. Мостова, Л. Соловйова), Франції (Є. Бражник, В. Єлманова, С. Єркович, С. Коршунов, І. Федоров); історичні, педагогічні праці з питань розвитку вищої освіти Великої Британії (Ю. Алферова, А. Барбарига, Г. Воронка, Н. Воскресенська, В. Гер'є, В. Ігнатович, З. Колонтай, І. Марцинківський, М. Нікандров, А. Парінов, Л. Пуховська, В. Рижов, Л. Торяник, Н. Федорова), США (Вортняк, Н. Пазюри, О. Тарасова, С. Тезікова); праці з філософії освіти (А. Валіцька, І. Зязюн, В. Кремень, В. Лутай); праці з порівняльної педагогіки О. Алексеєва, О. Арсентьєва, Б. Вульфсона,

В. Зубка, І. Козубовської, С. Корсака, А. Лігоцького, Н. Ничкало, Н. Пазюри, В. Поліщук.

Мета статті полягає в розкритті оптимальних шляхів підготовки бакалаврів з кібербезпеки високого кваліфікаційного рівня, з подальшою інтеграцією прогресивного досвіду в освіту України. Охарактеризувати особливості підготовки бакалаврів з кібербезпеки в США та дослідити перспективні напрями освіти з урахуванням посилення професійної спрямованості навчання.

Методи дослідження. Методичну основу дослідження складають аналіз та синтез психологічних і педагогічних наукових знань, систематизація та класифікація завдань та підходів, порівняння та узагальнення.

Виклад основного матеріалу. З огляду на те що перед Україною стоїть ряд стратегічних завдань у процесі інтеграції української освіти і науки до загальноєвропейського освітнього простору. Нам слід підняти освіту на новий Європейський рівень, що дасть гарантію високої професійної освіти, мобільної, відкритої для всього світу з прозорістю освітянських діянь, з врахуванням інтересів різних культур. Розглядаючи сьогоднішній стан кадрового забезпечення галузі інформаційної безпеки (ІБ), слід зазначити, що дане питання стосовно захисту інформації має в країні досить серйозну практичну реалізацію і деякі теоретико-методологічні узагальнення. На сьогоднішній день вже близько 20 років функціонує організована система підготовки молодих і підвищення кваліфікації працюючих фахівців із захисту інформації.

Подальше завдання в цій галузі полягає в створенні чіткої державної системи прогнозування потреби у фахівцях, розробці методології формування державного замовлення на їх підготовку, розвитку нових напрямків і освітніх програм підготовки кадрів. Більш того, навчання основам інформаційної безпеки і захисту інформації повинно стати

інваріантною складовою інформаційної підготовки в рамках всіх без винятку спеціальностей і напрямків професійної освіти, яка є формуванням інформаційної культури особистості на етапі переходу до постіндустріального суспільства.

На нашу думку рішення всіх цих завдань має бути засноване на системному підході до організації професійної освіти, котрий враховує методологічні, організаційні, змістовні, дидактичні та технологічні аспекти. Предметом нашого дослідження є представлені у статті деякі підходи до вирішення найбільш гострих проблем, що стоять сьогодні перед системою підготовки фахівців з забезпечення інформаційної безпеки.

Розглянемо ряд підходів до реформування системи вищої освіти в області підготовки бакалаврів з кібербезпеки в США шляхом доповнення та змін основних принципів функціонування і вдосконалення професійної освіти.

Пропонуємо для розгляду один із підходів до проведення реформ в системі вищої освіти. Аналіз показав, що демократизація системи підготовки бакалаврів з кібербезпеки при суворому дотриманні законодавства України щодо національної безпеки, загальновизнаних норм міжнародного права при підготовці кадрів з кібербезпеки є одним із важливих підходів удосконалення освіти. Такий підхід безперечно забезпечить якісний кадровий склад.

Сьогодні підготовка кадрів в області кібербезпеки є не тільки реакція на попит ринку в таких фахівцях, а й як важлива складова комплексу заходів держави щодо протидії загрозам в інформаційній сфері. Цим визначається і зміст підготовки зазначених фахівців, і особливі вимоги до освітніх установ при організації такої підготовки. У загальній системі забезпечення кібербезпеки держави кадровий супровід є самостійною підсистемою, а сама система підготовки фахівців є основою такого супроводу. Тому під підготовкою кадрів для галузі будемо розуміти систему, що включає всі рівні професійної освіти, перепідготовки та

підвищення кваліфікації фахівців. «В США освіта та підготовка здійснюється за великою кількістю програм та пропонує диверсифіковані шляхи набуття необхідних навичок. Освітні програми передбачають навчання як з набуттям сертифікатів так і програми, що передбачають одержання освітньо-кваліфікаційного рівня на базі середніх спеціальних або професійних закладів підготовки, а також програми, що пропонуються працедавцями, інтернатура, учнівство тощо» [3, с. 122].

З нашої точки зору суттєвою складовою реформ, що дасть позитивний результат при вирішенні досліджуваного питання стане інтегрований підхід до організації системи підготовки бакалаврів з кібербезпеки. Інтегрований підхід до вирішення поставлених завдань забезпечить якісну підготовку кадрів в галузі. З огляду на міжнародний характер проблем забезпечення кібербезпеки, корисно буде також використовувати при подальшому розвитку української системи підготовки відповідних кадрів, наявний світовий досвід у цій галузі шляхом інтеграції передових світових досягнень освіти шляхом запозичення досвіду США.

Коротко проаналізуємо, як вирішується проблема підготовки кадрів в області забезпечення кібербезпеки в інших країнах, і перш за все в США. Важливо відзначити, що в США протягом останніх 20 років під особливою суспільною увагою є питання захисту інформації та кібербезпеки. Так У 1998 році з метою запобігання, стримування, реагування та розслідування злочинів, спрямованих проти стабільності національної інформаційної інфраструктури було створено Національний центр захисту інфраструктури (National Infrastructure Protection Center) та трохи згодом Міжнародна асоціація фахівців з комп'ютерних досліджень (Міжнародна асоціація комп'ютерних фахівців-розслідувачів). Остання готує спеціалістів для комп'ютерно-технічної експертизи. В кінці 2009 року було створено Національний центр кібербезпеки (National Cyber Security і зв'язку Центр інтеграції), покликаний допомогти державі в розробці підходів до

вирішення проблем забезпечення ІБ, підвищити рівень освіти в цій сфері, а також координувати всі національні системи мережевого захисту. Співробітники даного центру займаються моніторингом і попередженням різного роду комп'ютерних атак. Окремо відзначимо компанії, які проводять навчання в області забезпечення кібербезпеки. Серед них слід виділити: Check Point Software Technologies, Cisco Systems, Microsoft, IBM Tivoli Systems Global Security Laboratory, Консорціум міжнародної сертифікації інформаційних систем безпеки, Internet Security Systems, Network Associates, Symantec. Крім згаданих приватних компаній, підготовку фахівців в області ІБ здійснюють і державні структури: аспірантура Військово-морської академії США пропонує дванадцять різних курсів, Агентство із захисту інформаційних систем (Defense Information Systems агентство то DISA) пропонує споживачам вісім різних курсів. Бере активну участь в цій роботі і коледж управління інформаційними ресурсами (Information Resource Management College).

Для вдосконалення методів навчання в міністерстві оборони США створено спеціальний підрозділ по управлінню програмами в галузі з кібербезпеки (Information Assurance Program Office). Агентством національної безпеки (АНБ) понад 10 років тому був сформований ряд центрів після вузівської освіти, до яких пізніше підключили 14 провідних університетів США. Одночасно Білий дім приступив до навчання урядовців (до 10 тисяч чол. щорічно) в рамках федеральної програми забезпечення безпеки інформаційних технологій. Після трагедії 11 вересня 2001 року, в містах США було впроваджено масове проведення семінарів, конференцій, зустрічей з проблем кіберзлочинності та кібертероризму. Навіть без детального розгляду структури підготовки фахівців в області забезпечення інформаційної безпеки та кібербезпеки в США, можна зробити висновок, що існуюча тут мережа підготовки фахівців потужна і

добре розвинена. Але навіть при таких масштабах, на думку експертів, в США відчувається нестача кваліфікованих фахівців даного профілю.

Наступним підходом, який ми пропонуємо до розгляду є досвід міжнародних консорціумів з сертифікації в області безпеки інформаційних систем у процесі підготовки бакалаврів з кібербезпеки. Міжнародні консорціуми є альтернативою здобуття сертифікату на професійну діяльність. Застосування цього досвіду відкриває додаткову можливість підвищити якість вітчизняної освіти. У США широко використовують такий спосіб підготовки кадрів через міжнародні консорціуми. Світовим лідером сертифікації фахівців з кібербезпеки є Міжнародний консорціум з сертифікації в області безпеки інформаційних систем (Консорціум міжнародної сертифікації безпеки інформаційних систем, Inc., або (ISC)2. Для отримання сертифікату Certified Information Systems Security Professional (CISSP) необхідно мати досвід роботи за фахом не менше 4 років (або 3 роки і ступінь бакалавра), здати непростий іспит, слідувати кодексу етики (ISC) 2 і постійно підтримувати свою кваліфікацію. Для підтвердження сертифікації CISSP досить кожні 3 роки проходити навчання на авторизованих курсах по ІБ, а також брати участь в конференціях за професійним спрямуванням [4].

На думку дослідників в США «традиційна сертифікація» – це програми навчання на базі 4-річних коледжів з напряму «освіта», що передбачає підготовку студентів та набуття ними базових компетенцій, які оцінюються через виконання письмових екзаменів відповідно до вимог штату [2; 6]. Термін «альтернативний шлях здобуття сертифікату на професійну діяльність» використовується в США для визначення всіх видів програм, які передбачають професійну освіту. Альтернативна сертифікація передбачає будь яке «відхилення» від традиційної спеціалізації у напрямі «освіта» та відкриває додаткову можливість підвищити якість вітчизняної освіти [2; 5].

У подальшому ході дослідження ми прийшли до висновку, що невід'ємним підходом у процесі підготовки бакалаврів з кібербезпеки є орієнтація на поєднання отримання освіти за партою з практикою через посилення зв'язків студента з можливо майбутнім місцем роботи. Однією з характерних особливостей світових систем підготовки бакалаврів з кібербезпеки США є орієнтованість на практику на засадах демократичних цінностей та чітко визначеним завданням: формування готовності майбутність фахівців шляхом поєднання навчання з практикою через посилення зв'язків студента з можливим майбутнім місцем роботи. Підготовка кадрів 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 між мережеві 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; - могти впроваджувати нове програмне забезпечення та / або технології; - проводити регулярні перевірки на відповідність використання.

Висновки та перспективи подальших наукових розвідок. Абсолютно очевидно, що задовольнити потребу в висококваліфікованих фахівцях в області забезпечення захисту інформації можна тільки на основі комплексного використання всіх можливостей середньої, вищої та альтернативної професійної освіти шляхом сертифікації, використовуючи підготовку кадрів у консорціумах міжнародного рівня. Підхід орієнтований на практику, через заплановане посилення зв'язків студента з можливим

майбутнім місцем роботи дозволяє побудувати єдину стрункy систему підготовки кадрів на основі безперервності освітнього процесу і задовольнити широкий спектр пропонованих споживачами вимог як в змістовному, так і в кваліфікаційному аспекті. Крім того, забезпечення скільки-небудь ефективного захисту від негативної інформації можливе лише за наявності розвиненої законодавчої та нормативно-правової бази, процес створення якої в Україні ще далеко не завершений. Таким чином, в світлі реалізації положень доктрини інформаційної безпеки і стратегії розвитку інформаційного суспільства в Україні стоїть досить складне завдання у цій галузі реформування шляхом інтеграції передового досвіду США в галузі вищої освіти.

БІБЛІОГРАФІЯ

1. Акредитація як механізм вимірювання якості освіти: досвід університетів США: матеріали науково-практичного семінару, (Київ, 17 черв. 2010 р.) / НАПН України та ВНЗ України / За заг. ред. О. І. Локшиної та Н. І. Поліхун. – К.: Інформаційні системи, 2010. – С. 85-87

2. 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/

3. Пазюра Н. В. Особливості підготовки фахівців з середньою кваліфікацією в США / Н. В. Пазюра // Науковий вісник Мукачівського державного університету. Серія «Педагогіка та психологія». Випуск 2 (2), 2015. – С. 120-125.

4. Чванова М. С. Подготовка кадров в области информационной безопасности в США Гуманитарные науки. Педагогика и психология. / М. С. Чванова // Вестник ТГУ. Выпуск 8 (112), 2012. – С. 126-133.

5. Innovation in education: Alternative routes to teacher certification. U.S. department of education, office of innovation and improvement. Washington, D.C., 2004. – 70 p.

6. Rubino, N., Soltys, M., Wright, G., Young, R. Alternative Teacher Certification: An Avenue for Quality and Diversity in Public Education. Wilmington College, 1994. – 35 p.

ВІДОМОСТІ ПРО АВТОРА

Бистрова Богдана Василівна – ст.викладач кафедри авіаційної англійської мови, національного авіаційного університету

Коло наукових інтересів: інформаційні технології в навчанні іноземної мови, тестовий контроль в навчанні іноземної мови впровадження інформаційно-комунікаційних технологій навчання у навчальний процес.