УДК 37.378.004

БИСТРОВА Богдана Василівна,
старший викладач кафедри авіаційної англійської мови, Київський національний авіаційний університет
e-mail: DanaUkraine@yandex.ru

ОСОБЛИВОСТІ ФОРМУВАННЯ СИСТЕМИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ У ВНЗ США

У статті розглядаються особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ США. Актуальність застосування підходу визначається динамікою сучасного технологічного розвитку. Інноваційний підхід стає в сучасних умовах методологічною платформою для організації дослідницької та проектної роботи студентів, їх наукового спілкування з професійним співтовариством.

Ключові слова: *бакалавр; кібербезпека; професійна підготовка; кібернетичний простір; Агентство національної безпеки (АНБ).*

Постановка проблеми. Детально проаналізувати особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ США.

Аналіз останніх досліджень та публікацій. Вагоме значення мали праці відомих вітчизняних та зарубіжних учених щодо дослідження сучасних процесів глобалізації, інформатизації суспільства, впровадження новітніх інформаційних технологій у навчальний процес (С. Дорогунцов, П. Дракер, М. Кастельс, К. Колін, К. Мей, В. Нечитайло, М. Онопрієнко, Р. Роберт, П. Саух, А. Чернов та ін.). Проблеми професійної підготовки фахівців за кордоном знайшли висвітлення у дослідженнях вітчизняних науковців з проблем порівняльної професійної педагогіки Н. Бідюк, Т. Десятова, В. Коваленко, Т. Кошманової, К. Корсака, Н. Пацевко, Л. Пуховської, А. Сбруєвої, Н. Собчак, Б. Шуневича та ін.

Мета статті – проаналізувати особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ США.

Виклад основного матеріалу дослідження. Науково-технічна революція спричинила в усьому світі глибокі системні перетворення. Насамперед завдяки удосконаленню досягнень у сфері новітніх інформаційних технологій із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем, сформувалися принципово нові всеохоплюючі матерії – інформаційне суспільство, а також інформаційний та кібернетичний простори, які на сьогоднішній день охоплюють практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

На сьогоднішній день існує необхідність у поглибленому аналізі інтеграційних процесів у різних галузях інформаційної безпеки, зокрема кібербезпеки, у зв'язку з розвитком ІТ-галузі і її проникненням в ключові компоненти професійної діяльності, так і в компоненти освітнього середовища самого ВНЗ. Крім того, стрімко розвиваються інноваційні розробки у напрямку інтелектуалізації інструментів професійної діяльності фахівця з кібербезпеки, що неминуче змушує задуматися про необхідність включення в освітнє середовище інфраструктурних компонентів розвитку інноваційної діяльності студентів та її вплив.

Найбільш досконало розвиненою системою на сьогоднішній день є система кіберзахисту критично важливої інфраструктури, насамперед інформаційної і кібернетичної, знищення або ураження якої призводить до втрати робото здатності відповідного простору й ставить під загрозу як суспільну так і державну безпеку в цілому, функціонує у США. Потреба у випускниках, здатних створювати інноваційний продукт або послугу, змушує вузи США формувати належну інноваційну інфраструктуру. Відповідно до цих позицій, розглянемо проблеми формування сучасного освітнього середовища у ВНЗ для підготовки бакалаврів в області кібербезпеки США. Слід зазначити, що національну політику країни в цій сфері формує Агентство національної безпеки (АНБ), 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 [1].

Для розуміння як формується сучасне освітнє середовище у ВНЗ США для підготовки фахівців в області кібербезпеки слід розглянути національну систему вищої освіти [2], приділяючи особливу увагу освітнім програмам бакалаврів в галузі кібербезпеки США [3]. Система має певну особливість що полягає у децентралізації управління освітою на рівні штатів. Практично всі питання освітньої політики вирішуються саме на цьому рівні, хоча існують і окремі федеральні програми, що фінансуються і контрольовані Міністерством освіти США. Система вищої освіти включає в себе коледжі та університети, загальне число яких перевищує 4300. Чотирирічна освіта в США дає можливість отримати академічні ступені бакалавра, професійні кваліфікації та професійно-технічні кваліфікації. Найбільш конкурентоспроможними освітніми програмами серед бакалаврів є: «Розслідування комп'ютерних інцидентів», «Інформаційна безпека», «Комп'ютерна безпека», «Безпека комп'ютерних мереж».

Детальніше розглянемо підготовку бакалаврів в області кібербезпеки. Перш за все вона базується на теоретичній та практичній основі, що дає студентам можливість опановувати технічні і аналітичні можливості для захисту даних, файлів, ресурсів комп'ютера, комп'ютерної мережі, застосування розумної політики безпеки в бізнесі і державних органах, а також захист критично важливих національних електронних інфраструктур. Студенти навчаються установці програмного забезпечення систем безпеки, моніторингу мережі з метою виявлення вторгнень, реагування на кібератаки, збору даних і доказів. [4]

Слід зазначити, що особливістю освітніх програм США є відсутність дисциплін з фізичного захисту та інженерно-технічного захисту інформації, традиційні для українських освітніх програм (які орієнтовані на збереження конфіденційності інформації). Американські освітні програми багато часу відводять на вивчення дисциплін, пов'язаних із забезпеченням інформаційної безпеки у відкритих бізнес системах і електронної комерції.

Всі програми підготовки бакалаврів розраховані на чотири роки навчання, після чого присуджується ступінь бакалавра комп'ютерних наук зі спеціалізацією в обраній галузі. Вагома кількість предметів являють собою обов'язкові курси навчання, які є спеціалізованими. Для кожного напряму підготовки характерне поєднання дисциплін з різних областей. Наприклад, для напряму підготовки «Кібербезпека» основними обов'язковими дисциплінами є: інформаційна безпека, розслідування комп'ютерних інцидентів, управління інформаційною безпекою, міжмережеві екрани і виявлення вторгнень, безпеку бездротових мереж, IT-аудит. Існують й дисципліни за власним вибором студента, що значно підвищує захопленість та цікавість студентів до змісту навчання. Студенти можуть самостійно вибрати невелику кількість дисциплін (3–4) за вибором, спрямованих на засвоєння додаткових знань та навичок в обраній галузі підготовки. До дисциплін за вибором відносяться: соціальні аспекти інформаційної безпеки, дані і інтелектуальний аналіз, безпеку розподілених баз даних, безпека електронної комерції, політика інформаційної безпеки, прикладна криптографія, практичні питання безпеки, спеціальні питання інформаційної безпеки, незалежні дослідження. Виходячи з цього, очевидно, що в американській системі навчання фахівців в області кібербезпеки дотримуються широкого профілю підготовки [5]

Як правило, студенти проходять практику протягом всього курсу навчання. У першому семестрі студенти в рамках практики проводять пошук літератури, складають план досліджень і ініціюють наукові дослідження або конструкторські роботи за фахом. Студенти старших курсів займаються вже безпосередньо дослідженням. Іншою частиною навчання є стажування, спрямоване на можливість придбання значущих навичок і професійних якостей і вивчення досвіду в промисловості, державних, приватних або бізнес структурах. Закінчується навчання в бакалавраті виконанням бакалаврського проекту під керівництвом викладача або групи професорсько-викладацького складу. Як правило, в кінці бакалаврату

студент має можливість отримати один з професійних сертифікатів, що підвищує його конкурентоспроможність на ринку праці.

На основі виявлених ключових відмінностей в розглянутих освітніх програмах можна виявити особливості формування освітнього середовища для підготовки бакалаврів з кібербезпеки в США:

– впровадження дисциплін, пов'язаних з розслідуванням комп'ютерних інцидентів;

– збільшення частки матеріалу, орієнтованого на правозастосовні технології в області кібербезпеки, в тому числі засновані на міжнародному праві;

– включення дисциплін, пов'язаних з впровадженням технологій інформаційної безпеки в бізнес, електронну комерцію, комерційним застосуванням інтелектуальних прав.

Виходячи з цього слід узагальнити, що такий підхід до організації навчання дозволяє випускникам володіти ключовими компетенціями: здатністю інсталювати і адмініструвати ресурси стандартних операційних систем і пристроїв зберігання даних, здатністю виконувати адміністративні функції, пов'язані з доступністю інформації та інформаційними технологіями, здатністю визначити відносини між інформаційними технологіями та юридичним аспектом комп'ютерної експертизи, здатністю застосовувати навички, пов'язані з документуванням обліку даних, отриманих з цифрових пристроїв, здатністю застосовувати фундаментальні судові методи в області інформаційних технологій, здатністю застосовувати політику для захисту комп'ютерних систем від кіберзагроз.

Висновки і перспективи подальших досліджень. Проведений аналіз американського досвіду професійної підготовки бакалаврів у сфері кіберзахисту дозволить у майбутньому окреслити можливості використання його прогресивних ідей у системі вищої освіти України, зокрема: удосконалення галузевих стандартів вищої освіти для підготовки бакалаврів з кібербезпеки (доповнення та структурування переліку спеціальностей з кіберзахисту у національному класифікаторі); забезпечення інформаційної підтримки довідкових Інтернет ресурсів; розробка й удосконалення змісту навчальних планів і освітніх програм для підготовки бакалаврів з кіберзахисту; удосконалення навчально-методичного забезпечення; ґрунтовне вивчення зарубіжного досвіду. Успішна реалізація обґрунтованих можливостей сприятиме удосконаленню професійної підготовки вітчизняних фахівців з кіберзахисту, прискоренню процесу реформування вітчизняної системи вищої освіти, наближенню до світових освітніх стандартів, забезпеченню їх конкурентоздатності на сучасному ринку праці.

Список використаної літератури

1. Макаренко Є.А. Геополітіка и прагматика стратегії зміцнення світового лідерства США у XXI столітті / Є.А. Макаренко // Дослідження світової політики. – 2012. 4 (61). – С. 3–12.
2. Чванова М.С., Анурьева М.С. Подготовка кадров в области информационной безопас-ности в США / М.С. Чванова, М.С. Анурьева // Вестник Тамбовского университета. Серия: Гуманитарные науки. Тамбов, 2012. – №8 (112). – С. 126–133.
3. Master of Science in Information Assurance and Security. Retrieved from http://www.mercy.edu/academics/school-of-liberal-arts/department-of-mathematics-and-cis/ms-in-informa-tion-assurance-and-security.
4. NIST, National Initiative for Cybersecurity Education Strategic Plan, National Institute of Standards and Technology (NIST), Editor. 2012, NIST: Washington, DC. p. 26.
5. DHS Task Force on CyberSkills, CyberSkills Taks Force Report, D.o.H. Security, Editor. 2012: Washington, DC. p. 1–41.

References

1. Makarenko, A.. (2012) Geopolitics and pragmatic strategies to strengthen the US global leadership in the XXI century. *Study of World Politics*. 4 (61). 3–12.
2. Chvanova, M., Anureva, M. (2012). Personnel training in information security sphere in the U.S.A. *Bulletin of the University of Tambov. Series: Humanities, Tambov, 8(112), 126–133*.
3. *Master of Science in Information Assurance and Security*. (2017). Retrieved from http://www.mercy.edu/academics/school-of-liberal-arts/department-of-mathematics-and-cis/ms-in-informa-tion-assurance-and-security.
4. NIST (2012). *National Initiative for Cybersecurity Education Strategic Plan*. National Institute of Standards and Technology (NIST), Editor. NIST: Washington, DC, 26.
5. *DHS Task Force on CyberSkills* (2012). CyberSkills Taks Force Report, D.o.H. Security, Editor. Washington, DC, 1–41.

BYSTROVA Bohdana,
Lecturer of the Department of Aviation English, National Aviation University (Ukraine)
e-mail: DanaUkraine@yandex.ru

SPECIFIC FEATURES OF FORMATION OF THE SYSTEM OF PROFESSIONAL TRAINING OF FUTURE BACHELORS IN CYBER SECURITY AT HIGHER EDUCATIONAL ESTABLISHMENTS IN THE USA

Abstract. *This paper 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. An innovative approach is a methodological platform for research and students' project work, their communication with professional scientific community.*

Purpose. The purpose of the article is to analyse in detail the basic features of the professional training of cyber security bachelor's degree in the U.S. higher education system.

Conclusion. 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 (additions and structuring the list of majors with the Cyber security in the national qualifier); 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.

Key words: *bachelor; cyber security; training; cyber space; the National Security Agency (NSA).*

Одержано редакцією 27.02.2017
Прийнято до публікації 03.03.2017