УДК 005.336.2:004.72.056.52(045)

Олена Матвійчук-Юдіна,
старший викладач, пошукач кафедри комп'ютерних мультимедійних технологій Національного авіаційного університету

ІНДУСТРІАЛЬНА МОДЕЛЬ ЯК ОСНОВА ФОРМУВАННЯ ПРОФЕСІЙНИХ КОМПЕТЕНТНОСТЕЙ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

У статті розглянуто сучасні підходи до формування компетентностей бакалаврів спеціальності «Кібербезпека» в Україні. Проаналізовано розбіжності у тлумаченні понять «фахова» або «спеціальна» компетентности бакалаврів спеціальності «Кібербезпека». У статті визначено основні чинники формування компетентностей бакалаврів спеціальності «Кібербезпека». Розкрито особливості основного підходу формування професійних або фахових компетентностей бакалаврів спеціальності «Кібербезпека» за індустріальною моделлю США.

Ключові слова: *індустріальна модель, компетентності, фахівці кібербезпеки, професійний стандарт.*

В статье рассмотрены современные подходы к формированию компетенций бакалавров специальности «Кибербезопасность» в Украине. Проанализированы разночтения в толкований понятий «профессиональной» или «специальной» компетентностей бакалавров специальности «Кибербезопасность». В статье определены основные факторы формирования компетентностей бакалавров специальности «Кибербезопасность». Раскрыты особенности основного подхода формирования профессиональных или специальных компетентностей бакалавров специальности «Кибербезопасность» в соответствии индустриальной модели США.

Ключевые слова: *индустриальная модель, компетентности, специалисты кибербезопасности, профессиональный стандарт.*

In the article considered modern state of the approach to the formation of competence of bachelors of specialty cybersecurity in Ukraine. Shown the problem of differences professional or special competencies of bachelors of specialty «Cyber Security». Determined features of the basic approach of formation professional competences for bachelors of specialty «Cyber Security» according to the industrial model of the USA. As a result of research we can draw the following conclusion that in the existing programs of the leading technical Higher education institutions of Ukraine approaches in the formation of professional competencies unequivocally present directions of knowledge provision in accordance with the educational field of knowledge «Information Technologies». However, these are indicated in the knowledge programs and

skills do not emphasize the difference special competencies of specialists in the specialty «Cyber Security» and practically do not differ from the general competences of the specialties «Computer Science» or «Computer Engineering». Defined the list and the classification of the basic professional and specialty competence of a specialist taking into account the world standardization system of the Industrial Model. Included modern requirements to specialists of the IT industry in the specialty «Cyber Security». Determined features of the basic approach of formation professional or specialty for bachelors of specialty «Cyber Security» according to the industrial model of the USA by properties of the information system and with considering international standards and requirements.

Key words: *industrial model, professional competence of cybersecurity specialists, information system, system of standardization, computer graphics.*

Сучасне суспільство країни, а також Міністерство освіти і науки України (МОНУ) обрало напрям на адаптацію системи атестації та/або сертифікації студенів і слухачів спираючись на світовий досвід підготовки фахівців, а саме розділяючи питання освітньої та професійної атестації. Даний розподіл не притаманний вищим навчальним закладам (ВНЗ) України та був введений тільки в 2016 році, що підтверджує Наказ Міністерства освіти і науки України від 09.11.2015 № 1152 «Про визнання таким, що втратив чинність, Наказ Міністерства освіти і науки України від 24 травня 2013 року» № 584. Таким чином, було відмінено «Положення про порядок створення та організацію роботи державної екзаменаційної комісії у вищих навчальних закладах України» [1].

Такий підхід розділив питання розробки інформування, а також впровадження освітніх стандартів на освітні та професійні стандарти галузі.

Зрозуміло, що згідно освітнього стандарту (освітньої програми ВНЗ), виключно навчальний заклад, як і у всьому світі, відповідає за надання знань, які формують у студентів компетентності за майбутнім фахом. Однак, стандарт освітній, а компетентності фахові, спеціальні або професійні.

На базі вище викладеного, можна зробити висновок, що необхідно визначити відмінність значення поняття компетентності фахівця (фахова або спеціальна компетентність), згідно освітньої програми ВНЗ і освітнього стандарту МОНУ, та поняття професійної компетенції за професійним стандартом.

Світовий досвід подвійної освіти (з точки зору взаємодії університет-підприємство галузі) формує, так звану ступеневу форму атестації фахівців: освітня та професійна.

З метою введення системи професійної атестації формується інтеграційна структура громадських об’єднань (університети, великі світові ІТ підприємства, громадські об’єднання) для розробки і впровадження професійних стандартів освіти та професійних компетентностей фахівців галузі.

З викладеного вище, постає актуальне питання якими компетентностями, вміннями, знаннями повинен володіти фахівець з галузі знань Інформаційних технологій (ІТ) з спеціальності Кібербезпека (КБ) у відповідності сучасним світовим стандартам.

Метою статті є аналіз існуючих підходів та розробка моделі формування системи фахових або професійних компетентностей фахівців зі спеціальності «Кібербезпека» з урахуванням міжнародних стандартів та вимог сектору індустрії послуг.

Дослідження питань пов'язаних з підходом до формування компетентностей бакалаврів спеціальності кібербезпека на платформі індустріальної моделі до даного часу провідними науковцями країни офіційно не розглядалося. Основою даного висновку є те що цей підхід є новим не тільки для нашої країни, але й для всієї інформаційної спільноти. Формування стандартів галузі Індустрії та відповідних їм функцій підприємств, організацій, а також компетентностей фахівців галузі інформаційних технологій та їх безпеки, сформувався тільки в період 2009–2016 р. Основними розробниками стандартів індустрії є громадські організації, так званої ініціативи робочої сили та освіти США.

Індустріальна Модель та професійні компетентності фахівців зі спеціальності «Кібербезпека».

Професійні компетентності ґрунтуються на наданих знаннях, формують навички і повинні відповідати професійним вимогам фахівця, щодо забезпечення і можливості надання переліку відповідних послуг інформаційної системи або безпосередньо організації чи установи. З цього приводу, на базі сукупності встановлених послуг для задоволення потреб особистості, суспільства та держави формується так звана – Індустріальна модель галузі [2].

Зазначена модель включає перелік базових, а також перелік обов'язкових професійних компетентностей та перелік установ організацій, центрів для навчання і подальшої професійної атестації (сертифікації).

Індустріальна модель Кібербезпеки, (Cybersecurity Industry Model USA) – це Модель Промисловості, що розроблена для систематизації та впровадження певного переліку компетентностей індустрії послуг, яким потрібно володіти фахівцям, чия професійна діяльність пов'язана з організацією безпеки кіберпростору (Переклад автора) [3].

Впровадження цієї Моделі поширюється на всі кваліфікаційні рівні (включно професійна сертифікація), від рівня – практик або користувач інформаційно-комунікаційними системами та мережами, до вищого рівня – професіонал.

З урахуванням вище зазначеного та враховуючи базові функції інформаційної системи, автор пропонує власне визначення поняття Індустріальної моделі.

Індустріальна модель Кібербезпеки (Cybersecurity Industry Model), – Промислова Модель менеджменту, яка розробляється та впроваджується з

метою представлення необхідного рівня професійних компетентностей фахівців підприємств, організацій та установ різних форм власності, чия діяльність пов'язана з системою обробки, передачі, збереження, захисту та висвітлення даних в кіберпросторі [3].

Метою Індустріальної моделі Кібербезпеки є визначення базових стратегій та політик послуг та процесів освіти сектору індустрії тощо, а також системи освітніх і професійних стандартів галузі інформаційної та\або КБ.

Індустріальна модель – певний перелік дій, функцій, компетентностей та задач фахівців в кіберпросторі (захист від несанкціонованого втручання, використання або модифікації інформаційних ресурсів, порушення режимів експлуатації та сталих бізнес процесів, системи надання послуг, тощо), а саме в інформаційних системах різних класів, інформаційно-комунікаційних системах та мережах загального та спеціального призначення, сховищах баз даних та знань тощо.

Наукові дослідження показали, що «кіберпростір» – це термін, який містить в собі не лише питання ІТ, але і більш широкий пласт Інформаційної Інфраструктури: інформаційне суспільство та його взаємозв'язки, устаткування і програмне забезпечення, системи висвітлення, передавання, обробки і зберігання даних, законодавчу базу та кадрові ресурси тощо.

Підтвердженням досліджень автора, є практично єдине визначення на даний час в законодавчих і нормативно-правових документах держави:

Кібернетична безпека – стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави [4].

Визнанням вважливості роботи інтеграційних структур суспільства, тобто громадських об'єднань і організацій (університети, великі світові ІТ підприємства, громадські фонди, тощо) для розробки і впровадження стандартів освіти та формування професійних компетентностей фахівців галузі є існування Громадських об'єднань Національної Ініціативи, а саме груп Робочої Сили та Освіти з КБ США [5]. Представлені об'єднання є розробниками Індустріальної моделі Кібербезпеки 2014 року, (Cybersecurity Industry Model USA – 2014), яка зараз визнана урядом США і світовою промисловістю, як стандарт галузі [6].

Зауважимо, що визначення термінів та їх зміст з галузевої точки зору (Глосарій галузі з Кібербезпеки, Glossaryofcommon Cybersecurityterms) формує у взаємозв'язку, ще одне громадське об'єднання – Громадське об'єднання Національної Ініціативи Кар'єри та Навчання (National Initiative for Cybersecurity Careersand Studies (NICCS)) [7]. Звертаючись до теми досліджень розділу, наведемо визначення поняття компетентності згідно Глосарію галузі з Кібербезпеки (NICCS, USA).

Компетентність – кластер взаємопов'язаних знань, навичок та

здібностей фахівця, що впливає на якісне виконання професійної роботи(ціль, функції та відповідальність), а також взаємопов'язаний з виконанням фахових дій з урахуванням всіх типів стандартів галузі та може бути вдосконалений через процеси навчання, особистого розвитку і професійної досвідченості (переклад автора) [8].

Межа між визначеннями Фахові (спеціальні) за вітчизняними вимогами МОНУ або Професійні компетентності промисловості за світовою системою, достатньо тонка. Згідно Методичних рекомендацій МОНУ, схваленої сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України від 29.03.2016 №3 «Щодо розроблення стандартів вищої освіти» пропонується визначення понять інтегральна компетентність та, як її складові загальні і фахові (спеціальні) компетентності [9].

Освітній стандарт повинен включати 2 види компетентності – загальні та фахові, формуючи навички сучасного студента.

Детально досліджуючи різні класи компетентностей (5 класів) за Індустріальною моделлю США, можемо визначити Академічну Компетентність фахівця (перелік класичних знань і предметів її формування), або такі, що формують робочі навички, які найбільше вимагають працедавці галузі: спеціальні (специфічні); компетентності промисловості (Технічні та Функціональні Компетентності області індустріального сектору). Такий підхід до формування кометентностей особистості, розроблений громадськими установами, університетами та ведучими організаціями, визнається світовою спільнотою та державними установами, як: стандарт освітньо-професійної діяльності галузі.

На базі викладеного, автор наголошує про розробку нової моделі до формування та класифікації компетентностей фахівців з урахуванням вітчизняних вимог до впровадження освітніх і в майбутньому професійних стандартів сфери ІТ та КБ.

Згідно світового досвіду і вимог сектору індустрії, та враховуючи освітньо-професійні стандарти галузі, а саме стандарт Індустріальної моделі Кібербезпеки, можемо визначити першу складову моделі формування компетентностей фахівця з кібербезпеки для освітніх та професійних стандартів галузі.

Класифікація компетентностей за освітнім стандартом: фундаментальні компетентності; особисті; академічні (замість загальна) [9]; фахові (спеціальні); робочого місця.

Класифікація компетентностей за професійним стандартом галузі включає всі чотири попередні та дві Професійні Компетентності Промисловості (сектор індустрії): професійні компетентності промисловості; технічні компетентності; функціональні компетентності.

Зрозуміло, що згідно рекомендацій МОНУ, не має можливості внести додаткові зміни та сформувати розділи та розширити їх за змістом стандарту Академічними та Компетентностями Робочого місця (присутня наявність

тільки фахових або спеціальних) тощо. Проте наступним кроком МОНУ, згідно світової системи атестації, має бути розробка і впровадження професійних стандартів, змістовною частиною яких, зрозуміло, будуть професійні компетентності.

Автор вважає, що узагальнення та обмеження представлення спеціальних компетентностей в освітньому стандарті безперечно приведе до невідповідності наближення освітніх процесів ВНЗ до потреб ІТ-індустрії. Таким чином, в подальшому професійний стандарт повинен бути більш розширений та деталізований для галузі.

Світовий досвід вказує, що Професійні (фахові, спеціальні) компетентності за освітньою програмою ВНЗ розвинених країн, відрізняються тільки невеликими розбіжностями від Стандарту Індустріальної Моделі, що формують перелік предметів навчання за встановленою пропорцією з базових Доменів освіти Індустріальної Моделі (або певний перелік вільного вибору ВНЗ) згідно напрямів подальшої спрямованості професійної атестації ІТ фахівців.

Наприклад, освітньо-професійні вимоги та переліки Професійних Компетентностей та відповідних їм Доменів освіти (включно предметів) Громадських об'єднань Information Systems Audit and Control Association (ISACA) [10] або Certified Information Systems Security Professional (CISSP) [11].

Стандарт Індустріальна модель повинен включати базові складові: мету і задачі введення індустріальної моделі; базові функції організацій і установ (їх інформаційних систем) та перелік послуг галузі; систему взаємодії між суб'єктами інформаційної і правової діяльності галузі; критерії якості надання послуг; професійні компетенції фахівців галузі з урахуванням забезпечення гарантованої якості надання послуг сектора індустрії; перелік навчальних закладів, центрів, підприємств та громадських організацій, що надають освітні та сертифікаційні послуги за певними освітніми програмами та встановленими системами світової сертифікації різних видів та класів; перелік первинних посад фахівців згідно системи освітньої та/або професійної атестації тощо.

Наведемо приклади таких відомих установ та університетів з світовим визнанням та досвідом. Університети та Центри, які проводять освітню та сертифікаційну діяльність в галузі Кібербезпеки:

Moraine Valley Community College- IT Security Specialist –Associate in Applied Science Degree;

Bellevue University – Cybersecurity Degrees (BS, MS); Computer Information Systems BS Degree; Management of Information Systems MS Degree; Master of Business Administration with a concentration in Cybersecurity of Management Information Systems;

Oklahoma City Community College – Cyber/Information Security A.A.S. and Certificate of Mastery;

Prince George's Community College – Information Security A.A.S.;

Cybercrime Investigation OPT. Criminal Justice, A.A.S.; Information Security Management Certificate; Cybercrime Investigation Certificate; Information Security Certificate.

Дана форма стандартизації індустрії послуг склалася практично в останні два роки та за своїм змістом наявно є не тільки галузевим стандартом послуг, а однозначно,освітнім або освітньо-професійним стандартом галузі за наявністю в змісті розширеного переліку професійних компетенцій і компетентностей, переліку навчальних закладів, їх програм, форм атестацій, а також переліку базових посад у відповідності кваліфікаційному рівню бакалавр та магістр.

Дана система підготовки кадрів має двохступеневу професійну освіту: 1) рівень бакалавр-практик (Systems Security Certified Practitioner, SSCP); 2) рівень магістр-професіонал. (Certified Information Systems Security Professional, CISSP).

Принцип 14-ти доменної структури надання освіти впроваджено і в сучасний стандарт 125 спеціальності з кібербезпеки України та має 12 фахових компетентностей згідно світової та вітчизняної системи стандартизації. Додаток №1.

ISC² 14 (2016) Перелік освітніх «Доменів» в галузі «Кібербезпека» за системою сертифікації ISC² 14 (2016): політика інформаційної безпеки; організація інформаційної безпеки; кадрові ресурси та їх безпека; управління активами; управління доступом; криптографія; фізична і екологічна безпека; функціонування інформаційної безпеки.; безпека інформаційно-комунікаційних систем; придбання, розробка та обслуговування системи; відносини з постачальниками; управління інцидентами інформаційної безпеки; аспекти інформаційної безпеки та управління безперервністю бізнесу; дотримання внутрішніх вимог, таких як політики, зовнішні вимоги, вимоги законодавчої бази.

Відстежуючи сучасні тенденції розвитку професійної освіти в галузі кібербезпеки, слід констатувати, що з березня 2017 року частина освітніх доменів була об’єднана світовою спільнотою галузі IT та кібербезпеки у нову оптимізовану форму з восьми освітніх доменів.

Освітні «Домени» в галузі Кібербезпеки за вимогами ISC² 8 domen (2017): Security and Risk Management (Безпека та Ризик Менеджмент); Asset Security (Безпека управління ресурсами); Security engineering (Інженерія систем безпеки); Communications and Network Security (Безпека інформаційно-комунікаційних систем); Identity and Access Management (Менеджмент систем ідентифікації та доступу); Security Assessment and Testing (Тестування та оцінка ефективності систем безпеки); Security Operations (Безпека процесів); Software Development Security (Безпека розробки (розвитку) програмного забезпечення).

У статті було проведено аналіз існуючих підходів та розроблено модель формування системи фахових або професійних компетентностей фахівців зі спеціальності «Кібербезпека» з урахуванням міжнародних

стандартів та вимог сектору індустрії послуг. На базі вище викладеного можна зробити висновки про наявність розбіжностей у тлумаченні значення поняття «компетентності фахівця», а саме фахова або спеціальна компетентність згідно освітньої програми ВНЗ і освітнього стандарту МОНУ та поняття професійної компетентності за професійним стандартом.

Виконане дослідження не вичерпує всіх аспектів проблеми. Перспективним напрямом подальших досліджень може бути вивчення проблеми формування професійної компетентності відповідно вимог професійного стандарту та оновлення змісту стандарту МОНУ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наказ Міністерства освіти і науки України від 09.11.2015 № 1152 Про визнання таким, що втратив чинність, наказу Міністерства освіти і науки України від 24 травня 2013 року №584, [Електронний ресурс] http://zakon2.rada.gov.ua/laws/show/z1457-15
2. Cyber security Competency Model, – 2017, [Електронний ресурс]. – Режим доступу: https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx
3. Industry models [Електронний ресурс] – Режим доступу: https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-home.aspx
4. Рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15 березня 2016 року № 96, [Електронний ресурс] – Режим доступу: http://www.president.gov.ua/documents/962016-19836
5. National Initiative for Cybersecurity Education’s (NICE) National Cybersecurity Workforce Framework), [Електроннийресурс] – Режим доступу: https://www.nist.gov/itl/applied-cybersecurity/nice
6. Cybersecurity Industry Model USA – 2014, [Електронний ресурс] – Режим доступу: http://niccs.us-cert.gov/research/draft -national-cybersecurity-workforce-framework-version-20
7. Glossary of common Cyber security terms [Електронний ресурс] – Режим доступу: https://niccs.us-cert.gov/glossary
8. Cyber Competitions [Електронний ресурс] – Режим доступу: https://niccs.us-cert.gov/formal-education/cyber-competitions
9. Методичні рекомендації щодо розроблення стандартів вищої освіти. Схвалено сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України протокол від 29.03.2016 №3, [Електронний ресурс] – Режим доступу: http://sau.kiev.ua/docs/20161220/recomendations.doc
10. Information Systems Audit and Control Association (ISACA), [Електроннийресурс] – Режим доступу: https://www.isaca.org/pages/default.aspx