УДК: 378:[007.001.25:004.056]

С.Р. КРАСИЛЬНИКОВ
Хмельницький національний університет

РОЗРОБКА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ПІДГОТОВКИ ФАХІВЦІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА» НА КОМПЕТЕНТНІСНІЙ ОСНОВІ

В статті проаналізована динаміка зміни переліку спеціальностей із захисту інформації, висвітлено підходи до розроблення освітньо-професійної програми підготовки фахівців спеціальності «Кібербезпека» на компетентнісній основі, охарактеризовано набір професійних компетентностей фахівця із захисту інформації, до яких віднесено соціально-особистісна, загальнонаукова, експериментальна, проектувальна, технологічна, організаційно-управлінська. Зміст кожної складової професійної компетентності розкрито через набір результатів навчання, які має досягти здобувач вищої освіти під час вивчення обов'язкових та вибіркових дисциплін. Доведено, що використання компетентнісного підходу при розробленні освітніх програм сприяє формуванню професійної компетентності майбутнього фахівця, підвищенню його конкурентоздатості на ринку праці.

Ключові слова: захист інформації, кібербезпека, компетентнісний підхід, освітньо-професійна програма.

S.R. KRASILNIKOV
Khmelnitsky National University

DEVELOPMENT OF EDUCATIONAL AND PROFESSIONAL TRAINING PROGRAMME SPECIALTY "CYBERSECURITY" ON THE BASIS COMPETENCE

The article analyzed the dynamics of changes in the list of specialties in information security, highlights approaches to the development of education and vocational training program of the specialty "cyber security" on the basis of competence. Consider revising a set of professional competences specialist in information security which include social, personal, scientific, experimental, design, technological, organizational and managerial. The content of each component of professional competence solved through a set of learning outcomes achieved applicant has higher education during the compulsory and optional subjects. It is proved that the use of competency approach in developing educational programs promotes the professional competence of future specialist, increased its competition the labour market.

Keywords: data protection, cyber security, competence approach, educational and professional program.

Постановка задачі

У зв'язку з впровадженням Закону України «Про вищу освіту» [1] актуальним є розроблення освітніх програм (ОП) підготовки фахівців за спеціальностями нового Переліку-2015 [2]. Особливо складним виявляється завдання створення ОП, які об'єднують у собі декілька напрямів та спеціальностей попередніх переліків [3, 4]. До них можна віднести спеціальність 125 «Кібербезпека».

Ретроспективний аналіз переліків напрямів підготовки і спеціальностей у вітчизняній вищій освіті свідчить про те, що захист інформації як об'єкт підготовки фахівців з'явився у 90-і роки XX сторіччя. На думку фахівців, це пов'язується зі стрімким розвитком комп'ютерної техніки і розвитком мережевих інформаційних технологій, зокрема, із поширенням сервісів Internet.

Так, у Переліку-1994 [5] у напрямі 6.0924 «Телекомунікації» з'явилася спеціальність «Захист інформації у телекомунікаційних системах», а у напрямі 6.0915 «Комп'ютерна інженерія» – спеціальність «Захист інформації в комп'ютерних системах» для кваліфікаційних рівнів молодшого спеціаліста і спеціаліста. Наступний перелік напрямів та спеціальностей 1997 року [6] містив два напрями підготовки 1601 «Інформаційна безпека» та 1602 «Національна безпека», у яких зосереджувався набір спеціальностей щодо захисту інформації у військовій справі та спецзв'язку для освітньо-кваліфікаційних рівнів бакалавра, спеціаліста та магістра.

Перелік напрямів підготовки 2006 року зберіг підходи щодо підготовки фахівців із захисту інформації за двома галузями 1601 «Військові науки» і 1701 «Інформаційна безпека». При цьому галузь 1701 «Інформаційна безпека» містила три базових бакалаврата: 6.170101 «Безпека інформаційних і комунікаційних систем»; 6.170102 «Системи технічного захисту інформації»; 6.170103 «Управління інформаційною безпекою».

Щодо ОКР спеціаліста (магістра) спектр спеціальностей із захисту інформації містив такі назви: 7.17010101 (8.17010101) «Безпека інформаційних і комунікаційних систем», 7.17010102 (8.17010102) «Безпека державних інформаційних ресурсів», 7.17010201 (8.17010201) «Системи технічного захисту інформації, автоматизація її обробки», 7.17010301 (8.17010301) «Управління інформаційною безпекою», 7.17010302 (8.17010302) «Адміністративний менеджмент у сфері захисту інформації».

Згідно з чинними на той час галузевими стандартами вищої освіти кожна із зазначених спеціальностей мала свій узагальнений об'єкт діяльності, набір виробничих функцій, типових задач діяльності та компетенцій щодо вирішення цих задач, що зумовлювало різний зміст освітньо-професійної програми підготовки фахівців. З прийняттям нового переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, усі вище зазначені спеціальності інтегрувалися в одну під загальною назвою «Кібербезпека».

Виклад основного матеріалу роботи

За даними [7] підготовку фахівців з вищою освітою у галузі знань «Інформаційна безпека» на ОКР бакалавра здійснюють 28 вітчизняних ВНЗ, а у галузі 1601 «Військові науки» - 24 вищі навчальні заклади.

Відповідно до «Методичних рекомендацій щодо розроблення стандартів вищої освіти» [8], які базуються на компетентісному підході, до освітніх програм висуваються такі вимоги:

1) обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти;

2) перелік компетентностей випускника;

3) нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання;

4) форми атестації здобувачів вищої освіти;

5) вимоги до наявності системи внутрішнього забезпечення якості вищої освіти;

6) вимоги до професійних стандартів (у разі їх наявності).

Структурно освітня програма складається з двох блоків інформації: обов'язкового та рекомендованого [9]. До обов'язкового блоку відносяться:

- титул програми;
- інформація про факультет (кафедру);
- цілі освітньої програми;
- складові професійної компетентності та результати навчання;
- матриця зв'язку між навчальними дисциплінами (модулями) та результатами навчання (компетентностями);
- перелік навчальних дисциплін (модулів) та їх анотації;
- форми організації та технології навчання;
- форми та методи оцінювання результатів навчання.

До рекомендованого блоку відносяться:

- вимоги до вступу та продовження навчання;
- підтримка студентів (система тьюторства, гранди тощо);
- соціально-економічне та інформаційно-технологічне забезпечення освітнього процесу;
- працевлаштування випускників та кар'єрні перспективи;
- механізм внутрішнього забезпечення якості вищої освіти;
- індикатори якості освітньої програми.

Освітня програма бакалавра «Кібербезпека» передбачає обсяг підготовки 240 кредитів ЄКТС, метою якої є формування особистості фахівця, здатного вирішувати типові та складні професійні завдання в галузі інформаційної безпеки. Фокус програми спрямований на галузях техніки та технологіях, що охоплюють сукупність проблем, пов'язаних з забезпеченням захисту об'єктів інформатизації в умовах існування загроз в інформаційній сфері. Особливість програми полягає у інтегрованій підготовці фахівців до вирішення завдань у сфері інформаційної безпеки, що передбачає розроблення, впровадження та експлуатацію комплексних (інформаційних, телекомунікаційних, технічних) систем захисту інформації на об'єктах інформаційної діяльності.

Складовими професійної компетентності виокремленні: соціально-особистісна (СО), загальнонаукова (ЗН), експериментальна (ЕК), проектувальна (ПР), технологічна (ТХ), організаційно-управлінська (ОУ). Зміст кожної складової розкривається через здатність та готовність реалізовувати різні функції у сфері захисту інформації. Так, технологічна складова трактується як здатність і готовність здійснювати встановлення, налаштування, експлуатацію та підтримку у робочому стані компонентів системи забезпечення компонентів інформаційної безпеки з урахуванням встановлених вимог.

Ключовим поняттям у компетентнісному підході є очікувані результати навчання (компетентності), якими має оволодіти здобувач відповідного ступеня вищої освіти. Згідно з [8] Програмними результатами навчання називають сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за певною освітньо-професійною, освітньо-науковою програмою, які можна ідентифікувати, кількісно оцінити та виміряти.

Для складових професійної компетентності фахівців з кібербезпеки сформовано 26 результатів навчання (таблиця 1) .

Таблиця 1

Результати навчання бакалаврів спеціальності 125 «Кібербезпека»

№ п/п	Результати навчання
1	2
1	РН СО1 Усвідомлювати необхідність дотримання правил і обов'язків громадянина України, громадянського обов'язку та прояву патріотизму
2	РН СО2 Уміння враховувати основні економічні закони, екологічні принципи та застосовувати знання у професійній діяльності
F3	РН СО3 Уміння враховувати процеси соціально-політичної історії України, правові засади та етичні норми у виробничій або соціальній діяльності

Продовження табл. 1

1	2
F4	РН СО4 Уміння спілкування, включаючи усну та письмову комунікацію українською мовою та принаймні однією із поширених європейських мов
F5	РН СО5 Уміння взаємодіяти із іншими людьми та працювати у команді
F6	РН СО6 Усвідомлення необхідності дотримання здорового образу життя
F7	РН СО7 Уміння самостійно здобувати нові знання, підвищувати свою кваліфікацію та майстерність
F8	РН ЗН1 Уміння застосовувати набуті знання основних природничо-наукових законів, використовувати математичний апарат в професійній діяльності
F9	РН ЗН2 Уміння використовувати досягнення інформатики та обчислювальної техніки, переопрацьовувати великі обсяги інформації, проводити цілеспрямований пошук необхідної інформації в різних джерелах, у тому числі в глобальних комп'ютерних мережах
F10	РН ЗН3 Уміння узагальнювати та аналізувати інформацію, ставити мету та обирати шляхи її досягнення, володіти культурою мислення
F11	РН ЕК1 Уміння виявляти сутність проблеми, що виникає у сфері забезпечення інформаційної безпеки, та проводити її дослідження
F12	РН ЕК2 Уміння аналізувати види і форми інформації, що попадають під дію загроз; види, методи і шляхи реалізації загроз на основі аналізу структури та змісту інформаційних процесів підприємств, установ, організацій, цілей та завдань їх діяльності
F13	РН ЕК3 Уміння прогнозувати стан інформаційної безпеки підприємства, установи, організації і визначати вплив ефективності задіяних заходів і засобів технічного та програмного захисту інформації
F14	РН ЕК4 Уміння аналізувати інформацію, надану інформаційними системами, з метою виявлення типових ознак можливого несанкціонованого доступу
F15	РН ПР1 Уміння збирати та аналізувати вихідні дані для проектування систем захисту інформації, визначати вимоги, здійснювати порівняльний аналіз підсистем за показниками інформаційної безпеки
F16	РН ПР2 Уміння здійснювати проектні розрахунки елементів систем забезпечення інформаційної безпеки
F17	РН ПР3 Уміння розробляти технологічну та експлуатаційну документацію
F18	РН ПР4 Уміння здійснювати попереднє техніко-економічне обґрунтування проектних розрахунків
F19	РН ТХ1 Уміння встановлювати, налаштувати, експлуатувати і підтримувати в робочому стані компоненти системи забезпечення інформаційної безпеки з урахуванням встановлених вимог
F20	РН ТХ2 Володіння досвідом участі у проведенні атестації об'єктів, приміщень, технічних засобів, систем, програм і алгоритмів на предмет відповідності вимогам державних або корпоративних нормативних документів щодо захисту інформації
F21	РН ТХ3 Уміння здійснювати адміністрування підсистем інформаційної безпеки об'єкта, та підсистем передачі даних
F22	РН ОУ1 Уміння використовувати нормативно-правові документи у професійній діяльності
F23	РН ОУ2 Уміння формувати комплекс заходів з інформаційної безпеки з урахуванням його правової обґрунтованості, адміністративно-управлінської, технічної реалізованості та економічної доцільності
F24	РН ОУ3 Уміння організовувати і підтримувати виконання комплексу заходів з інформаційної безпеки, управляти процесом їх реалізації з урахуванням вирішуваних завдань і організаційної структури об'єкта захисту, зовнішніх впливів, ймовірних загроз і рівня розвитку технологій захисту інформації
F25	РН ОУ5 Володіти основними методами захисту виробничого персоналу і населення від можливих наслідків аварій, катастроф, стихійних лих
F26	РН ОУ6 Уміння генерувати організаційно-управлінські рішення комплексних завдань і готовність нести за них відповідальність

Для зручності ідентифікації кожному результату навчання (РН) присвоєний відповідний шифр. На основі аналізу результатів навчання запропонований перелік обов'язкових дисциплін (таблиця 2).

Таблиця 2

Перелік обов'язкових дисциплін освітньої програми бакалаврів спеціальності 125 «Кібербезпека»

Шифр	Назва дисципліни
1	2
О1	Вища математика
О2	Фізика
О3	Дискретна математика

Продовження табл. 2

1	2
О4	Технологія програмування захищених систем
О5	Теорія ймовірності та математична статистика
О6	Основи теорії кіл, сигнали та процеси в електроніці
О7	Мережеві операційні системи
О8	Програмування алгоритмів захисту інформації
О9	Електроніка і схемотехніка систем захисту
О10	Захист інформації в інформаційно-комунікаційних системах
О11	Програмно-апаратне забезпечення мобільних пристроїв
О12	Безпека Web-ресурсів
О13	Побудова захищених комп'ютерних систем
О14	Проектування мікропроцесорних та мікроконтролерних систем
О15	Проектно-технологічна практика
О16	Безпека життєдіяльності, охорона праці та цивільний захист
О17	Комплексні системи захисту інформації: проектування, впровадження, супровід
О18	Атестаційний іспит

Між результатами навчання та навчальними дисциплінами виявлені зв’язки у табличній формі (таблиця 3).

Таблиця 3

Матриця зв’язків між обов’язковими навчальними дисциплінами (модулями) та результатами навчання (компетентностями)

Результати навчання	Навчальні дисципліни (модулі)																	
	О1	О2	О3	О4	О5	О6	О7	О8	О9	О10	О11	О12	О13	О14	О15	О16	О17	О18
F1															+			
F2															+			
F3															+			
F4															+			
F5															+			
F6																+		
F7															+			
F8	+	+			+	+			+									
F9			+							+	+							
F10	+	+	+															+
F11							+	+				+	+					
F12					+		+	+			+	+	+					
F13						+	+	+				+	+					+
F14			+		+		+					+						+
F15				+	+		+	+	+		+			+				
F16				+		+	+		+				+	+				+
F17										+			+		+		+	
F18														+				+
F19				+		+			+	+	+	+	+					
F20				+						+					+			
F21							+			+		+	+					
F22															+		+	
F23															+		+	
F24															+		+	
F25															+	+		
F26															+		+	

Навчальні дисципліни покладені в основу створення навчального плану підготовки з цієї спеціальності.

Висновки

Отже, використання компетентнісного підходу для розробки освітньо-професійних програм підготовки фахівців різних спеціальностей, у тому числі з кібербезпеки, дозволяє спроектувати результати

навчання, досягнення яких сприяє формуванню професійної компетентності майбутнього фахівця, підвищує його конкурентоздатність на ринку праці, дозволяє задовольнити сучасні динамічні умови виробництва та особисті потреби здобувача вищої освіти.

Література

1. Україна. Закони. Про вищу освіту [Електронний ресурс] : закон України від 01.07.2014 р. № 1556-VII. – Режим доступу : http:// www.vnz.org.ua/zakonodavstvo/ 111-zakon-ukrayiny-pro-vyschu-osvitu. – (дата звернення: 14.04.2016).

2. Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти [Електронний ресурс] : постанова № 266 : [прийнято КМУ 29.04.2015 р.]. – Режим доступу : http://www.kmu.gov.ua/control/uk/cardnpd?docid=248149695. – (дата звернення: 14.04.2016).

3. Перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра [Електронний ресурс] : постанова № 1719 : [прийнято КМУ 13.12.2006 р.]. – Режим доступу : http://www.kodeksy.com.ua›…КМУ…Постанова/1719…13.12.2006.htm. – (дата звернення: 14.04.2016).

4. Перелік спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра [Електронний ресурс] : постанова № 787 : [прийнято КМУ 27.08.2010 р.]. – Режим доступу : http://www.kodeksy.com.ua›…КМУ…Постанова/787…п-27.08.2010.htm. – (дата звернення: 14.04.2016).

5. Перелік напрямів підготовки фахівців з вищою освітою за професійним спрямуванням, спеціальностей різних кваліфікаційних рівнів та робітничих професій [Електронний ресурс] : постанова № 325 : [прийнято КМУ 18.05.1994 р.]. – Режим доступу : http://www.search. ligazakon.ua/l_doc2.../KP940325.html. – (дата звернення: 14.04.2016).

6. Перелік напрямів та спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за відповідними освітньо-кваліфікаційними рівнями [Електронний ресурс] : постанова № 507 : [прийнято КМУ 24.05.1997 р.]. – Режим доступу : http://www.zakon.rada.gov.ua›laws/show/507-97-п. – (дата звернення: 14.04.2016).

7. Перелік вищих навчальних закладів України, що здійснюють підготовку фахівців з вищою освітою у галузі знань «Інформаційна безпека». Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут» [Електронний ресурс]. – Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=112909&cat_id=112887. – (дата звернення: 14.04.2016).

8. Методичні рекомендації щодо розроблення стандартів вищої освіти [Електронний ресурс]. – Режим доступу : http://mon.gov.ua/activity/education/reforma-osviti/naukovo-metodichna-rada-ministerstva/metodichni-rekomendacziyi.html. – (дата звернення: 14.04.2016).

9. Тимчасове положення про освітні програми підготовки фахівців різних ступенів вищої освіти у Хмельницькому національному університеті. – Хмельницький : ХНУ, 2016. – 32 с.

10. Освітньо-професійна програма підготовки бакалавра спеціальності 125 «Кібербезпека». – Хмельницький : ХНУ, 2016. – 46 с.

Рецензія/Peer review : 26.5.2016 р. Надрукована/Printed : 6.6.2016 р.
Рецензент: д.т.н., проф.. Мясіщев О.А.