УДК 378.147:004.056.5

СЕРГІЙ МЕЛЬНИК

СЕРГІЙ ВОСКОБОЙНІКОВ

Національна академія Служби безпеки України

ДМИТРО СТУПАК

Житомирський військовий інститут імені С. П. Корольова

ОПТИМІЗАЦІЯ ФАХОВОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ НА ОСНОВІ ІННОВАЦІЙНОЇ ПЕДАГОГІКИ ТА ІНТЕГРОВАНОГО ПІДХОДУ В СИСТЕМІ РЕАЛІЗАЦІЇ КЛЮЧОВИХ КОМПЕТЕНЦІЙ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Обґрунтовано оптимізацію фахової підготовки майбутніх фахівців з кібербезпеки на основі інноваційної педагогіки та інтегрованого підходу в системі реалізації ключових компетенцій безпеки в інформаційному суспільстві. Визначено, що специфіка фахової підготовки й формування професійної компетентності майбутніх фахівців з кібербезпеки зумовлює застосування інтегрованого підходу, що базується на міжпредметних зв'язках фахових і фундаментальних навчальних дисциплін та ефективного розподілу навчальних модулів в системі професійної підготовки з урахуванням модернізаційних освітніх змін, педагогічної інноватики та застосуванні інноваційних освітніх технологій для формування комплексної готовності до реалізації фахових компетенцій з кібербезпеки.

Ключові слова: інформаційна безпека, кібербезпека, фахова підготовка, інноваційних освітніх технологій, інтегрований підхід

Загальна постановка проблеми. Стан розвитку інформаційного суспільства та інформаційної інфраструктури України визначає професійні вимоги державних та приватних структур для підготовки фахівців у галузі інформаційної безпеки та кібербезпеки. Сфери професійної діяльності фахівців інформаційної безпеки протягом останніх трьох десятиліть суттєво розвиваються, а сфера кібербезпеки з 2000 року (Національна система кібербезпеки в Україні юридично визначається лише в 2016 році). Науковці та практикуючі фахівці галузі відзначають, що зміст концепції кібербезпеки охоплює не тільки технології, але, насамперед, людські ресурси. Експерти та представники установ, залучених до національної системи кібербезпеки України, відзначають актуальність та необхідність належного кадрового забезпечення фахівцями спеціальності «Кібербезпека».

Аналіз останніх досліджень і публікацій. У зв'язку з політичною та економічною ситуацією в Україні професія фахівця із організації інформаційної безпеки, або фахівця по боротьбі з кіберзлочинністю, або фахівця з кібербезпеки, нині отримала широке розповсюдження. Відповідно, перед вищими навчальними закладами постає завдання задоволення зростаючого попиту українського суспільства на підготовку фахівців вищої кваліфікації в галузі інформаційної безпеки з високим рівнем володіння теорією та практикою. Проте досягнення високого ступеня професіоналізму можливе лише за умови належної фундаментальної освіти. Оскільки міжпредметні зв'язки є ефективним засобом формування практичних умінь і навичок застосування знань з однієї дисципліни при вивченні інших, то проблема інтеграції навчальних знань з базових та спеціальних дисциплін як чинник підвищення якості професійної підготовки майбутніх фахівців є наразі актуальною (Коржова, 2017).

Розвиток інформаційних та комунікаційних технологій спричинив глибокі системні перетворення в інформаційному та кібернетичному просторах. Останній, в силу своєї специфіки, породжує нові загрози та виклики фахівцям з інформаційної безпеки. Інформаційно-комунікаційні технології стали нині потужною силою перетворення суспільного життя та інноваційного розвитку. Їх активне впровадження практично в усі сфери життєдіяльності міжнародної спільноти змінило останнім часом світову економіку й спричинило глибокі системні перетворення в глобальному інформаційному та кібернетичному просторах. Маючи певну специфіку, ці глобальні субстанції породжують, в свою чергу, нові й, передусім, кібернетичні загрози і виклики, розв'язувати які мають фахівці з інформаційної безпеки, озброєні новими знаннями і вміннями та інноваційними підходами. Практикуючі фахівці з інформаційної безпеки зіштовхуються з новими специфічними завданнями, які вимагають від них нових знань та вмінь. Для забезпечення потреб силових структур, а також виробничої та банківської сфери України у фахівцях,

© С. Мельник, С. Воскобойніков, Д. Ступак, 2018

спроможних виявляти ознаки та активно протидіяти сторонньому кібернетичному впливу, авторами пропонується підхід до запровадження в системі вищої освіти України профілю навчання «кібернетична безпека». Крім того, чітко визначено критерії, яким мають відповідати такі фахівці (Бурячок та ін., 2016).

В умовах України, як на наш погляд, одною із головних проблем залишається при цьому саме незадовільне кадрове забезпечення фахівцями із кіберзахисту. Це підтверджено у матеріалах аналітичної доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України», а також результати аудиту нещодавно виведених з обігу стандартів вищої освіти у галузі знань 1701 «Інформаційна безпека», які показали, що професійні компетентності, задекларовані в цих галузевих стандартах, неповною мірою враховують стан та перспективу розвитку методів і засобів забезпечення кібербезпеки. Імовірно, саме це стало відправною точкою для прийняття постанови Кабінету Міністрів України від 29 квітня 2015 року №266, яка внесла зміни до «Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» та визначила для України безпекову спеціальність – 125 «кібербезпека», імплементація якої в освітній процес дасть змогу сформувати базис у виді компетентностей (соціально-особистісних, інструментальних, загальнонаукових, професійних тощо), виробничих функцій (дослідницьких, проектувальницьких, організаційних, управлінських, технологічних, контрольних, прогностичних, технічних тощо) та типових задач, що ним відповідають, а також умінь, якими мають володіти випускники й фактично закласти фундамент для їх практичної роботи за напрямом організації та забезпечення кібернетичної безпеки.

Надзвичайно загостреною ця проблема постає останнім часом. Цьому сприяє, перш за все, вибухове зростання обсягів інформації, до яких отримали доступ пересічні громадяни, винайдення потужних комп'ютерів і вбудованих мікроконтролерів, що привело переважну більшість країн світу як до глобальної інтелектуалізації та гіпершвидкого розвитку промисловості, так й зробило більш вразливими до загроз антропогенного і техногенного характеру, а також природних катаклізмів, передусім, критично-важливі сегменти та об‘єкти їх економіки (Бурячок та ін., 2016).

Дослідники акцентують у вагу на вимогах :

- вимоги сьогодення щодо усвідомлення таких понять, як кіберпростір, під яким переважна частина фахівців у галузі ІБ та захисту інформації розуміють віртуальне соціотехнічне середовище із завданнями програмного забезпеченням комп‘ютерної техніки, мережевого та телекомунікаційного обладнання, так і кібербезпека, під якою ті ж фахівці вбачають складову частину поняття інформаційної безпеки (розглядає ті ж самі загрози, методи, засоби і заходи захисту, але лише в просторі кібернетичному);
- вимоги міжнародного стандарту ISO/IEC 27032:2012(E), який виражає погляд на ці питання міжнародного експертного середовища й регламентує кібербезпеку окремим доменом безпеки, що забезпечує конфіденційність, цілісність і доступність інформації у кіберпросторі та має прояви лише у взаємодії людей і організацій в Інтернет;
- вимоги затверджених Указами Президента України Стратегії національної безпеки України та Стратегії кібербезпеки України, в яких пріоритетами забезпечення національної безпеки визначено, зокрема, удосконалення професійної підготовки у сфері інформаційної безпеки, створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони та залучення наукових установ, навчальних закладів, тощо до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

Означені вимоги, на думку науковців, спонукають до висновку, що значною мірою на суспільні запити впливає той факт, що нині більш затребуваним стає не захист інформації як такої, а забезпечення безпеки, власне, тієї інформаційно-комунікаційної системи, на вхід якої ця інформація потрапляє, де вона циркулює, накопичується та обробляється. Дослідження міжнародного досвіду підготовки фахівців у галузі ІКТ засвідчило урахування працедавців на зміст ІТ-освіти. Впродовж останніх десятиріч чотири професійні асоціації ACM, AIS, AITP, IEEE-CS займаються розробкою міжнародних стандартів підготовки ІТ-фахівців, таких як Computing Curricula Computer Science 2001 (CC 2001), Information Systems 2002 (IS 2002), Computer Engineering 2004 (CE 2004), Software Engineering 2004 (SE 2004), попередній версії Information Technology 2005 (IT2005), Computing Curricula 2005. Зокрема саме професійні асоціації розробляли кваліфікаційні вимоги до ІТ-фахівців і рекомендації щодо відповідних освітніх програм, стандарту «Computer Curriculum», котрий регулярно оновлюється. Однак, розроблені документи носять рекомендаційний характер щодо обсягу і змісту комп‘ютерних освітніх програм бакалаврського рівня. В CC 2001 допускаються три рівні вивчення дисциплін – ввідний, проміжний, поглиблений; також пропонуються різні моделі і стратегії навчання: для ввідного рівня – імперативна, об‘єктна, функціональна, широка, алгоритмічна, апаратна стратегії; для проміжного – тематична, стисла, системна, веб-орієнтована стратегії; для поглибленого рівня вивчення рекомендована індивідуальна, креативна стратегія, що розробляється для конкретної групи студентів. Разом з тим, обов‘язковий перелік тем і пропонований набір моделей навчання у поєднанні з іншими моделями, що використовують ЗВО дають

велику гнучкість при складанні навчальних планів у конкретному навчальному закладі, узагальнює аналітичний огляд В. Сєдов.

Загалом, для ІТ-освіти Європейських університетів притаманна гнучка система побудови індивідуальної траєкторії навчання. Студент вступає на напрям підготовки, а спеціальність отримує у результаті власного добору дисциплін, котрі відповідають сфері його професійних інтересів починаючи з другого або третього року навчання. Такий підхід дозволяє усвідомлювати коло професійних інтересів і перспективних напрямів дослідження вже на етапі вступу до магістратури. Важливо зазначити, що переважна більшість університетів тісно співпрацюють з бізнес-структурами у сфері інформаційних технологій, розміщують технопарки, дослідницькі лабораторії на власній території. Такий підхід значно посилює практичну підготовку майбутнього інженера-програміста та створює майданчик для проведення досліджень магістрами. Аналіз магістерських програм у галузі інформаційних технологій різних ЗВО України засвідчив, що підготовки магістрів проводиться за денною або заочною формою навчання. Термін навчання за магістерською програмою складає 1 рік для денної форми навчання (1,5 роки для заочної форми навчання) для осіб, які мають кваліфікацію спеціаліста, або 1,5 роки для денної форми навчання (2 роки для заочної форми навчання) для осіб, які мають кваліфікацію бакалавра (Седов, 2015; Седов, 2016).

Виклад основного матеріалу дослідження. В умовах інформаційного суспільства у вимірі соціотехнічних систем важливою складовою кібернетичного простору – технологічної платформи для формування глобального інформаційного суспільства без кордонів, всебічного розвитку особистості та ефективної комунікації між державою і суспільством є людина.

Саме тому в ієрархії її ключових компетентностей чільне місце займає компетентність безпеки у суспільстві, складовими якої є інформаційна та кібербезпека. Від інформаційної культури і освіченості самої людини, а також поведінкових комунікативних факторів і суспільних гарантій безпеки залежить безпека життєдіяльності в цілому.

Сучасні технічні інновації, що пов‘язані з розвитком технологій і сервісів мережі Інтернет, зумовили світову тенденцію у новому розумінні через приставку «Кібер» понять «інформаційний простір», «інформаційні ресурси», «інформаційна інфраструктура» та «інформаційна безпека». Отже, відносно нове поняття «кібербезпека» передбачає значно більший обсяг можливих реалізацій інформаційних загроз для людини, суспільства, держави та міжнародної спільноти, ніж ті, що мали місце у найближчі 10-15 років тому. Зазначені інновації світового технологічного розвитку призвели до відповідної трансформації професійної діяльності із забезпечення інформаційної безпеки, створення міжнародних та національних систем кібербезпеки зокрема, щоб гарантувати кібербезпеку людині на рівні внутрішньодержавних і міжнародних комунікацій.

Фахова підготовка в системі вищої освіти повинна трансформуватись і розвиватись відповідно до реалій розвитку професійних видів діяльності. Запровадження в Україні нової спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» актуалізувало увагу до проблеми підвищення якості професійної підготовки фахівців для приватного і державного сектору захисту інформації, а також правоохоронних структур, що протидіють проявам кіберзлочинності. Звісно, з‘явився додатковий мотиваційний важіль для переосмислення існуючих концептуальних підходів до організації професійної підготовки фахівців колишньої галузі знань 1701 «Інформаційна безпека» та наукового обґрунтування оптимізації фахової підготовки.

Завдання забезпечення кібербезпеки людини, суспільства, держави та міжнародної спільноти є надто важливим з позиції забезпечення громадської, національної та міжнародної безпеки, дотримання гарантії прав і свобод людини і громадянина у кіберпросторі.

Тому питання підготовки бакалаврів спеціальності «Кібербезпека» обговорювалось учасниками круглого столу, МОН України (2016 року). Експертне середовище висловило думку про важливість передусім практичної спрямованості професійної підготовки для цієї сфери діяльності. Міністр Л. Гриневич наголосила на тому, що ми маємо можливість показати новий підхід до творення стандарту вищої освіти. Це потрібно робити не тільки в освітянському середовищі, а в першу чергу, через діалог з роботодавцями і тими, хто формує своє замовлення на відповідні професійні кваліфікації (Експерти…, 2016).

Практичну складову формування професійної компетентності майбутніх фахівців з кібербезпеки, доцільно розглядати з урахуванням широти їх професійного профілю, який відповідає видам, змісту та технологіям сучасної професійної діяльності, динаміки її розвитку в найближчій та віддаленій перспективі.

Специфіка фахової підготовки й формування професійної компетентності майбутніх фахівців з кібербезпеки зумовлює застосування інтегрованого підходу, що базується на міжпредметних зв’язках фахових і фундаментальних навчальних дисциплін та ефективного розподілу навчальних модулів в системі професійної підготовки з урахуванням модернізаційних освітніх змін, педагогічної інноватики та

застосуванні інноваційних освітніх технологій для формування комплексної готовності до реалізації фахових компетенцій з кібербезпеки.

Аналіз освітньо-професійних програм та навчальних планів підготовки бакалаврів зі спеціальності 125 «Кібербезпека» дозволив зробити висновки, що більшість професійно-орієнтованих дисципліни, які забезпечують базові знання з усіх аспектів захисту інформації ґрунтуються на фундаментальній математичній підготовці. Оскільки математичні знання виконують роль методологічної основи наукового знання та базової складової більшості профілюючих дисциплін, математичні дисципліни вивчаються студентами даної спеціальності на першому та другому курсах. При вивченні дисциплін з циклу професійної підготовки: «Теорія інформації та кодування», «Основи криптографічного захисту інформації», «Комплексні системи захисту інформації» для вдалого шифрування даних необхідні сформовані компетенції застосування математичних методів, моделей. У «Теорії ризиків» для виконання моделювання ризику використовуються знання з «Теорії ймовірностей» та «Математичних методів і моделей», зокрема використовують кілька класів математичних моделей і методів: лінійне та стохастичне програмування, теорію ігор; теорію нечітких множин та ін. (Коржова, 2017).

Доцільно звернути увагу на певні складнощі у організації професійної підготовки майбутніх фахівців з кібербезпеки (та ІТ у цілому), зважаючи на такі аспекти як: час розроблення, затвердження та дії стандарту вищої освіти; час формування організаційно-методичного забезпечення навчального процесу; терміни навчання здобувача вищої освіти; динаміка розвитку технологій у професійної діяльності із забезпечення кібербезпеки та час «старіння» фахової інформації.

Якісне формування професійної компетентності майбутнього фахівця з кібербезпеки можливе лише в рамках концепції неперервної освіти. Тому принципи та підходи до побудови компетентнісної моделі випускника ЗВО (вимоги до стандартизації освіти) за спеціальністю «Кібербезпека» повинні враховувати потенціальні цілі та зміст його подальшого навчання.

Організацію професійної підготовки майбутніх фахівців з кібербезпеки доцільно розглядати в концепції ступеневої неперервної освіти та в рамках соціального партнерства між ЗВО, державою, бізнесом, вітчизняними та міжнародними громадськими організаціями. Загальною основою концепції розвитку неперервної освіти є інноваційний зміст і форми фахової підготовки в умовах вищого навчального закладу, розробка ефективних методів навчання в продовж життя і всеосяжного навчання, яке включає формальне, неформальне і позаформальне навчання) і сприяє професійному розвитку фахівців кібербезпеки.

Саме на інноваційну освітню діяльність цілеспрямовують Стратегія інноваційного розвитку України на 2010-2020 роки в умовах глобалізаційних викликів, адекватних стратегій і програм модернізаційних освітніх змін. Враховуючи специфіку діяльності та сфери компетенцій суб‘єктів Національної системи кібербезпеки (див. Укази Президента від15.03.2016 №96/2016; від 07.06. 2016 № 242/2016), пріоритетним вектором організації післядипломної освіти фахівців з кібербезпеки в Україні можна вважати форми та методи дистанційного навчання (у розумінні e-learning), що передбачають використання освітніх Інтернет-симуляторів для реалізації діяльнісного підходу у навчанні. На сьогодні основною тенденцією організації післядипломної освіти у сфері кібербезпеки (ІТ у цілому) є дистанційне навчання та сертифікація спеціалістів на національному і міжнародному рівнях. При цьому сертифікаційні центри достатньо часто визначають вимоги до попередньої освіти, спеціалізації та досвіду роботи, розробляють інноваційні форми практично орієнтованого навчання під кожну категорію фахівців, змінюють та удосконалюють зміст навчання з появою нових технологій кіберзахисту.

Висновки. Інноваційний зміст професійної підготовки майбутніх фахівців із кібербезпеки та її професійна спрямованість відповідно до сучасних потреб суспільства зумовлюють модернізацію навчальних планів і програм підготовки дворівневого неперервного навчального процесу «бакалавр-магістр» на основі інтегрованого підходу для формування комплексної готовності до реалізації фахових компетенцій з кібербезпеки.

Перспективами подальшого розвитку напряму дослідження є наукове обґрунтування системи формування професійної компетентності майбутніх фахівців кібербезпеки у вищих навчальних закладах.

Список використаних джерел

Бурячок В. Л., Пархомей І. Р., Степанов М. М., Толубко В. Б. (2016) Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «інформаційні технології» Сучасний захист інформації №2. С.4–8.

Експерти про підготовку фахівців у сфері інформаційних технологій: Програми навчання повинні бути практично орієнтовані та відповідати посадовим інструкціям. Education and training. URL: http://mon.gov.ua/usinovivni/novini/2016/ 10/04/kruglij-stil-1016.2

Коржова В. О. (2017) Теоретичні аспекти міжпредметних зв’язків математичних дисциплін з дисциплінами циклу професійної підготовки майбутніх фахівців із організації інформаційної безпеки Фізико-математична освіта. Вип.2(12), С.89–93.

Седов В. Є. (2015) Інформаційно-комунікаційні технології, як каталізатор змін компетентності викладача. Відкрите освітнє е-середовище сучасного університету: зб. наук. праць / [редкол. Н.В. Морзе та ін.]. К.: Київський університет ім. Б. Грінченка. С. 74-82.
Седов В. Є. (2016) Фахова компетентість інженера-програміста в умовах зміни стандартів освіти. Наука і освіта: наук.-практ. журн. Півден. наук. Центр НАПН України. Одеса: ПНЦ НАПН України. № 4. С. 42– 44.
Стратегія інноваційного розвитку України на 2010-2020 роки в умовах глобалізаційних викликів. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main. cgi?nreg=965-17
Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України».
Указ Президента України від 7 червня 2016 року № 242/2016 «Про Національний координаційний центр кібербезпеки».
Strategic framework for education and training. [Електронний ресурс]. URL: http://www.ec.europa.eu/education/policies/III/life/ memoen.pdf.
Capacity Building in Higher Education. [Електронний ресурс]. –URL: http://erasmusplus.org.ua/novyny.html

References

Buryachok V. L., Parkhomey I. R., Stepanov M. M., Tolubko V. B. (2016) Problem issues and urgent tasks of training specialists in cybernetic security of the field of knowledge "information technologies" Modern information protection #2. S.4–8.
Experts in the training of IT professionals: Training programs should be practically oriented and comply with job descriptions. Education and training. URL: http://mon.gov.ua/usinovivni/novini/2016/ 10/04/kruglij-stil-1016.2
Korzhova V. O. (2017) Theoretical aspects of interdisciplinary relations of mathematical disciplines with the disciplines of the cycle of professional training of future specialists in the organization of information security Physical and mathematical education. Vol.2(12), S.89–93.
Sedov V. Ye. (2015) Information and communication technologies, as a catalyst for teacher proficiency change. Open Educational E-Environment of the Modern University: Sb. sciences works / [redkol. N.V. Morze ta in.]. K.: Kyyivs'kyy universytet im. B. Hrinchenka. S. 74-82.
Sedov V. Ye. (2016) Professional competence of the programmer engineer in the conditions of changing educational standards. Science and Education: nauk.-prakt. zhurn. Pivden. nauk. Tsentr NAPN Ukrayiny. Odesa: PNTs NAPN Ukrayiny. # 4. S. 42– 44.
Strategy of innovation development of Ukraine for 2010-2020 in the context of globalization challenges. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main. cgi?nreg=965-17
Ukaz Prezydenta Ukrayiny vid 15 bereznya 2016 roku # 96/2016 «Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 27 sichnya 2016 roku «Pro stratehiyu kiberbezpeky Ukrayiny».
Ukaz Prezydenta Ukrayiny vid 7 chervnya 2016 roku # 242/2016 «Pro Natsional'nyy koordynatsiynyy tsentr kiberbezpeky».
Strategic framework for education and training. [Електронний ресурс]. URL: http://www.ec.europa.eu/education/policies/III/life/ memoen.pdf.
Capacity Building in Higher Education. [Електронний ресурс]. –URL: http://erasmusplus.org.ua/novyny.html

MELNYK S., VOSKOBOINICOV S.,

National Academy of Security Service of Ukraine

STUPAK D.

Zhytomyr Military Institute named after S.P. Korolyov, Ukraine

OPTIMIZATION OF PROFESSIONAL PREPARATION OF FUTURE FACTORS FROM CYBER SECURITY BASED ON INNOVATIVE PEDAGOGICS AND INTEGRATED APPROACH IN THE RELEASATION SYSTEM OF KEY SECURITY COMPETENCES IN INFORMATIONAL SOCIETY

The article substantiates the optimization of the professional training of future cybersecurity specialists on the basis of innovative pedagogy and an integrated approach in the implementation of key security competencies in the information society. It has been determined that the specificity of professional training and the formation of professional competence of future cyber security specialists results in the application of an integrated approach based on interdisciplinary links between professional and fundamental educational disciplines and an effective allocation of training modules in the system of professional training, taking into account modernization educational changes, pedagogical innovation and application innovative educational technologies for the formation of a comprehensive readiness for the implementation of professional competences in cybersecurity.

The task of ensuring the cyber security of a person, society, state and the international community is extremely important from the point of view of ensuring public, national and international security, observance of the guarantee of human and civil rights and freedoms in cyberspace.

Key words: *information security, cyber security, vocational training, innovative educational technologies, integrated approach*

Стаття надійшла до редакції 22.03. 2018 р.