Сергій Мельник

КОНЦЕПТУАЛЬНІ АСПЕКТИ ОРГАНІЗАЦІЇ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

На сьогодні люди у вимірі соціотехнічних систем є важливою складовою кібернетичного простору – технологічної платформи для формування глобального інформаційного суспільства без кордонів, всебічного розвитку особистості та ефективної комунікації між державою і суспільством. Сучасні технічні інновації, що пов'язані з розвитком технологій і сервісів мережі Інтернет, обумовили 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 ще 10-15 років назад.

Зазначені інновації світового технологічного розвитку призвели до відповідної трансформації професійної діяльності із забезпечення інформаційної безпеки, створення міжнародних та національних систем кібербезпеки зокрема.

Вочевидь, професійна освіта повинна реагувати на реалії 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 сучасного бачення проблематики.

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» обговорили учасники круглого столу, що відбувся під головуванням Міністра освіти і науки України Лілії Гриневич 3 жовтня 2016 року [1]. Експертне середовище висловило думку про важливість передусім практичної спрямованості професійної підготовки для цієї сфери діяльності. Міністр зауважила – «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».

Далі зазначимо, що 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.

Натомість 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.

За попередніми висновками вивчення проблеми забезпечення адекватності між результатами формування професійної компетентності майбутнього фахівця з кібербезпеки та поточними вимогами ринку праці, можна свідчити про наявність певного конфлікту інтересів між здобувачем вищої освіти, вищим навчальним закладом (ВНЗ) та потенційним роботодавцем. У заявленій послідовності мова йде про наступне: очікування здобувача отримати певну функціональну (професійну) мобільність та адаптованість до реалій ринку праці, що досягається за рахунок «універсалізації» фахівця, відповідно, і змісту освіти; намагання ВНЗ забезпечити академічність вищої освіти, що передбачає формування у майбутнього фахівця не лише знань-умінь-навичок, способів діяльності та психологічної готовності, а і життєво важливих цінностей гармонійно розвинутої особистості, спроможної системно мислити та здатної до самовдосконалення; прагнення роботодавця отримати фахівця який після закінчення ВНЗ здатен виконувати весь необхідний спектр професійних завдань відповідно до посадових інструкцій.

Аналізуючи викладене у зворотній послідовності, а також враховуючи такі чинники, як фізіологічна і соціальна зрілість, професійний досвід, наукові підходи до трактування етапів професійного самовизначення, розвитку та становлення фахівця, висловимо наступну думку. Якісне формування професійної компетентності майбутнього фахівця з кібербезпеки можливе лише в рамках концепції неперервної освіти. Тому принципи та підходи до побудови компетентнісної моделі випускника ВНЗ (вимоги до стандартизації освіти) за спеціальністю «Кібербезпека» повинні враховувати потенціальні цілі та зміст його подальшого навчання.

Як зазначається у Меморандумі неперервної освіти Європейського Союзу [2], повноцінний розвиток особистості у складному соціально-політичному середовищі стає неможливим без уміння активно брати участь у суспільних процесах

і адаптуватися до культурної, етнічної та мовної різноманітності. І лише освіта у найширшому розумінні цього слова може допомогти успішно впоратися з цим завданням. Її основою є ті базові навички, які людина отримує в юності. Надзвичайно важливими є уміння вчитися і бажання продовжувати своє навчання самостійно.

Ключовими факторами неперервної освіти стають особиста мотивація до навчання і наявність навчальних ресурсів, здатність планувати, організовувати й управляти власною навчальною (пізнавальною) діяльністю.

На разі, здається своєчасним питання донесення інформації до широкого кола абітурієнтів та роботодавців про сталу ілюзію, що ВНЗ може і повинен сформувати майбутнього фахівця з кібербезпеки, який знає і вміє абсолютно все, що потрібно у професійній діяльності. Студент та роботодавець повинен усвідомлювати, що у майбутньому випускнику ВНЗ прийдеться опановувати нові знання, пов'язані зі створенням нових технологій, новими сферами (спеціалізаціями) та рівнями (технологічний, управлінський) професійної діяльності із забезпечення кібербезпеки.

Загальною основою концепції розвитку неперервної освіти є інноваційна педагогіка (розробка ефективних методів навчання в продовж життя і всеосяжного навчання, яке включає формальне, неформальне і позаформальне навчання) [3]. Тому організацію професійної підготовки майбутніх фахівців з кібербезпеки доцільно розглядати в концепції ступеневої неперервної освіти та в рамках соціального партнерства між ВНЗ, державою, бізнесом, вітчизняними та міжнародними громадськими організаціями.

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.

Враховуючи специфіку діяльності та сфери компетенцій суб'єктів Національної системи кібербезпеки [4,5], 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.

Список використаної літератури

1. Експерти про підготовку фахівців у сфері інформаційних технологій: Програми навчання повинні бути практично орієнтовані та відповідати посадовим інструкціям [Електронний ресурс] // Education and training. — Режим доступу: http://mon.gov.ua/usinovivni/novini/2016/10/04/kruglij-stil-1016.

2. Strategic framework for education and training [Електронний ресурс] // Education and training. — Режим доступу: http://www.ec.europa.eu/education/policies/III/life/ memoen.pdf.

3. Олійник В. В. Освіта впродовж життя : як і чому вчити дорослих? [Електронний ресурс] / В. В. Олійник. — Режим доступу: http://www.apsu.org. ua/images/top3.jpg.

4. 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».

5. Указ Президента України від 7 червня 2016 року № 242/2016 «Про Національний координаційний центр кібербезпеки».