1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення системи ТЗІ. Стандартизація, сертифікація та випробовування засобів ТЗІ. Підготовка, перепідготовка та підвищення кваліфікації спеціалістів систем захисту інформації

УДК 354:378

ПІДГОТОВКА ФАХІВЦІВ ДЛЯ СФЕРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: РЕАЛІЇ СЬОГОДЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Євген Скулиш
Національна академія СБ України

Анотація: **Статья посвящена вопросам подготовки специалистов в области информационной безопасности.**
Summary: **The article is sacred to the questions of educational preparation of professionals in information security area.**
Ключові слова: **Інформатизація, інформаційна безпека, система підготовки кадрів.**

Глобальна інформатизація українського суспільства вимагає забезпечення його інформаційної безпеки. Забезпечувати інформаційний суверенітет нашої країни можуть висококваліфіковані фахівці, які могли б управляти інформаційними процесами, знати і керувати інформаційною інфраструктурою держави.

Крім того, реалізація державотворчих і соціально-економічних реформ сучасного етапу розвитку України чітко продемонструвала, що для її швидкого та ефективного здійснення бракує кваліфікованих працівників, здатних забезпечувати інформаційну безпеку держави.

На мою думку, початковим етапом створення національної системи підготовки кадрів у сфері інформаційної безпеки став 1995 рік. Саме цього року був підписаний спільний наказ МОН України та Державної служби України з питань технічного захисту інформації від 28. 12. 1995 № 66/358 «Про співробітництво між Міністерством освіти України й Державною службою України з питань технічного захисту інформації». З цього моменту в навчальних закладах України була започаткована підготовка фахівців за відомими спеціальностями: 7.160101 – «Захист інформації з обмеженим доступом й автоматизація її обробки (у комп'ютерних системах)»; 7.160102 – «Захист інформації з обмеженим доступом й автоматизація її обробки»; 7.160103 – «Системи захисту від несанкціонованого доступу»; 7.160104 – «Адміністративний менеджмент у системах захисту інформації з обмеженим доступом»; 7.160105 – «Захист інформації в комп'ютерних системах і мережах». Підготовка фахівців у вищих навчальних закладах до 2006 року велася відповідно до «Переліку напрямів та спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за відповідними освітньо-кваліфікаційними рівнями» (затвердженого Постановою Кабінету Міністрів України від 24 травня 1997 р. № 507).

На сьогодні більше 15 вищих навчальних закладів України готують фахівців з інформаційної безпеки (продовжують готувати до 2011 року).

З метою впорядкування системи підготовки кадрів та приведення у відповідність з європейськими стандартами, а також згідно з Постановою КМ України від 27.01.2007 року № 58 вищезазначені спеціальності були трансформовані в напрями підготовки за освітньо-кваліфікаційним рівнем «бакалавр» в галузі знань 1701 «Інформаційна безпека»: 6.170101 Безпека інформаційних і комутаційних систем; 6.170102 Система технічного захисту інформації; 6.170103 Управління інформаційною безпекою.

Пріоритет підготовки фахівців за першими двома напрямами мають вищі навчальні заклади технічного спрямування. Підготовку фахівців з третього напряму розпочали ВНЗ гуманітарного та юридичного профілю, з огляду на специфіку сфери інформаційної безпеки.

Відповідно до наказу міністра освіти і науки України від 11. 10. 2007 року № 897 (зі змінами та доповненнями від 05. 03. 2009 року № 215) Національна академія СБ України визначена вищим навчальним закладом, на базі якого розробляються Галузеві стандарти вищої освіти (далі – Стандарт) за напрямами підготовки 6.170103 «Управління інформаційною безпекою» та 6.160103 «Організація захисту інформації з обмеженим доступом».

Робочою групою МОН України на базі НА СБ України зроблено вагомий внесок у підготовку фахівців з інформаційної безпеки підготовкою Стандарту за напрямом підготовки 6.170103 «Управління інформаційною безпекою» (Наказ МОН України від 05. 02. 2010 р.№ 77). За цим стандартом і здійснюється підготовка фахівців за освітньо-кваліфікаційним рівнем бакалавр.

Ще один актуальний напрям підготовки фахівців є «Організація захисту інформації з обмеженим доступом». Варто зазначити також, що відповідно до статті 21 Закону України «Про державну таємницю» розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю на підприємствах, установах та організаціях, покладається на режимно-секретні органи (підрозділи) (далі –РСО).

На сьогодні в Україні функціонують понад 5 тисяч РСО, створених в органах місцевого самоврядування, установах та організаціях, на підприємствах, що провадять діяльність, пов'язану з державною таємницею.

Національна академія Служби безпеки України за погодженням із Службою безпеки України з 2004 року розпочала підготовку фахівців за напрямом підготовки 6.160103 «Організація захисту інформації з обмеженим доступом». Підготовка фахівця за цим напрямом зорієнтована на потреби РСО, а також аналогічні підрозділи органів державного управління та місцевого самоврядування підприємств, установ усіх форм власності. Наші випускники повною мірою задовольняють кадрові потреби державних органів (у тому числі правоохоронних), органів місцевого самоврядування, підприємств, установ і організацій. Дипломовані фахівці працюють (проходять службу) в підрозділах, службах безпеки, які забезпечують інформаційну безпеку.

Хочу зазначити, що професійна підготовка фахівця із захисту інформації ґрунтується на єдиній педагогічній концепції. Вона враховує, з однієї сторони, найактуальніші проблеми сучасної вищої освіти, з іншої – найперспективніші вітчизняні та світові тенденції її розвитку. Враховуючи міжнародні стандарти вищої освіти Академія вдосконалює навчальний процес. Основними напрямками в цьому контексті, в першу чергу, є поєднання навчальної, методичної, наукової та виховної роботи безпосередньо в навчальному процесі; переведення наукових досліджень студентів загальнотеоретичної тематики на аналіз проблем захисту інформації з обмеженим доступом в органах державної влади та управління, на підприємствах, в установах та організаціях усіх форм власності, розробку методичних рекомендацій; інтенсифікацію навчального процесу за рахунок посилення самостійної роботи студентів та її відповідного методичного забезпечення тощо.

Приводячи у відповідність забезпечення навчального процесу за напрямом підготовки «Організація захисту інформації з обмеженим доступом» у 2009 році до Національного класифікатора України ДК 003:2005 «Класифікатор професій» (далі – КП) включено запропоновані Службою безпеки України нові професійні назви робіт: «Професіонал у галузі організації захисту інформації з обмеженим доступом» (код 2149.2) та «Фахівець із організації захисту інформації з обмеженим доступом» (код 3119). Крім того, за напрямом підготовки 6.160103 «Організація захисту інформації з обмеженим доступом» НА СБ України підготовлений і затверджений МОН України Галузевий стандарт вищої освіти (Наказ МОН України від 02. 03. 2010 р.№ 164).

Створена за ці роки навчально-методична база та наукова школа забезпечують належні умови для здійснення безперервної професійної підготовки висококваліфікованих фахівців з організації захисту інформації з обмеженим доступом для потреб держави.

На даний час напрям підготовки «Організація захисту інформації з обмеженим доступом» галузі знань «Військові науки, національна безпека, безпека державного кордону» має частково спільні компетенції з напрямом підготовки «Управління інформаційною безпекою» галузі знань «Інформаційна безпека». З метою подальшого поліпшення підготовки висококваліфікованих фахівців із управління інформаційною безпекою та організації захисту інформації Академія успішно співпрацює з практичними підрозділами СБ України, зокрема, проводяться наукові конференції, щорічно проводяться збори науково-педагогічних працівників, які займаються освітньою діяльністю у сфері інформаційної безпеки, за їх результатами видано збірники матеріалів. Налагоджена тісна співпраця з науковими установами Національної академії

наук України, галузевими академіями та вищими навчальними закладами (співпраця з НАУ, КПІ, ДУІКТ). Значна робота проводиться Академією з іншими академічними установами.

Стратегічною метою реформування й модернізації вищої освіти і науки в Україні є створення ефективного інноваційного освітнього середовища у вищих навчальних закладах через сприяння прогресивним нововведенням, упровадження найсучасніших технологій і моделей навчання. Навчальний процес у сучасному вищому навчальному закладі здійснюється з урахуванням можливостей сучасних інформаційних технологій навчання та орієнтується на формування освіченої, гармонійно розвиненої особистості, здатної до постійного оновлення наукових знань, професійної мобільності та швидкої адаптації до змін у соціально-культурній сфері, системі управління та організації праці в умовах ринкової економіки.

У євроінтеграційному поступі України роль фахівця з інформаційної безпеки є надзвичайно важливою, оскільки від його рівня освіти залежить забезпечення інформаційного простору держави, що, в свою чергу, сприяє утвердженню України як високорозвиненої, соціальної за своєю сутністю, демократичної, правової держави, в якій інформаційна безпека відіграє одну з найважливіший функцій.

Українська наука й освіта, яка регулює питання інформаційної безпеки, розвивається під впливом як загальних цивілізаційних процесів, так і внутрішніх факторів державного розвитку та будівництва. Вища освіта в Україні нині набуває нового змісту і змінюється відповідно до розвитку знань та з урахуванням нових суспільних потреб.

Спектр професійних знань, умінь, навичок фахівця з інформаційної безпеки сьогодні значно розширився і вимагає від суб'єктів освітньої діяльності найрізноманітніших знань як у сфері інформаційної безпеки, так і в суміжних із інформаційною безпекою сферах, потребує ґрунтовної загальної та фахової методологічної підготовки, вільного володіння методикою і практикою досліджень у цій галузі. Головне завдання, яке стоїть перед викладачем, полягає в тому, щоб навчити нашого студента постійно вчитися, здобувати нові знання, сформувати навички самостійного дослідницького пошуку, виявляти творчість у вирішенні складних професійних проблем і ситуацій.

Підготовка студентів у Національній академії СБ України або у вищих навчальних закладах, які готують фахівців подібного профілю вже зараз будується з урахуванням соціального замовлення та максимально спрямована на майбутні його фахові потреби.

Зазначимо, що змінюється не тільки зміст, структура вищої освіти, але й її форми. Створення інноваційного освітньо-виховного середовища неможливе без внесення якісно нового змісту у вищу професійну освіту фахівця з інформаційної безпеки, без оптимізації кадрово-педагогічного потенціалу, підвищення рівня науково-методичного забезпечення навчального процесу, впровадження інноваційних технологій і методик викладання, оволодіння дослідно-експериментальними видами діяльності.

Актуальним науково-методичним завданням вищих навчальних закладів, що готують фахівця з інформаційної безпеки, зокрема, і нашого спеціального вищого навчального закладу, стає пошук нових ефективних форм і методів вищої освіти: від розроблення і введення в навчальні плани нових перспективних дисциплін до впровадження інноваційних методик і форм викладання.

Необхідність перегляду змісту навчальних дисциплін, які формують навички та уміння в сфері інформаційної безпеки, викликає і динамічний розвиток знання, збагачення його новими поняттями і категоріями, що спричинює відповідні зміни в системі зазначених наук, глобальне розширення інформаційно-правового простору тощо. Актуалізувались питання гармонізації українського та європейського законодавства з проблем інформаційної безпеки, зокрема проблеми імплементації міжнародно-правових норм у систему національного законодавства; питання неузгодженості правових норм та виникнення колізій у законодавстві після прийняття нових правових актів у зазначеній галузі тощо.

Необхідно зупинитися на проблемних питаннях щодо підготовки фахівців з інформаційної безпеки.

Через відсутність наразі в Україні чіткої державної стратегії система підготовки кадрів для інформаційної сфери в цілому, і, відповідно фахівців з інформаційної безпеки (ІТ-фахівців) в умовах реально виниклого попиту практично відсутня. Має місце процес створення лише елементів необхідної системи, що не завжди погоджені, а іноді суперечливі за своїм змістом та ідеологією. Дійсно, на базі в основному технічних вузів організовано підготовку фахівців у галузі захисту інформації, де навчальний процес проходить із акцентом на технічні й технологічні аспекти захисту інформації. У свою чергу, в юридичних навчальних закладах викладається гуманітарні (організаційно-правові) аспекти сфери інформаційних відносин, у тому числі інформаційної безпеки.

Важливими недоліками в підготовці фахівців є недостатній рівень вивчення:

- соціально-політичних (гуманітарних) проблем – впливу інформаційних технологій на людину та суспільство, значимості інформаційного протиборства, тактики і стратегії інформаційної війни;

- організаційно-правових аспектів захисту інформації, кримінологічних і криміналістичних методик протидії правопорушенням в інформаційній сфері;
- психологічних аспектів, як проявів злочинності в цій сфері, так і процесу протидії їй.

Тому сьогодні одним з першочергових завдань є належна організація процесу забезпечення

Національної системи інформаційної безпеки висококваліфікованими фахівцями з урахуванням певних особливостей даної сфери, а саме:

- інформаційна безпека – специфічна предметна галузь, що потребує комплексного підходу до процесу підготовки фахівців, тобто, викладання різних розділів фундаментальних і прикладних знань як інженерних, так і гуманітарних дисциплін;
- система освіти в галузі інформаційної безпеки має забезпечувати відповідність рівня підготовки фахівців темпам розвитку науково-технічного прогресу та Національного законодавства в сфері інформаційних відносин;
- загальну підготовку з питань інформаційної безпеки повинні мати всі суб'єкти інформаційної діяльності, а особливо керівний склад відомств, установ, підприємств, організацій;
- процес підготовки фахівців з захисту інформації всіх категорій має будуватися на єдиній методичній і правовій основі;
- система підготовки ІТ-фахівців потребує обов'язкового моніторингу з боку держави;
- розробка державних стандартів освіти за освітньо-кваліфікаційним рівнем «магістр».

УДК 681.3.06

ЗАСТОСУВАННЯ ТА ВИЗНАЧЕННЯ ТЕРМІНУ «ІНФОРМАЦІЙНА БЕЗПЕКА» В НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ

Олександр Корнейко, Сергій Корнейко
Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ»

Анотація: **Розглянуті основні складові терміну "інформаційна безпека" та його визначення і застосування в національному законодавстві.**
Summary: **The main forming of notion "information security" and its determination and usage in national legislation are considered.**
Ключові слова: **Інформаційна безпека, Доктрина інформаційної безпеки України.**

Інформаційна безпека (далі – ІБ) є одним із найважливіших чинників національної безпеки України. Інформаційна і національна безпека повною мірою узгоджуються і співвідносяться між собою за схемою «частина» і «ціле». Сьогодні інформаційна складова не існує поза межами загальної національної безпеки, так само, як і національна безпека не буде всеохоплюючою без інформаційної безпеки [1]. Загальним підґрунтям цих понять є, безумовно, поняття «безпека», що обумовлює стан захищеності життєвих інтересів людини як особистості, суспільства, держави. Сьогодні їх слід розглядати у геополітичному вимірі як невід'ємну частину державної політики із системою заходів економічного, політичного, організаційного та іншого спрямування, які адекватні загрозам життєво важливим інтересам громадян, суспільства і держави саме в такому контексті [1].

Тобто, ІБ є невід'ємною складовою кожної зі сфер національної безпеки. Водночас ІБ є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки [2].

Інформаційна безпека є складним, системним і багаторівневим феноменом, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: політична обстановка у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична обстановка в державі та ін. [2].

Суть ІБ полягає у захисті інформаційного простору України від небажаного інформаційного впливу, захисті національних інформаційних ресурсів, забезпеченні безпечного функціонування інформаційних та телекомунікаційних систем, а також у захисті інформації, що циркулює в них. Тому основними