УДК 378.14:004

О.І. Лозинський, Ю.І. Грицюк

Львівський державний університет безпеки життєдіяльності, Львів

ПІДГОТОВКА ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Наведено особливості підготовки фахівців з організації інформаційної безпеки у Львівському ДУ БЖД. Встановлено, що, незалежно від сфери виробничої діяльності, фахівець має володіти такими компетенціями: аналізувати цінність інформації, методи і засоби її надійного захисту та дотримання цілісності, джерела витоку і втрат, безпеку її зберігання; проектувати системи інформаційного захисту на основі комп'ютерного обладнання та мережевого устаткування; встановлювати, надійно використовувати та ефективно супроводжувати готові програмні продукти та технічні засоби, а також автоматизовані систем захисту інформації.

Ключові слова: *фахівець з інформаційної безпеки, інформаційна система безпеки.*

Вступ

Сучасний стан суспільного розвитку характеризується складними політичними, економічними та інформаційними процесами. Часто XXI ст. називають століттям інформаційних технологій, підкреслюючи при цьому, що саме інформація "володіє" сучасним світом. Українська держава, будучи ще молодою за історичними мірками, не може залишатися осторонь процесів загальної інформатизації суспільства та формування єдиного світового інформаційного простору. Водночас значно зросла кількість сторонніх втручань в різні інформаційні системи, блокуючи їхню роботу, а інколи й зовсім ви-

водячи їх з ладу. Значення та вагомість наслідків таких втручань з часом збільшилися настільки, що навіть розвинені держави, їх промислові та фінансові структури стали заручниками сучасних інформаційних технологій. Саме тому в Україні все більше уваги приділяється проблемі не тільки захисту інформаційних ресурсів, але й проблемі пошуку шляхів *управління інформаційною безпекою* [2].

Якщо раніше проблема захисту інформації була актуальною тільки для спеціальних служб [1], то згодом вона стала актуальною проблемою для всіх організацій та підприємств, в т.ч. і структурних підрозділів МНС України. Поверхневий аналіз надзвичайних ситуацій тільки природного характеру, які часто появляються в Україні та за її межами, показує тенденцію зростання їх кількості та масштабів можливих наслідків. У багатьох випадках вони провокують складні техногенні аварії та глобальні катастрофи (Японія, 2011 р.). Їхнє прогнозування, завчасне попередження, інформування населення про наявні джерела загроз та рівень їх небезпеки – основне завдання МНС України. У будь-якому випадку усі ці стратегічні та тактичні дії супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.

Основний матеріал досліджень

Найбільш ефективне вирішення питань інформаційної безпеки у системі Міністерства надзвичайних ситуацій зводиться до постійної та систематичної роботи компетентних фахівців у кожному із структурних підрозділів залежно від масштабів вирішуваних завдань. На сьогодні, в силу специфіки виконуваних робіт і вирішуваних завдань, проблема підготовки фахівців з інформаційної безпеки стосується навчальних закладів МНС України, одним із яких є Львівський ДУ БЖД. Впроваджені тут методики навчання поряд із традиційними методами і засобами захисту інформації пропонують курсантам і студентам вивчати сучасні технології забезпечення безпеки інформаційних ресурсів і комунікаційних систем. При цьому в університеті набувають все більшої вагомості інформаційно-комунікаційні технології навчання, які забезпечують загальну комп'ютеризацію навчального процесу на такому рівні, який дає змогу вирішувати курсантам, студентам і викладачам щонайменше три основні завдання:

– забезпечує входження в мережу Інтернет кожного учасника навчального процесу у будь-який час і з різних місць перебування;

– розвиває єдиний інформаційний простір освітніх індустрій, які сукупно забезпечують присутність в них у різній час і незалежно один від одного всіх учасників освітнього і творчого процесу;

– створює, удосконалює та ефективно використовує управляючі інформаційно-освітні ресурси – бази даних і банки знань, призначені особисто для курсанта, студента і викладача з можливістю повсюдного доступу для роботи з ними.

Різні підходи до визначення змісту сучасних інформаційних технологій навчання [2] виникають тому, що вони об'єднують різноманітну сукупність способів реалізації навчальних планів і програм, які є системою форм, методів і засобів навчання, а також спрямовані на досягнення освітніх цілей. Під інформаційними технологіями навчання у Львівському ДУ БЖД розуміємо систему наукових і інженерних знань [3], а також інформаційних методів і засобів, які використовують для створення, збирання, передачі, зберігання та оброблення інформації в системі МНС України. Завдяки цьому формується пряма залежність між ефективністю виконання традиційних навчальних програм і ступенем інтеграції в них відповідних інформаційно-комунікаційних технологій.

Основна мета вирішення проблеми інформатизації навчального процесу у Львівському ДУ БЖД полягає в тому, що внаслідок його запровадження має бути досягнута глобальна раціоналізація інтелектуальної діяльності охочих до навчання курсантів, студентів і навіть викладачів за рахунок використання сучасних інформаційних технологій з метою підвищення ефективності та якості підготовки фахівців з організації інформаційної безпеки до рівня інформаційного паритету, досягнутого хоча б у країнах Західної Європи. При цьому має бути забезпечена підготовка кадрів для потреб структурних підрозділів МНС з новим типом мислення, яке відповідатиме сучасним вимогам постіндустріального суспільства [3].

Використання сучасних інформаційно-комунікаційних систем у процесі навчання дає змогу курсантам, студентам і викладачам не тільки отримати інформацію про об'єкт управління інформаційною безпекою, але й допомагає їм усвідомити все розмаїття та складність зв'язків, характерних для реальних структурних підрозділів МНС України, простежити динаміку цих зв'язків у разі появи зовнішніх і внутрішніх джерел загроз, а також зруйнувати міжвідомчі бар'єри, що сформувалися у курсантів чи студентів ще зі школи, де нав’язувалась думка про ворожнечу між ними. Такий підхід до навчання дає змогу застосовувати сучасні інформаційні технології, які передбачають формування у курсантів і студентів неординарного мислення, творчого підходу до управління інформаційною безпекою, тобто спільної боротьби зі зловмисниками. Зрештою їх діяльність стає не набором стандартних прийомів, а ґрунтується на розумінні причинно-наслідкових зв'язків явищ і процесів у сфері інформаційної безпеки, що істотно підвищує їх умотивованість до навчання, а що більше, коли вони переконуються у його реальній результативності.

Сьогодні однією з характерних ознак інформаційно-освітнього середовища навчання у Львівському ДУ БЖД є можливість курсантів, студентів і викладачів звертатися до структурованих навчально-методичних матеріалів [3], до навчально-мультимедійних комплексів всього університету у будь-який час і з будь-якої точки місця перебування. Окрім доступності навчального матеріалу, поступово забезпечується можливість зв'язку курсантів чи студентів з викладачами через мережу Інтернет, отримання консультації в он-лайн режимі, а також можливість отримання індивідуальної "навігації" в освоєнні того або іншого предмету. При цьому багато хто прагне до гнучкого режиму набування знань, до реалізації модульних програм з однотипними предметами, які дають змогу швидко набирати залікові бали, завчасно здавати лабораторні та курсові роботи, дистанційно проводити тестовий контроль знань з урахуванням попереднього досвіду навчання, набутих знань і навиків. Як і раніше, важливою для курсантів і студентів залишається проблема особистого розвитку і професійного зростання; для багатьох це не вирішена дилема – піти на роботу після бакалаврату і продовжити навчання заочно, чи отримати ступіть магістра або фах спеціаліста за встановлений термін навчання; у декого виникає потреба продовження навчання в ад'юнктурі чи аспірантурі.

Відомо, що інформаційні технології навчання привносять нові можливості в систему будь-якої освіти, створюють потребу зміни самої моделі навчального процесу: перехід від репродуктивного навчання – "переливання" знань з однієї голови в іншу (тобто від викладача до курсантів чи студентів), до креативної системи освіти, коли в навчальній аудиторії за допомогою сучасних інноваційних методів і засобів моделюється надзвичайна ситуація або виробничий процес, а курсанти і студенти під керівництвом викладача мають застосувати свої знання, проявляти творчі здібності для аналізу модельованої ситуації та виробляти рішення на підставі отриманого завдання. При цьому в університеті розвиток традиційних і нових технологій навчання йде за принципом доповнюваності, що дає змогу вести мову про принципово нове значення інформаційно-освітнього середовища навчання, яке існує в реальному часі і поєднує в собі всю сукупність сучасних інформаційних технологій здобуття знань.

Немаловажне значення у навчальному процесі має мережа Інтернет, позаяк вона дає змогу створювати "віртуальні мережеві громади". Завдяки цьому віртуальні компаньйони володіють не тільки різними знаннями та інформаційними ресурсами, але й мають деякі абсолютно нові якісні та кількісні ознаки. Однією з таких ознак є їх глобальний характер, який дає змогу охочому до навчання здійснювати практично миттєвий зв'язок з Інтернет-ресурсом і скористатися ним. Уже зараз ця мережа незамінна для комерційних і фінансових структур, індустрії кіно, розваг та шоубізнесу, які залучають до контакту найрізноманітніші верстви населення, в т.ч. курсантів, студентів викладачів. Цим самим наявність мережі Інтернет є головною причиною як швидких темпів інформатизації суспільства, так і її найбільш наочним проявом у сфері захисту інформації. Понад це, саме глобалізація суспільства і визначає характер мережевих співтовариств, а також встановлює нові джерела загроз і небезпек інформаційним ресурсам.

Завдяки мережі Інтернет різні аспекти глобалізації (науковій, технологічний, економічний, культурний і освітній) мають значний вплив як на традиційні очні навчальні заклади, так і на розвиток різноманітних освітніх нововведень, таких як сучасна концепція дистанційного навчання та віртуальні університети. У всіх цих нововведеннях рух до інформатизації навчального процесу вимагає глибоких і радикальних змін у структурі навчальних дисциплін, у методиках викладання та проведення лабораторних досліджень, а також у підготовці управлінського і викладацького персоналу [3].

Аналізуючи специфіку підготовки фахівців з інформаційної безпеки у Львівському ДУ БЖД з напряму "Управління інформаційною безпекою", а також нормативні документи, що пов'язані з використанням конфіденційної та секретної інформації, з особливостей експлуатації об'єктів інформаційної безпеки МНС України, вважаємо, що професійні навики фахівців у сфері захисту інформації визначаються областю, об'єктами і видами їхньої професійної діяльності. Зокрема, областю професійної діяльності нашого випускника у структурних підрозділах МНС України є ефективне застосування:

– комп'ютерної та комунікаційної техніки, інформаційних систем, локальних і глобальних мереж;

– технічних засобів пасивного приховування інформації – фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани;

– технічних засобів приховування інформації (стеганографії) – вузько- та широкосмугові генератори лінійного та просторового зашумлення;

– програмно-технічних методів і засобів ідентифікації та автентифікації колективних користувачів, обслуговувального персоналу і мережевих ресурсів системи оброблення інформації та системи безпеки її зберігання;

– розмежування доступу користувачів до конфіденційної та секретної інформації, засобів комп'ютерної техніки і технічних засобів автоматизованих систем управління; цілісності інформації та конфігурації АС її оброблення; реєстрації та обліку дій користувачів; реагування (сигналізації, відключення, призупинення робіт, відмови в запиті) на спроби несанкціонованих дій зловмисників;

– антивірусних програмних засобів, програм архіваторів, дефрагментаторів, сканерів та ін.;

– програмно-технічних методів і засобів, які використовують для криптографічного шифрування та дешифрування інформації, а також крипто-аналізу конфіденційної та секретної інформації;

– програмного забезпечення АСУ програмними засобами, комплексами і системами захисту інформації;

– АСУ інформаційною системою безпеки силових і комерційних структур, у т.ч. і структурних підрозділів МНС України, систем автоматизованого проектування;

– математичного, інформаційного, технічного, економічного, організаційно-управлінського та правового забезпечення перерахованих вище систем.

На підставі проведеного аналізу підготовки фахівців з інформаційної безпеки у Львівському ДУ БЖД встановлено, що застосування інформаційних технологій навчання пов'язано з їхньою специфікою подальшої діяльності і вимагає наявності відповідних професійних компетенцій, особливо, коли це стосується інформаційної безпеки структурних підрозділів МНС України. У загальному випадку фахівець з інформаційної безпеки, незалежно від сфери захисту інформації, має володіти знаннями щодо: аналізу цінності інформації, методів і засобів її надійного захисту та цілісності; виявлення джерел витоку, втрат і оцінювання безпеки її зберігання; проектування систем інформаційного захисту на основі комп'ютерного обладнання та мережевого устаткування; встановлення, надійне використання та ефективний супровід готових програмних і технічних засобів, а також автоматизованих систем захисту інформації.

У процесі забезпечення інформаційної безпеки структурних підрозділів МНС України важливо розуміти характер, природу, сутність і зміст джерел загроз і рівнів їх небезпек, вміти своєчасно їх ідентифікувати. Найбільш важливими напрямами діяльності фахівців із захисту інформації тут є: спостереження, аналіз, оцінювання та прогнозування джерел загроз і рівнів їх небезпек, критичної безпеки інфраструктури, ступеню внутрішньої та зовнішньої уразливості; відпрацювання стратегії та тактики захисту інформації, планування попередження нападу, укріплення потенційними зв'язками, варіювання мережевими ресурсами забезпечення інформаційної безпеки; відбір сил і засобів протидії, нейтралізації та недопущення інформаційних атах, мінімізації шкоди від них; протистояння джерелам загроз природного, технічного або антропогенного характеру системам забезпечення інформаційної безпеки; управління наслідками інциденту (від інформаційних атак, інформаційних операцій, інформаційних воєн).

Список літератури

1. Бабак В.П. Підготовка фахівців із захисту інформації в Україні / В.П. Бабак, В.В. Козловський, В.О. Хорошко, Д.В. Чирков // Захист інформації: зб. наук. праць. – 2001. – № 4. – С. 57-69.

2. Богуш В.М. Інформаційна безпека : термінологічний навчальний довідник / В.М. Богуш, В.Г. Кривуца, А.М. Кудін / за ред. В.Г. Кривуци. – К.: ООО "Д.В.К.", 2004. – 508 с.

3. Грицюк Ю.І. Підготовка фахівців з інформаційної безпеки для потреб Міністерства надзвичайних ситуацій України / Ю.І. Грицюк, Т.Є. Рак // Шоста Міжнародна конференція "Нові інформаційні технології в освіті для всіх: навчальні середовища": матер. наук.-практ. конф. ITEA-2011, 22-23 листопада 2011 р., м. Київ. – К.: Міжнародний науково-навчальний центр інформаційних технологій і систем. – 2011. – С. 123-129.

Надійшла до редколегії 16.04.2012

Рецензент: д-р екон. наук, проф. О.І. Пушкар, Харківський національний економічний університет, Харків.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВО ЛЬВОВСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

О.И. Лозинский, Ю.И. Грицюк

Приведены особенности подготовки специалистов по организации информационной безопасности во Львовском ГУ БЖД. Установлено, что, независимо от сферы производственной деятельности, специалист должен владеть такими компетенциями: анализировать ценность информации, методы и средства ее надежной защиты и соблюдения целостности, источника происхождения и потерь, безопасность ее хранения; проектировать системы информационной защиты на основе компьютерного оборудования и сетевого оборудования; устанавливать, надежно использовать и эффективно сопровождать готовы программные продукты и технические средства, а также автоматизированные систем защиты информации.

Ключевые слова: *специалист по информационной безопасности, информационная система безопасности.*

TRAINING OF SPECIALISTS IN INFORMATION SECURITY IN LVIV STATE UNIVERSITY LIFE SAFETY

O.I. Lozinskiy, Yu.I. Gricyuk

Here are given the peculiarities of the training of specialists of information security in Lviv State University Life Safety is set that, regardless of the sphere of industrial activity specialist have to possess the following competencies: analyze the value of information, methods and means to it reliable protection and compliance integrity, sources of leak and losses, security of its storage; system design in-formation protection based on computer equipments and network equipments; in-stall, reliably use and effectively accompany ready software products and hard-ware, and automated system of information protection.

Keywords: *specialist on informative safety, informative system of safety.*