SPECIALISTS' TRAINING IN INFORMATIVE SAFETY FOR REQUIREMENTS OF MINISTRY EMERGENCIES OF UKRAINE

Yu. Gryciuk, T. Rak,
Lviv State University of Safety of Vital Functions, Ukraine

The features of specialists' training in informative safety for the requirements of Ministry Emergencies of Ukraine in the Lviv state university of safety of vital functions are analysed. It is set that application of modern information technologies is related to some specific features and requires the presence of the proper professional jurisdictions, especially when it touches informative safety of structural subdivisions of Ministry Emergencies of Ukraine.

ПІДГОТОВКА ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПОТРЕБ МІНІСТЕРСТВА НАДЗВИЧАЙНИХ СИТУАЦІЙ УКРАЇНИ

Ю.І. Грицюк, Т.Є. Рак
Львівський державний університет безпеки життєдіяльності, Україна

Проаналізовано особливості підготовки фахівців з інформаційної безпеки для потреб МНС України у Львівському державному університеті безпеки життєдіяльності. Встановлено, що застосування сучасних інформаційних технологій пов'язано з деякими специфічними особливостями і вимагає наявності відповідних професійних компетенцій, особливо коли це стосується інформаційної безпеки структурних підрозділів МНС України.

Вступ. За останні декілька десятиліть відбулися якісні зміни в процесах управління на всіх ієрархічних рівнях через інтенсивне впровадження сучасних інформаційних технологій. Їх швидкий розвиток призвів до зростання відносних цінностей суспільства взагалі й окремої людини зокрема – наявності конфіденційної інформації. Водночас стала зростати небезпека втручання в роботу інформаційних систем для несанкціонованого зчитування інформації. Значення та вагомість наслідків таких втручань з часом збільшилися настільки, що навіть розвинені держави, їх промислові та фінансові структури стали заручниками своїх інформаційних технологій. Саме тому в Україні все більше уваги приділяється проблемі не тільки захисту інформації, але й проблемі пошуку шляхів *управління інформаційною безпекою* [2].

Якщо раніше проблема захисту інформації була актуальною тільки для спеціальних служб, то згодом вона стала актуальною для всіх організацій та підприємств, так чи інакше пов'язаних з науковими чи виробничими здобутками, а також тих, які мали справу з комерційними чи банківськими таємницями. Окрім цього, навіть поверхневий аналіз надзвичайних ситуацій 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 структурних підрозділів МНС України. Водночас, швидка ліквідація надзвичайних ситуацій з найменшими витратами сил і засобів має немаловажне значення для фізичного і морального стану населення, а також економіки самої країни. У будь-якому випадку усі ці стратегічні та тактичні дії супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.

Найбільш ефективне вирішення питань інформаційної безпеки у структурних підрозділах МНС України зводиться до постійної та систематичної роботи компетентних фахівців у кожному з підрозділів залежно від масштабів вирішуваних завдань. Хоча проблема підготовки фахівців з захисту інформації донедавна була актуальною для спеціальних служб силових відомств [1], проте на сьогодні, в силу специфіки виконуваних робіт і вирішуваних завдань, вона стосується і навчальних закладів МНС України, одним із яких є Львівський ДУ БЖД. Запроваджені 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.

Мета нашого дослідження полягає у аналізі специфіки підготовки фахівців з інформаційної безпеки у Львівському ДУ БЖД, виявленні потенційних джерел загроз та рівнів їх небезпек для структурних підрозділів МНС України. При цьому, звернемо увагу на те, що багато дослідників у своїх роботах приділяють

значну увагу аналізові змісту поняття "інформаційна безпека", водночас такі поняття, як джерела загроз та рівень їх небезпек розглядаються ними дещо спрощено, здебільшого у відірваному від контексту поняття "інформаційна безпека", часто не пов'язаному із контекстом видового поняття "інформаційна загроза".

Загалом під джерелами загроз інформаційним ресурсам можна розглядати потенційно можливі дії природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на конфіденційну інформацію, що зберігається в ній. Ідентифікація джерел загроз, тобто розмежування пасивних дій від активних інформаційних зловмисників характеризується таким поняттям як уразливість інформаційних ресурсів. Саме за наявності вразливості як однієї з характеристик інформаційних систем і відбувається активізація джерел загроз. Безперечно, самі джерела загроз приховані [3, 4], за своєю суттю та відповідно до теорії множин – невичерпні, а отже й не можуть піддаватися достатньо повному аналізу та опису у будь-якому дослідженні, на що не претендуємо й ми у цій роботі.

Відповідно до Закону України "Про основи національної безпеки України", до джерел загроз інформаційній безпеці загалом, а також інформаційним ресурсам і комунікаційним системам зокрема належить:

- розголошення інформації, яка становить державну та іншу таємницю, передбачену відповідним законодавством, а також конфіденційної інформації, що є власністю структурних підрозділів МНС України;
- намагання маніпулювати суспільною свідомістю шляхом поширення недостовірної, неповної або упередженої інформації щодо появи надзвичайних ситуацій будь-якого характеру, а також їх наслідків на фізичний і моральний стан населення чи довкілля;
- комп'ютерна злочинність та мережевий тероризм – глобальний і локальний;
- розкриття інформаційних ресурсів, порушення їх цілісності, спричинення збоїв у роботі комп'ютерного обладнання та мережевого устаткування.

Аналізуючи специфіку підготовки фахівців у Львівському ДУ БЖД з напряму "Управління інформаційною безпекою" кваліфікації

"Фахівець з організації інформаційної безпеки", а також нормативні документи, що пов'язані з використанням конфіденційної та секретної інформації, з особливостей експлуатації об'єктів інформаційного захисту [3], ми вважаємо, що структура професійних навичок фахівців у галузі захисту інформації визначається областю, об'єктами і видами їхньої професійної діяльності. Зокрема, областю професійної діяльності нашого випускника, основними компетенціями якого є сукупність методів і засобів інформаційної діяльності, спрямованими на захист конфіденційної та секретної інформації, на керування системами інформаційної безпеки структурних підрозділів 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 активного 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 автоматизованих систем 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 використовуються для зручності криптографічного шифрування та дешифрування, а також криптографічного аналізу конфіденційної та секретної інформації;

- програмного забезпечення автоматизованих систем управління (програмних засобів, комплексів і систем);
- автоматизованих систем управління (за областями) системою інформаційної безпеки силових та комерційних структур, у тому числі і структурних підрозділів МНС України, систем автоматизованого проектування;
- математичного, інформаційного, технічного, ергономічного, організаційно-управлінського та правового забезпечення перерахованих вище систем.

Висновки. На підставі проведеного аналізу діяльності фахівців із захисту інформації, а також процесів функціонування систем інформаційної безпеки у структурних підрозділах МНС України, нами встановлено, що застосування інформаційних технологій пов'язано з їхніми специфічними особливостями і вимагає наявності відповідних професійних компетенцій, особливо коли це стосується інформаційної безпеки структурних підрозділів МНС України. У загальному випадку фахівець з організації інформаційної безпеки, незалежно від сфери захисту інформації, має володіти знаннями щодо: аналізу цінності інформації, методів і засобів її надійного захисту, цілісності, приховування, витоку, втрати та оцінки безпеки її зберігання; проектування системи 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).

Література

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. – 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. Мухачев В.А. Методы практической криптографии / В.А. Мухачев, В.А. Хорошко. – К. : ООО "Полиграф-Консалтинг", 2005. – 215 с.

4. Задірака В.К. Комп’ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях : навч. посібн. / В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк. – Київ-Тернопіль : Вид-во "Підручники і посібники", 2007. – 272 с.