М.Г. Коляда

СУТНІСТЬ І СПЕЦИФІКА ДІЯЛЬНОСТІ МАЙБУТНЬОГО ФАХІВЦЯ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Проблема підготовки фахівців в області захисту інформації донедавна була актуальною в основному для спеціальних служб силових відомств. На початку 90-х років двадцятого століття разом з руйнуванням так званого ідеологічного бар'єру у свідомості людей, у тому числі й тих, хто мав доступ до будь-якої закритої інформації, одержали бурхливий якісний і кількісний ріст технічні засоби передачі і збереження інформації. Поряд із традиційним способом захисту інформації особливу актуальність у даний час набуває безпека інформаційних технологій, у першу чергу пов'язаних зі збереженням і передачею інформації, яка міститься в персональних комп'ютерах і локальних мережах. Складність і різноманіття цих засобів обробки інформації, а також розширення можливостей каналів її передачі, відображення і збереження висувають ряд принципово нових вимог до фахівців інформаційної безпеки.

Відомо, що проблема захисту інформації актуальна зараз не тільки для спеціальних служб, але і для всіх організацій, так чи інакше пов'язаних зі збереженням і розробкою виробів разом з технологіями, що мають не тільки відношення до державної чи військової таємниці, але й до питань, що складають банківську, або іншу комерційну таємницю.

Останнім часом у світі відбуваються якісні зміни в процесах управління на всіх рівнях, обумовлені інтенсивним упровадженням сучасних інформаційних технологій. Паралельно зростає небезпека несанкціонованого втручання в роботу інформаційних і телекомунікаційних систем, причому вагомість можливих наслідків такого втручання для суспільства зросла настільки, що найбільш розвинені держави, їх фінансові і промислові структури стали якоюсь мірою "заручниками" своїх інформаційних систем. Саме тому в цих країнах все більше уваги приділяється проблемам не тільки захисту інформації, але й пошуку шляхів управління інформаційною безпекою.

Найбільш ефективне вирішення питань безпеки інформації організацій чи підприємств складається в постійній систематичній роботі компетентного фахівця такого підрозділу в залежності від масштабу розв'язуваних задач.

Початком історії створення національної системи підготовки кадрів у сфері інформаційної безпеки вважається підписання в 1995 році спільного наказу Державної служби України з питань технічного захисту інформації та Міністерства освіти України від 28.12.1995 № 66/358 "Про співробітництво між Міністерством освіти України й Державною службою України з питань технічного захисту інформації" [1, с. 57-69]. З цього часу в навчальних закладах України почалася підготовка фахівців з наступними спеціальностями: 7.160101 – "Захист інформації з обмеженим доступом та автоматизація її обробки (у комп'ютерних системах)"; 7.160102 – "Захист інформації з обмеженим доступом та 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 та мережах".

За узгодженою домовленістю сектору "Національна безпека" та науково-методичною комісією "Національна безпека" було встановлено нову відповідність спеціальностей галузі підготовки "Інформаційна безпека" і напрямів підготовки бакалаврів за новим переліком, який було закріплено Постановою Кабінету Міністрів України від 13 грудня 2006 р. № 1719 "Про перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра" [2]. Згідно з цими документами встановлено нові напрями підготовки фахівців галузі 1701 – "Інформаційна безпека" [3]:

1. "*Безпека інформаційних і комунікаційних систем*" – 6.170101 (бакалавр); 8.170101 (магістр); 2. "*Системи технічного захисту інформації*" – 6.170102 (бакалавр); 8.170102 (магістр); 3. "*Управління інформаційною безпекою*" – 6.170103 (бакалавр); 8.170103 (магістр).

Відповідно до Класифікатора професій [4], фахівці в галузі інформаційної безпеки (код 316) можуть займати такі первинні посади: 3163. *Фахівець з управління інформаційною безпекою*; 3163. *Фахівець з організації захисту інформації з обмеженим доступом*. Це можуть бути: технічні фахівці в галузі обчислювальної техніки (312), техніки-програмісти (3121), інспектори з безпеки та якості (315), технічні фахівці в галузі управління (343), помічники керівників (3434), інші помічники (3434.9), організатори діловодства (3435), інші технічні фахівці в галузі управління (3439), державні інспектори (344), інші державні інспектори (3449).

Згідно з Класифікатором видів економічної діяльності [5] (секції К – операції з нерухомим майном, оренда, інжиніринг та надання послуг підприємцям; розділ 74 – діяльність у сферах права, бухгалтерського обліку, інжинірингу; надання послуг підприємцям: група 74.6 – проведення розслідувань та забезпечення безпеки: клас 74.60 – проведення розслідувань та забезпечення безпеки), фахівець цього напряму може:

- консультувати в питаннях безпеки промислових об'єктів, помешкань і громадських будинків з оцінкою їхньої безпеки;
- вести охоронну діяльність, що здійснюється за допомогою механічних та електричних захисних пристроїв;
- надавати послуги із захисту інформації в комп'ютерних та інших технічних засобах від копіювання та несанкціонованого доступу;
- надавати інші послуги з охорони та захисту.

Перші публікації щодо методології підготовки фахівців із захисту інформації в Україні були надруковані ще в 1998 році (М.П. Карпінський, О.І. Фльоров, О.Г. Туровєров, Ю.І. Шпак), хоча перші аргументовані наукові праці з'явилися тільки у 2000–2001 роках (Г.П. Лазарєв, С.М.Кльоцкін, В.О. Хорошко, О.М. Богданов, О.Г. Додонов, О.В. Корнєйко, В.В. Мохор, Г.Ю. Маклаков, Е.В. Рижков). Стану підготовки фахівців у сфері інформаційної безпеки в Україні приділяли увагу такі науковці, як К.І. Бєляков і В.Д. Павловський. Всі ці наукові праці були направлені на обґрунтування і доцільність реформування системи підготовки фахівців такого профілю. Питання сутності і специфіки діяльності майбутнього фахівця із захисту інформації та управління інформаційною безпекою в них не підіймалися. Ця тема мало вивчена, розробка її дуже актуальна і своєчасна, тому що саме зараз готуються державні стандарти вищої освіти у вигляді вимог до підготовки фахівців освітньо-кваліфікаційного рівня бакалавр та магістр напряму підготовки 1701 "Інформаційна

безпека". Метою цієї статті як раз і є розкриттясутності і специфіки діяльності майбутнього фахівця із захисту інформації та управління інформаційною безпекою в контексті підготовки освітньо-професійних програм (ОПП) та освітньо-кваліфікаційних характеристик (ОКХ) бакалавра і магістра.

Наявні типові професійно-кваліфікаційні характеристики мають переважно констатуючий характер, прогностичний аспект змісту трудової діяльності і вимог до професійної підготовки спеціалістів відображений в них недостатньо. На наш погляд, повинні бути розроблені розширені дані про сутність і специфіку діяльності майбутнього фахівця із захисту інформації та управління інформаційною безпекою.

Професійна діяльність фахівця в сфері інформаційної безпеки умовно може бути розділена на такі напрями:*1. Інформаційно-комп'ютерний; 2. Інженерно-технічний; 3. Організаційно-управлінський.* При цьому, кожен із перелічених напрямків в свою чергу повинен мати такі компоненти: *виробничо-технологічний (технологічно-експлуатаційний); експериментально-дослідницький; аналітичний; проектувальний; контролюючий* та інші. Розберемо детальніше кожен з цих напрямів.

Сьогодні змінилася роль інформації, вона стала стратегічним ресурсом, що забезпечує конкурентні переваги любої фірми чи підприємства. Під дією інформаційних систем відбувається їх широкий вплив на організаційну структуру фірми, на формування інноваційної захисної політики і високої культури праці, на швидкісне володіння даними та виникає постійна потреба в навчанні її співробітників. За допомогою інформаційних технологій створюються на технологічному та виробничому рівнях мережі, оптимальні технологічні ланцюги, задля того, щоб фірми могли здійснювати свою діяльність на високому професійному рівні, швидше, ефективніше, з меншими витратами виконувати свої виробничі функції і надійно захищати комерційну та іншу конфіденційну інформацію.

Об'єктами професійної діяльності випускника за фахом "Інформаційна безпека" є захищені комп'ютерні системи і засоби обробки, збереження і передачі інформації; служби захисту інформації; математичні моделі процесів, що виникають при захисті інформації та управлінні інформаційною безпекою, на основі криптологічних методів та за допомогою технічних пристроїв. Тому інформаційні технології, комп'ютерна та комунікаційна техніка виступає не тільки об'єктом, але й інструментальним засобом професійної діяльності фахівця з захисту інформації.

До загальновживаного інформаційно-комп'ютер-ного забезпечення сфери захисту інформації можна віднести такі основні системи та технології – базові технології мережі Інтернет, у тому числі електронну пошту та технології архітектури "клієнт-сервер", операційні системи, системи автоматизованого проектування, інформаційно-пошукові системи, технології мережних засобів зв'язку, табличні процесори, системи управління розподіленими базами даних, системи документообігу, системи управління бізнес-проектами, інформаційні системи для статистичних обчислень, інформаційні системи управління підприємствами та організаціями, системи підтримки прийняття управлінських рішень і комп'ютерного моделювання, маркетингові інформаційні системи, банківські інформаційні системи, системи обліку кадрів і бухгалтерського обліку, фінансові інформаційні системи, експертні системи та інші.

До спеціального інформаційно-комп'ютерного забезпечення відносять:

- *перехоплювачі інформації, модифікатори інформації, програми підміни авторства інформації*;

- *аутентифікатори* (програми розпізнавачі користувача документу або системи), *програми визначники цілісності даних*, *програми, які призначені від запобігання несанкціонованого доступу до інформації* і т.п.;

- *шифратори та дешифратори; модулятори та демодулятори; перетворювачі файлів і даних* (кодувачі, декодувачі і т.п.);

- *прикладні криптологічні пакети* (програми для криптографічного шифрування, та програми для криптоаналізу);

- *антивірусні програмні середовища*, *засоби архівації та і стиснення даних і ущільнення носіїв інформації* (диспетчери архівів, програмні засоби, які тестують на цілісність структури архівів і даних, засоби відновлення ушкоджених архівів і даних, засоби від перегляду і несанкціонованої модифікації архівів і т.п.);

- *програмні компоненти локальних обчислювальних мереж* (мережні додатки, прикладні програмні комплекси, поштові програми, системи колективної роботи, мережні бази даних та ін.);

- *програмні компоненти глобальних комп'ютерних мереж* (IP-телефонія; Е-комерція – електронна комерція, системи електронних платежів, електронні платіжні засоби; відео-конференції);

- *брандмауери* – системи захисту в корпоративних інформаційних мережах (системи або комбінації систем, що дозволяють розділити мережу на дві чи більше частин і реалізувати набір правил, які визначають умови проходження пакетів з однієї частини в іншу); *пакетні фільтри, сервери прикладного рівня* і т.п.

- *інтерпретатори і компілятори мов програмування* (Pascal, Basic, C (Си), C++ (Си++), Java, мови програмування баз даних, скрипт-мови і т.д.) *та програмувальні середовища* (Visual Basic, Delphi та ін.);

- *системи штучного інтелекту* (експертні системи; програмні додатки продукційних, фреймових моделей, програм нечіткого моделювання; семантичних, нейронних мереж, мереж що самоорганізуються і т.п.)

- *засоби автоматизації науково-дослідних робіт* (Math Cad, Math Lab, Mathematica, програми інженерної та комп'ютерної графіки та ін.).

Аналізуючи специфіку підготовки фахівців з напряму підготовки "Інформаційна безпека", а також нормативні документи, які пов'язані з використанням конфіденційної інформації та з експлуатацією об'єктів інформаційного захисту, ми дійшли висновку, що структура професійних навичок фахівців у галузі захисту інформації визначається областю, об'єктами і видами їхньої професійної діяльності.

Областю професійної діяльності випускника є захист інформації та управління інформаційною безпекою – галузь науки і техніки, що включає в себе сукупність засобів, способів і методів людської діяльності, спрямованих на захист конфіденційної і секретної інформації, на керування системи, що забезпечує інформаційну безпеку і має на увазі застосування:

- комп'ютерної і комунікаційної техніки, комплексів, систем і мереж;

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

- технічних засобів активного приховування – вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення;

- програмних комп'ютерних засобів ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації; розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем; цілісності інформації та конфігурації автоматизованих систем; реєстрації та обліку дій користувачів; маскування оброблюваної інформації; реагування (сигналізації, відключення, зупинення робіт, відмови в запиті) на спроби несанкціонованих дій;

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

- програмних засобів, використовуваних для зручності криптографічного шифрування і криптографічного аналізу інформації;

- програмного забезпечення автоматизованих систем (програмних засобів, комплексів і систем);

- автоматизованих систем управління (по областях) інформаційною безпекою; систем автоматизованого проектування;

- математичного, інформаційного, технічного, ергономічного, організаційно-управлінського і правового забезпечення перерахованих систем.

Відповідно до фундаментальної і спеціальної підготовки, фахівець із захисту інформації незалежно від напрямку роботи, повинний виконувати наступні види професійної діяльності: *проектно-конструкторську; виробничо-технологічну; науково-дослідну; організаційно-управлінську; експлуатаційну.*

Аналізуючи типові професійні задачі діяльності майбутніх фахівців у галузі захисту інформації і управління інформаційною безпекою, можна виділити основний комплекс задач, що не залежать у загальному випадку від виду діяльності:

1) визначення цілей захисту інформації, об'єктів інформаційної безпеки, критеріїв ефективності захисту, ступеня безпеки інформації (ступеня секретності);

2) організація процесу розробки системи інформаційної безпеки з заданою якістю в заданий термін;

3) аналіз, теоретичне й експериментальне дослідження методів інформаційного захисту, програм і технологій, застосовуваних на всіх етапах життєвого циклу системи інформаційної безпеки;

4) системний аналіз об'єктів інформаційного захисту і управління інформаційною безпекою, їхній взаємозв'язок;

5) створення і дослідження математичних (криптографічних) і програмних моделей обчислювальних і інформаційних процесів, пов'язаних з дослідженням, проектуванням, функціонуванням і управлінням об'єктами інформаційної безпеки;

6) проектування архітектури апаратно-програмних комплексів захисту інформації і їхніх компонентів;

7) вибір технологій, інструментальних (технічних) засобів і засобів обчислювальної техніки при організації процесу розробки об'єктів інформаційної безпеки;

8) проектування математичного, криптологічного, лінгвістичного, інформаційного і програмного забезпечення обчислювальних систем і автоматизованих систем на основі сучасних технологій проектування, у тому числі з використанням систем автоматизованого проектування;

9) розробка на основі діючих нормативів і стандартів документації для різних категорій фахівців, що беруть участь у створенні, експлуатації і супроводі об'єктів інформаційного захисту;

10) управління інформаційною безпекою та організація впровадження систем інформаційного захисту в експлуатацію, супровід програмних продуктів, технічних (в тому числі; комп'ютерно-комунікаційних засобів);

11) оцінка надійності системи інформаційної безпеки, забезпечення умов безпечної життєдіяльності обслуговуючого персоналу;

12) вибір методів і засобів виміру експлуатаційних характеристик щодо цілісності, витоку, перекручуванню та втрати інформації та самих об'єктів інформаційної безпеки, їхнє дослідження, вироблення вимог і специфікацій по їхній модифікації.

Аналізуючи діяльності фахівців із захисту інформації, а також процесів функціонування систем інформаційної безпеки на основі комп'ютерної, комунікаційної і спеціальної техніки захисту, можна зробити *висновок*, що застосування інформаційних технологій у цих областях пов'язано з їхніми специфічними особливостями і вимагає наявності відповідних професійних здібностей. У загальному випадку фахівець незалежно від напрямку повинний виконувати три основних види професійної діяльності, пов'язаних з:

1) аналізом обробки, цінності, надійності, цілісності, приховування, витоку, втрати, оцінки безпеки інформації;

2) проектуванням систем інформаційного захисту на основі комп'ютерної та передавальної техніки;

3) супроводом і використанням готових програмних засобів і автоматизованих систем захисту.

ЛІТЕРАТУРА

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

2. Постанова Кабінету Міністрів України від 13 грудня 2006 р. № 1719 "Перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра" // Офіційний вісник КМ України від 25.12.2006 р., № 50, стаття 3333. – С. 160.

3. Наказ Міністерства освіти і науки України "Про введення в дію переліку напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра" від 27 січня 2007 р. – № 58.

4 . Національний класифікатор України. Класифікатор професій ДК 003:2005, введений в дію наказом Держспоживстандарту України від 26 грудня 2005 р. – № 375.

5. Національний класифікатор України. Класифікатор видів економічної діяльності ДК 009:2005.

Подано до редакції 30.01.09

РЕЗЮМЕ

В статье рассматривается сущность и специфика деятельности будущего специалиста по защите информации и управлении информационной безопасностью. Приводятся присущие специалистам такого профиля прогностические аспекты содержания трудовой деятельности.

РЕЗЮМЕ

У статті розглядається сутність і специфіка діяльності майбутнього фахівця із захисту інформації та управління інформаційною безпекою. Наводяться притаманні фахівцям такого профілю прогностичні аспекти змісту трудової діяльності.

SUMMARY

The article presents the essence and specificity of activity of future experts in protection of information andmanagement of informational security. The author demonstrates some prognostic aspects of the contents of labour activity inherent in experts of such structure.

Ключевые слова*: профессиональная деятельность, защита информации, информационная безопасность.*
Ключові слова*: професійна діяльність, захист інформації, інформаційна безпека.*
Keywords*: professional activity, informationalprotection, information security.*

_____