УДК 681.3

Головань С.М., Хорошко В.О., Щербак Л.М.
Державний університет
інформаційно-комунікаційних технологій

НАПРЯМИ ФОРМУВАННЯ СИСТЕМИ ЗНАНЬ ФАХІВЦІВ ІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Важливу роль у розвитку сучасних інформаційних технологій відіграє підготовка у вищих навчальних закладах України фахівців із інформаційної безпеки. Це тривалий процес послідовного, систематичного та цілеспрямованого формування системи знань у період навчання після завершення повної середньої освіти. Завершується цей процес отримання певної кваліфікації за підсумками державної атестації. Сучасна концепція функціонування інформаційних систем ставить нові вимоги до знань фахівців, які займаються питаннями обробки та захистом інформації з обмеженим доступом. На сьогодні актуальними є афоризм "без знання справи за неї не берись", який відомий з давніх часів і перевірений практикою діяльності суспільства.

Власник інформації зацікавлений у її збереженні та вказавши гриф обмеження доступу, визначають відповідний набір рівнів захисту та нагадується про необхідність забезпечення режиму доступу до інформації – порядок одержання, використання, поширення і збереження.

Про актуальність і важливість збереження інформації свідчить зростання накопичення інформації, що відображає ділову активність організації. Таким чином захист інформації з обмеженим доступом є одною з важливих проблем, вирішення якої залежить від рівня знань і вмілого практичного впровадження його фахівцями із інформаційної безпеки.

В даній роботі розглянуті основні напрями отримання знання фахівців які займаються захистом інформації з обмеженим доступом.

Формування спеціальних знань

Діяльність і практика формування ринку праці та світовий досвід обумовили необхідність переходу на ступеневу систему підготовки фахівців з вищою освітою із забезпеченням на кожній її ступені широких можливостей освіти, формування спеціальних знань.

Знання – результат процесу пізнання діяльності, перевірене суспільною практикою і логічно упорядковане відображенням в свідомості фахівця, а також категорія, яка відбиває зв'язок між пізнавальною і практичною діяльністю фахівця. Знання можна ідентифікувати тільки тоді коли вони проявляються у процесі використання умінь виконувати відповідні розумові та фізичні дії.

Уміння це здатність фахівця виконувати певні дії при здійсненні тієї чи іншої діяльності на основі системи знань, шляхом застосування інформаційних технологій, які включають правові (законодавчі), організаційні (адміністративні), фізичні і технічні (апаратні і програмні) засоби захисту інформації з обмеженим доступом. При цьому використовуються як діючі перераховані засоби, так і проводиться підготовка до застосування перспективних прогнозованих засобів.

Ступенева система освіти реалізує концепцію неперервної освіти і забезпечує можливість переривати та поновлювати навчання з інформаційної безпеки за будь-якою освітньо-професійною програмою. Така програма відображає структурно-логічну схему підготовки фахівця, вимоги до рівня освітньої та професійної підготовки, зміст та строки навчання, форми контролю та державної атестації, навчального плану містить графік навчального процесу, перелік та обсяг навчальних дисциплін, послідовність та форми їх проведення, форми та засоби поточного і підсумкового контролю, робочого навчального плану відображає конкретизацію навчальної роботи, передбачену навчальним планом, детальне

планування навчального процесу [1, 2, 3]. Структура нормативно-правової бази організації навчального процесу наведена на рис. 1.

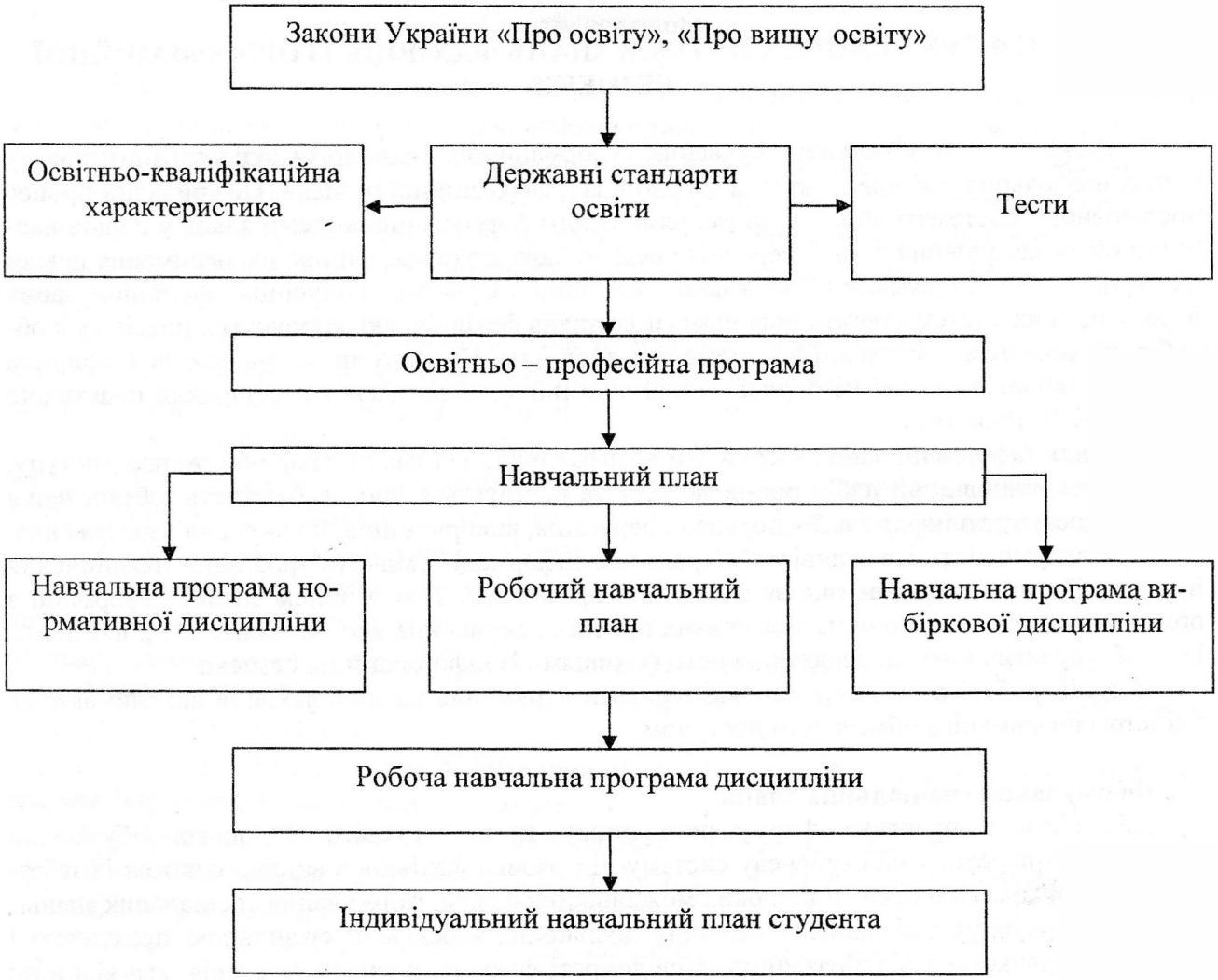

Рис. 1. Структура нормативно-правової бази організації навчального процес

Формування бази знань фахівців з інформаційної безпеки визначає перелік навчальних дисциплін, які відносяться до циклу дисциплін:

– гуманітарної та соціально-економічної підготовки (історія України, правознавство тощо);

– фундаментальних та професійно-орієнтованих дисциплін (фізика, основи інформаційної безпеки тощо);

– вибіркових професійно-орієнтованих дисциплін за переліком програми (основи менеджменту, криптографічні перетворення тощо);

– вільного вибору студентом (система обробки текстової, табличної та графічної інформації, економічна безпека діяльності організації, основи завадостійкості систем захисту інформації, охорона комерційної таємниці в організації, системи банківської безпеки тощо).

І завершуються присвоєнням особі освітньо-кваліфікаційного рівня базової вищої освіти – бакалавр. На рівні базової вищої освіти базується освітньо-кваліфікаційний рівень повної вищої освіти – магістр (спеціаліст).

За місцем праці бакалавра, магістра (спеціаліста) з інформаційної безпеки, однією з форм продовження навчання, є регулярні навчання по тематиці з різних областей діяльності, що дозволить своєчасно та повно ознайомлюватися з поточними і перспективними змінами. Формами оволодіння знань є лекції, практичні заняття, самостійна робота з нормативними документами, матеріалів отриманих на лекції та іншої спеціальної літератури. Оволодіння необхідними теоретичними і практичними знаннями в галузі інформаційної безпеки здійснюється під керівництвом викладача, що працює у цій галузі та самостійно.

Практика підтверджує наступний факт: в умовах невірних або неповних знань, які переносяться з інших галузей, дуже рідко це приводить до вірних логічних процедур, а частіше до некоректного чи невірного прийняття рішення у сфері систему захисту інформації з обмеженим доступом.

При плануванні і проведенні підвищення кваліфікації (тривалість підвищення кваліфікації з відривом від служби не повинна перевищувати чотирьох тижнів, без відриву від служби – шести місяців, тематичний семінар – до п'яти днів) основна увага приділяється вибору форми навчання (курси, семінари), виходячи з їх особливостей, мети підготовки та необхідному об'єму знань:

– курси – форма прискореної підготовки, перепідготовки і підвищення кваліфікації певного вузького фаху;

– семінар – форма групових занять з якогось предмету або теми, що відбувається під керівництвом викладача.

Як свідчить практика, підвищення кваліфікації доцільно проводити у такій послідовності:

– початкова підготовка;

– короткострокова програма навчання;

– курси підвищення кваліфікації;

– підготовка керівного складу.

З метою активізації пізнавальної діяльності слухачів, підвищення рівня знань, в окремих лекціях, що пропонуються слухачам, бажано застосовувати проблемний метод. Так, на лекції викладач визначає проблемну ситуацію, розкриває її сутність, значення і направляє мислення слухачів на самостійний пошук шляхів вирішення проблеми. Зазначена лекція може бути також реалізована у формі запитань і відповідей, аналізу, коротких обговорень. Для забезпечення наочності навчання та інтенсифікації навчального процесу використовуються навчальні плакати, схеми тощо.

Необхідно контролювати хід навчання фахівців на кожному етапі та регулярно проводити перевірку знань і формування відповідного відношення до практичної діяльності по забезпеченню інформаційної безпеки, ініціативи, творчого відношення до дорученої справи. Найбільш коректним засобом комплексної оцінки якості підготовки фахівців – тести професійної компетентності (психологічні методики і завдання для вимірювання та оцінювання досягнутого рівня розвитку здібностей, умінь та знань) які можуть використовуватися як для атестації фахівців, так і для добору кадрів.

Об'єм потоку інформації з обмеженим доступом, що надійшла до фахівця визначається різницею об'єму інформації, що засвоєна ним та передана у вигляді інформації. При позитивній різниці фахівець стає джерелом (передатчиком), а при негативній – приймачем інформації.

Відома класифікація баз знань, які містять інформацію про матеріали документів, книг, статей, звітів тощо:

– статична база знань, яка складає відомості, які в ході вирішення задач є незмінними;

– динамічна база знань, що змінюється у процесі вирішення завдань.

Формування знань базується на результатах праці (творчості) у визначені часові терміни (день, місяць, квартал, рік) при дії широкого кола зовнішніх факторів (оточення, пори року тощо).

Формування знань з безпека інформаційних технологій

Інформація з обмеженим доступом існує в різних формах. Її можливо зберігати і інформаційних системах (електронні документи), передавати по внутрішній (локальній) і зовнішній (глобальній) мережі, роздруковувати або записувати на папері, а також озвучувати в розмовах. З погляду безпеки усі види інформації з обмеженим доступом, включаючи паперову документацію, бази даних, машинні носії інформації, розмови та інші засоби вимагають захисту.

Інформації і підтримуючим її інформаційним системам та мережам можуть загрожувати такі небезпеки, як шахрайство, саботаж, вандалізм, а також інші джерела відмовлень і аварій. З'являються все нові погрози такі як віруси, хакери тощо.

Склад програмного забезпечення і засобів захисту інформації з обмеженим доступом залежить від конкретних умов роботи організації, зокрема від організаційної її структури та розміщення, знань фахівців, кількості і змісту організаційно-розпорядчих документів. Конфігурація апаратних засобів інформаційної системи залежить від фізичного розміщення апаратних засобів, кількості різноманітних категорій оброблюваної інформації, кількості і категорії користувачів, а також від виду мережі.

Керування безпекою інформаційних технологій – це процес, що його використовують для досягнення і забезпечення необхідних рівнів конфіденційності, цілісності, доступності, обліковості, достовірності і надійності [4, 5]. До функцій керування безпекою інформаційних технологій належать:

– визначення цілей, стратегій і методик організації захисту інформаційних технологій;

– визначення необхідних умов під час організації захисту інформаційних технологій;

– ідентифікація та аналіз загроз безпеки для матеріальних й нематеріальних цінностей інформаційних технологій організації;

– ідентифікація та аналіз ризиків;

– визначення відповідних засобів захисту;

– контроль за застосуванням і функціонуванням засобів захисту, що необхідне для ефективного захисту інформації і нормального функціонування організації в цілому;

– розроблення і реалізація програми компетентності в захисті;

– виявлення і реагування на інциденти.

Для реалізації цих функцій керування безпекою в системах інформаційних технологій захист повинен бути невід'ємною частиною загального плану керування організацією.

Виходячи з того, що формування знань з інформаційних технологій набуваються у процесі навчання та впровадження в дію законодавчих актів і стандартів України, нормативних документів з захисту інформації з обмеженим доступом та інших сфер знань. Умовно можна проілюструвати процес, підвищення рівня знань після введення в дію законодавчих актів і стандартів України, нормативних документів з захисту інформації з обмеженим доступом та інших сфер знань графіком, який наведено на рис. 2 де $\{P_j,\ j=1,\ldots 6\}$ – послідовність значень рівня знань.

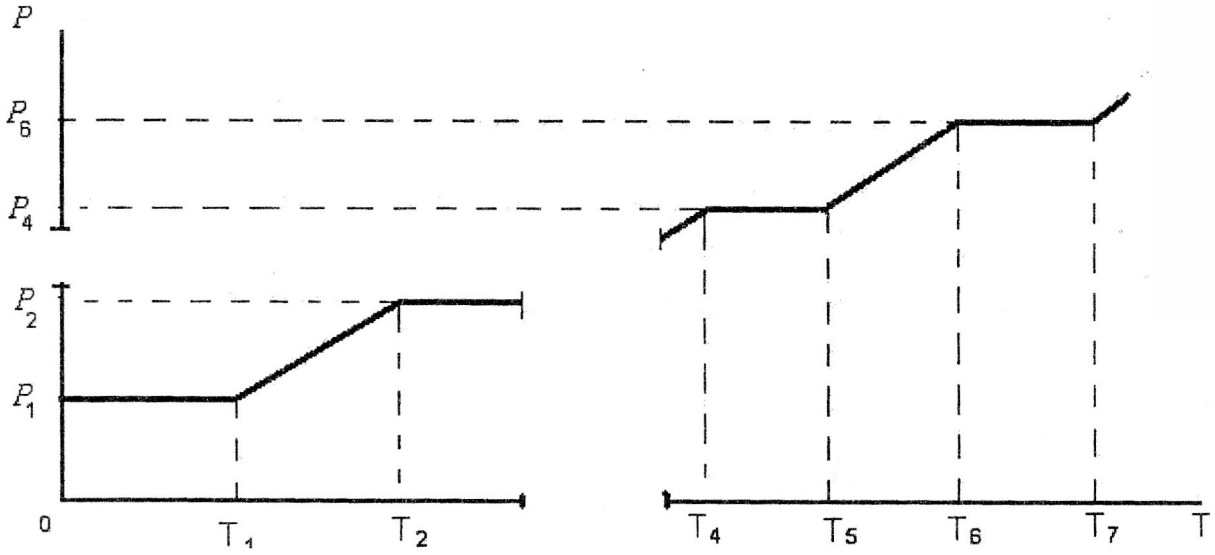

Рис. 2. Підвищення рівня знань після введення в дію законодавчих актів і стандартів

Наведений графік ілюструє позитивний ріст знань після опанування знаннями сучасних інформаційних технологій, введення в дію законодавчих актів і стандартів.

На часовій вісі t вказані поточні моменти часу початку T_j і завершення T_{j+1} використання результатів тієї чи іншої інформації.

Висновки

Проведений аналіз дозволяє визначити основні напрямки формування системи знань у вищих навчальних закладах України при підготовці фахівців за напрямом 1701 "Інформаційна безпека". Крім того, обґрунтована система постійного підвищення рівня знань фахівців з урахуванням змінення та розвитку сучасних інформаційних технологій, законодавчих актів і стандартів.

Список літератури

1. *Закон України* "Про освіту" // Відомості Верховної Ради, – № 34 – 1991 – ст. 451.

2. *Закон України* "Про вищу освіту" // Відомості Верховної Ради, – № 20 – 2002 – ст. 134.

3. *Давиденко А.М., Головань С.М., Щербак Л.М.* Система підготовки фахівців по напряму "Інформаційна безпека". // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.. 37. – К.: 2006. – С. 3-10.

4. *ДСТУ ISO/EC TR 13335-1:2003.* Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції та моделі безпеки ІТ. Чинний від 2004-10-01.

5. *Азаров С.С., Кривуца В.Г., Тітов О.В., Хорошко В.О.* Особливості підготовки фахівців із інформаційної безпеки // Захист інформації – № 1, 2006. – С. 4-18.