НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ "ЗАХИСТ ІНФОРМАЦІЇ" 1, 2006

УДК 638.253.231

С.С.Азаров, В.Г.Кривуца
О.В.Тітов, В.О.Хорошко

ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ ІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Важливою та невід`ємною складовою реалізації державної політики у сфері забезпечення інформаційної безпеки є підготовка кваліфікованих фахівців у цій галузі. На цей час в Україні створена та в цілому ефективно функціонує система підготовки, перепідготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки. Підготовку спеціалістів за навчальним напрямом 1601 „Інформаційна безпека" по п`яти спеціальностям здійснюють 20 вищих навчальних закладах, у тому числі і в Державному університеті інформаційно-комунікаційних технологій (ДУІКТ). Для перепідготовки та підвищення кваліфікації фахівців функціонують чотири навчальні центри, один з них є в ДУІКТ.

Система підготовки та перепідготовки фахівців із інформаційної безпеки, яка склалася у другій половині 70-х років, на сьогодні переживає нову трансформацію і модернізацію з урахуванням сучасних вимог, які висуваються до інформаційної безпеки у рамках Болонського процесу і як наслідок до рівня підготовки фахівця.

Для реалізації завдань вищої освіти України у нових умовах, необхідна невідкладна концентрація зусиль на наступних напрямках:

1. Пріоритетним напрямком розвитку вищої освіти України є її інтеграція у світовий та європейський освітній простір, приведення системи вищої освіти на державному, регіональному та університетському рівнях до вимог Болонської декларації, яка передбачає: прийняття загальної системи порівнянних учених ступенів, запровадження двох циклів навчання (бакалавр, магістр), впровадження кредитно-модульної системи та розширення мобільності студентів у межах загальноєвропейського освітнього простору, забезпечення європейської співпраці щодо забезпечення якості освіти, забезпечення працевлаштування випускників у межах загальноєвропейського ринку праці.

2. Організація навчального процесу у кожному навчальному закладі має забезпечувати можливість для кожного студента всебічного задоволення його освіти потреб завдяки його власної ініціативи та індивідуальних спрямувань. Інтенсивність та обсяг професійного зростання, виходячи із його особистих інтелектуальних та фізичних можливостей творчих спрямувань та соціальної активності. Для цього у повній мірі має бути використаний потенціал кредитно-модульної системи, яка повинна виступати механізмом перетворення навчального процесу у технологію навчання.

3. Якість вищої освіти напряму залежить від рівня впровадження інформаційно-комунікаційних технологій та формування інформаційної культури. Необхідне формування принципово нової парадигми освітньої діяльності в умовах інформаційного суспільства.

4. Необхідно вдосконалювати систему управління вищою освітою та впорядковувати мережу вищих навчальних закладів з урахуванням загальнодержавних та регіональних потреб у фахівцях з вищою освітою. Для розвитку національної системи вищої освіти мають діяти потужні навчально-наукові центри, роль яких мають узяти на себе провідні університети.

5. Для забезпечення працевлаштування випускників вищих навчальних закладів вдосконалювати професійно-практичну підготовку студентів, надавати їм сучасних знань, вмінь, навичок, що забезпечують випускникам конкурентоспроможність на ринку праці. Необхідно переглянути Перелік напрямів та спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах.

6. Створювати умови громадянам для більш рівних можливостей здобувати вищу освіту завдяки збільшенню обсягів державного замовлення на підготовку кадрів за всіма освітньо-кваліфікаційними рівнями. Студентам, які не потрапили на бюджетну форму

навчання, забезпечити необмежену можливість навчатися за контрактом за рахунок державних пільгових кредитів, субсидій.

7. Здійснити заходи щодо підвищення ефективності фінансово-економічних показників діяльності вищих навчальних закладів, передбачивши оптимізацію фінансових витрат на проведення навчально-виховного процесу, зменшення витрат на підготовку одного фахівця без зниження якості вищої освіти. Необхідно надати право вищому навчальному закладу в межах існуючого бюджетного або позабюджетного фінансування планувати рентабельність своєї діяльності.

Питання про підготовку, перепідготовку та підвищення кваліфікації фахівців з інформаційної безпеки (ІБ) вперше було поставлено у другій половині 60-х років.

Тоді воно розглядалося тільки у площині кадрового забезпечення захисту державних секретів, оскільки комерційної таємниці в СРСР не існувало, а захист несекретної інформації не був настільки актуальним, як сьогодні.

З початку 90-х років виникли нові фактори, які вплинули на підготовку і підвищення кваліфікації фахівців з ІБ. До числа найважливіших з них відносяться:

- розширення інформаційної сфери;
- розширення обсягу інформації, що підлягає захисту;
- ускладнення умов збереження та захисту інформації.

Хоча обсяг державних секретів України у порівнянні з СРСР знизився, але він продовжує залишатися значним у найважливіших сферах діяльності держави. Про це свідчать Закони України "Про інформацію", "Про державну таємницю" та інші нормативні документи. Обсяг інформації, що захищається, не скоротиться, оскільки в Україні, в силу її геополітичного положення, військового та економічного потенціалу, зберігається велика кількість інформації про політичні, військові, економічні, науково-технічні та інші сектори держави. Така інформація потребує надійного захисту, бо її витік здатний викликати політичні ускладнення, ослаблення військової та економічної потужності країни.

Разом з тим поряд з продовженням існування державної таємниці з'явилась і комерційна таємниця. По мірі зростання кількості підприємств недержавного сектора збільшується і обсяг інформації, що складає комерційну таємницю. Від надійності захисту цієї інформації залежить ефективність функціонування комерційних підприємств, їх безпека і конкурентоспроможність.

Не випадково, що при створенні спільних підприємств вимога до захисту комерційної таємниці висувається зарубіжними партнерами як одна з ключових. По мірі розвитку в Україні нових економічних відношень і розширення конкуренції підприємств, актуальність проблем захисту комерційної таємниці буде посилюватися. У надійному забезпеченні захисту комерційної таємниці зацікавлена і держава, враховуючи пряму залежність економічного положення країни від стану економіки на підприємствах недержавного сектора.

Перетворення інформації в основний фактор розвитку господарських структур, найважливіший ресурс і товар, джерело прибутку і умову виживання у конкурентній боротьбі вимагає підвищення захисту інформації, що становить державну і комерційну таємницю, так і тієї частини несекретної інформації, втрата якої обернеться негативними економічними та іншими наслідками.

В нинішній час під концепцією інформаційного забезпечення діяльності будь-якого об'єкту розуміється вирішення трьох макрозадач:

- формування і поточне корегування інформаційного кадастру об'єкту, вибір джерел інформації для регулярного поповнення і відновлення його;
- поточне відновлення і поповнення і функціональне використання інформаційного кадастру об'єкту відповідно до мети функціонування об'єкту;
- відслідковування відповідності вхідного потоку інформації стану інформаційного кадастру об'єкту та меті функціонування об'єкту і прийняття необхідних рішень і мір при неузгодженості значень перерахованих параметрів.

Тому з розширенням застосування при обробці інформації засобів обчислювальної техніки можливості втрати такої інформації різко зростають.

Ускладнення відбувається і за рахунок перегляду принципів засекречування інформації, модифікації правових основ її захисту [1,2,4].

Що стосується захисту комерційної таємниці, то тут діє ряд специфічних обставин, що впливають на організацію її захисту. На комерційних підприємствах інформаційна безпека є прерогативою самих підприємств. Об'єкти комерційної таємниці повинні встановлюватися і видозмінюватися індивідуально, на рівні їх власників, відповідно до норм права, виробничими, торговельними і фінансовими процедурами, укладеними угодами, спрямуванням інтересів конкурентів, споживчою цінністю і т.д. [3]. У таких умовах важливе значення мають характер і джерела комерційної таємниці, її носії, градації за ступенем захищеності, специфічні канали витоку інформації і т.д.

Зростання можливостей щодо несанкціонованого одержання інформації, розширення за рахунок появи нових конкурентів "контингента" організації і осіб, зацікавлених у несанкціонованому одержанні інформації, поява додаткових каналів витоку інформації, передусім у процесі обробки інформації засобами електронно-обчислювальної техніки, використання нових методів і засобів несанкціонованого здобуття інформації значно ускладнили умови ІБ, особливо в частині протидії технічній розвідці та попередження несанкціонованої модифікації інформації в АСОІ шляхом зараження її вірусами і програмними закладками різних видів і типів.

Забезпечення режиму інформаційної безпеки в обстановці, що постійно змінюється і ускладнюється, вимагає постійного проведення;

- фундаментальних та прикладних досліджень явищ і процесів у даній предметній області;
- необхідна кількість підготованих і компетентних фахівців.

Можна цілком погодитись з тим, що в нових умовах ситуація з забезпеченості кадрами у сфері ІБ не може бути визнана задовільною і потребує реорганізації. Ця проблема ще підсилюється і тим, що [6]:

- зменшилося фінансування освіти;
- з'явилася можливість втрати науково-педагогічного та професорсько-викладацького потенціалу, а також матеріально-технічної бази;
- відсутність системного підходу з програмно-цільовим плануванням і оптимальним розподілом ресурсів;
- відсутність планової політики в питаннях підготовки фахівців з інформаційної безпеки.

Рекомендації Постанови Кабінету Міністрів України, нещодавніх конференцій та семінарів, присвячених проблемі підготовки кадрів з ІБ зводяться до необхідності здійснення заходів [5,6,7]:

- збільшення чисельності фахівців, оскільки їх кількість не задовольняє існуючим потребам;
- гармонізація вітчизняної системи освіти до європейських критеріїв і стандартів, практичного приєднання до Болонського процесу;
- вдосконалення навчального процесу з метою підготовки висококваліфікованих фахівців, оскільки теорія і практика ІБ безперервно та інтенсивно розвиваються і нові досягнення повинні якнайшвидше знайти відображення у навчальних планах і програмах;
- розширення номенклатури спеціальностей з ІБ, оскільки сучасні системи забезпечення інформаційної безпеки стають все більш складними і комплексними як за метою, так і за методами і засобами, що використовуються.

Наслідком цього процесу і стала поява певної модифікації та тенденції у системі підготовки та підвищення кваліфікації фахівців з інформаційної безпеки.

Таким чином, саме життя ставить наступні довгострокові цілі у цій області[8]:

1) підготовка та перепідготовка фахівців, здатних ефективно вирішувати сучасні задачі ІБ в Україні;

2) збільшення чисельності фахівців, які проходять підготовку та перепідготовку за напрямком інформаційної безпеки;

3) об'єднання зусиль провідних освітніх, наукових колективів та адміністративних органів для вирішення масштабних практичних проблем ІБ;

4) створення та постійний розвиток регіональних наукових шкіл в області ІБ;

5) створення умов для забезпечення режиму ІБ держави в цілому, регіонів, підприємств та окремих громадян.

До короткострокових задач, на наш погляд слід віднести:

- створення та освоєння більш досконалого освітнього процесу за напрямком інформаційної безпеки в Україні;

- проведення наукових досліджень і формування на базі провідних вищих навчальних закладів (ВНЗ) та академічних інститутів регіональних наукових центрів здатних об'єднати широке коло дослідників для вирішення крупномасштабних задач інформаційної безпеки у регіоні;

- ефективне використання регіональних інформаційних баз та обладнання для навчання та проведення практичних занять студентів, аспірантів та фахівців, які проходять перепідготовку, з проблем забезпечення ІБ, а також для проведення НДР, залучення викладачів ВНЗ та співробітників центрів перепідготовки фахівців з інформаційної безпеки;

- здійснення допомоги у підготовці документів та первинної експертизи їх у ліцензіатів у сфері ІБ;

- вирішення спільно з регіональними адміністративними органами конкретних практичних задач в області інформаційної безпеки.

Слід відзначити, що деякі з цих короткострокових задач сьогодні вже вирішуються. Так з 1998 року працює Міжгалузевий міжрегіональний семінар Національної Ради НАН України "Технічні засоби захисту інформації", який має відділення у Києві при ДУІКТ, Львові при Національному університеті "Львівська політехніка", Харкові при Харківському Національному університеті радіоелектроніки, Дніпропетровську при Національному гірничому університеті України, у Севастополі при Севастопольському військово-морському ордена Червоної Зірки інституті ім. П.С.Нахімова, Вінниці при Вінницькому Національному технічному університеті та Одесі при Одеському Національному політехнічному університеті. Зараз опрацьовується можливість відкриття відділення семінару у місті Луганську при Східноукраїнському Національному університеті ім. В.Даля, у місті Миколаїв при Українському державному морському університеті імені адмірала Макарова та місті Запоріжжі при Запорізькому Національному технічному університеті.

Ми бачимо, що охоплені західні, центральні, східні та південні регіони України.

Крім того Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ разом з Міністерством освіти і науки при підтримці ДУІКТ були створені регіональні центри на базі Національного університету „Львівська політехніка" - Західний регіональний центр ТЗІ, на базі Національного гірничого університету Середньодніпровський регіональний центр ТЗІ та на базі Вінницького Національного технічного університету - Волинський регіональний центр ТЗІ. Зараз іде робота по створенню Кримського, Одеського (Південного) та Харківського (Східного) регіональних центрів.

Слід відзначити, що в умовах ринкових відносин самі регіони можуть виступати як суб'єкти конкурентних відносин. Самостійність регіонів та їх ринкова діяльність створює деякі протиріччя між регіонами та регіонів з центром - все це стимулює вирішення задач регіону та дослідження особливостей такого захисту у конкретних обставинах. Таким чином, існує периферійний аспект проблеми інформаційної безпеки, який цікавий та більш доступний периферійним дослідженням.

З цього видно, що регіональні відділення Семінару можуть стати об'єднуючим ядром

для вирішення як короткострокових, так і довгострокових задач у напрямку інформаційної безпеки.

Не претендуючи на оригінальність та враховуючи все вище зазначене, автори бачать слідуючи шляхи вирішення проблеми підготовки фахівців за напрямком ІБ [7,8]:

1. Удосконалення знань у процесі навчально-виховної підготовки у відповідних областях математики, фізики, інформатики та інших дисциплін таких як функціональний аналіз, теорія розпізнавання образів, нейромережеві алгоритми, сучасні методи цифрової обробки сигналів та інші.

2. Поетапна постановка лабораторних та практичних занять на наявній у ВНЗ як звичайній, так і спеціальній апаратурі, а також залучення до проведення лабораторних та практичних занять фахівців зацікавлених міністерств та відомств з технікою, яка знаходиться у них на озброєнні.

3. Науково-дослідна робота студентів та слухачів під час навчального процесу.

На даний час В Україні діє постанова Кабінету Міністрів від 24.05 1997 року № 507 „Про перелік напрямів та спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за відповідними освітньо-кваліфікаційними рівнями, зі змінами, які були проведені згідно наказів Міністерства освіти і науки у 1998 - 2003 роки. Але цей перелік вже не відповідає задачам сьогодення [6]. Тому 16.06.2005 був затверджений наказ Міністра освіти і науки України № 363 „По затвердження змін до Переліку напрямів та спеціальностей…."

Згідно з цим Наказом п.26 вилучено з напряму підготовки 0914 „Комп'ютерні системи, автоматика і управління" спеціальність „Захист інформації з обмеженим доступом та автоматизація її обробки".

А також введено до Переліку розділ „Національна безпека", напрям підготовки 1601 „Інформаційна безпека" (конкретний перелік спеціальностей визначається центральними органами виконавчої влади за погодженням з Міністерством освіти і науки). До розділу „Національна безпека" також введені напрями підготовки 1602 „Національна безпека" та 1603 „Охорона та захист державного порядку". Щодо підготовки фахівців з ІБ крім напрямку 1601 автори вважають, що до нього відноситься ще і спеціальність 7. 160203 „Організація захисту інформації з обмеженим доступом".

З метою уточнення напрямів удосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців у галузі ІБ у рамках VIII Міжнародної науково-практичної конференції „Безпека інформації в інформаційно-телекомунікаційних системах" (травень 2005 року) за участю представників державних органів та вищих навчальних закладів проведено „круглий стіл" на тему „ Підготовка, перепідготовка та підвищення кваліфікації в сфері захисту інформації". Автори також прийняли участь у роботі круглого столу.

За результатами круглого столу його учасниками запропоновано „Пропозиції щодо спеціальностей та спеціалізацій навчального напряму 1601 „Інформаційна безпека".

Відповідно пропозиціям пропонується чотири спеціальності за рівнем „бакалавр":

1) безпека інформаційних і комунікаційних систем;
2) системи технічного захисту інформації;
3) управління інформаційною безпекою;
4) безпека державних інформаційних ресурсів.

Крім того за рівнем „спеціаліст" та „магістр" учасниками круглого столу запропоновані слідуючі спеціалізації:

1,а) захист інформації в комп'ютерних системах і мережах;
1,б) захист інформації в телекомунікаційних системах;
1,в) комплексні системи захисту інформації;
2,а) фізико-технічні засоби захисту інформації;
2,б) системи захисту від несанкціонованого доступу;
3,а) захист інформації з обмеженим доступом та автоматизація її обробки;

3,б) адміністративний менеджмент захисту інформації;

3,в) організація комплексної безпеки об 'єктів інформаційної діяльності;

4,а) організація і технології безпеки державних інформаційних ресурсів;

4,б) криптологічне забезпечення спеціальних інформаційно-телекомунікаційних систем;

4, в) безпека систем урядового та конфіденційного зв 'язку.

Пропозиції круглого столу були обговорені у ВНЗ України і з урахуванням їх пропозицій, змін та доповнень був запропонований Міністерством освіти і науки України проект „Переліку галузевих знань, бакалаврських програм – fields of study підготовки фахівців у вищих навчальних закладах України".

Згідно з цим переліком до галузі знань „Інформаційна безпека" відносяться бакалаврські програми fields of study : криптографія; комп'ютерна безпека; системи технічного захисту інформації; безпека інформаційних і комунікаційних систем; управління інформаційною безпекою та безпека державних інформаційних ресурсів.

У зв'язку з тим, що на сьогодні ще не зроблено ніяких змін в Переліку спеціальностей, підготовка фахівців здійснюється у ВНЗ України, а також і в ДУІКТ за слідуючими спеціальностями: 7.160101 - захист інформації з обмеженим доступом та автоматизація її обробки (в 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 захисту інформації з обмеженим доступом; 7.160105 - захист інформації в комп'ютерних системах і мережах.

Однак потрібно визначити, що підготовка фахівців з інформаційної безпеки завжди мала індивідуальну спрямованість, не була "масовою" чи поставленою "на потік". Це дозволяло згуртувати в окремо визначених державою ВНЗ відповідних фахівців, вчених та методистів найвищого рівня підготовки, які зробили істотний вплив на коло професійних ознак студентів після випуску з ВНЗ.

Підготовка фахівців повинна ґрунтуватися на системному підході, що дозволяє структурувати і порівнювати різні технічні, природно-наукові та інші фахи і спеціалізації в області інформаційної безпеки в залежності від того, за яким призначенням будуть в майбутньому працювати випускники. Фахівці мають проходити підготовку по технічному і природно-науковому профілям, як вузькому так і широкому. Дотепер у рамках Міністерства освіти і науки України недостатньо пророблена з позиції аналізу сфери видів, об'єктів, методів і засобів професійної діяльності в цій галузі. При цьому необхідно враховувати існуючий дефіцит науково-педагогічних кадрів для ВНЗ і науково-дослідних закладів. Задача підготовки висококваліфікованих фахівців повинна вирішуватися в рамках системи підготовки, перепідготовки і підвищення кваліфікації в області інформаційної безпеки та захисту інформації, що у даний час в Україні лише удосконалюється Система, що відображає специфічні риси предметної сфери, повинна розглядатися як складова частина загальнодержавної системи підготовки, перепідготовки і підвищення кваліфікації кадрів.

Слід зазначити, що експертами Офісу безпеки Генерального секретаріату ЄС та Департаменту безпеки Європейської комісії у квітні поточного року під час проведення консультації з компетентними українськими структурами, високо оцінено створену в Україні систему інформаційної безпеки, ефективність функціонування якої обумовлена якістю та глибиною підготовки спеціалістів з питань криптографічного та технічного захисту інформації в інформаційних та комунікаційних системах, на об'єктах інформаційної діяльності.

Особливості проблеми захисту інформації пред'являють певні специфічні вимоги до студентів і, відповідно, до навчального процесу.

Насамперед, як показує досвід підготовки фахівців з інформаційної безпеки та захисту інформації, необхідно приділити особливу увагу доборові студентів і при цьому враховувати їхні індивідуально-психологічні особливості, риси характеру, технічну

підготовку і загальну культуру.

Важливим кроком у проведені державної політики щодо підготовки та підвищення кваліфікації в області ІБ є Постанова Кабінету Міністрів України від 8 жовтня 1997 року № 1126 „ Про концепцію технічного захисту інформації в Україні". Згідно з цією Постановою [5] у розділі 4 записано „ Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ є: ... визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ".

Для виконання положень Постанови у 2002 був створений в ДУІКТ факультет Інформаційної безпеки, а в 2004 році Інституту захисту інформації, як відокремлений структурний підрозділ Державного університету ІКТ. В зв'язку з цим змінився підхід до підготовки фахівців у галузі ІБ. В Інституті об'єднані спеціальності за напрямком 1601 "Інформаційна безпека": 7.160102, 7.160103, 7.160104 та 7.160105. Підготовка студентів проводиться на слідуючих кафедрах Інституту: комплексних систем захисту інформації, безпеки інформаційних технологій, вищої математики та обчислювальної техніки. Робота проводиться з кандидатами для відбору у спеціалізовані групи, протягом двох років їх підготовки в Інституті і лише на третьому курсі після тестування і співбесіди, де враховуються всі перераховані вище якості, вони зараховуються до навчальної групи. При цьому недостатня увага до людського чинника часто являє собою більш значну загрозу, ніж використання новітніх технічних засобів для здобування секретної інформації. Поняття "людський чинник" містить у собі особисті якості, що виражають цілісну характеристику особистості, її відмінність від інших людей. На думку фахівців, незважаючи на різноманітність та "витонченість" спеціальної техніки для одержання бажаної інформації, люди залишаються одним із самих ймовірних джерел витоку інформації. Саме людина виступає основою будь-якої інформації. При підборі кандидатів, яким треба буде працювати із секретною інформацією, необхідно враховувати їх ділові, професійні, моральні якості та психологічні особливості. Тут важливо скласти уявлення не тільки про окремі якості і риси кандидата, а також про особистість у цілому, її світоглядних установках, інтелекті, переконаннях, ціннісних орієнтаціях, здібностей до даного виду діяльності, рисах характеру і т.п. Необхідно формувати та виховувати у студентів пильність, обов'язковість, особисту відповідальність за виконання доручених завдань.

Сутність концепції підготовки фахівців грунтується на тому, що поведінка людини в життєвих ситуаціях позбавлена дискретності, побудованої на конкретних знаннях. Вона являє собою цілісне поле, яке містить в собі весь попередній досвід, що охоплює як суб'єкт (людину) так і об'єкт діяльності. Завдяки цьому поведінка логічна, адекватна, людська. Аналогічна форма професійної поведінки спостерігається у серйозних фахівців, у яких конкретні знання давно перетворилися у власне надбання, власне бачення професійних проблем, коли немає потреби щось конкретне пригадувати для того, щоб розібратися у ситуації.

Здатність людини в умовах обмеженого часу адекватно реагувати на зміни обстановки, швидко і безпомилково робити висновки та приймати логічно беззаперечні рішення слід розуміти як інтелект.

Коли така здатність може з'явитися? Зараз уже не викликає сумніву, що інтелектуальний розвиток не є сумою знань, умінь, навичок. Це системна якість людини, яка з'являється у неї за певних умов, які повинні бути реалізовані в ході навчального процесу.

Звідси можна зробити висновок, що адекватність поведінки залежить не стільки від конкретних знань, скільки від їх організації всередині людини. Як наслідок - систему освіти повинна цікавити в першу чергу не навчальна-інформація, а людина у навчальному середовищі, її розвиток в межах відповідно організованої та структурованої навчальної інформації. Останнім часом набуває поширення напрям формувати методологічну основу

розвитку інтелекту, розвитку людини. Цей напрям реалізується через використання основних принципів філософії нестабільності, синергетики.

Завдяки тому, що людина здатна до саморозвитку, саморегуляції та самоорганізації, стає можливою її універсальна адаптація до навколишнього середовища і навіть до глобальних змін, які майже не помітні на індивідуальному рівні.

Становлення внутрішнього світу людини та людської думки відносно об'єкта вивчення, розвиток вищих психічних функцій теж відбувається згідно з природними законами саморозвитку, саморегуляції та самоорганізації. Те, що відбувається у людини всередині, не може бути виключено із загальних процесів Всесвіту. При цьому слід зазначити, що розвиток людини відбувається не взагалі, а тільки в межах об'єкта пізнання, тобто в межах суб'єкт-об'єктних відносин. Ширина об'єкта розвитку в процесі становлення людини постійно зменшується. В дитинстві це може бути життя як таке, а у зрілому віці об'єкт розвитку звужується до певної професійної діяльності. Від розвитку людини в певному середовищі залежить ступінь розвитку її вищих психічних функцій.

За синергетичною методологією, для вирішення основних проблем сучасної освіти, для досягнення мети навчання і виховання педагогічні дії необхідно узгоджувати з природними законами, згідно з якими відбувається становлення такої самоорганізуючої системи, як людина.

Природний підхід до навчання є гуманістичним процесом. Цей підхід до педагогіки розвивається тому, що він є глибоко функціональним і практичним підходом до вирішення будь-якої проблеми. Тепер уже ні для кого не є таємницею, що некритичне слідування наперед визначеним конкретним істинам призводить до збільшення помилок раціонального характеру. Помилки є наслідком неадекватного сприйняття ситуації, коли вона розбігається з готовими істинами, засвоєними з книжок або з розповіді викладача. Життя завжди набагато складніше за будь-яку найбільш детальну інструкцію, що за своєю сутністю є однобічно фіксованим поглядом на ситуацію в конкретно визначених обставинах.

Тому гуманістичний підхід до навчання полягає в тому, щоб надати людині можливість виробити своє власне відношення до конкретних знань, завдяки чому вони стають особистим інтелектуальним надбанням. Таке надбання формується як результат саморозвитку у відповідному навчальному середовищі в напрямку оволодіння об'єктом вивчення. Створення такого середовища і має бути основою поведінки викладачів. Вони повинні створити умови, за яких той, хто навчається, мав би змогу та право на самостійний всебічний розгляд проблем, критичний аналіз, співставлення та підданий сумніву здавалось би непохитних істин, самостійне вироблення нових поглядів, сприйняття парадоксальних ідей. Все це є тим засобом, завдяки якому конкретні знання втрачають нерухомість, отримують динаміку розширення зони своєї дії, включаючи проблеми, на вирішення яких немає прямої готової відповіді.

Розвиток людини всередині об'єкта повинен здійснюватися у напрямку кінцевої форми, тобто оволодіння об'єктом пізнання як цілісністю незалежно від того, що розуміють під об'єктом. Із цілісності світу випливає цілісність кожної із його частин, Цілісність об'єкта несе в собі надзвичайно великий потенціал пізнання: практичний, творчий, гуманітарний, естетичний, художній та інші.

Цілісні знання є гуманітарними знаннями незалежно від об'єкта вивчення. Сюди слід включати також технічні, технологічні та інші системи, які відповідають природним критеріям цілісності. Природне ціле несе в собі естетичний, художній, гуманітарний потенціал, який запобігає можливим помилкам раціонального характеру. Метою навчання, як уже було зазначено, має бути оволодіння предметом пізнання як цілісністю [10].

Тому необхідно знайти таку структуру об'єкта вивчення, яка б критеріально відповідала структурі цілісного уявлення того, хто навчається, тобто критеріально відповідала б кінцевій формі структур мислення. Ці критерії мають бути наступні [10]:

• структурна взаємооборотність - можливість логічної структурної декомпозиції цілого поняття, а також наявність одночасної можливості повернення до цілого в результаті логічної деструктуризації;

• цілісна стійкість - збереження цілого на кожному етапі структурної декомпозиції;

• самодостатність - відповідність кожного структурного елемента на кожному етапі структурної декомпозиції вимогам цільності, яка відповідає тим же критеріям, що і вихідна цільність.

Таким чином об'єкт вивчення розподіляється на функціонально завершені частини - навчальні модулі. Уже на цьому етапі від об'єкта вивчення відсікаються ніби-то важливі деталі, які в той же час не мають прямого відношення до об'єкта вивчення або такі, без яких він не втрачає цільності, а тому ці деталі є необов'язковими для вивчення. Цим зменшується інформаційне навантаження на того, хто навчається.

І нарешті настав час звернутися безпосередньо до процесу розвитку студента в межах об'єкта вивчення в цілому, або в межах окремого навчального модуля. В останньому випадку ми маємо модульно-розвивальний процес, який технологічно найбільш прийнятний для застосування у закладах освіти. Використання закономірностей розвитку дозволяє обґрунтовано підійти до впровадження модульно-рейтингової системи навчання.

Щоб зрозуміти сутність процесу розвитку фахівця, необхідно вивести його основні закономірності та знайти форми вираження у ході навчального процесу. Ці закономірності та форми випливають із загальних закономірностей, за якими саморозвиваються, самоорганізуються, саморегулюються будь-які природні складні системи, в тому числі людина та її вищі психічні функції. Співставлення та аналіз розвитку різних природних систем, таких, наприклад, як цивілізація, етнос, людина, мислення, пам'ять дало змогу виділити у цьому процесі такі етапи: поштовх, підйом, ріст, внутрішній розвиток, надлом, розпад [10].

Перший етап розвитку - підйом - є найскладнішим. Складність полягає в тому, що коли людина вперше зустрічається з певною справою, об'єктом вивчення, по відношенню до них у неї майже немає ніякої інформації, ніяких уявлень, досвіду, а значить, здібностей, мислення тощо. Для того щоб розпочати новий відрізок життя, зайнятися новою справою, потрібні відповідні правила, рушійні сили для того, щоб з'явилась наполегливість і впертість піти по шляху засвоєння нового.

При формуванні навчального плану необхідно передбачити підготовку майбутніх фахівців, залежно від спеціальності, по якій здійснюється підготовка, також в області чинного законодавства, криптографічного і технічного захисту, організаційних і фізичних заходів захисту, а також в області психології, моралі й етики. Підготовка в такій області як психологія не менше важлива, чим в інших. Адже уміння визначити психологічний тип співрозмовника і правильно провести бесіду багато в чому визначає ефективність визначення наявності або відсутності каналів витому інформації.

У зв`язку з цим, розроблено навчальні плани підготовки фахівців із ІБ. Вони, у цілому, повинні забезпечити загальноосвітню та спеціальну підготовку фахівців. Розроблений навчальний план підготовки кадрів із ІБ також спрямований на підготовку фахівців-універсалів, які володіють методами, обізнані на засобах та технологіях захисту інформації, що містить будь-який вид таємниці, які володіють правовими, організаційними, програмно-математичними та інженерно-технічними основами ІБ та які здатні організувати і забезпечити комплексну систему ІБ. Однак, стало ясно, що в умовах розширення видів таємниці, ускладнення задач з ІБ, збільшення обсягу загальногуманітарних дисциплін необхідна для підготовки багатопрофільних фахівців кількість годин різко зменшується у рамках навчального плану за вимогами Болонського процесу.

Тому було прийнято рішення здійснювати підготовку фахівців за напрямом 1601 „Інформаційна безпека" на рівні „бакалавр" без поділу студентів по спеціальностям. Навчальні плани розроблені таким чином, що дисципліни за якими проводиться

підготовка студентів за всіма чотирма спеціальностями є однаковими.

Крім того слід враховувати, що підготовка фахівців ведеться як за державним замовленням, так і на контрактній основі. Це обумовлює, що частина фахівців в подальшому буде працювати в державних структурах, а частина у недержавних.

У зв'язку з цим вимагається розширити рамки і чисельність контингенту підготовки фахівців з інформаційної безпеки. Воно повинно відбуватися за рахунок введення в різноманітних навчальних закладах спеціалізацій, пов'язаних із безпекою інформації. Це в першу чергу відноситься до економістів, юристів, медиків і т. д..

В нинішній час намітився диференційний підхід до підготовки фахівців з ІБ. Порівняно невеликий обсяг інформації, що захищається на багатьох підприємствах державного і комерційного секторів диктує необхідність мати на цих підприємствах не вузьких фахівців по окремим напрямкам захисту, що було б недоцільно (а для малих підприємств просто неможливо), а універсального фахівця за всіма напрямками захисту, який володів би організаційно-технічними і інженерно-технічними навичками, знав би засоби та технологію захисту, міг би організувати та забезпечити комплексний ЗІ на підприємстві, направлений на досягнення максимальної ефективності захисту за рахунок одночасного використання взаємозв'язаної сукупності всіх напрямків, методів та засобів щодо забезпечення зберігання носіїв інформації, що захищається, та запобігання несанкціонованого доступу до неї.

В той же час, на великих оборонних державних підприємствах, а також великих комерційних об'єднаннях, кількість яких, як свідчить світовий досвід, буде постійно зростати, доцільно наряду з фахівцями-універсалами, мати фахівців за окремими напрямками захисту, що в силу їхньої спеціальної предметної підготовки краще ніж фахівець-універсал володіють методами, засобами та технологією ІБ у відповідному напрямку.

Таке диференціювання у певній мірі вже знайшло практичне втілення. Так, в результаті проведених консультацій та обговорювань, в тому числі за участю фахівців інших ВУЗів та зацікавлених міністерств і відомств, були вироблені наступні підходи [6,7,8,11]:

- при збереженні однакових сфер та об'єктів професійної діяльності повинні бути зазначені відмінності за видами професійної діяльності, оскільки вони впливають на характер знань та вмінь фахівця;
- повинен бути визначений склад базових дисциплін, які, як правило, необхідні для кожної спеціальності;
- необхідно посилити і диференціювати загальнопрофесійну підготовку фахівців за кожною спеціалізацією;
- склад і зміст спеціальних дисциплін за кожною спеціалізацією повинні охоплювати інформацію, що складає всі види таємниці, розкривати всі види, методи, засоби та технологію ЗІ, однак, при цьому необхідно враховувати специфіку професійної діяльності випускника;
- прийом кандидатів на навчання повинен здійснюватися не за спеціальностям та спеціалізаціям, а в загальний бакалаврат в цілому, розподіл студентів по спеціальностям та спеціалізаціям повинен здійснюватися за їх бажанням і на основі конкурсного відбору наприкінці 4-го курсу, коли вибір кваліфікації вже є усвідомленим; до безпосереднього розподілу за спеціальностями навчання повинно бути спільним за всіма дисциплінами, після розподілу, як це робиться зараз в ДУІКТ.

Крім того, також в Університеті проводиться навчання іноземних громадян за денною та заочною формою, організується за державним замовленням і за договорами між Університетом та замовниками.

Навчальним планом факультету інформаційної безпеки передбачено вивчення протягом терміну навчання як основних теоретичних, так і допоміжних професійно-орієнтованих дисциплін. Для іноземних громадян додатково читаються спецкурси за

основними дисциплінами, враховуючи їх професійну діяльність на батьківщині. Мова підготовки визначається бажанням студента і фіксується в Контракті на навчання. Опанування мовою передбачає комунікативні та виховні цілі, завдяки чому студенти набувають певних моральних, соціальних, культурних знань, які разом з курсом "Країнознавство" сприятимуть формуванню особистості та світогляду студента.

Вивчення іноземної мови (української або російської, за бажанням студента) забезпечується двома нормативними курсами (іноземна мова та теорія і практика перекладу). Вивчення другої іноземної мови за вибором розпочинається з другого семестру першого року навчання.

Важливим елементом навчального процесу є проходження іноземними студентами у кінці кожного навчального року професійної практики, покликаної зорієнтувати їх на виконання конкретних практичних завдань на рівні сучасних вимог, завершити фахову освіту і підготувати студентів до виконання ними конкретних службових обов'язків.

Необхідно звернути увагу на підвищення вимоги до якості підготовки фахівців. Поява нових каналів витоку інформації та засобів її несанкціонованого одержання, необхідність забезпечення надійної безпеки, зростаюча вартість інформації поставили питання про навчання фахівців не тільки традиційним методам та засобам ІБ, але і новим підходам та навичкам в області попередження витоку інформації, її несанкціонованого копіювання, модифікації, блокування, знищення, інших незаконних форм втручання в інформаційні ресурси та системи. Та й традиційні методи та засоби ІБ потребують подальшого вдосконалення прив`язки до умов, які змінюються.

Більш того, сучасний фахівець з ІБ повинен уміти визначати склад інформації, що захищається, її цінність, ступінь вразливості, розраховувати шкоду від можливої втрати інформації, оцінювати якість і ефективність різноманітних методів та засобів захисту, проводити спеціальні дослідження і сертифікацію різноманітних технічних засобів обробки і ІБ, орієнтуватися у вітчизняному та зарубіжному ринку засобів ЗІ, проектувати та впроваджувати системи ІБ, знати та використати зарубіжний досвід.

Впровадження технічних засобів обробки інформації, в першу чергу комп'ютерних, вимагає від фахівців уміння вільного користування ними, а входження українських підприємств в світову економіку створення спільних підприємств - різкого збільшення обсягу знань іноземних мов.

Крім того слід визначити, що згідно з вимогами Болонського процесу кожний випускник ВНЗ повинен знати дві іноземні мови. Зараз у ДУІКТ розпочата підготовка фахівців з ІБ англійської та німецької мов. Вимоги до знань та умінь будуть сформульовані у цьому навчальному році і вони будуть відповідати вимогам Болонського процесу та зацікавлених міністерств та відомств.

В сучасних умовах сформувався новий вид трудової діяльності, пов'язаний з одержанням, поширенням і збереженням інформації. Суттєвим фактором, що впливає на можливості безпосередньої участі українських спеціалістів у створенні та розвитку новітніх технологій в галузі захисту інформації є високі вимоги щодо підготовки з іноземних мов, насамперед європейських.

Досвід показує, що спілкування з іноземними спеціалістами з тематики, яка безпосередньо пов`язана з відповідним напрямком наукових досліджень, зазвичай проходить досить легко. З іншого боку, навіть під час такої бесіди труднощі викликає лексика, щодо знайомства, ділових, організаційних, побутових питань, або фразеологічних штампів.

Суттєвим є те, що присутні при такій бесіді професійний перекладач-філолог практично завжди не в стані адекватно передати специфічну термінологію, не кажучи вже про стандартну ситуацію, коли у неформальних обставинах між науковцями виникає дискусія, наприклад, щодо недавно запропонованого підходу до вирішення актуальної проблеми.

Тому необхідно щодо згаданого спеціаліста щоб його рівень володіння іноземною

мовою не обов'язково був занадто високим (ідеальна вимова, класична побудова фрази і. т. і.) але цей рівень принаймні має бути достатнім для того, щоб реагувати на загальний сенс фрази та допомагати перекладачу щодо спеціальної термінології.

Для підготовки з іноземної мови студентів технічних спеціальностей (у згаданому вище, очевидно, обмеженому обсязі) необхідно виходити з обставин в яких вони будуть застосовувати свої знання. Це можна врахувати, якщо мати загальний сценарій, згідно якого студент буде діяти на практиці. Оскільки сценарії на всі випадки не підготувати, то треба виходити з мінімально необхідної за сценарієм лексики. У процесі навчання, якщо буде можливість, мінімальний сценарій можна розвивати, як і після закінчення учбового закладу.

На наш погляд, бажаним є підхід, за якого частина навчального часу присвячена „тренінгу" студентів на рівні фраз за допомогою діалогів. На таких заняттях граматичні правила слід пояснювати лише в межах, що дозволяють зрозуміти модифіковану фразу. Це дозволяє використовувати розмовники, підручники з ділової мови і т.і.

При цьому, очевидно можна гнучко змінювати рівень, тематику та кількість занять, виходячи з наявності часу та спеціалізації студентів.

Зрозуміло, що для такого підходу у студента має бути початкова підготовка з іноземної мови.

Фактично, це є різновидом додаткових практичних занять, хоча за наявності часу, викладати спецкурси було б краще.

Результативність цього підходу, нажаль, залежить від якості підготовки з іноземної мови у середній школі. Але вибору немає, тому доведеться спочатку компенсувати недоліки шкільної освіти, можливо, присвятити цьому весь перший курс. Відповідно, другу іноземну мову слід починати з другого курсу.

Необхідно зауважити, що багато учнів та студентів мають досвід роботи з англомовними операційними системами, тобто мають своєрідний досвід спілкування іноземною мовою на рівні фраз.

В принципі, операційні системи дозволяють переналагодження на інші мови, зокрема німецьку. Це, без сумніву, зацікавить студентів, що можна використати для переходу до вивчення другої іноземної мови.

У загальну систему підготовки кадрів з ІБ входить не тільки освітня первинна підготовка відповідних фахівців у ВНЗ але й додаткова наукова підготовка, основне місце в якій належить підготовці науково-педагогічних кадрів в аспірантурі і докторантурі.

Перелік наукових спеціальностей на здобуття наукових ступенів кандидата і доктора наук, які пов`язані з питаннями інформаційної безпеки, затверджений згідно Наказу ВАК України № 288 від 10.06.1999 року, включає наступні: 01.05.02 - математичне моделювання та обчислювальні методи (науки - фізико-математичні, технічні); 05.13.06 - автоматизовані системи управління та прогресивні інформаційні технології (науки - технічні); 05.13.21 - системи захисту інформації (науки-технічні); 20.01.10 - розвідки та іноземні армії (науки - військові); 20.01.12 - радіоелектронна боротьба, способи та засоби (науки - військові, технічні); 20.02.12 - військова кібернетика, системи управління та зв'язок (науки - військові, технічні); 21.01.01 - основи національної безпеки держави (науки - юридичні, соціологічні, політичні); 21.07.02 - розвідувальна діяльність органів державної безпеки (науки - фізико-математичні, технічні, юридичні, військові) [7].

В ДУІКТ відкрита і працює Спеціалізована Вчена Рада СРД 26.861.02 з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора та кандидата наук за спеціальностями:

05.13.21 – системи захисту інформації (технічні науки);

20.02.12 – військова кібернетика, системи управління та зв'язок (технічні науки).

Важливою ланкою у системі підготовки фахівців з ІБ є підвищення кваліфікації [9].

Програма перепідготовки і підвищення кваліфікації повинна мати практичну направленість та мати чітко оговорену мету і задачі. Керівники і працівники з

інформаційної безпеки навчаються на курсах підвищення кваліфікації, не рідше одного разу на 5 років, а фахівці вперше прийняті на державну службу протягом першого року їхньої роботи, за професійними програмами та отримують свідоцтво при підвищення кваліфікації.

Однією з головних задач навчання, поряд з підвищенням ділової кваліфікації, є формування відповідного відношення до практичної діяльності по забезпеченню інформаційної безпеки, ініціативи і творчого відношення до дорученої справи.

Загальна мета навчання складається з підготовки фахівців інформаційної безпеки, які мають необхідну кваліфікацію, розроблення та здійснення заходів щодо забезпечення ІБ, постійного контролю за її дотриманням.

При плануванні і проведенні підвищення кваліфікації основна увага приділяється вибору форми (курси, семінар) виходячи з їх особливостей, мети підготовки та необхідному об'єму знань та навичок, що необхідно засвоїти :

- 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 в окремих лекціях, що пропонуються слухачам, застосовується проблемний метод. Так, на лекції викладач визначає проблемну ситуацію, розкриває її суттєвість, 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 технічні засоби та наглядні посібники.

З метою забезпечення актуальності передбачених заходів розробники плану повинні:

- постійно переглядати кваліфікаційні вимоги до кандидатів на навчання;
- періодично оновлювати методичну базу та здійснювати оцінку навчального плану;
- підвищувати якість контролю і управління.

Мета навчання, як правило, досягається дотриманням певної сукупності факторів [9]: цільова аудиторія; періодичність проходження курсів підвищення кваліфікації; перевірка засвоєння матеріалу; використання навчальних засобів та електронно-обчислювальних машин (комп'ютерів); високі вимоги до рівня підготовки кандидатів; система звітності окремих слухачів та підсумки проходження курсу;відшукання нових джерел та оновлення навчального матеріалу.

Для забезпечення ефективного виконання завдань навчання у ДУІКТ дотримують складання планів занять за наступною схемою: назва (предмет); тема; задачі навчального підрозділу, довідковий матеріал; введення; тематичний матеріал; особливості методики викладання; навчальні засоби; резюме; перевірка засвоєння матеріалу; закріплення викладеною матеріалу і попередня інформація по наступній темі; домашнє завдання (якщо необхідно); графік роботи.

Викладач слідкує за тим, щоб слухачі користувалися тільки тими навчальними засобами, котрі забезпечують найбільшу ефективність навчального процесу.

Основною метою педагогічного контролю є формуючий вплив на поточний процес навчання з метою покращення за рахунок встановлення зворотного зв'язку між слухачем та викладачем і одержання підсумкового результату навчання. Педагогічний контроль реалізується як при традиційних формах і методах, так і при широкому застосуванні

електронно-обчислювальних машин. Найбільш коректний засіб педагогічних вимірювань - тест, а також найбільш досконалий засіб комплексної оцінки якості підготовки фахівця - тест професійної компетенції, який може використовуватися як для атестації фахівців, так і для добору кадрів на заміщення посад.

Поточний контроль засвоєння матеріалу здійснюється у ході занять шляхом перевірки теоретичних знань і практичних навичок слухачів.

Теоретичний матеріал який видається слухачам має важливе значення в навчальному процесі і при цьому до програми перепідготовки доцільно включити рекомендації відносно складання та застосування таких матеріалів. Ці матеріали В ДУІКТ використовуються з такою метою:

- доповнити інформацію, викладену усно;
- відтворювати діаграми чи малюнки;
- відмітити основні моменти лекції;
- представити інформацію в самій точній формі (конспект лекцій);
- зменшити ведення записів під час занять;
- представити навчальний матеріал в збалансованому вигляді та логічній послідовності;
- забезпечити самостійне вивчення рекомендованого матеріалу;
- бути постійним джерелом інформації для послідуючих посилань і вивчення матеріалу.

Однією з традиційних форм контролю який застосовується в ДУІКТ при визначенні знань є реферат. Теми рефератів визначаються на початку навчання. Слухач може також обрати тему для рефератів, що пов'язана з проблемою, актуальною саме для конкретного органу державної влади, органу місцевого самоуправління підприємства, установи, організації де він працює. До обраної теми реферату у процесі навчання, за умови достатнього їх обґрунтування, можливо внесення уточнень і відповідних змін. Кожен реферат рецензується.

Отже, на наш погляд, підготовка та перепідготовка спеціалістів з інформаційної безпеки в Україні повинна проводитись в рамках єдиного спеціалізованого навчально-методичного центру, що зосереджує в собі провідних вчених та методистів найвищого рівня підготовки, які мають достатній досвід проведення такої навчально-наукової роботи, та спеціалізовану матеріально-технічну базу провідних ВНЗ та НДІ держави. Крім того, потрібно з`ясувати потреби держави та її силових відомств на кількість фахівців з цього напрямку діяльності для більш раціонального розподілу бюджетних коштів, що витрачаються на підготовку та перепідготовку кадрів в галузі забезпечення інформаційної безпеки держави.

Необхідно також згадати щодо системи конференцій та регулярних семінарів. На цих семінарах ведеться активний обмін досвідом, вивченням нових нормативних та керівних документів, підіймаються та обговорюються серйозні проблемні питання. Рішення таких семінарів як правило, допомагає розробляти перспективні плани розвитку систем підготовки фахівців, розробки нормативно-правових документів та інших питань інформаційної безпеки. За останні роки Департаментом СТСЗІ СБУ проведені в міжнародних науково-практичних конференцій "Безпека інформації у інформаційно-телекомунікаційних системах" та інші.

Однак сучасні високі затрати на підвищення кваліфікації призводять до того, що з'являються певні труднощі у наборі слухачів. Якщо ці затрати дещо знизяться та не будуть настільки обтяжливими для підприємств, до підвищення кваліфікації кадрів з ІБ можуть підключатися і вузи, які мають досвід підготовки відповідних фахівців, кваліфікований професорсько-викладацький склад та необхідну матеріальну та навчальну базу. Цей принцип застосовується у ДУІКТ.

Хотілося б звернути увагу і на те, що в системі навчання фахівців із ІБ не знайшла достатнього розвитку така ланка, як перепідготовка кадрів, хоча вона набуває в нинішній

час більшої актуальності, оскільки, з одною боку, дозволяє прискорити рішення кадрової проблеми за рахунок скорочення (у порівнянні з системою підготовки) термінів навчання, а з іншого - вносить внесок у рішення ще однієї проблеми - працевлаштування, у першу чергу, звільнених у запас офіцерів, забезпечуючи їх перепрофілювання. Перепідготовка кадрів може здійснюватися на базі ВУЗів. Вибір конкретного ВУЗу повинен проводиться з урахуванням характеру базової підготовки кожного фахівця.

Список літератури:

1. Закон України „Про державну таємницю".
2. Закон України „Про інформацію"
3. ДСТУ 3396.0-96 Технічний захист інформації. Основні положення.
4. Звіт відомостей, що становлять державну таємницю №52 від 01.03.2001р.
5. Постанова Кабінету Міністрів України від 8.10.1997 р. № 1126 „Концепція технічного захисту інформації в Україні".
6. Материалы VIII Международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах». К.: ДСТС ЗИ, 2005 г.
7. Богданов О.М., Додонов О.Г., Хорошко В.О. та інші. Проблеми становлення національної системи підготовки кадрів в області інформаційної безпеки. / Захист інформації, № 2, 2001 р. – с. 66-71.
8. Бабак В.П., Козловський В.В., Хорошко В.О., Чирков Д.В. Деякі аспекти підготовки фахівців із захисту інформації в Україні // Захист інформації, № 4. 2001. – с.57-69.
9. Гловань С.М. Організація навчального процесу на курсах підвищення кваліфікації з інформаційної безпеки // Захист інформації, № 4, 2002. – с.71-76.
10. Кривуца В.Г., Гніденко М.П. Закономірність природнго розвитку людини в ході сучасного навчального процесу. // Вісник ДУІКТ, 2004, т.2, № 3. – с.176-181.
11. Кривуца В.Г., Козловський В.В., Хорошко В.О., Чирков Д.В. Підготовка фахівців із інформаційної безпеки у ДУІКТ // Матеріали II МНМК „Болонський процес: Трансформація навчального процесу у технологію навчання, К.: ДУІКТ, 2005. – с.160-163

УДК 004.681

В.Г. Кононович
М. Ф. Тардаскін

ОСНОВНІ ПОЛОЖЕННЯ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Вступ

Сфера технічного захисту інформації (ТЗІ) набуває зростаючого значення з прискореним розвитком інформаційно-комунікаційних технологій (ІКТ). При цьому, задачі ТЗІ переростають у задачі захисту інформаційних ресурсів, що тепер називають інформаційною безпекою ІКТ [1]. Під інформаційним ресурсом розуміють сукупність інформації та засобів, в яких і за допомогою яких вона обробляється та циркулює, а також причетний персонал.

Система ТЗІ побудована у відповідності до Законів України «Про інформацію» (1994), «Про державну таємницю» (у редакції 1999), «Про захист інформації в автоматизованих системах» (1994), а також Концепції технічного захисту інформації в Україні (1997). В галузі зв'язку розроблена відповідна галузева концепція ТЗІ [2]. Нормативно-правовою та методично-правовою базою стали НД ТЗІ на програмно-керованих АТС, НД ТЗІ в комп'ютерних (автоматизованих) системах від несанкціонованого доступу, які гармонізовані з міжнародними стандартами [3], нормативно-методичні документи захисту інформації від