УДК 638.253.2

Хорошко В.О., Орєхова І.І.
(ДУИКТ)

Задачі і проблеми підвищення кваліфікації постійного складу вищих навчальних закладів з інформаційної безпеки

Вступ

Проблеми інформаційної безпеки в Україні в останні роки набули характеру актуальних, а в своєму розвитку все виразніше переростають з традиційного захисту інформації в системах її обробки в забезпечення комплексної безпеки об'єктів (підприємств, установ, організацій).

Враховуючи зазначені обставини в Україні була організована великомасштабна науково-дослідницька робота з інформаційної безпеки, в організації якої брала участь значна кількість вузів, серед яких був і Державний університет інформаційно-комунікаційних технологій.

Один із висновків, який був сформульований на основі проведених досліджень, полягає в тому, що проблеми, які розглядаються, є настільки складними, багатогранними і специфічними, що ефективно їх вирішити можуть тільки професійні спеціалісти досить високого рівня підготовки. У зв'язку з цим виникає задача підготовки таких спеціалістів. Оскільки кількість об'єктів, на яких має здійснюватися захист інформації, є досить великою, то підготовка відповідних спеціалістів має бути достатньо масовою. Відповідно, система підготовки спеціалістів даного профілю, що склалася до теперішнього часу, справлятися з даною задачею не може, назріла необхідність її розвитку та вдосконалення.

Насправді, в даний час в системі вищої школи підготовка професійних спеціалістів з інформаційної безпеки ведеться в 32 вузах [1]. Хоча необхідно відзначити, що більшість з них не володіє ані кадровим складом викладачів, ні учбово-лабораторною базою для вирішення цих задач.

Вже зараз є абсолютно очевидним, що система підготовки спеціалістів, яка склалася в даний час, не відповідає сучасним, а тим більше перспективним потребам як за кількістю спеціалістів, що випускаються, так і за спектром необхідних спеціальностей [2]. Майже всі вузи випускають спеціалістів технічних засобів захисту інформації, окрім цього існує проблема, яка полягає в тому, що підготовка спеціалістів, технологів, розробників та конструкторів таких засобів відсутня. Порівняно мало спеціалістів випускається з управління інформаційною безпекою, спеціалістів з програмних та криптографічних методів захисту, математиків, системних програмістів і програмістів-прикладників для систем захисту. Окрім цього, існують суттєві недоліки і в якості їх підготовки. Стає все більш очевидною необхідність суттєвого розширення масштабів підготовки спеціалістів із захисту інформації і серйозного вдосконалення учбових планів та навчальних процесів.

Основна частина

Роль вузів у вирішенні проблем, що розглядаються, велика і багатоаспектна. По-перше, вузи практично монопольно мають вирішити задачу підготовки молодих спеціалістів з інформаційної безпеки згідно з усім переліком необхідних спеціальностей. По-друге, вузи мають зробити вирішальний внесок в організацію і науково-методичне забезпечення функціонування системи підвищення кваліфікації спеціалістів з інформаційної безпеки та перепідготовки спеціалістів другого профілю. По-третє, вузи мають організовувати і забезпечувати підготовку висококваліфікованих науково-педагогічних кадрів у сфері інформаційної безпеки. По-четверте, вузи мають зробити суттєвий (якщо не вирішальний) внесок в наукові дослідження і розробку проблем

інформаційної безпеки. І нарешті, по-п'яте, вузи мають вирішити всю сукупність питань забезпечення власної безпеки, що пов'язано з вирішенням низки специфічних задач, в тому числі і задачі підготовки та підвищення кваліфікації спеціалістів підрозділів безпеки.

Відмінна особливість вузу як об'єкту захисту визначається його статусом, змістом і умовами діяльності. Основні особливості можуть бути визначені та охарактеризовані наступним чином.

Передусім сучасний вищий навчальний заклад – це організація масового доступу з неперервним та інтенсивним рухом людських потоків. Ця обставина створює значні труднощі в регулюванні та контролі доступу і переміщення людей. При цьому переважною більшістю людського контингенту є молодь – передусім студенти, тобто люди, які ще не мають достатнього життєвого загартування, свідомо та легко піддаються зовнішнім впливам, і в даний час ще й несуть в собі сліди сучасного масового впливу на молодь.

Мають місце суттєві особливості в структурі та змісті інформаційних потоків, які циркулюють в процесі функціонування вузу, а також в змісті їх обробки. По-перше, вхідні та вихідні потоки, як правило, великі за об'ємом, складні за структурою (в них регулярно передається як звичайна організаційно-розподільча, так і науково-методична та інша інформація), різноманітні за способом передачі (телефон, як звичайний, так і мобільний, електронна пошта, Internet), при чому ці потоки циркулюють достатньо інтенсивно. Своєрідність внутрішніх потоків полягає в тому, що в них окрім звичайної інформативно-розпорядчої інформації істотну долю складає рух учбової літератури і спеціальних зошитів (блокнотів), необхідних для забезпечення вивчення спеціальних дисциплін.

Для технології обробки інформації в вищих навчальних закладах характерні ті ж особливості, що і для більшості підприємств, установ і організацій, а саме: дедалі більш тісне зрощення традиційних (паперових) і автоматизованих (непаперових) технологій, масове використання ПЕОМ, ноутбуків, смартфонів, їх об'єднання в локальні та глобальні (Internet) мережі, доступ до ресурсів ЕОМ широкого кола користувачів. В вузах вищезазначені особливості проявляються особливо рельєфно, тобто ПЕОМ використовуються не тільки в повсякденній діяльності підрозділів і окремих посадових осіб, але і в навчальному процесі, при чому особливо інтенсивно. З цією метою кафедри та лабораторії оснащуються великою кількістю сучасних ПЕОМ, які широко використовуються як викладачами і співробітниками кафедр та лабораторій, так і студентами.

Досить своєрідна особливість вузу, яка має принципове значення, полягає у високій вірогідності раптової (незапланованої) появи так званої пріоритетної інформації. При цьому під пріоритетною розуміють таку інформацію, яка з'являється в процесі виконання НД ДКР і яка може являти собою державну, промислову і комерційну науку або просто ноу-хау. Висока вірогідність появи пріоритетної інформації обумовлюється тим, що вузи беруть безпосередню участь у виконанні НДДКР, залучаючи при цьому студентів, в тому числі і з оборонної тематики, а науковий потенціал багатьох вузів дуже високий.

Вже навіть за даними такого неглибокого аналізу особливостей сучасного вузу з точки зору забезпечення інформаційної безпеки достатньо переконливим є висновок про те, що забезпечення безпеки вузу пов'язане з вирішенням великої кількості різнопланових задач.

Їх перелік і зміст в загальному вигляді може бути сформульований і представлений наступним чином:

- загальна організація і забезпечення дотримання правил внутрішнього розпорядку;
- контроль доступу і переміщення людей;
- загальна організація та забезпечення безпечного документообігу;
- організація і забезпечення обігу документів, які містять конфіденційну інформацію;
- організація і забезпечення контролю за використанням засобів обчислювальної техніки і захисту інформації в процесі її автоматизованої обробки;

- організація контролю за перебігом виконання НДДКР з метою своєчасного визначення появи пріоритетної інформації та включення її в перелік, який підлягає спеціальному захисту.

Спадає на думку той факт, що з урахуванням розглянутих вище особливостей вузу зазначені задачі ефективно можуть бути вирішені лише при цілеспрямованій і взаємоузгодженій роботі широкого кола керівників, спеціалістів та користувачів інформаційних ресурсів електронно-обчислювальної техніки. Все коло осіб, які беруть участь в цій діяльності, особливо у вузах, де проходить підготовка спеціалістів з інформаційної безпеки, можна категорувати наступним чином:

1) ректор вузу і його проректори з різних напрямів діяльності (окрім проректора з безпеки, якщо він є);
2) проректор з безпеки;
3) керівники та відповідальні робітники забезпечувальних підрозділів і управління вузу;
4) директори інститутів, декани факультетів, завідувачі кафедрами і лабораторіями вузів;
5) професорсько-викладацький склад та інші співробітники кафедр і лабораторій;
6) керівники і спеціалісти підрозділів і служб безпеки вузів;
7) студенти, аспіранти, докторанти;
8) слухачі різних форм перепідготовки і підвищення кваліфікації.

Абсолютно очевидним є те, що робітники всіх перерахованих категорій можуть виконувати свої функції з безпеки лише в тому випадку, якщо вони будуть володіти необхідними для цього знаннями та навичками, чим передбачається необхідність відповідної системи навчання.

Форми навчання можуть бути різними, як наприклад:

- інструктаж з правил безпеки з підпискою про взяття зобов'язань щодо їх дотримання;
- короткострокові (одно-, двух-, триденні) семінари науково-технічного або інформаційно-інструктивного характеру;
- курси підвищення кваліфікації або перепідготовки спеціалістів;
- регулярні планові заняття в межах учбового плану.

Так наприклад, для підготовки студентів з питань безпеки в Навчально-науковому інституті захисту інформації Державного університету інформаційно-комунікаційних технологій використовуються перша і четверта форми навчання.

Так, перед допуском до роботи на ПЕОМ кожний студент вивчає інструкцію з правил безпеки і після співбесіди з інструктором (викладачем, що проводить заняття) дає підписку щодо їх дотримання. Що стосується четвертої форми навчання, то в учбових планах з напрямку 1701 «Інформаційна безпека», передбачено як вивчення теоретичних основ захисту інформації, так і вивчення найбільш розповсюджених методів і засобів захисту. Досвід викладання підтвердив високу ефективність такого вирішення проблеми: студенти виявляють до неї підвищений інтерес, а отримані знання і навики є необхідними не тільки в процесі навчання, але й в майбутній роботі за спеціальністю.

Керівники і спеціалісти підрозділів вузу, а також кафедр і лабораторій можуть в даний час бути охоплені лише інструктажем з підпискою, що при неформальному підході повністю відповідає реальним потребам сьогодення.

Основна увага приділяється професійній підготовці керівників і спеціалістів підрозділів безпеки. Кожний співробітник, що приймається на роботу, проходить підготовку в повному обсязі тих функцій, які потім на нього буде покладено. В даний час така підготовка здійснюється індивідуально і безпосередньо на робочому місці. Однак враховуючи достатньо велику кількість спеціалістів цієї категорії в масштабах Міністерства освіти і науки України і підвищеній значущості задач, які ними вирішуються, виявляється

досить необхідним і доречним проходження ними перепідготовки і підвищення кваліфікації на курсах при одному з вузів країни.

Самостійного розгляду заслуговують питання підготовки у сфері безпеки керівників вузів: ректорів, професорів з видів діяльності і особливо професорів з безпеки.

Передусім відзначимо, що до недавнішнього часу питання підготовки керівного складу вузів (як проректорів з безпеки) навіть не розглядались, а їх участь у вирішенні відповідних питань мала лише номінальний характер. Але в сучасних умовах з огляду на вищезазначені особливості вузу як об'єкту захисту і законодавчу установку на персональну відповідальність перших керівників за безпеку (принаймні, на рівні державної таємниці) їх участь має бути не номінальною, а змістовною, для чого їм, відповідно, необхідний деякий мінімум знань. Зміст цього мінімуму, очевидно має бути наступним: сучасна постановка завдання забезпечення безпеки вузу; теоретичні і практичні передумови забезпечення безпеки; законодавчі акти і сфери безпеки; особливості організації робіт з інформаційної безпеки вузу. Самостійним розділом знань (особливо для ректорів і проректорів з науки) мають стати способи і методи прогнозування і виявлення пріоритетної інформації з метою своєчасного включення її в коло об'єктів, які підлягають спеціальному захисту.

Самостійної і підвищеної уваги заслуговують питання підвищення кваліфікації проректорів з безпеки. Немає необхідності доводити, що проректор з безпеки – центральна фігура, від ефективності його діяльності рішучою мірою залежить ефективність забезпечення безпеки вузу. Абсолютно очевидним є те, що для досягнення такої гармонії проректор з безпеки має володіти широким кругозором з усіх питань безпеки, знаннями теоретичних і практичних основ безпеки, володіти способами і методами створення як сучасних систем забезпечення безпеки, так і атаки, організації і забезпечення функціонування цих систем.

Висновки

Таким чином, з наведеного аналізу виходить, що в системі підвищення кваліфікації керівного складу вузу доцільно передбачити три різні групи: ректори, проректори (крім проректора з безпеки) і проректори з безпеки. Що стосується такої категорії як директори інститутів і декани факультетів, то за необхідністю їх можна включити до проректорської групи.

Однак для вузів, де здійснюється підготовка спеціалістів з інформаційної безпеки, підготовку деканів і директорів інститутів необхідно проводити окремо.

Найбільш доцільною формою підвищення кваліфікації керівного складу є семінари: одноденні для ректорів, дводенні для проректорів (8 годин) і триденні – для проректорів з безпеки (12 годин). Для директорів інститутів, деканів, завідуючих кафедрами і лабораторіями – 24-годинні курси. Для всіх інших співробітників вузів від 36- до 72-годинних занять в залежності від необхідності.

Література

1. Махоніна О. Підготовка фахівців у сфері інформаційної безпеки /Махоніна О.// Бизнес и безопасность, №3, 2011.-с.88-100.

2. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Затверджено Наказом президента України №717/2011 від 30.06.2011р.

3. Лєнков С.В. Концептуальні і методологічні підходи до підготовки спеціалістів з інформаційної безпеки в Україні /Лєнков С.В., Орєхова І.І., Хорошко В.О.// Зб. наук. праць ВІКНУ ім. Т.Шевченка, вип. №33, 2011-с.

Рецензент:Лєнков С.В.
Надійшла 27.05.2011