

Учебные планы специализаций «ЗАС» и «ПС» по содержанию близки друг к другу и отличаются блоками технических и специальных дисциплин направления «Телекоммуникации». Базовая подготовка для этих специализаций по защите информации (криптографическая защита в телекоммуникационных системах) существенно дополняется дисциплинами по технической и организационно-правовой защите информации.

В связи с тем, что криптографические методы являются стержневыми при защите информации и атаках на нее, в настоящее время проводится большая работа по совершенствованию содержания дисциплин учебных планов специализаций ОТЗИ и КрОСИС. Не рассматривая блока специальных дисциплин учебного плана по этим специализациям, отметим, что основой подготовки специалиста по криптографии является прежде всего математическая подготовка в областях непрерывной, и в особенности дискретной математики.

Специализация «ОТЗИ» требует углубленных знаний по защите информации для современных и перспективных информационных технологий. Учебный план по специализации «ОТЗИ» включает дисциплины по криптографическим, программно-аппаратным, техническим и организационно-правовым методам защиты. Базой для этой подготовки являются дисциплины по математике, информатике, вычислительной технике, информационно-телекоммуникационным системам и сетям.

С 2000 года в институте планируется поставить подготовку специалистов еще по нескольким направлениям.

С середины 90-х годов в подготовке специалистов по информационной безопасности стали подключаться и гражданские ВУЗы г.г. Киева (НТУУ КПИ, КМУГА), Одессы (Академия связи), Харькова (ХГГУРЭ), Днепропетровска (Горная Академия), Николаева (УГМТУ).

Координация работы ВУЗов по подготовке кадров по защите информации возложена на Департамент специальных телекоммуникационных систем и ТЗИ СБ Украины.

В настоящее время в рамках Координационного Совета при ДСТС и ТЗИ ведется работа по интеграции гражданских и военных ВУЗов и учреждений других ведомств в этом важнейшем для национальной безопасности Украины направлении.

УДК 621.396

ОСОБЛИВОСТІ СИСТЕМИ ПІДГОТОВКИ СПЕЦІАЛІСТІВ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Олександр Архипов, Євген Мачуський, Олексій Новіков
Національний технічний університет України "КПІ"

Анотація: Розглянуто деякі питання, що стосуються процесу розбудови системи освітньої підготовки фахівців у галузі інформаційної безпеки.

Summary: Some problems are considered which concern development of a system of education for preparation of the experts in the field of information safety.

Ключові слова: інформаційна безпека, система освіти, методичне забезпечення.

Визначними рисами сучасного етапу розвитку суспільства є глобальна інформатизація і інтенсивне впровадження в усі сфери діяльності новітніх інформаційних технологій, створення автоматизованих систем обробки даних, локальних і розподілених обчислювальних мереж, систем електронної пошти, інтеграція відомчих мереж та їх під'єднання через телекомунікаційні канали до міжнародних корпоративних та глобальних мереж.

Все це з одного боку сприяє прогресу суспільства, держави та особистості, а з другого – створює виняткові передумови для небажаного витоку інформації або порушення її цілісності. Інтенсивний розвиток технічних інфраструктур, зокрема засобів інформаційного обліку, телекомунікацій, комутаційного обладнання та обчислювальної техніки приводить до того, що несанкціоноване отримання інформації може здійснюватися без часових і територіальних обмежень.

Слід додати, що одним із наслідків науково-технологічного прогресу останніх років стало створення надзвичайно ефективних технічних засобів та систем розвідки і промислового шпигунства.

Розвиток інформаційних технологій та апаратно-програмних комплексів перетворення інформації призвів до появи безпрецедентних за масштабом та глобальних за географією проявів загрози безпеці інформації. Втрата або небажане поширення інформації, що становить державну, підприємницьку або особисту таємницю – це одна з основних загроз сьогодення. Запобігти цій загрозі можна шляхом розробки та послідовної реалізації цілеспрямованої політики у цій сфері, причому ефективною та дієвою ця політика буде лише в тому разі, якщо спиратиметься на виважену та обґрунтовану методологічну базу.

Правову основу захисту в Україні становлять Конституція України, Концепція (основи державної політики) національної безпеки України, Закони України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про науково-технічну інформацію", інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

Системний підхід до захисту інформації у загальнодержавному масштабі та сформульовані на його основі головні принципи і напрями державної політики у сфері захисту інформації викладено у Концепції технічного захисту інформації в Україні. У розробленому на її базі Положенні про технічний захист інформації в Україні визначені правові та організаційні засади захисту інформації, охорона якої забезпечується державою відповідно до чинного законодавства. Окреслені у цих програмних документах головні проблеми захисту інформації, шляхи та заходи їх вирішення потребують справжнього професіоналізму кадрів, що в свою чергу передбачає існування системи регулярної підготовки спеціалістів. До останнього часу в Україні такої системи практично не було. Через відсутність чіткої державної стратегії системи підготовки спеціалістів в галузі інформаційної безпеки, в умовах реально виниклого попиту на певних фахівців цієї галузі мав місце процес стихійного утворення лише окремих елементів системи підготовки, не завжди взаємопогоджених, а інколи й суперечливих за своєю ідеологією і змістом.

Тому одним із першочергових завдань у створенні та підтримці національної системи інформаційної безпеки є гарантоване й надійне забезпечення її висококласними спеціалістами, що може бути забезпечено лише через побудову державної системи підготовки фахівців з інформаційної безпеки. При формуванні цієї системи мають бути враховані такі особливості:

- інформаційна безпека – специфічна предметна галузь, підготовка спеціаліста для якої передбачає необхідність викладання специфічних розділів фундаментальних та загальноінженерних дисциплін на міждисциплінарній основі: спеціальні розділи математики, електроніка, акустика, оптика, кібернетика та інші;
- система освіти в галузі інформаційної безпеки повинна забезпечувати відповідність рівня підготовки спеціалістів рівню наукових знань, що у реальному масштабі часу (без запізнення на декілька років) реалізується через центри регулярної перепідготовки та підвищення кваліфікації, а також шляхом підготовки висококваліфікованих науково-педагогічних кадрів у магістратурі, аспірантурі, докторантурі;
- загальну підготовку з питань інформаційної безпеки повинні мати усі спеціалісти та користувачі, що беруть участь у процесах, пов'язаних з обробкою та обміном інформацією, керівники підприємств, установ, організацій;
- підготовка спеціалістів з інформаційної безпеки усіх категорій має будуватися на єдиній науково-методичній та правовій основі, чому сприятиме створення централізованої системи навчально-методичного забезпечення (фахова рада з напрямку "Інформаційна безпека", навчально-методичні комісії), що працюватиме у тісній взаємодії з провідними кафедрами, координуючи спільну розробку перспективних планів розвитку освітньої галузі, розробку державних освітніх стандартів, навчальних планів, підготовки та видання підручників та навчальних посібників, підготовку науково-педагогічних кадрів і т. і.

Загроза пошкодження або небажаного витоку інформації виникає у місцях її утворення (давачі даних), у місцях прямого та зворотного перетворення (кодувально-декодувальні, модуляторно-демодуляторні системи), у лініях передавання (канали телекомунікацій), у засобах та системах оброблення (комп'ютерно-процесорні системи) та за місцем використання інформації (відтворювальні системи).

Заходи щодо захисту інформації можна класифікувати за трьома основними напрямками:

- фізико-технічні;
- логіко-математичні;
- організаційно-правові.

Наведений перелік напрямів вказує на те, що підготовка фахівців в галузі інформаційної безпеки має ґрунтуватися на поглибленому засвоєнні широкого кола дисциплін, виділення серед яких профільних за напрямками приводить до утворення кількох груп дисциплін, відчутно відмінних за своїм складом та спрямуванням.

Так у двох перших напрямках провідна роль належить математиці, фізиці, хімії, електроніці, радіофізиці, інформатиці, інформаційно-вимірювальній, комп'ютерній та телекомунікаційній техніці. Рівень знань спеціалістів у цих галузях повинен бути випереджальним відносно промислово-технічних реалізацій відповідних пристроїв чи технологій, бо найкращий засіб захисту інформації – профілактика витоку або пошкодження інформації ще на етапі проектування.

Організаційно-правові заходи захисту інформації потребують поглибленого вивчення психології, соціології, основ менеджменту, правознавства, високої загальної гуманітарної підготовки. Доцільно було б встановити таку фахову структуру в галузі інформаційної безпеки:

1. спеціальність "Фізико-технічні засоби захисту інформації" зі спеціалізаціями:
 - захист інформації в інформаційно-вимірювальних системах;
 - захист інформації в телекомунікаційних системах та мережах.

2. спеціальність "Математичні методи захисту інформації" зі спеціалізаціями:
 - системний аналіз інформаційної безпеки;
 - інформаційна безпека комп'ютерних систем.
3. спеціальність "Організація захисту інформації" зі спеціалізаціями:
 - захист інформації від несанкціонованого доступу;
 - адміністративний менеджмент в галузі інформаційної безпеки.

Пропонуємо не нарощувати кількість спеціальностей та спеціалізацій за напрямом "Інформаційна безпека", а основні зусилля спрямувати на розроблення навчальних планів, які повинні мати глибоко фундаментальний та системний характер, бути випереджальними щодо промислово-технологічного та загальнокультурного рівня суспільства.

Враховуючи специфіку вказаних профільних спеціальностей, бажано було б створити три окремі бакалаврати за напрямом «Інформаційна безпека».

УДК 654.924 (075)

ОПЫТ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАННОЙ СИГНАЛИЗАЦИИ

Владимир Волхонский

Санкт-Петербургский Государственный университет аэрокосмического приборостроения

Аннотация: Анализируются опыт организации подготовки и повышения квалификации специалистов в области средств охранной сигнализации в государственных институтах и частных учебных заведениях России и стран СНГ и вопросы подготовки учебной литературы.

Summary: Analysis of training and upgrading experience with alarm security systems in state institutes and private training centres in Russia and CIS states and preparing of training literature.

Ключевые слова: Обучение, квалификации, охранная сигнализация, литература.

Системы охранной сигнализации (СОС) являются одним из основных элементов практически любой системы безопасности, в том числе, и решающей комплекс задач по защите информации. Эффективность разработки, производства такой аппаратуры, проектирование и эксплуатация СОС невозможна без успешного решения задачи подготовки высококвалифицированных кадров, а также переподготовки и повышения квалификации действующих специалистов. Поэтому представляет интерес рассмотреть опыт решения подобной задачи с участием автора в ряде государственных и негосударственных учебных заведений России и стран СНГ.

В начале 90-х годов на кафедре физических и теоретических основ радиоэлектроники Санкт-Петербургского Государственного университета аэрокосмического приборостроения СПбГУАП (бывший Ленинградский институт авиационного приборостроения) было принято решение об организации новой специализации «Технические средства охранной сигнализации» в рамках специальности «Радиотехника». Ясно, что это было новое направление обучения студентов в рамках государственной системы образования в гражданских вузах. В частности, автор читал курс «Теория и техника систем охранной сигнализации». Параллельно шло создание частного негосударственного образовательного учреждения «Курсы Технических Средств Охраны». Несколько позже был создан Учебный центр C&K Systems — одной из крупнейших американских компаний разработчиков и производителей устройств охранной сигнализации.

Как при чтении курса, так и при создании учреждения возник ряд проблем, из которых можно выделить две основные, потребовавшие наибольших усилий и затрат. Во-первых, это организация современной лабораторной базы. И, во-вторых, подготовка учебно-методической и справочной литературы по новой специальности. Связано это было в известной мере с тем, что в гражданских вузах подготовка специалистов по такой специальности ранее не проводилась. Остановимся главным образом на второй проблеме: подготовки учебно-методической и справочной литературы. На начало организации обучения выяснилось, что в открытой печати не было издано практически ничего по этой тематике. Доступны были лишь частично технические описания аппаратуры советского производства и инструкции по установке импортного оборудования на английском языке. Уровень имевшихся переводов в фирмах-продавцах был, как правило, крайне низок.

Используя основные принципы подготовки учебных материалов – учет контингента обучаемых (уровня их базовой подготовки) и основной, конечной задачи обучения — можно выделить следующие направления обучения, имевшие место:

- общетеоретическая подготовка студентов дневной и заочной формы обучения;