высшем техническом училище МВД РК, Ташкентском высшем пожарно-техническом училище МВД РУз, Негосударственном образовательном учреждении Курсы Технических Средств Охраны и в ряде других.

Рассматриваемая проблема обучения специалистов в области технических средств охраны и подготовки учебно-методической литературы для этого достаточно сложна и многогранна. В работе была предпринята попытка рассмотреть лишь часть из особенностей ее решения. Ясно, что в различных учебных заведениях, различных странах будут иметь место свои особенности. Однако, учитывая значительный и вполне обоснованный интерес к литературе подобного профиля, автор поделился своими соображениями. Для заинтересованных лиц и организаций могут быть предоставлены образцы такой литературы.

Литература: 1. Волхонский В.В. Устройства охранной сигнализации: - СПб.: Экополис и культура, 1999. – 272 с. 2. Волхонский В.В., Жежерин А.Р., Нефедов В.Г. Централизованные системы охранной сигнализации: Учебное пособие. - СПб.: ГААП, 1995. – 123 с.

УДК 621.396

ПРАКТИКА КУРСОВИХ ФОРМ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ СПЕЦІАЛІСТІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Олександр Архипов
Національно-технічний університет України "КПІ"

Анотація: **Розглянуто досвід курсової форми навчання у системі підвищення кваліфікації фахівців з інформаційної безпеки, зокрема питання методичного забезпечення навчального процесу.**
Summary: **the experience of the course form of tutoring in a system of improvement of professional skill of the experts on information safety, in particular of problem of methodical security of educational process is considered.**
Ключові слова: **інформаційна безпека, підвищення кваліфікації, методичне забезпечення.**

До середини 90-х років освітніми закладами України підготовка фахівців у сфері інформаційної безпеки практично не проводилась, що спричинило утворення кадрового дефіциту спеціалістів у цій галузі. Для оперативного виправлення стану справ із кадровим забезпеченням розпочалося формування системи короткотермінової освіти, що повинна була шляхом підвищення кваліфікації та перепідготовки забезпечити існуючий попит на висококваліфікованих фахівців у галузі інформаційної безпеки. Одним з перших закладів такої системи став створений за ініціативою Держкомсекретів України у 1994 році на базі НТУУ "КПІ" науково-навчально-методичний центр підвищення кваліфікації фахівців з питань захисту секретної інформації та технічного захисту інформації (ТЗІ), пізніше – Спеціальні курси післядипломної освіти в галузі захисту інформації з обмеженим доступом (Курси).

З ліквідацією Держкомсекретів України подальша робота Курсів здійснювалася при безпосередній підтримці їх з боку Служби безпеки України (СБУ), зокрема Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ. Було значно розширено сферу діяльності та функції Курсів: введено нові навчальні напрями, змінено форми та методи організаційної роботи з інформування щодо набору слухачів, формування навчальних груп тощо. За цих обставин Курси реорганізовано у Навчальний центр перепідготовки та підвищення кваліфікації в галузі інформаційної безпеки (Центр), який введено як структурний підрозділ до складу фізико-технічного інституту (ФТІ) НТУУ "КПІ".

Впродовж шести років діяльності Центру кількість його випускників сягнула 640 осіб, певні позитивні результати отримані в навчально-методичному та кадровому забезпеченні навчального процесу. Насамперед сформовано стабільне ядро викладацького колективу Центру, до складу якого входять 2 доктори наук, 8 кандидатів наук, ряд провідних фахівців, які є співробітниками Департаменту спеціалізованих телекомунікаційних систем та захисту інформації СБУ, провідних установ та профільних інститутів України.

Суттєво позитивним фактором у роботі Центру є його тісний взаємозв'язок з факультетом інформаційної безпеки Фізико-технічного інституту НТУУ "КПІ", зокрема з базовою за напрямом 1601. кафедрою інформаційної безпеки, інтелектуальний, науковий та матеріально-технічний потенціал котрих сприяють загальному поліпшенню стану навчального процесу у Центрі.

Освітня діяльність Центру здійснюється за чотирма спеціальностями та однією спеціалізацією:

1.0. Основи технічного захисту інформації.

2.1. Організація захисту інформації в комп'ютерних системах.

2.2. Організація захисту мовної інформації та інформації у телекомунікаційних системах і системах зв'язку.

3.0.Організація захисту секретної інформації (Спеціалізація 3.0.1. Комп'ютерні технології у діловодстві та документаційному забезпеченні роботи режимно-секретних підрозділів).

Тривалість занять навчальних груп за кожною із спеціальностей становить 2 тижні, форма занять очна. Навчання проводяться за 72-годинними програмами, розробленими фахівцями НТУУ "КПІ" та СБУ й затвердженими обома сторонами. При розробці програми головна увага приділялась питанням практичної діяльності фахівців з відповідних спеціальностей. Три перші спеціальності з наведеного вище переліку належать до напряму "Технічний захист інформації". Для них у таблиці 1 наведено головні тематичні розділи навчального плану, із змісту яких випливає загальноосвітня спрямованість першої спеціальності "Основи ТЗІ". Навчання слухачів за двома іншими спеціальностями має на меті забезпечити більш змістовне та цілеспрямоване підвищення кваліфікації спеціалістів ТЗІ з відповідних вузьких диференційованих фахових напрямів. Однак ці обидві спеціальності мають однакову загальну частину обсягом 22 години (приблизно 30% від повного обсягу програми), що у стислому вигляді містить головні відомості загальноосвітнього курсу, тобто і за цими двома спеціальностями слухачі повинні отримати певний кваліфікаційний рівень обов'язкових знань.

Таблиця 1

№	Напрям	Головні тематичні розділи навчального плану	Приміт-ка
1	Основи технічного захисту інформації	Загрози безпеці інформації. Сучасний стан законодавчого та нормативно-правового забезпечення захисту інформації. Основні відомості про захист інформації в комп'ютерних системах та системах зв'язку. Основні відомості про технічний захист мовної інформації та інформації, що обробляється технічними засобами. Організація будівельно-монтажних, науково-дослідних, дослідно-конструкторських, дослідно-технологічних робіт та промислового виробництва з урахуванням вимог технічного захисту інформації. Основи криптографічного захисту інформації.	Загально-освітній курс
2	Організація захисту інформації на об'єктах інформаційної діяльності та в інформаційних системах	Загрози безпеці інформації. Сучасний стан законодавчого та нормативно-правового забезпечення захисту інформації. Основні відомості про захист інформації в комп'ютерних системах та системах зв'язку. Норми і вимоги з технічного захисту інформації. Атестація об'єктів інформаційної діяльності. Основні відомості про захист мовної інформації та інформації, що обробляється технічними засобами. Норми і вимоги з технічного захисту інформації. Організація будівельно-монтажних, науково-дослідних, дослідно-конструкторських, дослідно-технологічних робіт та промислового виробництва з урахуванням вимог технічного захисту інформації. Основи криптографічного захисту інформації. Вимоги до засобів забезпечення технічного захисту інформації, порядок розроблення, виготовлення та сертифікації. Контроль за ефективністю технічного захисту інформації.	Загальна частина спеціалізованого курсу
2.1	Організація захисту інформації в комп'ютерних системах	Загрози інформації у КС. Методологія захисту КС. Політика безпеки КС, моделі та механізми захисту. Критерії та оцінки захищеності КС, методика оцінювання захищеності КС. Криптографічні засоби захисту інформації, орієнтовані на застосування ЕОМ. Шифри з відкритими ключами, розподіл ключів, криптографічні протоколи. Автентифікація інформації, цифровий підпис.	Фахова частина спеціалізованого курсу
2.2	Організація захисту мовної інформації та інформації у телекомуніка-ційних мере-жах і системах зв'язку	Основні канали витоку мовної інформації та інформації, що обробляється методи та засоби її захисту. Закриття мовних сигналів у телефонних каналах, цифрові системи закриття мовних сигналів в каналах зв'язку. Криптографічні методи захисту інформації в каналах зв'язку. Сучасні телекомунікаційні мережі та системи зв'язку і інформація, що передається ними, загрози інформації, заходи та засоби її захисту. Міжнародні та національні стандарти в галузі взаємодії відкритих систем і систем передачі інформації	Фахова частина спеціалізованого курсу

Більш детальне уявлення про зміст програм із спеціальностей ТЗІ дає наведений у таблиці 2 перелік тем та розподіл між ними погодинного навантаження за спеціальністю 2.2. Організація захисту мовної інформації та інформації у телекомунікаційних системах і системах зв'язку.

Таблиця 2

№ теми	Назва теми	Кіль-кість годин
1.	***Загальна частина***	
1.1	Інформація, її властивості та форми, історія розвитку проблеми захисту інформації	2
1.2	Законодавчі та нормативно-правові засади захисту інформації.	2
1.3	Технічний захист інформації (ТЗІ). Головні поняття, визначення та завдання, стратегія та мета ТЗІ.	2
1.4	Технічні канали витоку інформації. Засоби технічної розвідки.	2
1.5	Організаційне, нормативно-правове та апаратне забезпечення ліцензованих робіт у галузі ТЗІ. Атестація об'єктів інформаційної діяльності, оцінювання захищеності інформації на об'єктах інформаційної діяльності.	2
1.6	Основні відомості про захист інформації в комп'ютерних системах. Програмно-апаратні засоби захисту.	2
1.7	Організація будівельно-монтажних, науково-дослідних, дослідно-конструкторських, дослідно-технологічних робіт та промислового виробництва з урахуванням вимог ТЗІ.	2
1.8	Основи криптографічного захисту інформації.	6
1.8.1	Механізми шифрування. Симетричні криптосистеми.	2
1.8.2	Асиметричні криптосистеми.	4
1.9	Комп'ютерна технологія керування інформаційною безпекою корпоративної структури.	2
	Разом	**22**
2.	***Фахова частина***	
2.1	Захист мовної інформації та інформації, що обробляється технічними засобами.	24
2.1.1	Мовна інформація як об'єкт технічної розвідки. Загальна характеристика портативних та мікромініатюрних засобів акустичної розвідки.	2
2.1.2	Основні канали витоку мовної інформації.	2
2.1.3	Методи та засоби захисту мовної інформації в приміщеннях. Активні засоби боротьби з закладними пристроями.	2
2.1.4	Захист телефонних мереж та мереж радіомовлення від витоку мовної інформації в пасивному режимі їх роботи. Методи захисту від витоку мовної інформації через засоби оргтехніки.	3
2.1.5	Методи захисту мовних сигналів в телефонних каналах. Аналогові скремблери. Принципи побудови. Тактичний та стратегічний рівні захисту.	3
2.1.6	Цифрові системи захисту мовної інформації при передачах в системах зв'язку. Дискретизація мовних сигналів з наступним їх шифруванням.	4
2.1.7	Широкосмугові та вузькосмугові вокодерні системи з цифровим захистом мови. Принципи їх побудови, надійність захисту та якість передачі мовної інформації.	4
2.1.8	Методи та засоби забезпечення безпеки в системах циркуляції мовної інформації. Огляд апаратури засекречування мовної інформації.	2
2.1.9	Тенденції розвитку систем захисту мовної інформації.	2
2.2	Організація технічного захисту інформації в телекомунікаційних мережах і системах зв'язку.	16
2.2.1	Сучасні телекомунікаційні мережі, системи зв'язку та інформація, що передається ними	2
2.2.2	Міжнародні та національні стандарти в галузі взаємодії відкритих систем і систем передачі інформації.	2
2.2.3	Загрози інформації в системах зв'язку і телекомунікаціях, заходи і засоби їх захисту	4
2.2.4	Захист інформації в робочих станціях та мережевих операційних системах (Novell, Windows NT, Internet).	6
2.2.5	Експлуатація управління та супроводження систем захисту інформації в системах зв'язку та телекомунікаціях.	2
2.3	Криптографічні засоби захисту інформації в телекомунікаційних мережах та системах зв'язку.	4
2.3.1	Проблема автентифікації та цифровий підпис.	2
2.3.2	Генерація, розподіл та збереження ключів. Криптографія в сучасних мережевих технологіях.	2
	Разом	**44**

Продовження таблиці 2

№ теми	Назва теми	Кількість годин
3.	***Інші види занять***	
3.1	Співбесіда	2
3.2	Тестовий контроль знань	2
3.3	Підведення підсумків навчання	2
	Разом	**6**
	Загальний обсяг занять, год.	**72**

УДК 378.147

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КУРСА «ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Любовь Новикова, Александр Скатков
Севастопольский государственный технический университет

Аннотация: **В статті розглядається методика викладання дісципліни «Основи захисту інформації» при подготовці бакалаврів, фахівців та магістрів за напрямками «Комп'ютерна інженерія» та «Комп'ютерні науки».**
Summary: **This article describes the principles of teaching «The Basics of Information Security» course to students, achieving Bachelor, Engineer, and Master Degrees in «Computing» and «Computer Science».**
Ключевые слова: **Защита информации, криптология, отказоустойчивость, программное обеспечение.**

I Введение

В данной статье рассматриваются следующие вопросы: почему возникла необходимость в преподавании дисциплины "Основы защиты информации", какие направления в этом курсе следует рассматривать и какие проблемы остались не решенными при преподавании дисциплины.

Развитие компьютерной техники и в частности компьютерных сетей, которые позволили связать потоки информации не только между организациями, пользователями в отдельных странах, но и установить связь между этими странами, явились толчком к тому, что бурно начали развиваться вопросы связанные, с защитой передаваемой информации. Осознание важности знаний по этой проблеме привело к необходимости включения в программу обучения отдельного предмета, который называется «Основы защиты информации». Эта дисциплина преподается студентам старших курсов при подготовке бакалавров, специалистов и магистров по направлениям «Компьютерная инженерия» и «Компьютерные науки».

II Методика преподавания дисциплины «Основы защиты информации»

Целью преподавания дисциплины "Основы защиты информации" является изучение студентами теоретических и практических методов защиты данных в ЭВМ от несанкционированного доступа, кражи, уничтожения и других действий, связанных с информацией, хранящейся в вычислительной системе.

В результате изучения дисциплины студент должен знать:

* основы криптологии;
* технические средства для хранения и защиты информации от несанкционированного доступа;
* методы парольной защиты;
* вопросы обеспечения безопасности сетей;
* принципы создания вирусов и антивирусные средства вычислительной техники;
* существующие методы защиты авторских прав на информационные продукты: программы, алгоритмы, данные, результаты.

При изучении дисциплины студент должен уметь:

- выбирать средства и методы для защиты информации в ЭВМ;
- разрабатывать алгоритмы, реализующие шифрование данных и используемые для электронной подписи;