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;

- осуществлять выявление и лечение от вирусов в ЭВМ существующими антивирусными программными продуктами;
- разрабатывать рекомендации по защите сетей различного типа от несанкционированного доступа.

При преподавании дисциплины предусмотрены основные виды учебных занятий: лекции, практические занятия и лабораторные работы.

Для восприятия данной дисциплины необходимо знание пользовательского интерфейса, умение работать в операционных системах и сетях, знание работы и взаимодействия с компьютером периферийных устройств, знание вопросов, связанных с моделированием, проектированием и анализом вычислительных систем. Ранее изученные дисциплины дают возможность говорить о том, что студенты получают эти знания до того, как начинают знакомиться с курсом «Основы защиты информации».

Основная особенность дисциплины «Основы защиты информации» заключается в том, что она носит синтетический характер. Накопленные знания должны быть переосмыслены с точки зрения решения задач защиты. Это предполагает освещение вопросов защиты во всех аспектах:

- защита при хранении информации;
- защита полученных при обработке данных;
- защита программных продуктов, находящихся в ЭВМ;
- защита вычислительной техники от несанкционированного доступа;
- контроль и защита техники от отказов и сбоев в работе.

В то же время студентов необходимо научить самостоятельно разрабатывать методы и средства защиты. Для этого необходимо:

- научить студентов умению проводить анализ имеющихся систем и программ с точки зрения защиты;
- производить самостоятельно разработку моделей и методов, предназначенных для создания и оптимизации средств защиты.

В результате изучения дисциплины студент должен понять, что защиту информации можно рассматривать с различных точек зрения:

- тематической: необходимость защиты как техники, передающей информацию, так и разработка новых технических устройств для ее передачи;
- экономической: потеря информации или ее несанкционированное использование могут нанести большой материальный урон, как организации, так и отдельному индивидууму;
- социальной: вопросы, связанные с профессиональной этикой, использованием различных видов информационного обеспечения, включая лицензионные программные продукты, создание и распространение собственной информации, и ее защита, составляют социальные аспекты защиты;
- государственной: умение и понимание необходимости сохранения информации, составляющей государственную тайну.

Отдельным направлением в рассмотрении вопросов защиты необходимо выделить защиту прав граждан на интеллектуальную собственность. Этим вопросам до настоящего времени не уделяется достаточного внимания при подготовке специалистов.

Для получения целостного подхода к содержанию курса можно выделить три направления в изложении имеющихся знаний по защите информации: общий, функциональный и принципиальный. Рассмотрение общих вопросов обычно производится во время чтения лекционного материала. По вопросам защиты информации издано много статей, популярных книг и сборников, поэтому перед нами стояла задача выбора лекционного материала. Ниже приводится список тем, рассматриваемых в лекционном курсе по дисциплине «Основы защиты информации»:

1. Анализ возможных каналов утечки информации в вычислительных системах. Классификация видов компьютерных преступлений.
2. Защита компьютеров от несанкционированного доступа к информации. Специальное программное обеспечение по защите информации ПК.
3. Криптология - наука о безопасности. Проблемы секретности и имитостойкости. Криптоаналитические нападения. Принципы проектирования систем защиты информации. Безусловная и теоретическая стойкость. Элементы теории секретной связи Шеннона. Криптография с открытым ключом. Применение криптографии с открытым ключом для аутентификации. Примеры использования алгоритмов с открытыми ключами в современной компьютерной технике.
4. Стандарт шифрования DES.
5. Стеганография. Зашифровка информации в изображении и звуке, зашифровка с помощью архиваторов.
6. Аутентификация: пароли и их современные разновидности. Средства обхода парольной защиты.
7. Криптографические протоколы. Несостоятельность протоколов криптосистем.
8. Система защиты информации PGP.

9. Компьютерные вирусы. Деление по логике функционирования. Структура построения вирусных программ. Общие рекомендации на случай заражения персонального компьютера компьютерным вирусом. Знакомство с наиболее распространенными компьютерными вирусами.

10. Антивирусные продукты. Ложные тревоги. "Вакцинация" программ. Способы защиты EXE файлов.

11. Отказоустойчивость ЭВМ и вычислительных сетей. Обеспечение отказоустойчивости на уровне пользователя. Обеспечение отказоустойчивости при хранении данных. Аппаратные средства. Программные средства. Обеспечение отказоустойчивости по питанию. Обеспечение отказоустойчивости сети в целом. Оценка различных методов.

12. Сравнение свойств обеспечения отказоустойчивости основных сетевых операционных систем.

13. Безопасная связь с внешним миром: мосты, маршрутизаторы, шлюзы, блокираторы. Как тип сети влияет на риск.

Функциональную часть знаний по курсу желательно излагать во время практических занятий. На практических занятиях студенты должны разобрать более подробно существующие алгоритмы и научиться разрабатывать алгоритмы шифрования, а также понять на каких принципах построено проектирование технических средств защиты. Исходя из этого, на практические занятия вынесены следующие вопросы:

1. Простейшие методы шифрования данных. Подстановка, перестановка и полиалфавитные шифры.
2. Использование сдвиговых регистров для шифрования информации.
3. Алгоритмы гаммирования.
4. Методы защиты программ от компьютерных вирусов. «Вакцинация» программ, существующие алгоритмы. Методы защиты существующих EXE- файлов.
5. Стандарт создания электронной подписи.
6. Алгоритмы нахождения больших простых чисел.

Принципиально важным моментом при изучении дисциплины «Основы защиты информации» является знания, приобретаемые студентами при выполнении лабораторных работ, которые позволяют на практике опробовать теоретические положения и рассмотренные алгоритмы, реализующие отдельные элементы криптосистем. Для выполнения лабораторных работ были выбраны следующие темы:

1. Простейшие методы шифрования данных. Подстановка, перестановка и полиалфавитные шифры.
2. Шифрование с использованием ГПЧ.
3. Алгоритмы шифрования с открытыми ключами. Алгоритм RSA.
4. Создание электронной подписи в документе.
5. Организация парольной защиты.

Некоторые работы студенты могут выполнять в виде индивидуальных заданий. Такие работы могут содержать элементы криптоаналитических заданий, разработка своих систем шифрования и проверка их на криптостойкость, определение длины периода генератора псевдослучайных чисел, для различных видов генераторов и выбор лучшего из них для шифрования. Эти работы позволяют студентам лучше понять принципы действия криптографических систем.

Преподавание дисциплины «Основы защиты информации» выявило те проблемы, которые пока не удалось решить. В настоящее время при довольно большом количестве литературы, по данному направлению отсутствуют учебные пособия, учебники. У большинства из нас сложился стереотип компьютера с пиратским программным обеспечением, редко встречаются лицензионные программы. Особенно при преподавании этого предмета необходимо прививать студентам работу в рамках законности, как с информацией, так и с программными продуктами, которые используются для ее хранения и обработки. В рамках университета отсутствуют реально действующие лицензированные криптографические системы, с помощью которых можно было бы усилить курс выполняемых лабораторных работ. Невелик выбор и средств антивирусных программных продуктов. Это не позволяет провести их практическое сравнение и представить студентам возможность выбирать, какой из них удобнее и эффективнее использовать при проверке программного обеспечения и файлов, содержащих информацию.

III Выводы

Предлагаемый подход на наш взгляд может служить основой методического обеспечения курса, так как он системно учитывает все аспекты, возникающие при изучении вопросов защиты. Данный подход был апробирован при обучении студентов по специальности «Компьютерные системы и сети» факультета «Автоматика и вычислительная техника» Севастопольского государственного университета. Техническое обеспечение основывалось на сетевом классе с операционной системой Window98. Дальнейшее развитие курса возможно по следующим направлениям:

- введение курсового проектирования, что позволит студентам самостоятельно разрабатывать отдельные элементы и анализировать работу действующих криптосистем;

· включение вопросов защиты информации в программу практики;
· выделение в дипломном проектировании раздела по специальным вопросам защиты информации при разработке, как программных продуктов, так и решении технических задач.

УДК 621.396

НАВЧАЛЬНА БАЗА ДИСЦИПЛІН ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Юрій Зіньковський, Вадим Клименко, Михайло Прокофьєв.
Національний технічний університет України "КПІ"

Анотація: **Розглядається досвід, набутий у взаємодії учбового процесу на кафедрі і в науково-дослідній установі галузі технічного захисту інформації у вищому навчальному закладі (ВНЗ). Така взаємодія є засобом забезпечення найбільш ефективного навчального процесу, високого рівня практичної кваліфікації випускників кафедри і перспективою їх працевлаштування за напрямом.**
Викладено досвід підвищення ефективності підготовки фахівців при взаємодії навчальних і науково-дослідних підрозділів ВНЗ.
Summary: **Learning base of discipline defense the information**

I Вступ

Технічні засоби захисту інформації можуть бути ефективними при адекватній їх відповідності загрозам, що можуть мати місце.

Основні потенціальні загрози безпеці і відповідні типові (концептуальні) завдання захисту декларуються в основоположних організаційно-методичних стандартах ISO (Єдині критерії безпеки інформаційних технологій - CCITSE), а також у відповідних державних стандартах (ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення., ДСТУ 3396.1-98 Захист інформації. Технічний захист інформації. Порядок виконання робіт). Ці завдання такі:

- захист від загроз конфіденціальності (несанкціонованого відбору) інформації за всіма каналами її витоку (мовному, видовому, електромагнітному, оптичному, віброакустичному), особливо, за рахунок ПЕМІН і таємних каналів зв'язку (закладних пристроїв, радіомікрофонів і ін.);
- захист від загроз цілісності (несанкціонованої зміни інформації);
- захист від загроз досяжності інформації (несанкціонованого чи випадкового обмеження інформації і ресурсів самої системи);
- захист від загроз аудиту системи (наприклад, загрози несанкціонованого вторгнення в систему, маніпуляції з протоколами обміну і аудиту, загальносистемним програмним забезпеченням і ін.).

Захист інформації - це виявлення і аналіз технічних каналів витоку інформації, які пов'язані з дослідженням радіотехнічних і електричних кіл, поширенням радіохвиль, пристроїв генерування і приймання сигналів. Для вирішення завдань захисту необхідно визначити і виконати аналіз загроз, розробити систему захисту інформації, виконувати контроль функціонування та керування системою захисту інформації.

II Основна частина

Концептуальні завдання захисту інформації визначають зміст навчальних планів підготовки спеціалістів цього профілю, зміст програм спеціальних дисциплін, а також необхідну тематику лабораторних робіт за основними навчальними дисциплінами.

В деяких випадках для досягнення необхідної високої ефективності технічних засобів захисту інформації виникає потреба в унікальній апаратній підтримці, що не завжди може бути реалізована серійними промисловими електронними приладами і, навіть, потребує відповідної апаратної науково-дослідної розробки. Використання в навчальному лабораторному практикумі дослідних взірців апаратури, розробленої за індивідуальними технічними завданнями в науково-дослідних установах галузі технічного захисту інформації, є дуже бажаним як засіб забезпечення найбільш ефективного навчального процесу.

Про це свідчить досвід, набутий у взаємодії учбового процесу за профілем захисту інформації кафедри радіоконструювання і виробництва радіоапаратури радіотехнічного фокультету Національного технічного