МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования
«**Оренбургский государственный университет**»

Кафедра программного обеспечения вычислительной техники
и автоматизированных систем

УТВЕРЖДАЮ
Декан факультета информационных технологий
_____ А.М. Пищухин
« ___ » _____ 2007 г.

Рабочая программа

дисциплины «Методы и средства защиты компьютерной информации»

Направление подготовки: 654600 «Информатика и вычислительная техника»
Специальность: 230105.65 «Программное обеспечение вычислительной техники и автоматизированных систем»
Факультет информационных технологий
Форма обучения: очная

Оренбург 2007

Рецензент: кандидат технических наук, доцент Боровский А.С.

Рабочая программа дисциплины «Методы и средства защиты компьютерной информации» /сост. А.В. Каменев. – Оренбург: ГОУ ОГУ, 2007. - 20 с.

Рабочая программа предназначена для преподавания дисциплины общепрофессионального цикла студентам очной формы обучения специальности 230105.65 – «Программное обеспечение вычислительной техники и автоматизированных систем» в 8 семестре.

Рабочая программа составлена с учетом Государственного образовательного стандарта высшего профессионального образования по направлению подготовки дипломированных специалистов 654600 – ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, утвержденного 27.03.2000 Министерством Образования Российской Федерации.

Составитель: _____ А.В. Каменев
20.05.2007 г.

©Каменев А.В., 2007
© ГОУ ОГУ, 2007

Содержание

с.

1 Цели и задачи дисциплины…….
2 Место дисциплины в учебном процессе……
3 Организационно-методические данные дисциплины……...
4 Содержание дисциплины…….
4.1 Выписка из ГОС ВПО «Требования к обязательному минимуму содержания основной образовательной программы» по дисциплине
4.2 Разделы дисциплины, их содержание и виды занятий ……..……..
5 Тематический план изучения дисциплины ……..…….
5.1 Лабораторные работы……..
5.2 Курсовая работа
5.3 Самостоятельное изучение разделов дисциплины…….……..
6 Учебно-методическое обеспечение дисциплины…….
6.1 Рекомендуемая литература…….……
6.1.1 Основная литература……
6.1.2 Дополнительная литература……
6.2 Средства обеспечения освоения дисциплины……..…….
6.2.1 Методические указания и материалы по видам занятий…….…….
6.2.2 Программное обеспечение использования современных информационно-коммуникационных технологий (по видам занятий) …….……
6.2.3 Контрольные вопросы для самоподготовки…….…….
6.2.4 Критерии оценки знаний, умений и навыков……
7 Материально-техническое обеспечение дисциплины……..
7.1 Учебно-лабораторное оборудование …….……
Лист согласования рабочей программы ……
Дополнения и изменения в рабочей программе……

1 Цели и задачи курса

Целью преподавания дисциплины является ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

В результате изучения программ курса студенты должны

Знать:

- правовые основы защиты компьютерной информации;
- организационные, технические и программные методы защиты информации в АСОИУ;
- стандарты, модели и методы шифрования;
- методы идентификации пользователей,
- методы защиты программ от вирусов;

Уметь:

- применять методы защиты компьютерной информации при проектировании АСОИУ в различных предметных областях;

Иметь представление:

- о направлении развития и перспективах защиты информации.

2 Место дисциплины в учебном процессе

Дисциплина относится к циклу общепрофессиональных дисциплин и федеральному компоненту ООП.

Изучение данной дисциплины базируется на следующих дисциплинах:

- математический анализ;
- вычислительная математика;
- программирование;
- дискретная математика;

математическая логика и теория алгоритмов

Знания и навыки, полученные при изучении данной дисциплины, используются при выполнении курсовых работ и расчетно-графических заданий по специальным дисциплинам и дипломном проектировании.

3 Организационно-методические данные дисциплины

Вид работы	8 семестр	Всего
Общая трудоемкость	**110**	**110**
Аудиторная работа	68	68
Лекции (Л) Практические занятия (ПЗ) Лабораторные работы (ЛР)	34 17 17	34 17 17
Самостоятельная работа	50	50
Курсовая работа (КР) Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.), (СР)	17 25	17 25
Вид итогового контроля	**экзамен**	

4 Содержание дисциплины

4.1 Выписка из ГОС ВПО «Требования к обязательному минимуму содержания основной образовательной программы» по дисциплине «Методы и средства защиты компьютерной информации»:

Основные понятия и определения; источники, риски и формы атак на информацию; политика безопасности; стандарты безопасности; криптографические модели; алгоритмы шифрования; модели безопасности основных ОС; администрирование сетей; алгоритмы аутентификации пользователей; многоуровневая защита корпоративных сетей; защита информации в сетях; требования к системам защиты информации.

4.2 Содержание дисциплины

Таблица 3 – Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов и их содержание	Количество часов				Внеауд. работа СР
		Всего	Аудиторная работа			
			Л	ПЗ	ЛР	
1	Законодательные и правовые основы защиты компьютерной информации и информационных технологий		2	2		
2	Проблемы защиты информации в АСОИУ		2	2	2	
3	Теоретические основы компьютерной безопасности		6		2	
4	Современные криптосистемы для защиты компьютерной информации		10	6	6	
5	Методы идентификации и проверки подлинности пользователей компьютерных систем		4	2	2	
6	Защита компьютерных сетей от удаленных атак		4	2	2	
7	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)		2			
8	Комплексная защита процесса обработки информации в компьютерных системах		4	3	3	
	Итого:		34	17	17	

5 Тематический план изучения дисциплины

5.1 Лекции

№ лекции	№ раз-дела	Тема	Кол-во часов
1	2	3	4
1	1	*Лекция 1.* Законодательство Российской Федерации в области информационной безопасности. 1. Информация как объект юридической и физической защиты. 2. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. 3. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. 4. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.	2
2	2	Лекция 2. Основные непреднамеренные и преднамеренные угрозы информационной безопасности АСОИУ. 1. Меры противодействия угрозам безопасности. Меры по обеспечению сохранности информации в АСОИУ. 2. Основные задачи обеспечения безопасности информации в АСОИУ. Защита локальных сетей и операционных систем. 3. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения АСОИУ. Рекомендации по защите информации в Internet.	2
3	3	*Лекция 3.* Модели безопасности 1. Архитектура электронных систем обработки данных; формальные модели; 2. Политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; 3. Стандарты по оценке защищенных систем; примеры практической реализации;	2

№ лекции	№ раз-дела	Тема	Кол-во часов
4	3	*Лекция 4*. Парольные системы 1. Построение парольных систем; особенности применения криптографических методов; 2. Способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами; 3. Концепция защищенного ядра; методы верификации;	2
5	3	*Лекция 5*. Защита систем 1. Защищенные домены; 2. Применение иерархического метода для построения защищенной операционной системы; 3. Исследование корректности систем защиты; методология обследования и проектирования защиты; 4. Модель политики контроля целостности.	2
6	4	*Лекция 6*. Криптосистемы 1. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. 2. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.	2
7	4	*Лекция 7*. Симметричные системы шифрования 1. Поточные шифры, блочные шифры. Аддитивные поточные шифры. 2. Методы генерации криптографически качественных псевдослучайных последовательностей.	2
8	4	*Лекция 8*. Стандарты шифрования 1. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. 2. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.	2
9	4	*Лекция 9*. Асимметричные системы шифрования. 1. Понятия однонаправленной функции 2. Понятие однонаправленной функции с лазейкой.	2

№ лекции	№ раз-дела	Тема	Кол-во часов
10	4	*Лекция 10.* Функции дискретного логарифмирования 1. Схема Диффи-Хеллмана. 2. Схема Эль-Гамаля. 3. Разложения числа на простые сомножители. 4. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.	2
11	5	*Лекция 11.* Идентификация 1. Основные понятия и концепции. 2. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. 3. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний.	2
12	5	*Лекция 12.* Аутентификация 1. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. 2. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. 3. Отечественный стандарт хэш-функции. Алгоритм цифровой подписи RSA. 4. Алгоритм цифровой подписи Эль-Гамаля (EGSA). 5. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.	2
13	6	*Лекция 13.* Режим функционирования межсетевых экранов и их основные компоненты. 1. Маршрутизаторы. Шлюзы сетевого уровня. 2. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. 3. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.	2

№ лекции	№ раз-дела	Тема	Кол-во часов
14	6	*Лекция 14.* Программно-аппаратные средства защиты ПЭВМ и сетей. 1. Методы средства ограничения доступа к компонентам сети; 2. Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям: 3. Методы и средства хранения ключевой информации; Защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.	2
15	7	*Лекция 15.* Методы защиты программ от излучения и разрушающих программных воздействий 1. Классификация способов защиты. Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. 2. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. 3. Методы перехвата и навязывания информации. Методы внедрения программных закладок. 4. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.	2
16	8	*Лекция 16.* Комплексное обеспечение информационной безопасности автоматизированных систем 1. Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем; состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ); 2. Функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной	2

№ лекции	№ раз-дела	Тема	Кол-во часов
17	8	*Лекция 17*. Внедрение и эксплуатация КСИБ 1. Этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение; 2. Особенности проектирования на современном уровне и синтез КСИБ; типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД); 3. Мониторинг и контроль окружающей среды; ведение специальной информационной базы данных КСИБ.	2

5.2 Практические занятия

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	3	4
1	1	Изучение Российского законодательства по защите информационных технологий. Изучение нормативно-правовой информации, определяющей функционирование систем защиты.	2
2	2	Построение моделей нарушителя и системы защиты информации с помощью теории графов.	2
3	4	Разработка программного макета системы шифрования информации методом Вернама. Генерация псевдослучайных последовательностей чисел в системах защиты информации.	2
4	4	Изучение американского стандарта шифрования данных DES. Изучение отечественного стандарта шифрования данных (ГОСТ 28147-89).	2
5	4	Разработка программного макета упрощенной модели системы шифрования данных типа RSA. Алгоритм шифрования Диффи-Хеллмана.	2

6	5	Однонаправленные хэш-функции. Изучение алгоритмов электронной цифровой подписи в системах защиты информации.	2
7	6	Исследование основных функций межсетевых экранов для фильтрации сообщений и защиты информации. Изучение основных схем сетевой защиты информации на базе межсетевых экранов. Изучение особенностей защиты информации протокола SET в системе электронной торговли.	2
8	8	Инструментально-моделирующий комплекс для оценки качества функционирования защищенных информационных систем.	3

5.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	3	4
1	2	Исследование компьютерной системы на предмет наличия уязвимых мест и разработка рекомендаций по их устранению.	2
2	3	Построение моделей нарушителя и системы защиты информации с помощью теории графов.	2
3	4	Разработка программного средства шифрования информации методом Вернама.	2
4	4	Разработка программного средства упрощенной модели системы шифрования данных типа RSA.	2
5	4	Разработка программного средства на основе алгоритма шифрования Диффи-Хеллмана.	2
6	5	Реализация алгоритмов электронной цифровой подписи в системах защиты информации.	2
7	6	Реализация основных функций межсетевых экранов для фильтрации сообщений и защиты информации.	2
8	8	Разработка инструментально-моделирующего комплекса для оценки качества функционирования защищенных информационных систем.	3

5.3 Курсовая работа

Целью курсового проектирования является систематизация, расширение, углубление полученных знаний и реализация одного из методов для решения практической задачи. Необходимо разработать систему защиты для заданной АС с использованием всех известных програмно – аппаратных средств, составить: модель системы, модель нарушителя, список угроз, разработать политику безопасности. Разработать и реализовать программный продукт, отражающий один из методов защиты информации. Результат предоставить в виде Пояснительной записки.

Примерные темы курсовых работ:

1. Реализация системы идентификации и аутентификации субъектов на основе поддержания привязки субъекта к процессу, выполняемому для субъекта.
2. Реализация системы регистрации действий субъекта и его процесса.
3. Реализация системы реакции на попытки НСД.
4. Реализация системы очистки оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными.
5. Реализация системы учета выходных печатных и графических форм и твердых копий в АС.
6. Реализация системы контроля целостности программной и информационной части системы разграничения доступа и обеспечивающих ее средств.
7. Реализация монитора обращений к АС.
8. Реализация доступа к информации на основе модели Биба.
9. Реализация доступа к информации на основе модели Гогена-Мезигера.
10. Реализация доступа к информации на основе Сазерлендской модели защиты
11. Реализация доступа к информации на основе модели защиты Кларка-Вильсона
12. Защита информационного потока на основе шифра MARS.
13. Защита информационного потока на основе шифра RC6.
14. Защита информационного потока на основе шифра Serpent.
15. Защита информационного потока на основе шифра TwoFish.
16. Защита информационного потока на основе шифра Rijndael.
17. Шифрование исходного файла случайным ключом.
18. Реализация архивации данных на основе алгоритма Хаффмана.
19. Реализация архивации данных на основе алгоритма Лемпеля-Зива.
20. Реализация схемы симметричной криптосистемы
21. Реализация технологии цифровых подписей
22. Обмен ключами по алгоритму Диффи-Хеллмана
23. Защита сервера от несанкционированного доступа.
24. Защита от получения несанкционированного доступа к услугам АС.

25. Защита от попытки вывода из рабочего режима определенного класса услуг.
26. Защита среды передачи информации от НСД в сетях с пакетной обработкой.
27. Защита среды передачи информации от НСД в сетях с соединением "точка-точка".
28. Защита от получение доступа к таблице маршрутизации маршрутизатора.
29. Защита информации на канальном уровне.
30. Защита информации на сетевом уровне.
31. Защита информации на транспортном уровне.
32. Защита информации на сеансовом уровне.
33. Реализация защиты от НСД элемента операционной системы.
34. Реализация защиты от НСД прикладных программ.
35. Реализация защиты от MACRO-вирусов.
36. Реализация программного сканера резидентных программ.
37. Шифрование с использованием стандарта шифрования данных ГОСТ 28147-89.
38. Защита цифровой информации методами стеганографии.
39. Реализация схемы управление ключами в криптосистеме.
40. Реализация системы восстановления паролей.
41. Реализация шифрования случайным ключом
42. Реализация межсетевого экрана – фильтра-мапшрутизатора.
43. Реализация межсетевого экрана – 2-портового шлюза.
44. Защита информации в электронных платежных системах.
45. Защита пользователя «система».
46. Защита пользователя «Процесс».
47. Оценка эффективности системы защиты системы обработки информации.
48. Оценка эффективности системы защиты системы передачи информации.
49. Реализация системы управленияя доступом пользователей к ресурсам.
50. Реализация механизмов контроля целостности.
51. Реализация механизмов регистрации (аудита).
52. Реализация парольной защиты файловой системы.
53. Реализация парольной защиты на основе применения меток безопасности объектам доступа
54. Разграничение доступа к реестру ОС.
55. Реализация мандатного управления доступа к ресурсам АС.
56. Реализация мандатного управления доступа к каналам связи
57. Реализация канонической модели управления доступа к исполняемым файлам
58. Управление доступом к каталогам, не разделяемым системой и приложениями
59. Реализация диспетчера доступа к ресурсам АС.
60. Реализация диспетчера доступа к сетевым ресурсам.

5.3 Самостоятельное изучение разделов дисциплины

№	Вопросы, выносимые на самостоятельное изучение

раздела	
1	2
1-8	Элементы реализации основных направлений информационной безопасности в операционных системах.

6 Учебно-методическое обеспечение дисциплины

6.1 Рекомендуемая литература

6.1.1 Основная литература

1. Хорошко, В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков; под ред. Ю.С. Ковтанюка. - Киев : ЮНИОР, 2003. - 504 с.
2. Методы и средства защиты компьютерной информации [Электронный ресурс] : метод. указ. к лабор. практикуму / Т. Н. Шалкина. - Оренбург : ОГУ. – 2006.
3. Богомолов, А.В. Средства защиты обеспечения безопасности информации в современных автоматизированных системах; А.В. Богомолов, Д.С. Чуйков, Ю.А. Запорожский // Информационные технологии. - 2003.

6.1.2 Дополнительная литература

1. Технические методы и средства защиты информации / Под ред. В.Г. Сонникова. -СПб. : Полигон, 2000. - 320 с.
2. Организация и современные методы защиты информации: Метод.пособие / Под общ.ред.С.А.Диева,А.Г.Шаваева. - М. : Концерн "Банковский Деловой Центр", 1998. - 472с
3. Бондаренко, И.И. Криптографические средства защиты информации [Текст] : метод. указ. к лабораторной и самостоятельной работе студентов / И. И. Бондаренко, И. В. Влацкая, М. Ю. Нестеренко. - Оренбург : ГОУ ОГУ, 2005.
4. А.А. Малюк Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие / . - 2004. - 280 с.

6.2 Средства обеспечения освоения дисциплины

6.2.1 Методические указания и материалы по видам занятий

6.2.1.1 Методические указания к лабораторным занятиям

Методические указания к проведению лабораторных работ. Разработка кафедры.

6.2.2 Программное обеспечение современных информационно-коммуникационных технологий по видам занятий

6.2.2.1 Программное обеспечение для выполнения лабораторных работ

Программа реализации языка программирования «Паскаль».

6.2.3 Контрольные вопросы для самопроверки

Раздел 1. Законодательные и правовые основы защиты компьютерной информации информационных технологий

Законодательство Российской Федерации в области информационной безопасности. Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. Нормативно0правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.

Раздел 2. Проблемы защиты информации в АСОИУ

Основные непреднамеренные и преднамеренные угрозы информационной безопасности АСОИУ. Меры противодействия угрозам безопасности. Меры по обеспечению сохранности информации в АСОИУ. Основные задачи обеспечения безопасности информации в АСОИУ. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения АСОИУ. Рекомендации по защите информации в Internet.

Раздел 3. Теоретические основы компьютерной безопасности

Архитектура электронных систем обработки данных; формальные модели; модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; стандарты по оценке защищенных систем; примеры практической реализации; построение парольных систем; особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами; концепция защищенного ядра; методы верификации; защищенные домены; применение иерархического метода для построения защищенной операционной системы; исследование корректности систем защиты; методология обследования и проектирования защиты; модель политики контроля целостности.

Раздел 4. Современные криптосистемы для защиты компьютерной информации

Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Дисковые шифраторы.

Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.

Симметричные системы шифрования (системы с секретным ключом): поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.

Асимметричные системы шифрования (системы с открытым ключом). Понятия однонаправленной функции и однонаправленной функции с лазейкой.

Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля.

Разложения числа на простые сомножители.

Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.

Раздел 5. Методы идентификации и проверки подлинности пользователей компьютерных систем

Основные понятия и концепции. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль-Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

Раздел 6. Защита компьютерных сетей от удаленных атак

Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.

Программно-аппаратные средства защиты ПЭВМ и сетей; методы средства ограничения доступа к компонентам сети; методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям: методы и средства хранения ключевой информации; защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.

Раздел 7. Методы защиты программ от излучения и разрушающих программных воздействий (программных закладок и вирусов)

Классификация способов защиты. Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.

Раздел 8. Комплексная защита процесса обработки информации в компьютерных системах

Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем; состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ); функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной безопасности в технологическую среду; этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение; особенности проектирования на современном уровне и синтез КСИБ; типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД); мониторинг и контроль окружающей среды; ведение специальной информационной базы данных КСИБ.

6.2.4 Критерии оценки знаний, умений и навыков

Итоговыми формами контроля знаний, умений и навыков по дисциплине являются зачет и экзамен. Зачет выставляется при условии, если студент не имеет задолжностей по лабораторным работам и выполнил отчет по РГЗ. Экзамен проводится по билетам, которые включают два теоретических вопроса.

Оценка знаний студентов производится по следующим критериям:

–оценка *«отлично»* выставляется студенту, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, причем не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач;

–оценка «*хорошо*» выставляется студенту, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;

–оценка «*удовлетворительно*» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает

неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;

–оценка «*неудовлетворительно*» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

7 Материально-техническое обеспечение дисциплины

7.1 Учебно-лабораторное оборудование

Лабораторные работы проводятся в компьютерных классах кафедры ПОВТАС – ауд. №№ 14406 (а, б), 14422, 14423 или 14424.

ЛИСТ

согласования рабочей программы

Направление подготовки: 654600 «Информатика и вычислительная техника»

Специальность: 230105.65 «Программное обеспечение вычислительной техники и автоматизированных систем»

Дисциплина: Методы и средства защиты информации

Форма обучения: очная

Учебный год 2007 / 2008

Рекомендована заседанием кафедры программного обеспечения вычислительной техники и автоматизированных систем

протокол от « ___ » _____ 2007 г.

Ответственный исполнитель, заведующий кафедрой
ПОВТАС _____ Н.Соловьев « ___ » _____ 200 г.

Исполнитель
доцент кафедры ПОВТАС
_____ А. Каменев « ___ » _____ 200 г.

СОГЛАСОВАНО:
Заведующий кафедрой ПОВТАС _____ Н.Соловьев « __ » _____ 200 г.

Председатель методической комиссии по специальности
230105.65 «Программное обеспечение вычислительной техники и автоматизированных систем»
_____ Н.Соловьев « __ » _____ 200 г.

Заведующий отделом комплектования научной библиотеки
_____ « __ » _____ 200 г.

Начальник УСИТО
_____ « __ » _____ 200 г.