МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Программно-аппаратные средства обеспечения информационной безопасности»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ /Толстых Н.Н./

Заведующий кафедрой
Систем информационной
безопасности _____ / А.Г. Остапенко /

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины- обучение студентов принципам построения систем защиты информации (СЗИ) в операционных системах (ОС), вычислительных сетях (ВС) и системах управления базами данных (СУБД).

1.2.Задачиосвоениядисциплины

- освоение принципов построения подсистем защиты в ОС, ВС и СУБД различной архитектуры;
- изучение средств и методов несанкционированного доступа (НСД) к ресурсам ОС, ВС и СУБД;
- обучение принципам функционирования современных систем идентификации и аутентификации;
- изучение методологии анализа, синтеза и оценки эффективности использования систем защиты информации инфокоммуникационных комплексов в условиях кибервойн.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Программно-аппаратные средства обеспечения информационной безопасности»относитсякдисциплинамбазовойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Программно-аппаратные средства обеспечения информационной безопасности»направленнаформированиеследующихкомпетенций:

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ОПК-8	**Знать:** -принципы построения и структуру подсистем защиты современных ОС и СУБД инфокоммуникационных систем.
	Уметь: - осуществлять выбор необходимого и достаточного для реализации целевых функций защищаемого объекта (инфокоммуникационного комплекса) набора средств и методов его защиты в условиях ограниченного ресурса.
	Владеть: - способами решения основных задач теории защиты

	информации инфокоммуникационных комплексов в условиях кибервойн.
ПК-12	**Знать:** - информационные воздействия на защищенные ОС, ВС и СУБД и их признаки.
	Уметь: - синтезировать и планировать политику безопасности организации и ее реализацию с учетом реальной обстановки в организации или выделенной сети.
	Владеть: - методами анализа инфокоммуникационных систем в аспекте обеспечения информационной безопасности.
ПК-27	**Знать:** - средства и способы проведения информационных воздействий и методы их обнаружения и нейтрализации.
	Уметь: - организовывать защиту сегмента инфокоммуникационного комплекса, подключаемого к открытым телекоммуникационным сетям.
	Владеть: - методами оценки эффективности систем защиты информации с учетом реальных условий реализации их целевых функций, класса защищенности.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Теория информации»составляет3 з.е.
Распределениетрудоемкостидисциплиныповидамзанятий

Видыучебнойработы	Всегочасов	Семестры
		9
Контактная работа по видам занятий (всего)	100	100
В томчисле:		
Лекции	60	60
Лабораторные работы (ЛР)	20	20

Практические занятия (ПЗ)	20	20
Самостоятельнаяработа	116	116
Часынаконтроль	36	36
Видыпромежуточнойаттестации - экзамен	+	+
Общая трудоемкость час з.е.	252 7	252 7

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. работы	Практ. зан.	СРС	Всего, час
1	Подсистема защиты информации в ОС UNIX	Основные компоненты подсистемы защиты UNIX. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Создание и удаление бюджетов пользователей.	6	2	2	10	20
2	Подсистема защиты информации в ОСWindowsNT	Основные компоненты подсистемы защиты WindowsNT и Windows 2000. Политики. Понятие домена. Особенности установления доверительных отношений.	6	2	2	10	20
3	Защита информации при интеграции UNIX и WindowsNT	Основы взаимодействия элементов гетерогенных сетей. Использование сервера Samba для разделения доступа к сетевым ресурсам в домене WindowsNT.	6	2	2	12	22
4	Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ. Защита программ	Методы и средства ограничения доступа к компонентам ЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.Защита от разрушающих программных воздействий. Защита от изменения и контроль целостности.	6	2	2	12	22
5	Атаки на сетевые службы. Адаптивная безопасность в ВС	Понятие атаки. Типы угроз. Классификация атак по основным механизмам реализации угроз. Сетевые сканеры.Понятие адаптивной безопасности и системы обнаружения атак. Классификация по используемым механизмам обнаружения атак, и по принципам их практической реализации. Особенности применения различных типов систем обнаружения атак.	6	2	2	12	22
6	Межсетевые экраны. Удалённый доступ к сети	Понятие межсетевых экранов. Основные примеры конфигурации защищенных сетей с использованием МЭ. Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов.Проблемы обеспечения безопасности при удалённом доступе. Протоколы аутентификации PAP и CHAP. Протоколы аутентификации удалённого доступа в программных средствах Microsoft.	6	2	2	12	22

7	Виртуальные частные сети. Политика безопасности	Понятие виртуальной частной сети, её предназначение. Стандартные возможности каналообразующего оборудования различных производителей. Основные принципы функционирования и использования протокола PPTP.Понятие политики информационной безопасности для организации. Основные требования к политике безопасности.	6	2	2	12	22
8	Понятие безопасности БД. Модели безопасности в СУБД	Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит.Критерии защищенности БД Критерии оценки надежных компьютерных систем. Понятие политики безопасности. Совместное применение различных политик безопасности в рамках единой модели. Интерпретация TCSEC для надежных СУБД (TDI).Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД. Дискреционные (избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS).	6	2	2	12	22
9	Механизмы обеспечения целостности СУБД	Основные виды и причины возникновения угроз целостности. Способы противодействия. Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представления словаря. Фиксация транзакции. Прокрутки вперед и назад. Контрольная точка. Откат. Транзакции как средство изолированности пользователей. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности. Цели использования правил. Способы задания, моменты выполнения. Назначение механизма событий. Сигнализаторы событий. Типы уведомлений о происхождении события.	6	2	2	12	22
10	Механизмы обеспечения конфиденциальности в СУБД	Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Особенности применения криптографических методов. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Метки безопасности. Использование представлений для обеспечения конфиденциальности	6	2	2	12	22

		информации в СУБД. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Журнализация. Регистрация действий пользователя. Управление набором регистрируемых событий.					
		Итого	**60**	**20**	**20**	**116**	**216**

5.2Переченьлабораторных работ

1. Установка операционной системы Windows XP на виртуальной машине – 2 ч.
2. Восстановление логинов пользователя и администратора ОС и ВС – 2 ч.
3. Использование списков доступа (ACL) в ОС Windows NT и UNIX – 2 ч.
4. Дизассемблирование программных модулей – 2 ч.
5. Использование редактора реестра – 2 ч.
6. Управление дисками из командной строки – 2 ч.
7. Обеспечение безопасности папок и документов – 2 ч.
8. Просмотр журнала аудита – 2 ч.
9. Защита программ и данных от несанкционированного копирования – 2 ч.
10. Защита от вредоносных воздействий компьютерных вирусов и программных закладок – 2 ч.

5.2Переченьпрактических занятий

1. Создание бюджетов пользователя в ОС WindowsNT и UNIX – 2 ч.
2. Использование списков доступа (ACL) в ОС WindowsNTи UNIX –2 ч.
3. Аудит в WindowsNT и UNIX – 2 ч.
4. Конфигурация межсетевого экрана на примере ipchains. Использование сканера защищённости Nessus– 2 ч.
5. Применение хост-ориентированной системы обнаружения вторжений Portsentry– 2 ч.
6. Применение сеть-ориентированной системы обнаружения вторжений Snort– 2 ч.
7. Представления словаря данных СУБД Oracle7. Среда разработки приложений OracleDesigner/2000 – 2 ч.
8. Средства управления транзакциями в Oracle7 – 2 ч.
9. Анализтехнико-экономической эффективности системы защиты информации в компьютерных системах – 2 ч.
10. Использование блокировок для обеспечения многопользовательской работы в Oracle7 – 2 ч.

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Учебным планом по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» предусмотрено выполнение курсового проекта.Тема курсового проекта: «Защита от вредоносных воздействий компьютерных вирусов и программных закладок».

Курсовой проект включает в себя разработку системы защиты от вредоносных воздействий компьютерных вирусов и программных закладок. Курсовой проект выполняется студентами в соответствии с заданным вариантом в соответствии с «Методическими указаниями к выполнению курсового проекта… ».

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ОПК-8	**Знать:** - принципы построения и структуру подсистем защиты современных ОС и СУБД инфокоммуникационных систем.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - осуществлять выбор необходимого и достаточного для реализации целевых функций защищаемого объекта (инфокоммуникационного комплекса) набора средств и методов его защиты в условиях ограниченного ресурса.	Решениестандартныхпрактическихзадач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - способами решения основных задач теории защиты информации инфокоммуникационных комплексов в условиях кибервойн.	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

ПК-12	**Знать:** - информационные воздействия на защищенные ОС, ВС и СУБД и их признаки.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - синтезировать и планировать политику безопасности организации и ее реализацию с учетом реальной обстановки в организации или выделенной сети.	Решениестандартныхпрактическихзадач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - методами анализа инфокоммуникационных систем в аспекте обеспечения информационной безопасности.	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-27	**Знать:** - средства и способы проведения информационных воздействий и методы их обнаружения и нейтрализации.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - организовывать защиту сегмента инфокоммуникационного комплекса, подключаемого к открытым телекоммуникационным сетям.	Решениестандартныхпрактическихзадач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - методами оценки эффективности систем защиты информации с учетом реальных условий реализации их целевых функций, класса защищенности.	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9семестре по черырехбальной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл**	**Неудовл**

ОПК-8	**Знать:** - принципы построения и структуру подсистем защиты современных ОС и СУБД инфокоммуникационных систем.	знание учебного материала и использование учебного материала в процессе выполнения заданий	Студент демонстрирует полное понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать знание, умение, навык выражена слабо	1. Студент демонстрирует незначительное понимание материала. 2. Студентдемонстрирует непонимание заданий. 3. У студента нет ответа. Не было попытки выполнить задания.
	Уметь: - осуществлять выбор необходимого и достаточного для реализации целевых функций защищаемого объекта (инфокоммуникационного комплекса) набора средств и методов его защиты в условиях ограниченного ресурса.	умение использовать учебный материал в процессе выполнения лабораторных работ				
	Владеть: - способами решения основных задач теории защиты информации инфокоммуникационных комплексов в условиях кибервойн.	применение учебного материала при решении практических задач				
ПК-12	**Знать:** - информационные воздействия на защищенные ОС, ВС и СУБД и их признаки.	знание учебного материала и использование учебного материала в процессе выполнения заданий				
	Уметь: - синтезировать и планировать политику безопасности организации и ее реализацию с учетом реальной обстановки в организации или выделенной сети.	умение использовать учебный материал в процессе выполнения лабораторных работ				
	Владеть: - методами анализа инфокоммуникационных систем в аспекте обеспечения информационной безопасности.	применение учебного материала при решении практических задач				
ПК-27	**Знать:** - средства и способы проведения информационных воздействий и методы их обнаружения и нейтрализации.	знание учебного материала и использование учебного материала в процессе выполнения				

		заданий				
	Уметь: - организовывать защиту сегмента инфокоммуникационного комплекса, подключаемого к открытым телекоммуникационным сетям.	умение использовать учебный материал в процессе выполнения лабораторных работ				
	Владеть: - методами оценки эффективности систем защиты информации с учетом реальных условий реализации их целевых функций, класса защищенности.	применение учебного материала при решении практических задач				

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

(минимум 10 вопросов для тестирования с вариантами ответов)

Вариант 1

1. Подсистема … АС должна идентифицировать и проверять подлинность субъектов доступа при входе в систему:

- управления доступом;
- регистрации и учета;
- обеспечения целостности.

2. Система, обладающая всеми возможными способами защиты и способная в любой момент своего существования спрогнозировать наступление угрожающего события за время, достаточное для приведения в действие адекватных способов защиты – это:

- абсолютно упорядоченная система;
- абсолютная система защиты;
- абсолютная система уничтожения.

3. Прекращение выполнения задачи при возникновении условий, исключающих возможность ее дальнейшего выполнения – это аварийный:

- завершение;
- ситуация;

- отказ.

4. Существуют … группы требований к системе защиты:

- формализованные (обязательные);
- достаточные;
- дополнительные;
- все выше перечисленные.

5. Совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений – это автоматизированная:

- информационная система;
- система;
- система в защищенном исполнении.

6. Степень соответствия действительному состоянию тех реалий, которые отображает оцениваемая информация – это … информации:

- адекватность;
- полнота;
- целостность.

7. Субъект, ответственный за обеспечение безопасности информации в автоматизированных сетях – это администратор:

- безопасности;
- защиты;
- доступа.

8. Совокупность взаимосвязанных данных, организованных в соответствии со схемой базы данных таким образом, чтобы с ними мог работать пользователь – это банк:

- памяти;
- данных.

9. Наиболее высока скорость изменения … групп требований к системе защиты:

- формализованных;
- достаточных;
- дополнительных.

10. Процедура добавления в кадр перед его передачей в физический канал (и удаление их после передачи) битов, обеспечивающая прозрачность информационного канала – это:

- бифуркация;
- битстаффинг.

11. Свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта – это;

- доступность;
- целостность;
- ценность.

12. Лицо (группа лиц, организация), имеющее право на пользование услугами вычислительной системы – это:

- абонент;
- оператор;
- администратор.

13. Подсистема АС, которая обеспечивает периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год – это подсистема:

- регистрации и учета;
- обеспечения целостности;
- управления доступом.

14. Схема обеспечения автоматического доказательства правильности программ – это автоматический:

- верификатор;
- анализатор;
- модулятор.

15. Механизмы по обеспечению безопасности … ОС дополняются механизмами защиты СУБД:

- логических дисков (томов);
- файлов;
- таблиц;
- каталогов.

16. Действие модема, которое позволяет программе обслуживания передачи данных по линии связи отвечать на запросы и осуществлять запись передаваемых файлов – это автоматический:

- запрос;
- ответ;
- переадресация.

17. Способность системы к целенаправленному приспособлению при изменении физической, функциональной, логической структуры, технологических схем или условий функционирования информационных систем – это … системы:

- гибкость;
- расширяемость;
- устойчивость.

18. Угроза преднамеренного несанкционированного изменения состояния системы является:

- активной;
- пассивной;
- отложенной.

19. Упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов – это:

- алгоритм;
- процедура;
- функция.

20. Первая группа АС включает в себя наиболее распространенные многопользовательские АС, в которых:

- одновременно обрабатывается информация разных уровней конфиденциальности;
- одновременно обрабатывается информация одного уровня конфиденциальности;
- все пользователи имеют право доступа ко всей информации АС;

21. Свойством компьютерного оборудования подсоединяться к оборудованию другого типа без его модификации или использования эмулятора является аппаратная:

- расширяемость;
- совместимость;
- переносимость.

22. Средства, обеспечивающие связь между ЭВМ в системах телеобработки данных – это аппаратура … данных:

- передачи;
- шифрования;
- обработки.

23. Нарушение безопасности информационной системы, позволяющее захватчику

управлять операционной средой – это:

- угроза;
- атака.

24. Оценка чего-нибудь с проставлением отметки – это:

- аттестация;
- верификация;
- лицензирование.

25. Первая группа АС подразделяется на … класса безопасности:

- 3
- 4;
- 5;
- 6.

7.2.4Примерныйпереченьвопросовдляподготовкикэкзамену

1. История противоборства в сфере информационных технологий.
2. Общая схема системы защиты программного обеспечения (ПО).
3. Классификация угроз безопасности ПО. Оценка уязвимости ПО.
4. Задачи защиты программного обеспечения .
5. Правовые аспекты защиты программного обеспечения от несанкционированного использования.
6. Классификация способов и средств защиты программного обеспечения от несанкционированного использования. Требования, предъявляемые к средствам и системам защиты.
7. Схемы разграничения доступа к программному обеспечению.
8. Показатели защищенности средств вычислительной техники (СВТ) от НСД к информации. Классификация СВТ по требованиям безопасности информации.
9. Контроль защищенности СВТ с помощью инструментальных средств.
10. Порядок проведения контроля отсутствия недекларированных возможностей программного обеспечения СВТ.
11. Инструментальные средства контроля отсутствия недекларированных возможностей программного обеспечения СВТ.
12. Порядок сертификации программных средств защиты информации (СЗИ) в системе сертификации ФЭСТЭК России.
13. Порядок разработки, изготовления и эксплуатации программных СЗИ.
14. Каналы несанкционированного доступа к программному обеспечению. Статистика преступлений, связанных с несанкционированным использованием программного обеспечения.
15. Методы осуществления несанкционированного использования

программных средств путем вскрытия и модификации алгоритма защиты.

16. Методы дискредитации криптографической защиты. Вскрытие логической защиты. Вскрытие ключевых файлов.
17. Использование дизассемблирования и декомпилирования для модификации программных механизмов защиты.
18. Типовые сценарии несанкционированного доступа, основанные на несовершенстве алгоритмов защиты.
19. Методика оценки времени, необходимого для вскрытия программных средств защиты.
20. Оценка времени, необходимого для дискредитации программных средств криптографической защиты информации.
21. Оценка времени, необходимого для вскрытия логической защиты.
22. Основные методы защиты программного обеспечения.
23. Классификация автоматизированных систем по требованиям безопасности информации.
24. Требования по обеспечению безопасности информации в автоматизированных системах различных классов защищенности.
25. Порядок контроля защищенности от НСД к информации при проведении аттестационных испытаний объектов информатизации.
26. Инструментальные средства аттестационных испытаний.
27. Организационные меры защиты программного обеспечения при функционировании компьютерных систем (КС).
28. Технические меры защиты программного обеспечения при функционировании КС.
29. Комплексное оснащение КС системами безопасности типовых решений.
30. Защита программного обеспечения от несанкционированного копирования.
31. Законы РФ об охране интеллектуальной собственности.
32. Требования руководящих документов ФЭСТЭК России по защите оригиналов программ.
33. Средства и методы копирования дистрибутивных носителей информации.
34. Способы затруднения анализа программ. Приемы против отладчиков.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочного средства
1	Подсистема защиты информации в ОС UNIX	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта

2	Подсистема защиты информации в OCWindowsNT	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
3	Защита информации при интеграции UNIX и WindowsNT	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
4	Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ. Защита программ	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
5	Атаки на сетевые службы. Адаптивная безопасность в ВС	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
6	Межсетевые экраны. Удалённый доступ к сети	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
7	Виртуальные частные сети. Политика безопасности	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
8	Понятие безопасности БД. Модели безопасности в СУБД	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
9	Механизмы обеспечения целостности СУБД	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта
10	Механизмы обеспечения конфиденциальности в СУБД	ОПК-8 ПК-12 ПК-27	Тест, решение практических задач, выполнение лабораторных работ, выполнение курсового проекта

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

При преподавании дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» в качестве формы оценки знаний студентов используются: тесты, решение практических задач различной сложности, выполнение лабораторных работ, выполнение курсового проекта, экзамен.

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменаторомивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартных и прикладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Выполнение лабораторных работ осуществляется согласно учебного плана в соответствии с «Методическими указаниями по выполнению лабораторных работ …».

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная:

1. Проскурин В.Г.Программно-аппаратные средства обеспечения информационной безопасности: Защита в операционных системах: Учеб.пособие / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. - М.: Радио и связь, 2000. - 168с. : ил. - Дар РУНЦ. - ISBN 5-256-01414-5 : 50.00.Рекомендовано Мин. обр. РФ в качестве учеб.пособия для студентов вузов
2. Белкин П.Ю.Программно-аппаратные средства обеспечения информационной безопасности : Защита программ и данных: Учеб.пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков, Д.И. Правиков. - М.: Радио и связь , 1999. - 168с. : ил. - Дар РУНЦ. - ISBN 5-256-01416-1 : 50.00.Рекомендовано Мин. обр. РФ в качестве учеб.пособия для студентов вузов

681.3
П 784
Программно-аппаратные средства обеспечения информационной безопасности : Защита программ и данных:Учеб.пособие для вузов. - М. : Радио и связь , 2000. - 168 с. : ил. - ISBN 5-256-01533-8 : 56.00.

3. Дуров В.П.Программно-аппаратная защита информации [Электронный ресурс] : учеб.пособие / В. П. Дуров. - Электрон.дан. (1 файл :6681088 байт). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

Дополнительная:

1. Толстых Н.Н.Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс] : Учеб.пособие / Н. Н. Толстых. - Электрон.текстовые, граф. дан. (1,75 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.
2. Толстых Н.Н.Введение в теорию конфликтного функционирования информационных и информационно-управляющих систем: учеб.пособие / Н. Н. Толстых, В. А. Павлов, Е. И. Воробьева. - Воронеж: ВГТУ, 2003. - 169 с. - 30-00.
3. Владимиров А.А., Гавриленко К.В., Михайловский А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / пер. с англ. А.А. Слинкина. — М.: НТ Пресс, 2005. – 463 с.
4. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 21.07.2014) «О связи» (с изм. и доп., вступ. в силу с 01.08.2014, с.3
5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации», с.2

Методические разработки:

1. Толстых Н.Н.Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс] : Методические указания к практическим занятиям по дисциплине "Программно-аппаратные средства обеспечения информационной безопасности" для студентов специальностей 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем", 090301 "Компьютерная безопасность", 090302 "Информационная безопасность телекоммуникационных систем" очной формы обучения / Каф.систем ин-формационной безопасности; Сост. Н.Н. Толстых. -

Электрон.текстовые, граф. дан. (273 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 00-00.

2. Толстых Н.Н.Методические указания к лабораторным работам по дисциплине "Программно аппаратные средства обеспечения ИБ" для студентов специальностей 090302 "Информационная безопасность", 090302 "Информационная безопасность телекоммуникационных систем", 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост. Н. Н. Толстых. - Электрон.текстовые, граф. дан. (613 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.
3. Толстых Н.Н.Методические указания к практическим занятиям по дисциплине "Программно-аппаратные средства обеспечения ИБ" для студентов специальностей 090302 "Информационная безопасность телекоммуникационных систем", 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост. Н. Н. Толстых. - Электрон.текстовые, граф. дан. (626 Кбайт). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл.
4. Методические указания к самостоятельным работам по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для студентов специальностей 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост. Н. Н. Толстых. - Электрон.текстовые, граф. дан. (417 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществленииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

http://eios.vorstu.ru/
http://www.studentlibrary.ru/

http://znanium.com/
http://ibooks.ru/
http://e.lanbook.com/
http://www.iprbookshop.ru/
http://fstec.ru/ - Официальный сайт ФСТЭК России [Электронный ресурс] / ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
http://bdu.fstec.ru - Банк данных угроз безопасности информации[Электронный ресурс] / ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
http://www.gost.ru/ - Каталог национальных стандартов[Электронный ресурс] / Федеральное агентство по техническому регулированию и метрологии

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторных и практических занятий.

Натурные лекционные демонстрации:

- реальные и обезвреженные средства проведения информационных воздействий;
- аппаратура и элементы системы обеспечения информационной безопасности автоматизированных телекоммуникационных систем.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Программно-аппаратные средства обеспечения информационной безопасности» читаются лекции, проводятся лабораторные и практические занятия.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяна иболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражения вучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивметодических указаниях к лабораторным работам по данной дисциплине.

На практических занятияхпроводитсятестирование и решение задач в соответствии с темой занятия.Методики решения задачприведенывметодических указанияхкпрактическим занятиям.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойвыпол

нения тестов, решения практический задач, выполнения лабораторных работ, выполнения курсового проекта.Освоение дисциплины оценивается на экзамене.

Видучебныхзанятий	Деятельностьстудента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторные работы	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных работ для подготовки к ним необходимо: разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебного пособия по данной дисциплине, проработать дополнительную литературу и источники, подготовиться к выполнению в соответствии с методическими указаниями к лабораторным работам.
Практические занятия	Практические занятияпозволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности практических занятий для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебного пособия по данной дисциплине, проработать дополнительную литературу и источники, решить задачи для самостоятельного решения из соответствующего раздела методических указаний к практическим занятиям.
Самостоятельнаяработа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточнойаттестации.
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. При подготовке к зачету необходимо выполнение расчетного задания.