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

«Разработка и эксплуатация защищенных автоматизированных систем»

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 _____ /Карпеев Д.О./

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

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины формирование компетенций в области разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации

1.2. Задачи освоения дисциплины

Изучение основных угроз безопасности информации в автоматизированных системах и освоение методик оценки данных угроз; изучение методой, способов, средств, последовательности и содержания этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; изучение основных мер по защите информации в автоматизированных системах; изучение содержания и порядка деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» относится к дисциплинам базовой части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» направлен на формирование следующих компетенций:

ОПК-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий;

ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;

ПК-11 - способностью разрабатывать политику информационной безопасности автоматизированной системы;

ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-11	знать методы и модели анализа угроз безопасности подсистем автоматизированных систем
	уметь разрабатыватьполитикуинформационнойбезопасностиавтоматизированнойсистемы
ПК-23	знать основные меры по защите информации в автоматизированных системах

	уметь определять комплекс мер для обеспечения информационной безопасности автоматизированных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	80	80
В том числе:		
Лекции	40	40
Практические занятия (ПЗ)	40	40
Самостоятельная работа	64	64
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
1	Защищенные АИС. Основные понятия и классификация	Цели и задачи курса. Содержание дисциплины. Рекомендуемаялитература. Классификация АИС. Информационные технологии, используемые в АИС. Жизненный цикл АИС. Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах	8	6	10	24
2	Основы организации разработки защищенных АИС	Последовательность и содержание этапов разработки АИС. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.	8	6	10	24

		Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АИС. Методыобеспеченияинформационнойбезопасности АИС				
3	Общие принципы проектирования защищенных АИС	Проектирование защищенных АИС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. Построение комплексной защиты АИС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АИС. Технологии создания отказоустойчивых систем	6	6	10	22
4	Основыэксплуатациязащищенных АИС	Аттестация АИС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АИС на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе АИС. Порядок обеспечения защиты информации при эксплуатации АИС.Технические и программные средства защиты АИС от несанкционированного доступа. Организация технического обслуживания защищенных АИС. Содержание и порядок ведения эксплуатационной документации. Методы проверки	6	6	10	22

		защищенных АИС. Содержание и порядок ведения эксплуатационной документации				
5	Средствадиагностированиязащищенных АИС	Контрольно-измерительное оборудование, используемое при поиске неисправностейаппаратных средств АИС. Технологическое оборудование для ремонтааппаратныхсредств АИС	6	8	12	26
6	Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования	Аппаратно-программные средства диагностики АИС. Аппаратно-программные средства контроля функционирования отдельныхэлементов, узлов, блоков	6	8	12	26
		Итого	**40**	**40**	**64**	**144**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-11	Знать методы и модели анализа угроз безопасности подсистем автоматизированных систем	знаниеметодов и моделейанализа угроз безопасности подсистем автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	уметь разрабатывать политику информационной безопасности автоматизированной системы	умение разрабатывать политику информационной безопасности автоматизированной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-23	знать основные меры по защите информации в автоматизированных системах	знание основных мер по защите информации в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь определять комплекс мер для обеспечения информационной безопасности автомати-зированных систем	умение определять комплекс мер для обеспечения информационной безопасности автомати-зированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-11	знать методы и модели анализа угроз безопасности подсистем автоматизированнных систем	Тест	Выполнение тестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь разрабатывать политику информационной безопасности автоматизированнной системы	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
ПК-23	знать основные меры по защите информации в автоматизированнных системах	Тест	Выполнение тестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь определять комплекс мер для обеспечения информационной безопасности автомати-	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные	Продемонстрирован верный ход решения всех, но не получен	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

	зированных систем		ответы	верный ответ во всех задачах		

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыковили(или)опытадеятельности)

7.2.1Примерный перечень заданий для подготовки к тестированию

1.Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, - это…

Вариант 1 информационная технология

Вариант 2 информационно - телекоммуникационная сеть

Вариант 3 информационная система

Вариант 4 автоматизированная система

2. Как называются действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц?

Вариант 1 **распространение информации**

Вариант 2 предоставление информации

3. Как называются помещения, специально предназначенные для проведения конфиденциальных мероприятий?

Вариант 1 ограниченные помещения

Вариант 2 конфиденциальные помещения

Вариант 3 **защищаемые помещения**

Вариант 4 контролируемые помещения

4. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?

Вариант 1 доступность

Вариант 2 **конфиденциальность**

Вариант 3 целостность

5. Какое свойство информации нарушено, если в результате действий злоумышленников легитимный пользователь не может получить доступ к социальной сети?

Вариант 1 целостность

Вариант 2 **доступность**

Вариант 3 конфиденциальность

6. Наказание за распространение вредоносного программного обеспечения, предусмотренное законодательством РФ, относится к…

Вариант 1 техническим методам защиты информации

Вариант 2 криптографическим методам защиты информации

Вариант 3 **правовым методам защиты информации**

Вариант 4 методам физической защиты

7. Сведения в военной области относятся к:

Вариант 1 **государственной тайне**

Вариант 2 служебной тайне

Вариант 3 коммерческой тайне

Вариант 4 персональным данным

8. Персональные данные гражданина РФ относятся к…

Вариант 1 государственной тайне

Вариант 2 коммерческой тайне

Вариант 3 общедоступной информации

Вариант 4 **конфиденциальной информации**

9.Технические средства и системы не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается/циркулирует, называются:

Вариант 1 Дополнительные технические средства и системы

Вариант 2 Основные технические средства и системы

Вариант 3 **Вспомогательные технические средства и системы**

Вариант 4 Конфиденциальные технические средства и системы

10. Как называется принцип контроля доступа, который предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретных пользователей или групп?

(Отметьте один правильный вариант ответа.)

Вариант 1 **дискреционный доступ**

Вариант 2 регистрируемый доступ

Вариант 3 мандатный доступ

Вариант 4 комбинированный доступ

11.Как называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров?

Вариант 1 **объект информатизации**

Вариант 2 объект защиты

Вариант 3 информационная система

Вариант 4 автоматизированная система

12. Как называется система, состоящая из персонала и комплекса средств

автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций?

Вариант 1 информационная система обработки персональных данных

Вариант 2 автоматизированная система

Вариант 3 информационная система

Вариант 4 средство вычислительной техники

13. К какой группе относятся АС, в которых работает один пользователь, допущенный ко всей информации в АС, размещённой на носителях одного уровня конфиденциальности?

Вариант 1 III группа

Вариант 2 II группа

Вариант 3 I группа

14.Какой тип доступа предполагает назначение объекту грифа секретности, а субъекту - уровня допуска?

Вариант 1 дискреционный доступ

Вариант 2 комбинированный доступ

Вариант 3 **мандатный доступ**

Вариант 4 регистрируемый доступ

7.2.2Примерный перечень заданий для решения стандартных задач

Вопрос 1. Какую цель преследуют хакеры – дилетанты:

1) добиться доступа к системе, чтобы выяснить ее назначение;

2) модифицировать или стереть данные, а также оставить преднамеренный след, например, в виде непристойной записки;

3) совершенствуют систему безопасности предприятия

Вопрос 2 Кого обычно относят к категории хакеров-профессионалов:

1) лиц, стремящихся получить информацию в целях промышленного шпионажа;

2) «белые воротнички» работаюшие на разные компании, чтобы усовершенствовать их систему безопасности;

3) группировки отдельных лиц, стремящихся к наживе.

Вопрос 3. Что относится к техническим средствам НСД:

1) телефонные автонабиратели;

2) логические бомбы;

3) экранный имитатор;

4) получение паролей.

Вопрос 4. Что относится к программным средствам НСД:

1) антивирусные программы;

2) троянский конь;

3) протоколы связи;

4) получение паролей.

Вопрос 5. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

1) получить, изменить, а затем передать ее конкурентам;

2) размножить или уничтожить ее;

3) получить, изменить или уничтожить;

4) изменить и уничтожить ее;

5) изменить, повредить или ее уничтожить.

Вопрос 6. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?

1) любая информация;

2) только открытая информация;

3) запатентованная информация;

4) закрываемая собственником информация;

5) коммерческая тайна.

Вопрос 7. Кто может быть владельцем защищаемой информации?

1) только государство и его структуры;

2) предприятия акционерные общества, фирмы;

3) общественные организации;

4) только вышеперечисленные;

5) кто угодно.

Вопрос 8. Какие сведения на территории РФ могут составлять коммерческую тайну?

1) учредительные документы и устав предприятия;

2) сведенья о численности работающих, их заработной плате и условиях труда;

3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;

4) другие;

5) любые.

Вопрос 9. Какой самый прямой и эффективный способ склонения к сотрудничеству?

1) психическое давление;

2) подкуп;

3) преследование;

4) шантаж;

5) угрозы.

Вопрос 10. Завершающим этапом любого сбора конфиденциальной информации является

1) копирование;

2) подделка;

3) аналитическая обработка;

4) фотографирование;

5) наблюдение.

Вопрос 11.Причины связанные с информационным обменом приносящие наибольшие убытки?

1) остановка или выход из строя информационных систем;

2) потери информации;

3) неискренность;

4) проникновение в информационную систему;

5) перехват информации.

Вопрос 12. Какие цели преследуются при активном вторжении в линии связи?

1) анализ информации (содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;

2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;

3) инициализация ложных соединений;

4) варианты 1 и 2;

5) варианты 2 и 3.

7.2.3Примерный перечень заданий для решения прикладных задач

Отметьте соответствие подсистем и требований по защите в зависимости от ценности (конфиденциальности) информации и классов защищённости АС от НСД ("-" нет требований к данному классу; "+" есть требования к данному классу).

Подсистемы и требования	Классы								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. Подсистема управления доступом	+	+	+	+	+	+	+	+	+
1.1. *Идентификация*, проверка подлинности и контроль доступа субъектов: в систему;									
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и	+	+	+	+	+	+	+	+	+
учет: входа/выхода *субъектов доступа* в/из системы (узла сети);									
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ *субъектов доступа* к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий *субъектов доступа*;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых	-	+	-	+	-	+	+	+	+
областей оперативной памяти ЭВМ и внешних накопителей.									
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование	-	-	-	+	-	-	-	+	+
конфиденциальной информации.									
3.2. Шифрование информации, принадлежащей	-	-	-	-	-	-	-	-	+

различным *субъектам доступа* (группам субъектов) на разных ключах.									
3.3. Использование аттестованных (сертифицированных) *криптографических средств*.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое *тестирование* СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

7.2.4Примерный перечень вопросов для подготовки к зачету

Непредусмотрено учебным планом

7.2.5Примерный перечень заданий для решения прикладных задач

Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Классификация АИС. Информационные технологии, используемые в АИС. Жизненный цикл АИС. Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах. Последовательность и содержание этапов разработки АИС. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АИС. Методы обеспечения информационной безопасности АИС. Проектирование защищенных АИС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторскойдокументации. Структура и содержание технического задания.Построение комплексной защиты АИС. Основы проектированиякомплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АИС. Технологии созданияотказоустойчивых систем

Аттестация АИС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведенияаттестации. Особенности эксплуатации АИС на объекте защиты. Требования и рекомендации по защите служебной тайны и персональныхданных при работе АИС. Порядок обеспечения защиты информациипри эксплуатации АИС.

Технические и программные средства защиты АИС от несанкционированного доступа. Организация технического обслуживания защищенных АИС. Содержание и порядок ведения эксплуатационной документации. Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации.

Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АИС. Технологическое оборудование для ремонта аппаратных средств АИС.

Аппаратно-программные средства диагностики АИС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Защищенные АИС. Основные понятия и классификация	ПК- 11, ПК-23	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Основы организации разработки защищенных АИС	ПК- 11, ПК-23	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Общие принципы проектирования защищенных АИС	ПК- 11, ПК-23	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Основыэксплуатациизащищенных АИС	ПК- 11, ПК-23	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Средствадиагностированиязащищенных АИС	ПК- 11, ПК-23	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Диагностические программы и пакеты диагностических про- грамм, их назначение, возможности и порядок использования	ОПК-8, ПК- 11, ПК-23	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1.Белоножкин В.И.Автоматизированные защищенные системы [Электронный ресурс] : Учеб.пособие. - Электрон.текстовые, граф. дан. (1.38 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

2.Остапенко А.Г.Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс] : Учеб.пособие. - Электрон.текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Дополнительная литература

1.Методические указания к практическим занятиям по дисциплинам «Методы проектирования защищенных распределенных систем» «Разработка и эксплуатация защищенных автоматизированных систем», для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: А. Г. Остапенко, М. В. Бурса. - Электрон.текстовые, граф. дан. (348 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2.Методические указания к самостоятельным работам по дисциплинам «Методы проектирования защищенных распределенных информационных систем», «Разработка и эксплуатация защищенных автоматизированных

систем» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: А. Г. Остапенко, Д. А. Никулин. - Электрон.текстовые, граф. дан. (400 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

3. Карпов В.В. Технология построения защищенных автоматизированных систем [Электронный ресурс]: учебное пособие/ Карпов В.В., Мельник В.А.— Электрон.текстовые данные.— Москва: Российский новый университет, 2009.— 232 с.— Режим доступа: http://www.iprbookshop.ru/21326.html.— ЭБС «IPRbooks».

4. Методологические основы построения защищенных автоматизированных систем [Электронный ресурс]: учебное пособие/ А.В. Душкин [и др.].— Электрон.текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2013.— 260 с.— Режим доступа: http://www.iprbookshop.ru/47427.html.— ЭБС «IPRbooks».

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
https://marsohod.org/howtostart/marsohod2
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Разработка и эксплуатация защищенных автоматизированных систем» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков расчета:

Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах.

Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.

Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.

Методы обеспечения информационной безопасности АИС.

Методы проектирования защищенных АИС. Структура и содержание технического задания.

Основы проектирования комплексной защиты информационной безопасности от НСД. Технологии создания отказоустойчивых систем.

Аттестация АИС по требованиям безопасности. Особенности эксплуатации АИС на объектезащиты. Порядок обеспечения защиты информации при эксплуатации АИС.

Технические и программные средства защиты АИС от несанкционированного доступа. Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации.

Контрольно-измерительное оборудование, используемое при поиске неисправностей и ремонте аппаратных средств АИС.

Аппаратно-программные средства диагностики АИС. Аппаратно-программные средстваконтроля функционирования отдельных элементов, узлов, блоков.

Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
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.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	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 промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.