МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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 «Обеспечение информационнной безопасности распределѐнных информационных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ / Остапенко А.Г. /

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

Руководитель ОПОП _____ / Остапенко А.Г./

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:

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

ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;

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

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-11	знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	уметь разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем
	владеть профессиональной терминологией в области информационной безопасности
ПК-20	знать автоматизированную систему как объект

	информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности
	уметь администрировать подсистемы информационной безопасности автоматизированных систем
	владеть навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем
ПК-23	знать методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем
	проводить мониторинг угроз безопасности автоматизированных систем
	владеть навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем, а также использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
ПК-11	знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	уметь разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем
	владеть профессиональной терминологией в области информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	100	100
В том числе:		
Лекции	60	60
Лабораторные работы (ЛР)	40	40
Самостоятельная работа	116	116
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 252 7

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	Лаб. зан.	СРС	Всего, час
1	Защищенные АИС. Основные понятия и классификация	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	10	8	18	36
2	Основы организации разработки защищенных АИС	Последовательность и содержание этапов разработки АИС. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.	10	8	18	36
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	10	6	20	36
4	Основы эксплуатации защищенных 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.	10	6	20	36

		Организация технического обслуживания защищенных АИС. Содержание и порядок ведения эксплуатационной документации. Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации				
5	Средства диагностирования защищенных АИС	Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АИС. Технологическое оборудование для ремонта аппаратных средств АИС	10	6	20	36
6	Диагностические программы и пакеты диагностических про-грамм, их назначение, возможности и порядок использования	Аппаратно-программные средства диагностики АИС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков	10	6	20	36
		Итого	**60**	**40**	**116**	**216**

5.2 Перечень лабораторных работ

Укажите перечень лабораторных работ

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».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-11	знать основные угрозы безопасности	знание основных угроз безопасности	Выполнение работ в срок, предусмотренн	Невыполнение работ в срок, предусмотренн

	информации и модели нарушителя в автоматизированных системах	информации и модели нарушителя в автоматизированных системах	ый в рабочих программах	ый в рабочих программах
	уметь разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем	умение разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть профессиональной терминологией в области информационной безопасности	владение профессиональной терминологией в области информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-20	знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	знание автоматизированной системы как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь администрировать подсистемы информационной безопасности автоматизированных систем	умение администрировать подсистемы информационной безопасности автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем	владение навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-23	знать методы, способы,	знание методов,	Выполнение	Невыполнение

	средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	способов, средств, последовательности и содержания этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	работ в срок, предусмотренный в рабочих программах	работ в срок, предусмотренный в рабочих программах
	проводить мониторинг угроз безопасности автоматизированных систем	проводить мониторинг угроз безопасности автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем, а также использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем	владеть навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем, а также использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных 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 основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь разрабатывать и исследовать аналитические и компьютерные модели автоматизированных	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	систем и подсистем безопасности автоматизированных систем		ответы			
	владеть профессиональной терминологией в области информационной безопасности	Решение прикладных задач в конкретной предметной области	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	Задачи не решены
ПК-20	знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь администрировать подсистемы информационной безопасности автоматизированных систем	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	Задачи не решены
	владеть навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем	Решение прикладных задач в конкретной предметной области	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	Задачи не решены
ПК-23	знать методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	проводить мониторинг угроз безопасности автоматизированных систем	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	Задачи не решены
	владеть навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных	Решение прикладных задач в конкретной предметной области	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	Задачи не решены

	систем, а также использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем					

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

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 1ограниченные помещения

Вариант 2конфиденциальные помещения

Вариант 3защищаемые помещения

Вариант 4контролируемые 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 3конфиденциальность

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

Вариант 1техническим методам защиты информации

Вариант 2криптографическим методам защиты информации

Вариант 3правовым методам защиты информации

Вариант 4методам физической защиты

7. Сведения в военной области относятся к:

Вариант 1государственной тайне

Вариант 2служебной тайне

Вариант 3коммерческой тайне

Вариант 4персональным данным

8. Персональные данные гражданина РФ относятся к…

Вариант 1государственной тайне

Вариант 2коммерческой тайне

Вариант 3общедоступной информации

Вариант 4конфиденциальной 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 1дискреционный доступ

Вариант 2регистрируемый доступ

Вариант 3мандатный 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 3информационная система

Вариант 4автоматизированная 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, размещѐнной 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

7.2.2 Примерный перечень заданий для решения стандартных задач

ПК-11 – способностью разрабатывать политику информационной безопасности автоматизированной системы	
1.	Этапы развития информационных систем.
2.	Классификация задач, решаемых с использованием АС.
3.	Отображение предметной области.
4.	Сущности и связи.
5.	Методы абстрагирования данных.
6.	Области применения моделей данных.
7.	Оценка защищенности на основе отечественных стандартов.
8.	Международные стандарты оценки защищенности.
9.	Классификация угроз безопасности АС.
10	Реальные и мнимые угрозы.
11	Цели и задачи оценки угроз безопасности АС.
12	Методы и модели анализа угроз.
ПК-20 – способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	
1.	Принципы построения защищенных АС.
2.	Элементы и подсистемы, управление и информация, самоорганизация в АС.
3.	Понятие сложной системы.
4.	Основные принципы системного подхода при создании сложных систем.
5.	Понятие качества и эффективности.
6.	Характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем.
7.	Функциональная и обеспечивающая часть сложной системы.
8.	Технология функционирования сложной системы.
9.	Задачи и этапы проектирования АС.
10.	Цели проектирования.
11.	Этапы проектирования АС.
12.	Принципы построения защищенных АС.
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	

1.	Методологии проектирования.
2.	Организация работ, функции заказчиков и разработчиков.
3.	Жизненный цикл автоматизированной системы.
4.	Структуризация предметной области. Классификация объектов проектирования.
5.	Средства автоматизации проектирования АС: общая характеристика, назначение и возможности, классификация.
6.	Практические методы реализации моделей безопасности.
7.	Реализация ядра безопасности. Мониторинг взаимодействий в системе.
8.	Технологический цикл реализации защищенной системы обработки и хранения информации.
9.	Условия, способствующие повышению эффективности защиты информации в АС.
10.	Реализация систем контроля доступа.
11.	Способы представления информации о правах доступа.
12.	Принципы построения распределенных защищенных АС.
13.	Основные положения концепции построения и использования распределенных АС.
14.	Механизмы защиты в распределенных АС.
15.	Архитектура механизмов защиты АС.
16.	Применяемые в распределенных АС методы защиты.

7.2.3 Примерный перечень заданий для решения прикладных задач

ПК-11 – способностью разрабатывать политику информационной безопасности автоматизированной системы	
1	*К какому уровню обеспечения ИБ относится «Политика информационной безопасности», утвержденная руководителем в конкретной организации?* а) законодательный **б) административный** в) процедурный г) научно-технический
2	*Если риск приемлемый, на что будет направлена политика информационной безопасности?:* **а) принятие** б) смягчение в) передача г) уклонение
3	*Если риск оправданный, на что будет направлена политика информационной безопасности?* а) принятие **б) смягчение** **в) передача** г) уклонение
4	*Если риск недопустимый, на что будет направлена политика информационной безопасности?* а) принятие б) смягчение в) передача

	г) уклонение
5	*Главная цель мер, предпринимаемых на административном уровне:* **а) сформировать программу безопасности и обеспечить ее выполнение** б) выполнить положения действующего законодательства в) отчитаться перед вышестоящими инстанциями
6	*Политика безопасности:* а) фиксирует правила разграничения доступа **б) отражает подход организации к защите своих информационных активов** в) описывает способы защиты руководства организации
7	Политика безопасности строится на основе: а) общих представлений об ИС организации б) изучения политик родственных организаций **в) анализа рисков** г) закона РФ "О государственной тайне"
8	*В число целей политики безопасности верхнего уровня входят:* **а) решение сформировать или пересмотреть комплексную программу безопасности** **б) обеспечение базы для соблюдения законов и правил** в) обеспечение конфиденциальности почтовых сообщений
9	*В число целей политики безопасности верхнего уровня входят:* а) определение правил разграничения доступа **б) формулировка целей, которые преследует организация в области информационной безопасности** ***в)*** **определение общих направлений в достижении целей безопасности**
10	*В число целей программы безопасности верхнего уровня входят:* **а) управление рисками** б) определение ответственных за информационные сервисы *в)* определение мер наказания за нарушения политики безопасности
11	*В число целей программы безопасности верхнего уровня входят:* а) составление карты информационной системы **б) координация деятельности в области информационной безопасности** ***в)*** **пополнение и распределение ресурсов**
12	*В число целей программы безопасности нижнего уровня входят:* **а) обеспечение надежной защиты конкретного информационного сервиса** **б) обеспечение экономичной защиты группы однородных информационных сервисов** *в)* координация деятельности в области информационной безопасности
ПК-20 – способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	
1	*Какой из перечисленных аспектов не является составляющей защищенности информации:* а) конфиденциальность, б) целостность, **в) формат представления,** г) доступность
2	*В каком случае энтропия системы максимальна:* а) если в системе имеются несколько маловероятных состояний, б) если в системе имеются несколько наиболее вероятных состояний,

	в) **если в системе все состояния равновероятны,** г) если в системе имеется одно маловероятное и одно наиболее вероятное состояние
3	*Случайным образом вынимается карта из колоды в 32 карты. Какое минимальное количество бинарных вопросов (то есть вопросов с ответами «да» / «нет») требуется задать, чтобы угадать, что это за карта?* а) 10, б) 8, **в) 5**, г) 3
4	*Какой тип угроз безопасности информации не рассматривается в РД ГТК:* а) **нарушение доступности информации,** б) несанкционированный доступ к информации, в) нарушение целостности информации, г) ни один из перечисленных
5	*Какому уровню представления информации соответствует информационное воздействие на ТКС посредством постановки электромагнитных помех:* а) **сигнальному,** б) семантическому, в) прагматическому, г) ни одному из перечисленных
6	*Какая из перечисленных математических дисциплин является основой классической теории надежности:* а) логика, б) **математическая статистика,** в) теория игр, г) теория множеств
7	*Какая из перечисленных угроз безопасности информации является наиболее опасной:* а) удаление данных, б) несанкционированный доступ к данным, **в) перехват управления в системе,** г) разрушение системы
8	*Какое количество информации содержится в 1 букве 100-буквенного алфавита, если вероятности всех букв одинаковы?* а) 10 десятичных единиц, б) 7 десятичных единиц, в) 4 десятичных единицы, г**) 2 десятичных единицы**
9	*Как в общем случае изменяется ненадежность (по Шеннону) перехваченного сообщения при увеличении его длины:* а) не изменяется, б) возрастает, в) **убывает,** г) ни один из вариантов
10	*Каково должно быть соотношение длины сообщения и ключа в совершенно секретной (по Шеннону) системе:* а) длина ключа строго больше длины сообщения, б) длина сообщения строго больше длины ключа, в) **длина ключа не меньше длины сообщения,** г) длина ключа равна длине сообщения
11	*Что характеризует ненадежность (по Шеннону):*

	а) безусловную энтропию переданного сообщения, **б) условную энтропию переданного сообщения после перехвата противником криптограммы некоторой длины,** в) безусловную энтропию источника сообщений, г) условную энтропию получателя сообщений после передачи криптограммы некоторой длины
12	*Как известно, количественно мера неопределенности опыта с n равновероятными исходами определяется числом log(n). По какому основанию должен быть взят логарифм?* а) по основанию 2, б) по основанию 8, в) **по основанию 10**, г) возможны все перечисленные варианты
13	*В теории надежности неприменимо непосредственно следующее распределение наработки:* а) **нормальное,** б) экспоненциальное, в) Эрланга, г) Вейбулла-Гнеденко
14	*Техническое обслуживание не включает:* а) текущее обслуживание, б) контроль работоспособности и диагностику отказов, в) ремонтно-восстановительные работы, **г) модернизацию**
15	*Системам без старения соответствует распределение наработки:* а) равномерное, б) **экспоненциальное,** в) логнормальное, г) Вейбулла-Гнеденко
16	*Система без старения характеризуется постоянством:* а) времени от начала работы элемента до отказа, б) вероятности отказа за некоторый промежуток времени, **в) интенсивности отказов,** г) плотности вероятности отказа за некоторый промежуток времени
17	*Функция корреляция хорошего генератора псевдослучайных чисел близка к:* а**) дельта-функции**, б) гамма-функции, в) экспоненте с отрицательным показателем, г) экспоненте с положительным показателем
18	*Типичная кривая интенсивности отказов примерно выглядит как:* а) константа – рост – спад, **б) спад – константа – рост,** в) рост – константа – спад, г) спад – рост – константа
19	*С точки зрения устойчивости по Ляпунову, хороший криптоалгоритм должен быть:* а) устойчив при вариациях ключа, устойчив при вариациях шифруемой последовательности, б) устойчив при вариациях ключа, неустойчив при вариациях шифруемой последовательности, **в) неустойчив при вариациях ключа, неустойчив при вариациях шифруемой последовательности,**

	г) неустойчив при вариациях ключа, устойчив при вариациях шифруемой последовательности
20	*Нагруженный резерв реализуется в системах:* а**) параллельных**, б) последовательных, в) и в тех, и в других, г) ни в тех, ни в других
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
1	*Что отражает модель жизненного цикла ИС?* **а) события, происходящие с системой в процессе ее создания и использования +** б) процесс проектирования ИС в) организационные процессы внедрения ИС
2	*Укажите свойства каскадной модели ЖЦ* а) **Информационное оружие** б) Информационное превосходство в) Информационная война
3	*Укажите свойства спиральной модели ЖЦ* **а) На каждом витке спирали выполняется создание очередной версии продукта, уточняются требования проекта** **б) На каждом витке спирали планируются работы следующего витка** в) Переход на следующий этап означает полное завершение работ на предыдущем этапе **г) Требования проекта постоянно уточняются** д) Позволяет планировать сроки завершения всех работ и соответствующие затраты
4	*Укажите свойства поэтапной модели ЖЦ с промежуточным контролем* а) **учитывает взаимовлияние результатов разработки на различных этапах** б) переход на следующий этап означает полное завершение работ на предыдущем этапе **в) время жизни каждого из этапов растягивается на весь период разработки** г) на каждом этапе формируется законченный набор проектной документации, отвечающий критериям полноты и согласованности
5	*Какую модель жизненного цикла следует использовать при создании простых ИС?* а) каскадную модель + б) спиральную модель в) поэтапную модель с промежуточным контролем
6	*Какие из перечисленных действий являются стадиями создания ИС?* **а) формирование требований к ИС** б) обследование объекта в) проведение научно-исследовательских работ
7	*Что представляет собой стандарт ISO/IEC 27799?* **а) стандарт по защите персональных данных о здоровье** б) новая версия BS 17799 в) определения для новой серии ISO 27000 г) новая версия NIST 800-60
8	*Какие из указанных этапов создания ИС входят в стадию технического проектирования?*

	а) разработка предварительных проектных решений по системе и её частям б) разработка проектных решений по системе и её частям в) разработка и адаптация программ **г) разработка и оформление документации на поставку комплектующих изделий**
9	На какой стадии создания ИС осуществляется разработка и адаптация программ? а) эскизного проектирования **б) разработки рабочей документации** в) технического проектирования
10	*Сформулируйте цель методологии проектирования ИС* **а) регламентация процесса проектирования ИС и обеспечение управления этим процессом с тем, чтобы гарантировать выполнение требований как к самой ИС, так и к характеристикам процесса разработки** б) формирование требований, направленных на обеспечение возможности комплексного использования корпоративных данных в управлении и планировании деятельности предприятия в) автоматизация ведения бухгалтерского аналитического учета и технологических процессов
11	*Как изменяется интенсивность отказов ненагруженного резерва в процессе эксплуатации системы без отказов:* а) уменьшается, б) не изменяется, **в) возрастает,** г) сперва уменьшается, затем возрастает
12	*Мерой чего является энтропия в теории информации:* а) энергии, б) неустойчивости, **в) неопределенности,** г) криптостойкости
13	*Какое из перечисленных положений противоречит рекомендациям стандарта ISO 7498-2:* а) **число альтернативных способов обеспечения безопасности должно быть максимальным,** б) услуги безопасности могут работать более чем на одном уровне при построении безопасной системы, в) функции безопасности по возможности не должны дублировать существующие аналогичные коммуникационные функции, г) рекомендуется не нарушать независимость уровней
14	*Какая из перечисленных услуг не входит в состав базовых услуг стандарта ISO 7498-2:* а) конфиденциальность, б) аутентификация, в) **восстановление,** г) контроль доступа
15	*Какая из перечисленных групп пользователей не выделена в «Общих критериях»:* а) потребители объекта оценки, б) разработчики объекта оценки, в) оценщики объекта оценки, г) **бета-тестеры объекта оценки**

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный 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 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

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 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-20 ПК-23	Тест, защита практических работ
2.	Основы организации разработки защищенных АИС	ПК-11, ПК-20 ПК-23	Тест, защита практических работ
3.	Общие принципы проектирования защищенных АИС	ПК-11, ПК-20 ПК-23	Тест, защита практических работ
4.	Основы эксплуатации защищенных АИС	ПК-11, ПК-20 ПК-23	Тест, защита практических работ
5.	Средства диагностирования защищенных АИС	ПК-11, ПК-20 ПК-23	Тест, защита практических работ
6.	Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования	ПК-11, ПК-20 ПК-23	Тест, защита практических работ

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: www.iprbookshop.ru/21326.html.

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 лабораторные работы.

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

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

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.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и

	выполнить другие письменные задания.
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.