МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3,4
Семестр	6,7,8

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

1.

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

Цели освоения дисциплины

Целью дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» является ознакомление обучающихся с основными подходами анализа безопасности сложных систем, со средствами защиты информации, используемыми в составе АС в защищенном исполнении; в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2. Место дисциплины в структуре ООП подготовки специалиста

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» входит в базовую часть блока 1 образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин «Основы информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Организационное и

правовое обеспечение информационной безопасности», «Методы выявления нарушений информационной безопасности, аттестация АИС», «Безопасность сетей ЭВМ».

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин: «Информационная безопасность распределенных информационных систем», «Анализ рисков информационной безопасности», «Управление информационной безопасностью», учебной и производственной практик, ГИА и подготовки ВКР.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Разработка и эксплуатация защищенных автоматизированных систем» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	
Знать:	• Модель жизненного цикла и порядок создания АС; • структуру, порядок составления, оформления и утверждения Технического задания по созданию АС • Типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ • Общую характеристику и структуру стандартов (ГОСТов), регламентирующих порядок проектирования АС в защищенном исполнении. • Определять потребности в технических средствах защиты и контроля
Уметь:	• Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ • Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов. • Разрабатывать требования по защите автоматизированных систем • Отображать предметную область на конкретную модель данных
Владеть:	• методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • Практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать: •	• Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем • Основные принципы построения защищенных распределенных компьютерных систем • Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Современные принципы построения архитектуры ИС.

Структурный элемент компетенции	Планируемые результаты обучения
Уметь:	• Осуществлять анализ несложных процессов проектирования создавать дополнительные средства защиты; • Осуществлять анализ и оптимизацию несложных процессов проектирования • Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы • разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов
Владеть:	• Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации • Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации • Определять уровни защищенности и доверия программно-аппаратных средств защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем • Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации • Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
Знать:	• Модель жизненного цикла и порядок создания АС; • структуру, порядок составления, оформления и утверждения Технического задания по созданию АС • Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия
Уметь:	• Анализировать и оценивать угрозы информационной безопасности объекта • Определять потребности в технических средствах защиты и контроля • Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов • Разрабатывать требования по защите компьютерных систем отображать предметную область на конкретную модель данных • Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем • Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
Владеть:	• методиками анализа и синтеза структурных и функциональных схем

Структурный элемент компетенции	Планируемые результаты обучения
	защищенных автоматизированных информационных систем • навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем

4 Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 9 зачетных единицы 324 акад. часов, в том числе:

– контактная работа – 176,9 акад. часов:
– аудиторная – 170 акад. часов;
– внеаудиторная – 6,9 акад. часов
– самостоятельная работа – 111,4 акад. часов;
- подготовка к экзамену – 35,7;
– формы промежуточной аттестации – зачет, зачет, экзамен, защита курсовой работы

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
Тема 1. Защищенные автоматизированные системы. Основные понятия и классификация.	6							
Классификация АС. Информационные технологии, используемые в АС. Жизненный цикл АС. Современные принципы построения архитектуры АИС.	6	4		8/4И	20	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ОПК-8 з** **ПК-9 зу** **ПК-15 зу**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
Тема 2. Основы организации разработки защищенных АС.	6							
Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении. Последовательность и содержание этапов разработки АС. Методы, способы и средства разработки АС и подсистем безопасности АС.	6	4		8/2И	6	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ОПК-8 зув** **ПК-9 зу**
Алгоритмы проектирования «интеллектуальных» микропроцессорных систем автоматизации для увеличения надежности, помехозащищенности преобразователей информации. Методы, способы и средства обеспечения отказоустойчивости АС.	6	2		4/2И	10	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; - индивидуальные задания.	**ОПК-8 зув** **ПК-9 зу** **ПК-15 зу**
Критерии оценки защищенности АС. Причинно-следственный подход для анализа безопасности сложных систем.	6	2		4/2И	6	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы	**ОПК-8 зу** **ПК-15 зу**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
						(работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками		
Принципы построения модели сложных систем. Выбор мер защиты информации для реализации в информационной системе в рамках системы защиты информации.	6	3		6/2И	4,05	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; - индивидуальные задания.	**ОПК-8 зув** **ПК-15 зу**
Организация коллективной разработки программного обеспечения АС. Системы управления проектами. Основные возможности.	6	2		4/2И	10	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; - индивидуальные задания.	**ОПК-8 зув** **ПК-9 зу**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
Итого по разделу	6	**17**		**34/14И**	**56,05**		**Промежуточная аттестация (зачет)**	
Тема 3. Проектирование защищенных АС.	7							
Основные принципы проектирования сложных технических систем. Схема проектирования. Состав мер ЗИ и их базовые наборы для соответствующего класса защищенности ИС.	7	8		8/2И	8	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ПК-9 зу**
Основы ведения конструкторской документации. Структура и содержание технического задания. Разработка частных технических заданий на создание АИС в защищенном исполнении.	7	4		4/2И	8	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; **-** индивидуальные задания.	**ПК-9 зув** **ПК-15-зув**
Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от	7	4		4/2И	8,2	Подготовка к практическим занятиям Поиск дополнительной	– устный опрос (собеседование); – контрольные работы	**ОПК-8 зу** **ПК-9**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
НСД.						информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками		**зув** **ПК-15 зу**
Средства обеспечения надежности и защищенных АС. Организация хранения информации в защищенных АС. Защита технических средств.	7	4		4/2И	4	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ПК-9** **зув**
Тема 4. Основы эксплуатации защищенных АС.	7							
Обеспечение доступности и целостности информации и информационной системы. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи порядок проведения аттестации.	7	6		6/2И	4	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями,	– устный опрос (собеседование); – контрольные работы	**ПК-15** **зув**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
						энциклопедиями Работа с электронными библиотеками		
Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС.	7	4		4/2И	4	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ПК-15 зув**
Организация технического обслуживания защищённых АС. Средства диагностирования защищенных АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.	7	4		4/2И	2	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ПК-15 зув**
Итого по разделу	7	**34**		**34/14И**	**38,2**		**Промежуточная аттестация (зачет)**	
Тема 5. Основы администрирования АС								

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования.	8	3		8/6И	6,15	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ПК-15 зув**
Тема 6. Безопасность критической информационной инфраструктуры РФ								
ФЗ от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Субъекты КИИ. Значимые объекты КИИ. Категорирование объектов КИИ. Обеспечения безопасности объектов КИИ.	8	8		14/4И	6	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ПК-9 зув** **ПК-15 зув**
Указ президента №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на	8	6		8/4И	5	Подготовка к практическим занятиям Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; **-** индивидуальные задания.	**ПК-9 зув** **ПК-15 зув**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
информационные ресурсы РФ». Функции центров ГосСОПКА. Правила эксплуатации центров ГосСОПКА. Построения собственного центра ГосСОПКА.						(работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Работа с электронными библиотеками		
Итого по разделу	8	**17**		**34/14И**	**17,15**		**Промежуточная аттестация (экзамен, защита курсовой работы)**	**ОПК-8 зув ПК-9 зув ПК-15 зув**
Подготовка к экзамену					**35,7**			
Итого по дисциплине		**68**		**102/42 И**	**111,4 +35,7**			

И – в том числе, часы, отведенные на работу в интерактивной форме.

5 Образовательные и информационные технологии

1. Традиционные образовательные технологии ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к обучающемуся (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность обучающегося носит в таких условиях, как правило, репродуктивный характер.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы.

Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Практическая работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.

Лекция «вдвоем» (бинарная лекция) – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации.

3. Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения в рамках предложенных сценарных условий.

Формы учебных занятий с использованием игровых технологий:

Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Ролевая игра – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.

4. Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлксию.

Основные типы проектов:

Исследовательский проект – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).

Творческий проект, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

5. Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды.

Формы учебных занятий с использованием специализированных интерактивных технологий:

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.

Семинар-дискуссия – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).

6. Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией.

Формы учебных занятий с использованием информационно-коммуникационных технологий:

Лекция-визуализация – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).

Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

6.Учебно-методическое обеспечение самостоятельной работы обучающихся

Перечень тем практических занятий

1. Технологии создания отказоустойчивых АС
   1) Нормативно-методическая база создания защищенных автоматизированных систем.
   2) Идентификация, спецификация и оценивание объектов защиты и угроз безопасности в объекте информатизации.
   3) Классы защищенности и функциональные требования по защите информации в АС.
   4) Показатели защищенности автоматизированных систем и СВТ.
   5) Требования безопасности к изделиям ИТ
   6) Предпроектные работы при создании АС
   7) Стадии и этапы создания ЗАС и требования по защите информации.
   8) Разработка технического задания на создание защищенной АС или системы защиты информации АС.

9) Синтез программно-аппаратных средств ЗАС.
10) Структура подсистем защиты информации от несанкционированного доступа (НСД).
11) Методы, способы и средства обеспечения отказоустойчивости ЗАС.

2. Настройка сетевой подсистемы защищенной АС
   1) Разработка профиля защиты изделия ИТ и задания по безопасности при создании изделия ИТ.
   2) Технологии и средства проектирования АС.
   3) Управление проектированием, планирование работ
   4) Защита клиентских рабочих мест «Комплекс средств защиты информации ViPNet».
3. Содержание и система эксплуатации защищенной АС.
4. Оценка защищенности на этапах жизненного цикла ЗАС
5. Администрирование СЗИ.
6. Мониторинг ЗАС и защита от вторжений.
7. Эксплуатационная документация СЗИ АС.
8. Аудит безопасности ЗАС и управление рисками.
9. Управление дисковой подсистемой АС

Перечень тем устных опросов

1) Основные понятия и определения стандартов и руководящих документов.
2) Основные положения «Концепции защиты СВТ и АС от НСД к информации»
3) Определение перечней защищаемых ресурсов и их критичности.
4) Основные подходы к защите данных от НСД.
5) Иерархический доступ к информации
6) Доступ к данным со стороны процесса.
7) Методы опознавания пользователей
8) Аппаратные средства опознавания пользователей
9) Определение перечня защищаемых ресурсов и их критичности
10) Основные положения базовой модели угроз безопасности.
12) Основные положения модели нарушителя ИБ.
13) Общая классификация методов и средств ЗИ в АС
14) Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.
15) Классы защищенности и функциональные требования по защите информации в АС.
16) Автоматизированные системы и требования к ним.
17) Порядок создания и проектирования защищенных КС.
18) Методы, способы и средства обеспечения отказоустойчивости ЗАС.
19) Задачи ведения системного журнала
20) Средства активного аудита компьютерных систем

Перечень1 вопросов к контрольной работе (N 149-ФЗ и ГОСТ Р 51624-2000)

1. Классификация информации в зависимости от категории доступа
2. Классификация информации в зависимости от порядка ее предоставления или распространения
3. Какая информация подлежит ограничению доступа
4. Какие сведения о программах для ЭВМ включаются в реестр российского программного обеспечения
5. Классификация информационных систем
6. Кто утверждает требования к порядку создания и эксплуатации государственных информационных систем
7. На что направлены меры по защите информации

8. Обязанности обладателя информации (оператор информационной системы) в сфере обеспечения защиты информации
9. Функции системы защиты информации
10. Компоненты, подлежащие защите в АСЗИ
11. Перечень общих требований к АСЗИ
12. Перечень функциональных требований к АСЗИ
13. Общая цель защиты информации
14. Частные цели защиты информации
15. Задачи защиты информации в АСЗИ
16. Перечень технических требований к АСЗИ
17. Перечень экономических требований к АСЗИ

Перечень2 вопросов к контрольной работе (ГОСТ 51275 50922 53114)

1. Правовая защита информации
2. Физическая защита информации
3. ТЗИ
4. ЗИ от НСВ
5. Защита от непреднамеренного воздействия
6. ЗИ от НСД
7. ЗИ от ПДВ
8. Политика безопасности информации в организации
9. Безопасность информации
10. Угроза информационной безопасности
11. Фактор, воздействующий на защищаемую информацию
12. Уязвимость информационной системы
13. Модель угроз информации
14. Средство защиты информации
15. Мониторинг безопасности информации
16. Конфиденциальность информации
17. Целостность информации
18. Доступность информации
19. ИСПДн
20. АС в защищенном исполнении
21. Инцидент ИБ
22. Нарушитель ИБ организации
23. НСД
24. Недекларированные возможности
25. Закладочное устройство
26. Программная закладка
27. Компьютерная атака
28. Программное воздействие

Перечень 3 вопросов к контрольной работе (по 1 и 2 и по РД ФСТЭК__АС Защита от НСД Классификация АС)

Вопросы по РД ФСТЭК_СВТ Защита от НСД Показатели защищенности от НСД КЛАССЫ СВТ

1. Основные характеристики классов защищенности СВТ
2. Характеристика 7 класса СВТ
3. Существенные различия в классах СВТ

Вопросы по РД ФСТЭК__АС Защита от НСД Классификация АС и требования по защите информации

1. Цели классификации АС по условиям их функционирования
2. Этапы классификации АС
3. Исходные данные для проведения классификации
4. Основные определяющие групповые признаки в классификации АС
5. Основные требования к подсистеме обеспечения целостности 3 класса защищенности
6. Основные требования к подсистеме обеспечения целостности 2 класса защищенности
7. Основные требования к подсистеме управления доступом 1 класса защищенности
8. Перечислить организационные мероприятия для обработки или хранении в АС информации, не отнесенной к категории секретной

ОПРОС по терминам и содержаниям нормативных документов

- Вопросы по документам: № 149-ФЗ и ГОСТ Р 51624-2000
- Определение «Конфиденциальность информации»
- Определение «Служебная тайна»
- Определение «Секретная информация»
- Определение «Защищаемая информация»
- Определение «Автоматизированная система в защищенном исполнении»
- Определение «Система защиты информации автоматизированной системы»
- Определение «Фактор, воздействующий на защищаемую информацию»
- Определение «Угроза безопасности информации»
- Функции системы защиты информации
- Компоненты, подлежащие защите в АСЗИ
- Общая цель защиты информации
- Частные цели защиты информации
- Задачи защиты информации в АСЗИ
- Перечень технических требований к АСЗИ
- Перечень экономических требований к АСЗИ
- Вопросы по документам ГОСТ – 51275 – 50922 – 53114
- Физическая защита информации
- ЗИ от НСВ
- ЗИ от НСД
- ЗИ от ПДВ
- Уязвимость информационной системы
- Инцидент ИБ
- Нарушитель ИБ организации
- Недекларированные возможности
- Вопросы по РД ФСТЭК_СВТ Защита от НСД Показатели защищенности от НСД КЛАССЫ СВТ
- Существенные характеристики 6 класса защищенности СВТ
- Существенные отличия 5 класса защищенности СВТ от предыдущего класса
- Существенные отличия 4 класса защищенности СВТ от предыдущего класса
- Существенные отличия 3 класса защищенности СВТ от предыдущего класса
- Существенные отличия 2 класса защищенности СВТ от предыдущего класса
- Существенные отличия 1 класса защищенности СВТ от предыдущего класса
- Характеристика 7 класса СВТ
- Существенные различия в классах СВТ
- Вопросы по РД ФСТЭК__АС Защита от НСД Классификация АС и требования по защите информации
- Цели классификации АС по условиям их функционирования
- Этапы классификации АС
- Исходные данные для проведения классификации
- Основные определяющие групповые признаки в классификации АС

- Основные требования к подсистеме обеспечения целостности 3 класса защищенности
- Основные требования к подсистеме обеспечения целостности 2 класса защищенности
- Основные требования к подсистеме управления доступом 1 класса защищенности
- Перечислить организационные мероприятия для обработки или хранении в АС информации, не отнесенной к категории секретной
- Вопросы по ГОСТ Р 51583-2014 2014 Порядок создания АС в защищенном исполнении Цель создания системы ЗИ АСЗИ

- Общие требования к АСЗИ
- Участники процесса создания АСЗИ
- Этапы создания АСЗИ
- Мероприятия по ЗИ на стадиях разработки
- Порядок примсенения ТС и ПС для создания АСЗИ
- Содержание и порядок выполнения работ по созданию АСЗИ
- формирование требований к системе ЗИ АСЗИ;
- разработка (проектирование) системы ЗИ АСЗИ;
- внедрение системы ЗИ АСЗИ;
- аттестация АСЗИ на соответствие требованиям безопасности информации и ввод ее в действие;
- сопровождение системы ЗИ в ходе эксплуатации АСЗИ

Перечень индивидуальных заданий

Задание 1

Разработать терминологический тезаурус по терминам и определениям из стандартов.

Взаимосвязь основных понятий из ГОСТ Р 53114-2008 Защита информации.

Обеспечение информационной безопасности в организации. Разработать схему.

Задание 2 Объект информатизации автоматизированная система «Отдел кадров предприятия»

Составить перечень защищаемых ресурсов.

Определить класс автоматизированной системы

Задание 3 Разработка определенных классов информационных систем в защищенном исполнении:

1. Информационно-поисковые системы
2. Электронный документооборот и делопроизводство
3. Электронные архивы
4. Системы управления ресурсами организации
5. Системы автоматизации проектирования
6. Информационно-аналитические системы
7. Системы поддержки принятия решений
8. Системы видеоконференцсвязи и цифровой телефонии
9. Ситуационные и управляющие центры

Найти информацию о таких информационных системах (рыночные предложения и/или реально функционирующие объекты)

- техническое обеспечение;
- программное обеспечение;
- обеспечение людскими ресурсами;
- спец требования по размещению объектов информатизации.

Изучить существующую функциональную структуру организации, использующей данную ИС:

•Изучить бизнес-процессы организации;

•Определить объект защиты (архитектура, процессы, данные);

•Определить целевые характеристики обеспечения защиты;
•Разработать модели угроз и нарушителя;
•Выявить требования к организации доступа к данным;
•Отобразить комплекс требований в технологическое решение.

7 Оценочные средства для проведения промежуточной аттестации

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по каждой дисциплине (модулю) за определенный период обучения (семестр) и может проводиться в форме зачета, экзамена, защиты курсовой работы.

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий		
Знать:	• Модель жизненного цикла и порядок создания АС; • структуру, порядок составления, оформления и утверждения Технического задания по созданию АС • Типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ • Общую характеристику и структуру стандартов (ГОСТов), регламентирующих порядок проектирования АС в защищенном исполнении. • Определять потребности в технических средствах защиты и контроля	1. Понятие, виды и структура автоматизированных систем 2. Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения безопасности информации в АС. 3. Классификация, идентификация (инвентаризация, каталогизация) и оценивание (категорирование) объектов защиты в АС. 4. Классификация (каталогизация), идентификация, спецификация и оценивание угроз безопасности в АС. 5. Человеческий фактор в угрозах безопасности. Модель нарушителя безопасности ин-формации в АС. 6. Декомпозиция назначения, целей и задач функционирования АС. Функциональная структура АС и функциональные требования к защищенным СВТ, АС, продуктам и системам ИТ. 7. Система и структура функциональных требований по защите от НСД к информации в СВТ, классы защищенности СВТ. 8. Система и структура функциональных требований по защите от НСД в АС, группы и классы защищенности АС. 9. Общая структура требований безопасности к изделиям и системам ИТ, классы функциональных требований безопасности. 10. Услуги (сервисы) безопасности при взаимодействии открытых систем и реализующие их механизмы безопасности. 11. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении. 12. Техническое задание на создание АС, требования по структуре, содержанию, порядку разработки, оформления, согласования и утверждения. 13. Особенности Технического задания на создание АС в защищенном исполнении. Составляющие общих требований к АСЗИ и структуру функциональных требований. 14. Жизненный цикл изделий (продуктов и систем) ИТ, общая схема и

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		последовательность создания изделий ИТ 15. Классификация изделий ИТ и функциональные пакеты требований безопасности. Классы защищенности изделий ИТ и пакеты требований доверия безопасности. 16. Структура, порядок разработки, регистрации и опубликования профилей защиты для изделий ИТ. 17. Структура, назначение и порядок разработки задания по безопасности при создании изделий ИТ, соотношение между профилем защиты и заданием по безопасности. Техническое задание на создание системы ИТ. 18. Содержание процесса разработки и ввода в действие изделий (систем) ИТ. Уровни представления проектных решений 19. Проектирование АС как особый вид деятельности, объекты проектирования при создании АС (по РД 50-680-88) 20. Методология (методы и средства) проектирования АС. 21. Каноническое (индивидуальное) проектирование АС. Технологическая схема этапов технического и рабочего проектирования. 22. Типовое проектирование АС и его методы. Технологическая схема проектирования. 23. Управление процессом проектирования АС, его компоненты и специфика. 24. Организационная структура, схемы организации работ при проектировании АС и организационные формы проектного коллектива. 25. Содержание и специфика управленческого цикла при проектировании АС. 26. Методы планирования и управления проектами. Диаграммы Ганта, сетевые графики проектов. 27. Автоматизированные системы управления проектами. 28. Общие положения по эксплуатации изделий, комплексов, средств деятельности. Составляющие организационных и технических мероприятий по эксплуатации. 29. Особенности эксплуатации КС (АС) и защищенных КС (АС в защищенном исполнении). Администрирование КС (АС). 30. Органы управления и планирования эксплуатации защищенных АС.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		31. Эксплуатационная документация на АС (изделия ИТ). Руководства пользователя и администратора. 32. Конструкторские эксплуатационные документы на ТСО и ПО, эксплуатационные доку-менты предприятия **Перечень вопросов к экзамену** 1. Понятие системы ЗИ. Дестабилизирующие факторы для СЗИ. Системный подход и его принципы. 2. Рационализация расходов на информацию и ее защиту. 3. Причинно-следственный подход для анализа безопасности сложных систем. 4. Выбор мер защиты информации для реализации в информационной системе. 5. Методы и модели анализа угроз (Процесс НСД). 6. Требования к СЗИ. 7. Система общеметодологических принципов ЗИ. 8. Понятие сложной системы и основные признаки. 9. Жизненный цикл АС. 10. Методика использования метода экспертных оценок. 11. Основные концептуальные требования к задачам защиты. 12. Защита информационной системы, ее средств, систем связи и передачи данных 13. Множество функций защиты информации. 14. Задача распределения значений кодов доступа. 15. Вероятность нарушения защиты информации в типовом структурном компоненте. 16. Рекомендации по использованию моделей защищенности. 17. Факторы, влияющие на требуемый уровень защиты информации. 18. Субъекты КИИ и их действия. 19. Значимые объекты КИИ. Категорирование объектов. 20. Функции центров ГосСОПКА. Правила эксплуатации центров. 21. Построения собственного центра ГосСОПКА.
Уметь:	• Осуществлять сбор, обработку, анализ и систематизацию научно-технической	***Задание***

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	информации в области программных и программно-аппаратных средств ЗИ • Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов. • Разрабатывать требования по защите автоматизированных систем • Отображать предметную область на конкретную модель данных	Разработать терминологический тезаурус по терминам и определениям из стандартов. Взаимосвязь основных понятий из ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Разработать схему. ***Задание*** Объект информатизации автоматизированная система «Отдел кадров предприятия» Сформировать таблицу доступа персонала по категориям. Составить перечень защищаемых ресурсов. Определить класс автоматизированной системы
Владеть:	• методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • Практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	**Перечень тем курсовых работ:** 1. Разработка концепции защищенной автоматизированной системы предприятия (по видам деятельности). 2. Разработка эффективных систем защиты информации в автоматизированных системах. 3. Разработка системы программно-аппаратной защиты автоматизированной системы объекта информатизации. 4. Разработка проекта СЗИ от НСД для АС учреждения. 5. Интеграция средств информационной безопасности в технологическую среду. 6. Формирование правил функционирования подразделений службы информационной безопасности. 7. Эксплуатация комплексной системы защиты информации на объекте защиты. 8. Выявление защищаемой информации и анализ структуры автоматизированной системы объекта информатизации. 9. Разработка профилей защиты для изделий ИТ объекта защиты.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать: •	• Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем • Основные принципы построения защищенных распределенных компьютерных систем • Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Современные принципы построения архитектуры ИС.	1. Понятие, виды и структура автоматизированных систем 2. Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения без-опасности информации в АС. 3. 6. Декомпозиция назначения, целей и задач функционирования АС. Функциональная структура АС и функциональные требования к защищенным СВТ, АС, продуктам и системам ИТ. 4. 7. Система и структура функциональных требований по защите от НСД к информации в СВТ, классы защищенности СВТ. 5. 8. Система и структура функциональных требований по защите от НСД в АС, группы и классы защищенности АС. 6. Общая структура требований безопасности к изделиям и системам ИТ, классы функциональных требований безопасности. 7. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении. 8. Техническое задание на создание АС, требования по структуре, содержанию, порядку разработки, оформления, согласования и утверждения. 9. Особенности Технического задания на создание АС в защищенном исполнении. Составляющие общих требований к АСЗИ и структуру функциональных требований. 10. Жизненный цикл изделий (продуктов и систем) ИТ, общая схема и последовательность создания изделий ИТ 11. Классификация изделий ИТ и функциональные пакеты требований безопасности. Классы защищенности изделий ИТ и пакеты требований доверия безопасности. 12. Структура, порядок разработки, регистрации и опубликования профилей защиты для изделий ИТ. 13. Структура, назначение и порядок разработки задания по безопасности при создании изделий ИТ, соотношение между профилем защиты и заданием по безопасности. Техническое задание на создание системы ИТ. 14. Содержание процесса разработки и ввода в действие изделий (систем) ИТ.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Уровни представления проектных решений 15. Проектирование АС как особый вид деятельности, объекты проектирования при создании АС (по РД 50-680-88) 16. Методология (методы и средства) проектирования АС. 17. Типовое проектирование АС и его методы. Технологическая схема проектирования. 18. Управление процессом проектирования АС, его компоненты и специфика. 19. Организационная структура, схемы организации работ при проектировании АС и организационные формы проектного коллектива. 20. Содержание и специфика управленческого цикла при проектировании АС. **Перечень вопросов к экзамену** 1. Понятие системы ЗИ. Дестабилизирующие факторы для СЗИ. Системный подход и его принципы. 2. Рационализация расходов на информацию и ее защиту. 3. Причинно-следственный подход для анализа безопасности сложных систем. 4. Выбор мер защиты информации для реализации в информационной системе. 5. Методы и модели анализа угроз (Процесс НСД). 6. Требования к СЗИ. 7. Система общеметодологических принципов ЗИ. 8. Понятие сложной системы и основные признаки. 9. Жизненный цикл АС. 10. Методика использования метода экспертных оценок. 11. Основные концептуальные требования к задачам защиты. 12. Защита информационной системы, ее средств, систем связи и передачи данных 13. Множество функций защиты информации. 14. Задача распределения значений кодов доступа. 15. Вероятность нарушения защиты информации в типовом структурном компоненте. 16. Рекомендации по использованию моделей защищенности. 17. Факторы, влияющие на требуемый уровень защиты информации.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		18. Субъекты КИИ и их действия. 19. Значимые объекты КИИ. Категорирование объектов. 20. Функции центров ГосСОПКА. Правила эксплуатации центров. Построения собственного центра ГосСОПКА.
Уметь:	• Осуществлять анализ несложных процессов проектирования создавать дополнительные средства защиты; • Осуществлять анализ и оптимизацию несложных процессов проектирования • Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы • разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	***Задание*** Взаимосвязь основных понятий из ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Разработать схему. ***Задание*** Разработка определенных классов информационных систем в защищенном исполнении.
Владеть:	• Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации • Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации • Определять уровни защищенности и доверия программно-аппаратных средств	**Перечень тем курсовых работ:** 1. Разработка концепции защищенной автоматизированной системы предприятия (по видам деятельности). 2. Разработка эффективных систем защиты информации в автоматизированных системах. 3. Разработка системы программно-аппаратной защиты автоматизированной системы объекта информатизации. 4. Разработка проекта СЗИ от НСД для АС учреждения. 5. Интеграция средств информационной безопасности в технологическую

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем • Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации • Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	среду. 6. Формирование правил функционирования подразделений службы информационной без-опасности. 7. Эксплуатация комплексной системы защиты информации на объекте защиты. 8. Выявление защищаемой информации и анализ структуры автоматизированной системы объекта информатизации. 9. Разработка профилей защиты для изделий ИТ объекта защиты.
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем		
Знать:	• Модель жизненного цикла и порядок создания АС; • структуру, порядок составления, оформления и утверждения Технического задания по созданию АС • Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований	**Перечень вопросов к экзамену** 1. Понятие системы ЗИ. Дестабилизирующие факторы для СЗИ. Системный подход и его принципы. 2. Рационализация расходов на информацию и ее защиту. 3. Причинно-следственный подход для анализа безопасности сложных систем. 4. Выбор мер защиты информации для реализации в информационной системе. 5. Методы и модели анализа угроз (Процесс НСД). 6. Требования к СЗИ. 7. Система общеметодологических принципов ЗИ. 8. Понятие сложной системы и основные признаки. 9. Жизненный цикл АС.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия	10. Методика использования метода экспертных оценок. 11. Основные концептуальные требования к задачам защиты. 12. Защита информационной системы, ее средств, систем связи и передачи данных 13. Множество функций защиты информации. 14. Задача распределения значений кодов доступа. 15. Вероятность нарушения защиты информации в типовом структурном компоненте. 16. Рекомендации по использованию моделей защищенности. 17. Факторы, влияющие на требуемый уровень защиты информации. 18. Субъекты КИИ и их действия. 19. Значимые объекты КИИ. Категорирование объектов. 20. Функции центров ГосСОПКА. Правила эксплуатации центров. Построения собственного центра ГосСОПКА.
Уметь:	• Анализировать и оценивать угрозы информационной безопасности объекта • Определять потребности в технических средствах защиты и контроля • Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов • Разрабатывать требования по защите компьютерных систем отображать предметную область на конкретную модель данных • Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	***Задание*** Разработка определенных классов информационных систем в защищенном исполнении:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	• Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	
Владеть:	• методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	**Перечень тем курсовых работ:** 1. Разработка концепции защищенной автоматизированной системы предприятия (по видам деятельности). 2. Разработка эффективных систем защиты информации в автоматизированных системах. 3. Разработка системы программно-аппаратной защиты автоматизированной системы объекта информатизации. 4. Разработка проекта СЗИ от НСД для АС учреждения. 5. Интеграция средств информационной безопасности в технологическую среду. 6. Формирование правил функционирования подразделений службы информационной без-опасности. 7. Эксплуатация комплексной системы защиты информации на объекте защиты. 8. Выявление защищаемой информации и анализ структуры автоматизированной системы объекта информатизации. 9. Разработка профилей защиты для изделий ИТ объекта защиты.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

– на оценку **«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.

Показатели и критерии оценивания экзамена:.

– – на оценку «**отлично**» (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку «**хорошо**» (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку «**удовлетворительно**» (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку «**неудовлетворительно**» (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала или не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

Курсовая работа выполняется под руководством преподавателя, в процессе ее написания обучающийся развивает навыки к научной работе, закрепляя и одновременно расширяя знания, полученные при изучении дисциплины. При выполнении курсовой работы обучающийся должен показать свое умение работать с нормативным материалом и другими литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

В процессе написания курсовой работы обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

Показатели и критерии оценивания курсовой работы:

– на оценку «**отлично**» (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «**хорошо**» (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку «**удовлетворительно**» (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку «**неудовлетворительно**» (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи, обучающийся не может воспроизвести и объяснить содержание, не может показать интеллектуальные навыки решения поставленной задачи.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1) Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. http://znanium.com/bookread2.php?book=957144

б) Дополнительная литература:

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учеб. пособие для вузов / П.Н. Девянин .— 2-е изд., испр. и доп. — М. : Горячая линия – Телеком, 2013 .— 339 с. — ISBN 978-5-9912-0328-9 . — Режим доступа: http://ibooks.ru/reading.php?productid=344413
2. УнижаевН.В. Информационно-аналитическое обеспечение безопасности орга-низации: учебное пособие/Унижаев Н.В.–СПб.: Издательскийцентр «Интермедия», 2018.–408с. https://ibooks.ru/reading.php?productid=356934
3. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true . - Макрообъект. - ISBN 978-5-9967-1031-7.
4. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: Учебное пособие / Е.Г. Воробьев –СПб.: Издательский центр «Интермедия», 2016. –432 с. https://ibooks.ru/reading.php?productid=351534
5. Царегородцев А. В., Тараскин М. М. Методы и средства защиты информации в государственном управлении : учебное пособие. — Москва : Проспект, 2017. — 208 с. https://ibooks.ru/reading.php?productid=356008
6. Информационная безопасность при управлении техническими системами: учебное пособие / С.А. Баркалов, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов.—СПб : ИЦ «Интермедия», 2016. —528с.: илл. https://ibooks.ru/reading.php?productid=356935
7. Грибанова-Подкина М.Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования // Вопросы безопасности. — 2017. - № 2. - С.25-34. DOI: 10.7256/2409-7543.2017.2.22065. URL: http://e-notabene.ru/nb/article_22065.html
8. Коваленко, В. В. Проектирование информационных систем [Электронный ресурс]: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с. - (Высшее образование). –Режим доступа: http://znanium.com/bookread.php?book=473097 .–Заглавие с экрана. –ISBN 978-5-91134-549-5.
9. Шаньгин, В.Ф Комплексная защита информации в корпоративных системах [Электронный ресурс]: Учебное пособие - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.- (Высшее образование).–Режим доступа: http://znanium.com/bookread.php?book=402686 .–Заглавие с экрана. –ISBN 978-5-8199-0411-4.

Интернет – ресурсы

1. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" http://www.studentlibrary.ru/catalogue/switch_kit/x2016-034.html
2. Банк данных угроз безопасности информации [Электронный ресурс] – Режим доступа: https://bdu.fstec.ru .– Загл. с экрана. Яз. рус.

3. 1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
4. 2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_18.htm – Загл. с экрана. Яз. рус.
5. 3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
6. 4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД".http://www.osp.ru/os/– Загл. с экрана. Яз. рус.
7. 5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.
8. 6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru . Яз. рус.
9. 7. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.
10. 8. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
11. 9. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/ .– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)	Персональные компьютеры с ПО: - Операционная система MS Windows - *Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; - Пакет MS Office 2007 (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; - Архиватор 7zip - *GNU LGPL, бессрочная*; - - выход в Интернет.
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	Комплект учебного оборудования «Беспроводные компьютерные сети ЭВМ»; Комплект учебного оборудования «Системы контроля доступа»; Комплект учебного оборудования «Сенсорные сети ZigBee в системах автоматического управления»; Комплект учебного оборудования «Сетевая безопасность» SECURITY-CISCO-3M; Модуль «Низкоуровневый контроллер Ethernet».
Лаборатория систем передачи информации, ауд. 2124	Стенд коммуникационного оборудования с сервером для моделирования облачного сервиса.
Аудитории для самостоятельной работы (ауд.132а): компьютерные классы; читальные залы библиотеки	Персональные компьютеры с ПО: - Операционная система MS Windows - *Microsoft Imagine* - *Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; - Пакет MS Office 2007 (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; - Архиватор 7zip - *GNU LGPL, бессрочная*; - Выход в Интернет и с доступ в электронную информационно-образовательную среду университета