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)

МЕТОДЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ 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	4
Семестр	7

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)

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	

1. Цели освоения дисциплины

Целями изучения дисциплины «Методы проектирования защищенных распределенных информационных систем» являются: освоение моделей управления, получение знаний о закономерностях и свойствах процессов управления распределенными объектами, систематическое изучение основ теории и практики математического и имитационного моделирования систем; изучение основных подходов и математических схем к построению имитационных моделей; изучение возможностей применения имитационных моделей; освоение методологий и актуальных CASE-средств для имитационного моделирования систем и процессов в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2. Место дисциплины в структуре образовательной программы подготовки специалиста

Дисциплина «Методы проектирования защищенных распределенных информационных систем» входит в базовую часть блока 1 образовательной программы.

Для освоения дисциплины обучающиеся используют знания, умения и компетенции, сформированные в ходе изучения основных положений курсов «Разработка и эксплуатация защищенных автоматизированных систем», «Технология построения защищенных распределенных приложений».

Дисциплина является предшествующей для изучения дисциплин: «Информационная безопасность распределенных информационных систем», «Моделирование систем и процессов защиты информации».

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

В результате освоения дисциплины «Методы проектирования защищенных распределенных информационных 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	– принципы построения и функционирования, примеры реализаций современных операционных систем; – принципы работы элементов и функциональных узлов электронной аппаратуры; – типовые схемотехнические решения основных узлов и блоков электронной аппаратуры
Уметь	– уметь определять особенности современных программных, технических средств и информационных технологий; – эксплуатировать современные программные, технические средства и информационные технологии; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;
Владеть	– методикой эксплуатации современные программных, технических средств и информационных технологий; – навыками обеспечения безопасности информации с помощью типовых программных средств;
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
Знать	– источники и классификацию угроз информационной безопасности;

Структурный элемент компетенции	Планируемые результаты обучения
	– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
Уметь	– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
Владеть	– навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; – методами формирования требований по защите информации; – навыками анализа основных узлов и устройств современных автоматизированных систем; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	
Знать	– методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; – современную нормативно-правовую базу создания защищенных распределенных информационных систем; – инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей
Уметь	– разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; – применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем
Владеть	– методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; – навыками разработки комплексной инфраструктуры защищенной информационной системы; – навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
Знать	– способы анализа и оценки угроз информационной безопасности; нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
Уметь	– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; – разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности;

Структурный элемент компетенции	Планируемые результаты обучения
	– разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем
Владеть	– навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; – навыками проведения экспериментально-исследовательских работ при аттестации автоматизированных систем – нормативными требованиями по защите информации; – навыками организации и обеспечения режима секретности

Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет **4** зачетных единиц **144** акад. часов, в том числе:

– контактная работа – 73 акад. часов:
  – аудиторная – 68 акад. часов;
  – внеаудиторная – 5 акад. часов
– самостоятельная работа – 35,3 акад. часов;
– подготовка к экзамену – 35,7 акад. часов;

Форма аттестации:

- 7 семестр – экзамен/курсовая работы.

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		Лекции	Практич. Занятия				
Раздел 1. Теоретические основы проектирования информационных систем							
Тема 1.1. Стандарты и профили в области информационных систем	7	2	2/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию	тестирование	ОПК-8 з ПК-6 з ПК-8 з ПК-21 з
Итого по разделу		2	2/1И	2			
Раздел 2. Технологии проектирования ИС							
Тема 2.1. Моделирование функциональной области внедрения ИС	7	4	2/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к	АКР-1; тестирование; курсовая работа	ОПК-8 зу ПК-6 зу ПК-8

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
					контрольной работе; подготовка к тестированию; выполнение курсовой работы		зу ПК-21 зу
Тема 2.2. Типовое проектирование ИС	7	2	2/1И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию; выполнение курсовой работы	АКР-2; тестирование; курсовая работа	ОПК-8 зу ПК-6 зу ПК-8 зу ПК-21 зу
Тема 2.3 Автоматизированное проектирование ИС	7	2	4/1И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию; выполнение курсовой работы	тестирование; курсовая работа	ОПК-8 зу ПК-6 зу ПК-8 зу ПК-21 зу
Тема 2.4 Управление проектированием ИС	7	2	2/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию; выполнение курсовой работы	тестирование; курсовая работа	ОПК-8 зув ПК-6 зув ПК-8 зув ПК-21 зув
Итого по разделу		10	10/4И	12			
Раздел 3. Характеристика основных угроз безопасности в распределенных информационных систем							

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
Тема 3.1. Классификация угроз безопасности	7	2	2/1И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию; выполнение курсовой работы	АКР-3; тестирование; курсовая работа	ОПК-8 зу ПК-6 зу ПК-8 зу ПК-21 зув
Тема 3.2. Общая характеристика нарушителей информационной безопасности в распределенных информационных системах	7	4	4/1И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию; выполнение курсовой работы	АКР-4; тестирование; курсовая работа	ОПК-8 зу ПК-6 зу ПК-8 зу ПК-21 зу
Тема 3.3. Формирование общих требований к организации безопасности распределенных информационных систем с учетом анализа угроз и различных групп нарушителей.	7	4	4/1И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию; выполнение курсовой работы	тестирование; курсовая работа	ОПК-8 зув ПК-6 зув ПК-8 зув ПК-21 зув
Итого по разделу		10	10/3И	12			
Раздел 4. Общие принципы построения защищенных распределенных информационных систем.							

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
Тема 4.1 Технологические, законодательные и организационные предпосылки организации защиты распределенных информационных систем.	7	4	4/2И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию; выполнение курсовой работы	АКР-5; тестирование; курсовая работа	ОПК-8 зу ПК-6 зу ПК-8 зу ПК-21 зу
Тема 4.2 Проектирование процессов защиты данных	7	4	4/2И	3,3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию; выполнение курсовой работы	тестирование; курсовая работа	ОПК-8 зув ПК-6 зув ПК-8 зув ПК-21 зув
Тема 4.3 Построение защищенного решения для распределенных информационных систем	7	4	4/2И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию; выполнение курсовой работы	АКР-6; тестирование; курсовая работа	ОПК-8 зув ПК-6 зув ПК-8 зув ПК-21 зув
Итого по разделу		12	12/6И	9,3			
Подготовка к экзамену				35,7		**Промежуточная аттестация (экзамен)**	
Итого за семестр		**34**	**34/14 И**	**71**		**Промежуточная аттестация (экзамен/защита курсовой работы)**	

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
Итого по дисциплине		**34**	**34/14 И**	**71**		**Промежуточная аттестация (экзамен/защита курсовой работы)**	

5 Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Методы проектирования защищенных распределенных информационных систем» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций , учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

Формы учебных занятий с использованием традиционных технологий:

- ***обзорные лекции*** – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;
- ***информационные*** – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;
- ***Практическое занятие***, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

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

- ***проблемная*** - для развития исследовательских навыков и изучения способов решения задач.
- ***лекции с заранее запланированными ошибками*** – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.
- ***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

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.

Технологии проектного обучения

- ***Творческий проект*** – учебно-познавательная деятельность обучающихся осуществляется в

рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов 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).

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.

- ***методы IT***
  - Подготовка и проведение практических работ по поиску информации в сетях. Задание критериев поиска информации. Работа с поисковыми системами университета и внешними ресурсами.
  - Подготовка и проведение лабораторных работ по архивации данных с целью дальнейшего использования в средствах телекоммуникационных технологий: электронной почте, чате, телеконференции т.д.
  - Организация доступа обучающихся к основным и дополнительным лекционным материалам с использованием клиент-серверных технологий (платформа e-Learning).
  - Использование электронных образовательных ресурсов для организации самостоятельной работы обучающихся. Разработка преподавателями кафедры авторских ЭОР, подготовка перечня и ориентация обучающихся на государственные образовательные интернет-ресурсы.
  - Использование в образовательном процессе электронных учебников, компьютерных обучающих систем, интерактивных упражнений.
  - Компьютерный практикум.
- ***работа в команде***
  - Разработка Web-проектов.
- ***case-study***
  - Разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.
- ***проблемное обучение***
  - Подготовка тематических рефератов, содержащих разделы, частично или полностью выносимые на самостоятельное изучение.
- ***учебная дискуссия***
  - Проведение семинаров, посвященных вопросам информатики, подготовка тематических презентаций по заданным темам, и дальнейший обмен взглядами по конкретной проблеме.
- ***использование тренингов***
  - Подготовка и проведение демонстрационных, тематических и итоговых компьютерных тестирований как в качестве локальных, так и внешних контрольных мероприятий.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Методы проектирования защищенных распределенных информационных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания и вопросы по темам:

Перечень вопросов контрольных работ по темам разделов 1-4:

1. Стадии процесса разработки программных систем.
2. Основные модели процессов разработки программных систем.
3. Основные принципы защиты от НСД, сформулированные в «Концепция защиты СВТ и АС от НСД к информации».
4. Итеративные модели разработки. RUP.
5. Сложные программные системы. Пять признаков сложных систем.
6. Структурный подход к проектированию. Алгоритмическая декомпозиция.
7. Объектно-ориентированный подход к проектированию. Основные принципы и преимущества.
8. Понятие модели системы. Задачи модели. Основные принципы моделирования сложных систем. Схема взаимосвязей моделей сложных программных систем.
9. Состав операций, выполняемых при проектировании системы защиты данных в ИБ.
10. Состав операций, выполняемых на предпроектной стадии.
11. Понятие несанкционированного доступа, основные пути несанкционированного доступа.
12. Методы защиты от НСД.
13. Защита от несанкционированного копирования ценной компьютерной информации и методы ее обеспечения.
14. Состав и функции подсистем, включаемых в систему защиты данных.
15. Состав и функции подсистемы «Подсистему регистрации и учета».
16. Состав и функции подсистемы «Подсистема обеспечения целостности».
17. Содержание механизма управления доступом.
18. Алгоритмы криптографической защиты данных.
19. Содержание механизма обеспечения целостности данных.
20. Состав документации по системе защиты и ее содержание.
21. Содержание процедуры администрирования системы защиты данных.
22. Анализ и диагностика систем защиты компьютерных сетей.
23. Тестирование и диагностика защищенных систем связи.
24. Выбор оптимальной технологии проектирования СЗИ.
25. Сравнение проектирования СЗИ при различных технологиях.
26. Построение модели системы защиты информации.
27. Средства моделирования бизнес-процессов.

Курсовая работа выполняется обучающимся самостоятельно под руководством преподавателя. 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 начале изучения дисциплины преподаватель предлагает обучающимся на выбор перечень тем курсовых работ. Обучающийся самостоятельно выбирает тему курсовой работы. Совпадение тем курсовых работ у обучающихся одной учебной группы не допускается. Утверждение тем курсовых работ проводится ежегодно на заседании кафедры.

После выбора темы преподаватель формулирует задание по курсовой работе и рекомендует перечень литературы для ее выполнения. Исключительно важным является использование информационных источников, а именно системы «Интернет», что даст возможность обучающимся более полно изложить материал по выбранной им теме.

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

Преподаватель, проверив работу, может возвратить ее для доработки вместе с письменными замечаниями. Обучающийся должен устранить полученные замечания в установленный срок, после чего работа окончательно оценивается.

Курсовая работа должна быть оформлена в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления».

Примерный перечень тем курсовых работ и пример задания представлены в разделе 7 «Оценочные средства для проведения промежуточной аттестации».

7. Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент	Планируемые результаты обучения	Оценочные средства
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий		
Знать	– принципы построения и функционирования, примеры реализаций современных операционных систем; – принципы работы элементов и функциональных узлов электронной аппаратуры; – типовые схемотехнические решения основных узлов и блоков электронной аппаратуры	1. Теоретические основы проектирования информационных систем 2. Технологии проектирования ИС 3. Стандарты и профили в области информационных систем 4. Моделирование функциональной области внедрения ИС 5. Автоматизированное проектирование ИС 6. Типовое проектирование ИС 7. Проектирование процессов защиты данных 8. Управление проектированием ИС

Структурный элемент	Планируемые результаты обучения	Оценочные средства
Уметь:	– уметь определять особенности современных программных, технических средств и информационных технологий; – эксплуатировать современные программные, технические средства и информационные технологии; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;	1. Определить состав и функции подсистем, включаемых в систему защиты данных. 2. Определить состав и функции подсистемы «Подсистему регистрации и учета». 3. Определить состав и функции подсистемы «Подсистема обеспечения целостности». 4. Выполнить анализ и диагностику систем защиты компьютерных сетей. 5. Выполнить тестирование и диагностику защищенных систем связи. 6. Произвести выбор оптимальной технологии проектирования СЗИ. 7. Выполнить сравнение проектирования СЗИ при различных технологиях. 8. Выполнить построение модели системы защиты информации.
Владеть	– методикой эксплуатации современные программных, технических средств и информационных технологий; – навыками обеспечения безопасности информации с помощью типовых программных средств;	**Темы курсовых работ:** 1. Разработка проекта технического задания на создание автоматизированного рабочего мета конфиденциального делопроизводства. 2. Проектирование защищенной локальной вычислительной сети предприятия. 3. Разработка проекта технического задания на создание автоматизированного рабочего мета обработки персональных данных кадровой службы. 4. Выбор технологии проектирования систем защиты информации. 5. Информационная модель комплексной системы защиты информации. 6. Разработка проекта технического задания на создание локальной вычислительной сети обработки информации ограниченного доступа. 7. Разработка модели системы защиты персональных данных.

Структурный элемент	Планируемые результаты обучения	Оценочные средства
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности		
Знать	– источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;	1. Теоретические основы проектирования информационных систем 2. Технологии проектирования ИС 3. Стандарты и профили в области информационных систем 4. Моделирование функциональной области внедрения ИС 5. Автоматизированное проектирование ИС 6. Типовое проектирование ИС 7. Проектирование процессов защиты данных 8. Управление проектированием ИС
Уметь	– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;	1. Определить состав и функции подсистем, включаемых в систему защиты данных. 2. Определить состав и функции подсистемы «Подсистему регистрации и учета». 3. Определить состав и функции подсистемы «Подсистема обеспечения целостности». 4. Выполнить анализ и диагностику систем защиты компьютерных сетей. 5. Выполнить тестирование и диагностику защищенных систем связи. 6. Произвести выбор оптимальной технологии проектирования СЗИ. 7. Выполнить сравнение проектирования СЗИ при различных технологиях. 8. Выполнить построение модели системы защиты информации.
Владеть	– навыками разработки, документирования баз данных с учетом требований по	**Темы курсовых работ:** 1. Разработка проекта технического задания на создание автоматизированного рабочего мета конфиденциального делопроизводства.

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	обеспечению информационной безопасности; – методами формирования требований по защите информации; – навыками анализа основных узлов и устройств современных автоматизированных систем; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	2. Проектирование защищенной локальной вычислительной сети предприятия. 3. Разработка проекта технического задания на создание автоматизированного рабочего мета обработки персональных данных кадровой службы. 4. Выбор технологии проектирования систем защиты информации. 5. Информационная модель комплексной системы защиты информации. 6. Разработка проекта технического задания на создание локальной вычислительной сети обработки информации ограниченного доступа. 7. Разработка модели системы защиты персональных данных.
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем		
Знать	– методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; – современную нормативно-правовую базу создания защищенных распределенных информационных систем; – инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей	1. Теоретические основы проектирования информационных систем 2. Технологии проектирования ИС 3. Стандарты и профили в области информационных систем 4. Моделирование функциональной области внедрения ИС 5. Автоматизированное проектирование ИС 6. Типовое проектирование ИС 7. Проектирование процессов защиты данных 8. Управление проектированием ИС
Уметь	– разрабатывать и анализировать проектные решения по обеспечению	1. Определить состав и функции подсистем, включаемых в систему защиты данных. 2. Определить состав и функции подсистемы «Подсистему регистрации и учета». 3. Определить состав и функции подсистемы «Подсистема

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	безопасности автоматизированных систем; – применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем	обеспечения целостности». 4. Выполнить анализ и диагностику систем защиты компьютерных сетей. 5. Выполнить тестирование и диагностику защищенных систем связи. 6. Произвести выбор оптимальной технологии проектирования СЗИ. 7. Выполнить сравнение проектирования СЗИ при различных технологиях. 8. Выполнить построение модели системы защиты информации.
Владеть	– методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; – навыками разработки комплексной инфраструктуры защищенной информационной системы; – навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации	**Темы курсовых работ:** 1. Разработка проекта технического задания на создание автоматизированного рабочего мета конфиденциального делопроизводства. 2. Проектирование защищенной локальной вычислительной сети предприятия. 3. Разработка проекта технического задания на создание автоматизированного рабочего мета обработки персональных данных кадровой службы. 4. Выбор технологии проектирования систем защиты информации. 5. Информационная модель комплексной системы защиты информации. 6. Разработка проекта технического задания на создание локальной вычислительной сети обработки информации ограниченного доступа. 7. Разработка модели системы защиты персональных данных.
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем		
Знать	– способы анализа и оценки угроз информационной безопасности; нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной	1. Теоретические основы проектирования информационных систем 2. Технологии проектирования ИС 3. Стандарты и профили в области информационных систем 4. Моделирование функциональной области внедрения ИС 5. Автоматизированное проектирование ИС 6. Типовое проектирование ИС 7. Проектирование процессов защиты данных 8. Управление проектированием ИС

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	безопасности; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	
Уметь	– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; – разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной	1. Определить состав и функции подсистем, включаемых в систему защиты данных. 2. Определить состав и функции подсистемы «Подсистему регистрации и учета». 3. Определить состав и функции подсистемы «Подсистема обеспечения целостности». 4. Выполнить анализ и диагностику систем защиты компьютерных сетей. 5. Выполнить тестирование и диагностику защищенных систем связи. 6. Произвести выбор оптимальной технологии проектирования СЗИ. 7. Выполнить сравнение проектирования СЗИ при различных технологиях.

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	безопасности; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	8. Выполнить построение модели системы защиты информации.
Владеть	– навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; – навыками проведения экспериментально-исследовательских работ при аттестации автоматизированных систем – нормативными требованиями по защите информации; – навыками организации и обеспечения режима секретности	**Темы курсовых работ:** 1. Разработка проекта технического задания на создание автоматизированного рабочего мета конфиденциального делопроизводства. 2. Проектирование защищенной локальной вычислительной сети предприятия. 3. Разработка проекта технического задания на создание автоматизированного рабочего мета обработки персональных данных кадровой службы. 4. Выбор технологии проектирования систем защиты информации. 5. Информационная модель комплексной системы защиты информации. 6. Разработка проекта технического задания на создание локальной вычислительной сети обработки информации ограниченного доступа. 7. Разработка модели системы защиты персональных данных.

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

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета и экзамена.

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, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

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.

– на оценку **«неудовлетворительно»** (1 балл) – задание преподавателя выполнено частично, 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. Бухтояров, В.В. Поддержка принятия решений при проектировании систем защиты информации: Монография / В.В. Бухтояров, В.Г. Жуков, В.В. Золотарев. - М.: НИЦ ИНФРА-М, 2014. - 131 с. – Режим доступа: http://znanium.com/bookread.php?book=445551 Заглавие с экрана.– ISBN 978-5-16-009516-6.

2. 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 .

б) Дополнительная литература:

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] — М. : ДМК Пресс, 2014. — 702 с. Режим доступа: http://e.lanbook.com/view/book/50578/.– Заглавие с экрана.

2. Жук, А.П. Защита информации [Электронный ресурс]: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.- (Высшее образование: Бакалавриат; Магистратура). –Режим доступа: http://znanium.com/bookread.php?book=474838 .– Заглавие с экрана.– ISBN 978-5-369-01378-6.

в) Интернет – ресурсы:

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.

2. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

3. Государственная публичная научно-техническая библиотека России [Электронный ресурс] – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.

4. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз. рус.

5. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.

6. 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.

7. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/.– Загл. с экрана. Яз. рус.

9. Материально-техническое обеспечение дисциплины

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 (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; Архиватор 7zip - *GNU LGPL, бессрочная*; Система компьютерной математики MathCad - *43813518 D-1662-13 от 22.11.2013*; выход в Интернет.
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 (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

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03 Информационная безопасность автоматизированных систем. Специализация «Обеспечение информационной безопасности распределенных информационных систем».*