МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Директор ИЭиАС
С.И. Лукьянов
_____
26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7

Магнитогорск
2019 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО) ,
_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 01 сентября 2020 г. № 1

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __

Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Информационная безопасность распределенных информационных систем» является систематизация и обобщение у обучающихся понятий о методах анализа угроз и уязвимостей, проектируемых и эксплуатируемых распределенных информационных систем, моделей угроз и нарушителя информационной безопасности распределенных информационных систем, получение практических навыков проектирования средств защиты информации в распределенных информационных системах, построения распределенных информационных систем.

Овладение обучающимися необходимым и достаточным уровнем компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Информационная безопасность распределенных информационных систем входит в базовую часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Введение в специальность

Основы информационной безопасности

Организация ЭВМ и вычислительных систем

Технологии и методы программирования

Безопасность систем баз данных

Языки программирования

Сети и системы передачи информации

Технология построения защищенных распределенных приложений

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Подготовка к защите и защита выпускной квалификационной работы

Научно-исследовательская работа

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

В результате освоения дисциплины (модуля) «Информационная безопасность распределенных информационных систем» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-3 способностью проводить анализ защищенности автоматизированных систем	
Знать	Критерии оценки эффективности и надежности средств защиты распределенных информационных систем (РИС). Принципы построения и функционирования распределенных информационных систем в защищённом исполнении. Методики анализа и контроля защищенности РИС в защищённом исполнении.

Уметь	Анализировать техническую и сопроводительную документацию по обеспечению ИБ. Анализировать программные и архитектурно-технические решения компонентов автоматизированных систем в защищённом исполнении. Проводить выбор технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты.
Владеть	Навыками анализа основных узлов автоматизированных систем. Навыками анализа основных узлов автоматизированных систем в защищённом исполнении. Методами и технологиями проектирования, моделирования, исследования автоматизированных систем в защищённом исполнении.
ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	
Знать	Основы организационного и правового обеспечения ИБ. Основные нормативные и правовые акты в области обеспечения ИБ. Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. Методики проектирования АС в защищенном исполнении.
Уметь	Реализовывать разработанную автоматизированную систему с учетом требований ИБ. Организовывать реализацию разработанной АС с учетом требований информационной безопасности. Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.
Владеть	Навыками разработки автоматизированных систему с учетом требований ИБ. Навыками контроля разработки АС с учетом требований ИБ. Навыками контроля эффективности применения разработанной АС в защищенном исполнении. Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	
Знать	Принципы построения современных защищенных распределенных АС. Способы разработки политики безопасности распределенных ИС. Нормативные документы по стандартизации и сертификации программной защиты. Способы управления разработкой политики безопасности распределенных ИС. Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.

Уметь	Разрабатывать частные политики безопасности распределенных ИС. Проводить мониторинг и аудит защищенности информационно-технологических ресурсов распределенных ИС. Руководить разработкой и реализацией частных политики безопасности РИС. Осуществлять мониторинг и аудит безопасности АС.
Владеть	Методиками анализа политики безопасности РИС. Методиками разработки политики безопасности РИС. Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС. Методиками руководства разработкой политики безопасности РИС. Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС.
ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	
Знать	Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Способы координирования деятельности подразделений по ЗИ на предприятии, в учреждении, организации. Подходы создания междисциплинарных и инновационных проектов.
Уметь	Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации. Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации. Принимать участие в междисциплинарных и инновационных проектах.
Владеть	Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации. Навыками организации и реализации междисциплинарных и инновационных проектов.
ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	
Знать	Основные принципы организации программных и программно-аппаратных СЗИ. Основные подходы создания программных и программно- аппаратных СЗИ. Основные подходы и способы реализации СКЗИ.
Уметь	Проводить комплексное тестирование и отладку программных и программно-аппаратных СЗИ. Администрировать программные и программно-аппаратные СЗИ. Проводить комплексное тестирование и отладку СКЗИ. Администрировать СКЗИ.

Владеть	Навыками комплексного тестирования и отладки программных и программно-аппаратных систем защиты информации. Навыками администрирования программных и программно-аппаратных СЗИ. Навыками комплексного тестирования и отладки СКЗИ. Навыками администрирования СКЗИ.
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать	Основные положения методики моделирования угроз безопасности информации Основные положения базовой модели угроз безопасности ПДн при их обработке в ИС ПДн
Уметь	Применять методику моделирования угроз безопасности информации для разработки частных моделей угроз и нарушителя Применять базовую модель угроз безопасности ПДн для разработки частных моделей угроз и нарушителя ИС ПДн
Владеть	Навыками классификации угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных Навыками разработки частых моделей угроз безопасности информации
ПСК-7.3 способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	
Знать	Принципы организации распределенных корпоративных ИС. Основные этапы аудита информационной безопасности. Основные мероприятия при проведении аудита защищенности ИС
Уметь	Определять порядок организации информационного обмена между структурными подразделениями Обследовать системы на предмет наличия уязвимостей
Владеть	Методами оценки соблюдения требований стандартов и законов, на соответствие которым проводится аудит Навыками проведения инструментального анализа защищенности (оценка достаточности имеющихся и используемых на предприятии программных и

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе в форме практической подготовки 10 часов:
– контактная работа – 72 акад. часов:
– аудиторная – 68 акад. часов;
– внеаудиторная – 4 акад. часов
– самостоятельная работа – 36,3 акад. часов;
– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Методика построения системы ИБ предприятия								
1.1 Определение сведений, представляющих для организации интеллектуальную собственность. Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них. Этапы формирования Перечня	7	2		2/1И	2,3	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение индивидуального домашнего задания (ИДЗ).	ИДЗ-1	ПК-3, ПК-27, ОПК-5
1.2 Методика определения границ обеспечения ИБ		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-1	ПК-3, ПК-27, ОПК-5
1.3 Анализ рисков		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-1	ПК-3, ПК-27, ОПК-5

1.4 Методика выбора контрмер, обеспечивающих ИБ объекта		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС. Выполнение ИДЗ.	ИДЗ-1	ПК-3, ПК-27, ОПК-5
1.5 Методика выбор варианта ЗИ, в наибольшей степени удовлетворяющий заказчика. Математические методы оценки эффективности гипотетической СЗИ		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС. Выполнение ИДЗ.	ИДЗ-1	ПК-3, ПК-27, ОПК-5
1.6 Принципы разработки пакета планирующих документов по построению системы ИБ, с помощью и на основе которого реализуется принятая политика ИБ		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС. Выполнение ИДЗ.	ИДЗ-1	ПК-3, ПК-27, ОПК-5
Итого по разделу		12		12/6И	12,3			
2. Методики проведения мониторинга и аудита безопасности автоматизированной системы по требованиям безопасности информации								
2.1 Стандарты, используемые при проведении аудита безопасности информационных систем. Виды аудита информационной безопасности	7	1		1	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3

2.2 Этапы работ по проведению мониторинга и аудита безопасности автоматизированных информационных систем		1		1	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
2.3 Перечень документации на АИС.		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
2.4 Подходы к анализу данных мониторинга и аудита		2		2/2И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
2.5 Методика формирования рекомендаций, выдаваемые аудитором по результатам анализа состояния ИС		2		2/2И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
2.6 Структура отчета по результатам аудита безопасности ИС и анализу рисков		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3

2.7 Обзор программных продуктов, предназначенных для анализа и управления рисками.		2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
Итого по разделу		12		12/7И	12			
3. Коммуникация в распределенных информационных системах, проектирование системы защиты информации в распределенных информационных системах								
3.1 Организация безопасности сетевых подключений распределенных информационных систем.	7	2		2/1И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к контрольному тестированию (КТ).	КТ	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
3.2 Сложные распределенные системы-сферы применения		2		2	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	КТ	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
3.3 Централизованная и децентрализованная модель организации распределенных информационных систем		2		2	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	КТ	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3

3.4 Этапы работ по проектированию системы ИБ.		2		2	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС. Подготовка к КТ.	КТ	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
3.5 Перечень работы по внедрению системы ЗИ		2		2	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС. Подготовка к КТ.	КТ	ПК-20, ПК-27, ОПК-5
Итого по разделу		10		10/1И	12			
4. Экзамен								
4.1 Экзамен	7					Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС. Подготовка к экзамену.	Экзамен	ПК-3, ПК-20, ПК-27, ОПК-5, ОПК-3
Итого по разделу								
Итого за семестр		34		34/14И	36,3		экзамен	
Итого по дисциплине		34		34/14И	36,3		экзамен	ПК-3,ПК-27,ОПК-5,ПК-20,ОПК-3

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) **Традиционная технология**, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

a) ***Вводная лекция*** – для целостного представления об учебном предмете и анализа учебно-методической литературы;

b) ***Обзорные лекции*** – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

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

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

e) ***Практическое занятие***, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

f) ***Лабораторная работа*** – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) **Разделно-компетентностная технология**, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Разделно-компетентностной технологии:

a) ***Кейс-методы*** – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

3) **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 интерактивных технологий:

a) ***Case-study*** – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.

b) ***Методы IT*** – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

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

d) ***Семинар-дискуссия*** – коллективное обсуждение какого-либо спорного вопроса,

проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).

e) ***Контекстное обучение*** – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

f) ***Междисциплинарное обучение*** – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

4) **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:

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

b) ***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.).

c) ***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.

d) ***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. разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

5) **Игровые технологии** – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. Формы учебных занятий с использованием игровых технологий:

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

b) ***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.

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

6) **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 рефлексию. Основные типы проектов:

a) ***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).
b) ***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.).
c) ***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).

7) **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:
   a) ***Лекция-визуализация*** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
   b) ***Практическое занятие в форме презентации*** – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся с использованием методов IT .

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а также с применением Кейс-технологий. Ниже приведены данные по срокам, объему часов и ссылки на учебно-методическое обеспечение (источники) самостоятельной работы:

Задания и вопросы по разделам:

Раздел 1. Распределенные информационные системы: основные понятия:

Анализ угроз безопасности при обработке данных в распределенных информационных систем.

Цели и задачи построения информационных систем, их место в современном информационном обществе.

Классификация распределенных информационных систем, особенности работы.

Раздел 2. Автоматизированные системы и их связь с информационной безопасностью распределенных информационных систем:

Автоматизированные системы и их связь с информационной безопасностью распределенных информационных систем.

Концепция обеспечения информационной безопасности распределенных информационных систем.

Принципы построения системы защиты распределённой информационной

системы.

Комплект типовых документов и нормативных (законодательных) актов по эксплуатации и разработке распределенных информационных систем.

Проведение аудита и мониторинга распределенных информационных систем. Модульная работа, примеры концепции.

Раздел 3. Коммуникация в распределенных информационных системах, проектирование системы защиты информации в распределенных информационных системах:

Безопасность сетевых подключений распределенных информационных систем.

Сложные распределенные системы-сферы применения.

Централизованная и децентрализованная модель организации распределенных информационных систем.

7 Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-3 - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности**.**		
Знать	Основные принципы организации программных и программно-аппаратных СЗИ. Основные подходы создания программных и программно-аппаратных СЗИ. Основные подходы и способы реализации СКЗИ.	Вопросы к экзамену: 1. Основные принципы организации программных и программно-аппаратных СЗИ. 2. Обзор рынка имеющихся сертифицированных программных и программно-аппаратных СЗИ. 3. Обзор рынка имеющихся сертифицированных СКЗИ.
Уметь	Проводить комплексное тестирование и отладку программных и программно-аппаратных СЗИ. Администрировать программные и программно-аппаратные СЗИ. Проводить комплексное тестирование и отладку СКЗИ. Администрировать СКЗИ.	1. Провести тестирование работоспособности СЗИ «Страж NT». 2. Провести тестирование работоспособности СКЗИ «КриптоПро CSP». 3. Провести тестирование работоспособности СКЗИ «КРИПТОН-ЗАМОК».
Владеть	Навыками комплексного тестирования и отладки программных и программно-аппаратных систем защиты информации. Навыками администрирования программных и программно-аппаратных СЗИ. Навыками комплексного тестирования и отладки СКЗИ. Навыками администрирования СКЗИ.	1. Произвести снятие СКЗИ «КРИПТОН-ЗАМОК». Затем восстановить работоспособность и настроить СКЗИ. 2. Произвести аварийное снятие СЗИ. Затем восстановить подсистему идентификации и работоспособность основных служб СЗИ

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		«Страж NT».
ОПК-5 - способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами		
Знать	Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Способы координирования деятельности подразделений по ЗИ на предприятии, в учреждении, организации. Подходы создания междисциплинарных и инновационных проектов.	Вопросы к экзамену: 1. Принципы построения информационно-логической модели. 2. Принципы разработки пакета планирующих документов по построению системы ИБ, с помощью и на основе которого реализуется принятая политика ИБ.
Уметь	Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации. Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации. Принимать участие в междисциплинарных и инновационных проектах.	1. Составьте подробное описание прохождения критичной информации через все элементы выбранной СОИ и опишите все возможные точки атак. 2. Составить список ранжированных угроз для выбранного ОИ.
Владеть	Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации. Навыками организации и реализации междисциплинарных и инновационных проектов.	1. Распределите работы по проведению аудита среди обучающихся группы с учетом их возможностей. Оцените результаты их работы. 2. Распределите работы для расследования компьютерного инцидента среди обучающихся группы с учетом их возможностей. Оцените результаты их работы. 2. Распределите работы по предпроектному диагностическому обследованию среди обучающихся группы с учетом их возможностей. Оцените результаты их работы.
ПК-27 - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы		
Знать	Принципы построения современных защищенных	Вопросы к экзамену: 1. Математические методы

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	распределенных АС. Способы разработки политики безопасности распределенных ИС. Нормативные документы по стандартизации и сертификации программной защиты. Способы управления разработкой политики безопасности распределенных ИС. Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.	оценки эффективности гипотетической СЗИ. 2. Методика выбора контрмер, обеспечивающих ИБ объекта. 3. Методика выбор варианта ЗИ, в наибольшей степени удовлетворяющий заказчика. 4. Методика CRAMM. 5. Стандарты, используемые при проведении аудита безопасности ИС.
Уметь	Разрабатывать частные политики безопасности распределенных ИС. Проводить мониторинг и аудит защищенности информационно-технологических ресурсов распределенных ИС. Руководить разработкой и реализацией частных политики безопасности РИС. Осуществлять мониторинг и аудит безопасности АС.	1. Разработайте частную политику безопасности для выбранного предприятия. 2. Сформируйте совокупность вариантов построения СЗИ, которые характеризуются различными значениями показателей эффективности. 3. Составьте перечень детальной информация о структуре ИС необходимой для аудита выбранного предприятия.
Владеть	Методиками анализа политики безопасности РИС. Методиками разработки политики безопасности РИС. Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС. Методиками руководства разработкой политики безопасности РИС. Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС.	1. Сформируйте совокупность правовых, организационных и инженерно-технических мероприятий, для формирования частной политики безопасности выбранного предприятия. 2. Проведите анализ данных аудита выбранного предприятия, используя подход основанный на использовании стандартов ИБ. 3. Сформируйте примерную структуры аудиторского отчета по результатам анализа рисков, связанных с осуществлением угроз безопасности в отношении обследуемой ИС.
ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности.		
Знать	Основы организационного и правового обеспечения ИБ. Основные нормативные и правовые акты в области	Вопросы к экзамену: 1. Методика выявления сведений, представляющих интеллектуальную

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	обеспечения ИБ. Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. Методики проектирования АС в защищенном исполнении.	собственность, и организаций, заинтересованных в них. 2. Этапы формирования Перечня сведений, содержащих служебную или коммерческую тайну, для структурных подразделений (отделов, служб) организации. 3.Подсистемы интегрированной архитектуры систем ИБ.
Уметь	Реализовывать разработанную автоматизированную систему с учетом требований ИБ. Организовывать реализацию разработанной АС с учетом требований информационной безопасности. Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.	1. Разработайте ТЗ на создание системы информационной безопасности для выбранного ОИ. 2. Разработайте ТЗ на создание системы информационной безопасности для выбранной АИС. 3. Разработайте архитектуру системы ИБ.
Владеть	Навыками разработки автоматизированных систему с учетом требований ИБ. Навыками контроля разработки АС с учетом требований ИБ. Навыками контроля эффективности применения разработанной АС в защищенном исполнении. Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении.	1. Разработайте модель системы управления ИБ (на основе процессно-ролевой модели) для выбранного ОИ. 2. Разработайте модель системы управления ИБ (на основе процессно-ролевой модели) выбранной АИС. 3. Разработайте технически-рабочий проект создания системы ИБ.
ПК-3 - Способностью проводить анализ защищенности автоматизированных систем.		
Знать	Критерии оценки эффективности и надежности средств защиты распределенных информационных систем. Принципы построения и функционирования распределенных информационных систем в защищённом исполнении. Методики анализа и контроля защищенности РИС в защищённом исполнении.	Вопросы к экзамену: 1. Определение сведений, представляющих для организации интеллектуальную собственность. 2. Примерный перечень сведений, составляющих служебную или коммерческую тайну организации. 3. Этапы работ по проектированию системы

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		ИБ.
Уметь	Анализировать техническую и сопроводительную документацию по обеспечению ИБ. Анализировать программные и архитектурно-технические решения компонентов автоматизированных систем в защищённом исполнении. Проводить выбор технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты.	1. Составьте предварительный Перечень сведений, содержащих служебную или коммерческую тайну, для структурных подразделений (отделов, служб) выбранной организации. 2. Определите возможный ущерб, в результате несанкционированного распространения сведений, включаемых в Перечень для выбранного предприятия. 3. Определите затраты на защиту рассматриваемых сведений для выбранного предприятия. 4. Определите перечень контрмер, обеспечивающих ИБ выбранного объекта.
Владеть	Навыками анализа основных узлов автоматизированных систем. Навыками анализа основных узлов автоматизированных систем в защищённом исполнении. Методами и технологиями проектирования, моделирования, исследования автоматизированных систем в защищённом исполнении.	1. Разработайте сценарий осуществления противоправных действий и список ранжированных угроз для выбранного предприятия. 2. Определите величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость для выбранного предприятия. 3. Создайте информационно-логическую модель для выбранного предприятия.
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах		
Знать	Основные положения методики моделирования угроз безопасности информации Основные положения базовой модели угроз безопасности ПДн при их обработке в ИС ПДн	1. Классификация угроз по используемым уязвимостям 2. Классификация угроз по объекту воздействия 3. Элементы описания угроз НСД 4. Общая характеристика источников угроз НСД в ИС ПДн 5. Уязвимости отдельных протоколов стека протоколов TCP/IP

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Уметь	Применять методику моделирования угроз безопасности информации для разработки частных моделей угроз и нарушителя Применять базовую модель угроз безопасности ПДн для разработки частных моделей угроз и нарушителя ИС ПДн	1. Составить карту уязвимостей прикладного программного обеспечения Google Chrome 2. Составить карту атак для реализации угроз стека протоколов TCP/IP
Владеть	Навыками классификации угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных Навыками разработки частых моделей угроз безопасности информации	1. Классифицировать нарушителей выбранной ИС ПДн 2. Разработать частную модель угроз выбранной ИС
ПСК-7.3 способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем		
Знать	Принципы организации распределенных корпоративных ИС. Основные этапы аудита информационной безопасности. Основные мероприятия при проведении аудита защищенности ИС	1. Аудита безопасности с точки зрения злоумышленника 2. Определение направления потенциальных угроз 3. Схема реализации угрозы "Анализ сетевого трафика" 4. Схема реализации угрозы "Подмена доверенного объекта сети" 5. Схемы реализации атаки "Навязывание ложного маршрута" 6. Схема реализации угрозы "Внедрение ложного ARP-сервера"
Уметь	Определять порядок организации информационного обмена между структурными подразделениями Обследовать системы на предмет наличия уязвимостей	1. Составить список уязвимостей прикладного программного обеспечения используемого на выбранном ОИ
Владеть	Методами оценки соблюдения требований стандартов и законов, на соответствие которым проводится аудит	1. Реализовать атаку перехвата трафика на спроектированной по выбранному варианту

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	Навыками проведения инструментального анализа защищенности (оценка достаточности имеющихся и используемых на предприятии программных и технических СЗИ и полноты их использования)	виртуальной ИС 2. Реализовать атаку на DHCP Server на спроектированной по выбранному варианту виртуальной ИС

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

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** – обучающийся должен показать 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»** – обучающийся должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку **«удовлетворительно»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«неудовлетворительно»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 24.02.2020).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж: Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 26.02.2020)

б) Дополнительная литература:

1. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 26.02.2020)

2. Брюхомицкий, Ю. А. Искусственные иммунные системы в информационной безопасности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 147 с. - ISBN 978-5-9275-3212-4. - Текст: электронный. - URL:

https://new.znanium.com/catalog/product/1088177 (дата обращения: 26.02.2020)

Архитектура и принципы работы вычислительных систем [Электронный ресурс] : учебное пособие [для вузов] / В.В. Баранков, И.И. Баранкова, М.В. Афанасьева, М.В. Коновалов; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1306-6 URL : https://magtu.informsystema.ru/uploader/fileUpload?name=3924.pdf&show=dcatalogues/1/1530495/3924.pdf&view=true . – Макрообъект*.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта.

Примечание: при открытии макрообъектов учитывать особенности настройки антивирусной защиты.

в) Методические указания:

1. Баранкова И.И. Определение перечня защищаемых ресурсов и их критичности [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Моделирование угроз информационной безопасности» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Баранкова И.И., Пермякова О.В.. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 18 с.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое	бессрочно
LibreOffice	свободно распространяемое	бессрочно
Браузер Yandex	свободно распространяемое	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
СЗИ Страж NT в.3	К-271-12 от 16.10.2012	бессрочно
СКЗИ КриптоПро CSP	К-271-12 от 16.10.2012	бессрочно

FAR Manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Федеральная служба по техническому и экспортному контролю России (ФСТЭК	URL: www.fstec.ru
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Федеральное агентство по техническому регулированию и метрологии (Росстандарт)	URL: https://www.rst.gov.ru/portal/gost/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:
- Мультимедийные средства хранения, передачи и представления информации.

Компьютерный класс:
- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Лаборатория программно-аппаратных средств обеспечения информационной безопасности:

1. Комплекс программно-аппаратный ViPNet Coordinator HW100C
2. Средство ограничения доступа к компьютеру "КРИПТОН-ЗАМОК/У"
3. Средство ограничения доступа к компьютеру "КРИПТОН-ЗАМОК/Е"(2 шт)
4. СКЗИ Крипто БД (лицензия: договор К-271-12 от 16.10.12)
5. Комплекс программно-аппаратный ViPNet Coordinator HW1000
6. Комплекс программно-аппаратный ViPNet Coordinator HW1000
7. Электронный ключ Guardant
8. Электронный ключ Etoken
9. Система защиты информации от несанкционированного доступа СТРАЖ NT(версия 3.0)
10. Устройство идентификации (Электронный ключ Guardant ID сертифицированный)
11. Компьютер Destene Volution i560 на базе Windows Server 2008 R2(Standart) MSDN
12. ПЭВМ на базе Windows 7 – 12 шт

Помещения для самостоятельной работы обучающихся:
- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.