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)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 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	5
Семестр	9

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

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 в структуре ООП подготовки специалиста

Дисциплина «Информационная безопасность распределенных информационных систем» входит в цикл дисциплин (базовая часть) Б1.Б.36 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Для усвоения данной дисциплины обучающемуся необходим объём знаний, умений и владений предусмотренный курсами «Введение в специальность», «Основы информационной безопасности», «Безопасность систем баз данных», «Организации ЭВМ и вычислительных систем», «Технологии и методы программирования», «Языки программирования», «Сети и системы передачи информации», «Технологии построения защищенных распределенных приложений», «Методы проектирования защищенных распределенных информационных систем» и т.д. Данная дисциплина необходима для последующего успешного выполнения научно-исследовательской работы и ВКР.

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

В результате освоения дисциплины «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. 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.

Структурный элемент компетенции	Планируемые результаты обучения
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.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы 144 акад. часа, в форме практической подготовки 10 часов, в том числе:

– контактная работа – 72 акад. часов:

– аудиторная – 68 акад. часов;

– внеаудиторная – 4 акад. часа;

– самостоятельная работа – 36,3 акад. часов;

– подготовка к экзамену – 35,7 акад. часа.

Форма аттестации – Экзамен.

Раздел дисциплины	Семестр	**Аудиторная контактная работа (в акад. часах)**			**Вид самостоятельной работы**	**Формы текущего контроля успеваемости и**	**Код и структурный**
		Лекции	Практич.	раб.Самост.			
Раздел 1. Методика построения системы ИБ предприятия. Тема 1.1. Определение сведений, представляющих для организации интеллектуальную собственность. Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них. Этапы формирования Перечня. Тема 1.2. Методика определения границ обеспечения ИБ. Тема 1.3. Анализ рисков. Тема 1.4. Методика выбора контрмер, обеспечивающих ИБ объекта. Тема 1.5. Методика выбор варианта ЗИ, в наибольшей степени удовлетворяющий заказчика. Математические методы оценки эффективности гипотетической СЗИ. Тема 1.6. Принципы разработки пакета планирующих документов по построению системы ИБ, с помощью и на основе которого реализуется принятая политика ИБ.	9	12	12/ 5И	12,3	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-1	ПК-3-зув ПК-27-зув ОПК-5-зув
Раздел 2. Методики проведения мониторинга и аудита безопасности автоматизированной системы по требованиям безопасности информации. Тема 2.1. Стандарты, используемые при проведении аудита безопасности информационных систем. Виды аудита информационной безопасности. Тема 2.2. Этапы работ по проведению мониторинга и аудита безопасности автоматизированных информационных систем. Тема 2.3. Перечень документации на АИС. Тема 2.4. Подходы к анализу данных мониторинга и аудита.	9	12	12/ 5И	12	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Выполнение ИДЗ.	ИДЗ-2	ПК-3-зув ПК-27-зув ОПК-5-зув ОПК-5-зув

Тема 2.5. Методика формирования рекомендаций, выдаваемые аудитором по результатам анализа состояния ИС. Тема 2.6. Структура отчета по результатам аудита безопасности ИС и анализу рисков. Тема 2.7. Обзор программных продуктов, предназначенных для анализа и управления рисками.							
Раздел 3. Коммуникация в распределенных информационных системах, проектирование системы защиты информации в распределенных информационных системах. Тема 3.1. Организация безопасности сетевых подключений распределенных информационных систем. Тема 3.2. Сложные распределенные системы-сферы применения. Тема 3.3. Централизованная и децентрализованная модель организации распределенных информационных систем. Тема 3.4. Этапы работ по проектированию системы ИБ. Тема 3.5. Перечень работы по внедрению системы ЗИ.	9	10	10/ 10И	12	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	КТ-1	ПК-20-зув ПК-27-зув ОПК-5-зув
Экзамен	9			35,7	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к экзамену.	Экзамен	ПК-3-зув ПК-27-зув ОПК-5-зув ОПК-5-зув ПК-20-зув
Итого по курсу:		**34**	**34/ 20И**	**36,3 + 35,7**	**144**		

И – занятия в интерактивной форме, СР – самостоятельная работа, АКР – аудиторная контрольная работа, ИДЗ – индивидуальное домашнее задание, КТ – контрольное тестирование.

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:

а) ***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 так же 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 «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.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		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 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.	Вопросы к экзамену: 1. Математические методы 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 обеспечения ИБ. Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. Методики проектирования АС в защищенном исполнении.	Вопросы к экзамену: 1. Методика выявления сведений, представляющих интеллектуальную 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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		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 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,	1. Разработайте сценарий осуществления противоправных действий и список ранжированных угроз для выбранного предприятия. 2. Определите величины рисков для каждой тройки: угроза – группа ресурсов –

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	моделирования, исследования автоматизированных систем в защищённом исполнении.	уязвимость для выбранного предприятия. 3. Создайте информационно-логическую модель для выбранного предприятия.

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

а) Основная литература:

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - Режим доступа: http://znanium.com/bookread.php?book=405000 .–Заглавие с экрана. - ISBN 978-5-369-01178.

2. Информационная безопасность и защита информации: [Электронный ресурс]: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. - Режим доступа:http://znanium.com/bookread2.php?book=957144. - Загл. с экрана. – ISBN 978-5-369-01761-6.

б) Дополнительная литература:

1. Ажмухамедов И.М. Основы организационно-правового обеспечения информационной безопасности: [Электронный ресурс]: учеб. пособие / И.М. Ажмухамедов, О.М. Князева. - СПб.: Издательский центр «Интермедия», 2017. – 264 с. - Режим доступа: https://ibooks.ru/product.php?productid=356930 - Загл. с экрана. - ISBN: 978-5-4383-0160-8.

2. Унижаев Н.В. Информационно-аналитическое обеспечение безопасности организации: [Электронный ресурс]: учеб. пособие / Н.В. Унижаев - СПб.: Издательский центр «Интермедия», 2018. – 408с. - Режим доступа: https://ibooks.ru/product.php?productid=356934. - Загл. с экрана. - ISBN: 978-5-4383-0158-5.

3. Царегородцев А.В. Методы и средства защиты информации в государственном управлении: [Электронный ресурс]: учеб. пособие / А.В. Царегородцев, М.М. Тараскин. - Москва: Проспект, 2017. - 208 с. - Режим доступа: https://ibooks.ru/product.php?productid=356008 . - Загл. с экрана. - ISBN: 978-5-392-20353-6.

4. Баркалов С.А. Информационная безопасность при управлении техническими системами: [Электронный ресурс]: учеб. пособие /, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов. – СПб.: ИЦ «Интермедия», 2016. – 528с.: илл. - 208 с. - Режим доступа: https://ibooks.ru/product.php?productid=356935 - Загл. с экрана. - ISBN: 978-5-4383-0133-2.

5. Информационная безопасность и защита информации: [Электронный ресурс]: учеб. пособие / Баранова Е.К., Бабаш А.В. - 3-е изд., перераб. и доп. - М. : РИОР: ИНФРА-М, 2017. - 322 с. - Режим доступа: http://znanium.com/bookread2.php?book=763644. - Загл. с экрана. – ISBN 978-5-369-01450-9.

в) Программное обеспечение и Интернет-ресурсы:

1. Журнал Information Security. Информационная безопасность [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
2. Журнал «Безопасность информационных технологий» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.
3. Журнал «Вопросы кибербезопасности» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
4. «Журнал сетевых решений LAN»: [Электронный ресурс]: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". – Режим доступа: http://www.osp.ru/os/ – Загл. с экрана. Яз. рус.
5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз. рус.
6. Российская национальная библиотека. [Электронный ресурс] / – Режим доступа: http://www.nlr.ru. Яз. рус.
7. Безопасник [Электронный ресурс]. – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.
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.
9. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/.– Загл. с экрана. Яз. рус.

9. Материально-техническое обеспечение дисциплины (модуля)

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 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.
Лаборатория программно-аппаратных средств защиты информации, ауд. 2124	**Система компьютерной защиты информации КриптоПро CSP.** Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636C-Y0000- 01W74-WPDLF- QQBYU, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» версии 3.6 на сервере MS Windows (Серийный номер: 36369-V0000-02NGL-YN8P4- YNFR0, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636E-D0000- 01CHL-ZV2NZ- TXXDZ, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS (Серийный номер: 3636E-H0000- 01LB9-TFBF0- 9MPEX, бессрочная);

Тип и название аудитории	Оснащение аудитории
	Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 36363-L0000- 01Z7X-AQ47B- CGF5M, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 36362-10000-01E6F- TTA6U-4BVAD, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636W-50000- 01CR0-4C5Y2- 5WDH9, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 36364-R0000- 0136K-K81XR DLN6G, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636W-H0000- 01TAY-OLZOM- EQ0M6, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636U-V0000-0108W-CM6XF-H9763, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636W-Q0000- 01NKG-UD8N1- 5MUHQ, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636V-K0000-01CNV-GFKKA- DDDVQ, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636M- 30000-01CCB- A5EQL-YH02R, бессрочная). Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021). СЗИ от НСД Страж NT 3.0 № лицензии: D1B4D8C0F28854B0, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: 49F19FCF20457E46, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: B0CE6203861DE71A, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: 3DDCF2F25EB5446D, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: 0F984E80A43783D3, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: E5593458BB84BB40, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: FEFFCC97CAE0DCF5, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: 58PE4EEF00376D64, бессрочная; СЗИ от НСД Страж NT 3.0 № лицензии: E6F42E5B5704A2D7, бессрочная; СЗИ от НСД Страж NT 3.0 N° лицензии: 42D08B0C46D41EA3, бессрочная; СЗИ от НСД Страж NT 3.0 N° лицензии: 14AB5EB9CC9C3790, бессрочная; СЗИ от Нед Страж NT 3.0 № лицензии: D6125FCAB3A84B9F, бессрочная.
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	Комплект учебного оборудования «Системы контроля доступа», «Системы видеонаблюдения».
Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021);

Тип и название аудитории	Оснащение аудитории
библиотеки.	Пакет MS Office (Microsoft Open License 42649837, бессрочная); Выход в Интернет и 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».*