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)

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ 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	3, 4
Семестр	6, 7, 8

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 «Разработка и эксплуатация защищенных автоматизированных систем» является изучение обучающимися основных подходов анализа безопасности сложных систем, средств защиты информации, используемыми в составе АС в защищенном исполнении; в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Разработка и эксплуатация защищенных автоматизированных систем входит в базовую часть учебного плана образовательной программы.

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

Основы информационной безопасности

Программно-аппаратные средства обеспечения информационной безопасности

Организационное и правовое обеспечение информационной безопасности

Безопасность сетей ЭВМ

Методы выявления нарушений информационной безопасности, аттестация АИС

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

Информационная безопасность распределенных информационных систем

Анализ рисков информационной безопасности

Управление информационной безопасностью

Производственная-преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

Подготовка к защите и защита выпускной квалификационной работы

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

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

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

Структурный элемент компетенции	Планируемые результаты обучения
ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать	□ понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем □ основные принципы построения защищенных распределенных компьютерных систем □ документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. □ современные принципы построения архитектуры ИС.

Уметь	□ осуществлять анализ несложных процессов проектирования □ применять государственные стандарты при проектировании автоматизированных систем в защищенном исполнении □ разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов
Владеть	□ приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем □ приемами разработки проектов нормативных документов, регламентирующих работу по защите информации □ навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	
Знать	□ типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ □ способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы;
Уметь	□ осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ □ применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы □ применять новые информационные технологии в сфере защиты данных
Владеть	□ методами исследования новых образцов программных, технических средств и информационных технологий, применяемых в области информационной безопасности
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	

Знать	• уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; • требования к разработке и производству, проведению испытаний, поддержке безопасности СЗИ для определения уровня доверия • положение о системе сертификации средств защиты информации; • продукцию, которую необходимо сертифицировать; • состав участников системы сертификации и их основные функции; • этапы сертификации; • требования к защищенность информации в автоматизированных системах; • требования к проведению испытаний СЗИ; • порядок проведения сертификационных испытаний.
Уметь	• составлять техническое задание на выполнение работ по проведению сертификационных испытаний; • составлять акт отбора образца; • подать заявку на сертификацию; • оформить экспертное заключение и проект сертификата соответствия по результатам сертификации.
Владеть	• навыками проведения испытаний средств защиты информации, а также обеспечения безопасности средств защиты информации в ходе их применения

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 176,9 акад. часов:

– аудиторная – 170 акад. часов;

– внеаудиторная – 6,9 акад. часов

– самостоятельная работа – 111,4 акад. часов;

– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - зачет, курсовая работа, 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. Защищенные автоматизированные системы. Основные понятия и классификация								
1.1 Классификация АС. Информационные технологии, используемые в АС. Жизненный цикл АС. Современные принципы построения архитектуры АИС.	6	4		8/4И	14	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9, ОПК-8, ПК-15
Итого по разделу		4		8/4И	14			
2. Разработка защищенных АС								
2.1 Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении (АСЗИ). Последовательность и содержание этапов разработки АС. Формирование требований к АСЗИ.	6	3		4/2И	10	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9, ОПК-8

2.2 Методы, способы и средства обеспечения отказоустойчивости АСЗИ		2		10/2И	20	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы; - индивидуальные задания.	ПК-9, ОПК-8, ПК-15
2.3 Разработка АСЗИ. Выбор мер защиты информации для реализации в АС		8		12/6И	12,05	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9, ОПК-8, ПК-15
Итого по разделу		13		26/10И	42,05			
Итого за семестр		17		34/14И	56,05		зачёт	
3. Основы эксплуатации защищенных АС								
3.1 Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС.	7	6		6/2И	4	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9, ПК-15
3.2 Анализ защищенности АС		8		6	4	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9, ПК-15

3.3 Организация технического обслуживания защищённых АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.		8		6	2	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9, ПК-15
Итого по разделу		22		18/2И	10			
4. Основы администрирования АС								
4.1 Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования.	7	6		8/6И	7,2	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9
Итого по разделу		6		8/6И	7,2			
5. Безопасность критической информационной инфраструктуры РФ								
5.1 ФЗ от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Субъекты КИИ. Значимые объекты КИИ. Категорирование объектов КИИ. Обеспечения безопасности объектов КИИ.	7	4		4/4И	6	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы	ПК-9, ПК-15
5.2 Указ президента №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ». Функции центров ГосСОПКА. Правила эксплуатации центров ГосСОПКА. Построения собственного центра ГосСОПКА.		2		4/2И	15	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы; - индивидуальные задания.	ПК-9, ПК-15, ОПК-8
Итого по разделу		6		8/6И	21			
Итого за семестр		34		34/14И	38,2		зачёт	
6. Сертификации средств защиты информации автоматизированных систем								

6.1 Положение о системе сертификации средств защиты информации. Состав участников системы сертификации и их основные функции	8	3		4/4И	2	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы.	ПК-15
6.2 Руководящие нормативные и методические документы в системе сертификации средств защиты информации. Сертификация автоматизированных систем, средств вычислительной техники, межсетевых экранов, программного обеспечения.		2		8	1	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы.	ПК-15
6.3 Требования по безопасности информации. Уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий		6		10/5И	6,15	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы.	ПК-15
6.4 Порядок сертификационных испытаний. Подготовка к проведению сертификационных испытаний программного обеспечения в системе сертификации ФСТЭК России		6		12/5И	8	Подготовка к практическим занятиям Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС.	– устный опрос (собеседование); – контрольные работы.	ПК-15, ПК-9, ОПК-8
Итого по разделу		17		34/14И	17,15			
Итого за семестр		17		34/14И	17,15		экзамен,кр	
Итого по дисциплине		68		102/42 И	111,4		зачет, курсовая работа, экзамен	ПК-9,ОПК-8,ПК-15

5 Образовательные технологии

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

Формы учебных занятий с использованием традиционных технологий:

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

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

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

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

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

Формы учебных занятий с использованием технологий проблемного обучения:

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

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

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

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

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

Формы учебных занятий с использованием игровых технологий:

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

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

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

4. Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и

задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлксию.

Основные типы проектов:

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

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

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

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

Формы учебных занятий с использованием специализированных интерактивных технологий:

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

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

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

Формы учебных занятий с использованием информационно-коммуникационных технологий:

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

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

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Перечень тем практических занятий

Технологии создания отказоустойчивых АС

Нормативно-методическая база создания защищенных автоматизированных систем.

Идентификация, спецификация и оценивание объектов защиты и угроз безопасности в объекте информатизации.

Классы защищенности и функциональные требования по защите информации в АС.

Показатели защищенности автоматизированных систем и СВТ.

Требования безопасности к изделиям ИТ

Предпроектные работы при создании АС

Стадии и этапы создания ЗАС и требования по защите информации.

Разработка технического задания на создание защищенной АС или системы защиты информации АС.

Синтез программно-аппаратных средств ЗАС.

Структура подсистем защиты информации от несанкционированного доступа (НСД).

Методы, способы и средства обеспечения отказоустойчивости ЗАС.

Разработка профиля защиты изделия ИТ и задания по безопасности при создании изделия ИТ.

Технологии и средства проектирования АС.

Управление проектированием, планирование работ

Содержание и система эксплуатации защищенной АС.

Оценка защищенности на этапах жизненного цикла ЗАС

Администрирование СЗИ.

Мониторинг ЗАС и защита от вторжений.

Эксплуатационная документация СЗИ АС.

Уровни доверия СЗИ АС

Общий порядок проведения сертификации СЗИ

Сертификация автоматизированных систем

Сертификация межсетевых экранов

Сертификация ПО

Сертификационные испытания программного обеспечения

Перечень тем устных опросов

1) Основные понятия и определения стандартов и руководящих документов.

2) Основные положения «Концепции защиты СВТ и АС от НСД к информации»

3) Определение перечней защищаемых ресурсов и их критичности.

4) Основные подходы к защите данных от НСД.

5) Иерархический доступ к информации

6) Доступ к данным со стороны процесса.

7) Методы опознавания пользователей

8) Аппаратные средства опознавания пользователей

9) Определение перечня защищаемых ресурсов и их критичности

10) Основные положения базовой модели угроз безопасности.

12) Основные положения модели нарушителя ИБ.

13) Общая классификация методов и средств ЗИ в АС

14) Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.

15) Классы защищенности и функциональные требования по защите информации в АС.

16) Автоматизированные системы и требования к ним.

17) Порядок создания и проектирования защищенных КС.

18) Методы, способы и средства обеспечения отказоустойчивости ЗАС.

19) Задачи ведения системного журнала

20) Средства активного аудита компьютерных систем

21) Требования к составу документации, а также номенклатура показателей защищенности средств вычислительной техники (СВТ)

22) Основные положения руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации»

23) Основные положения руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»

25) Участники системы сертификации и их основные функции
25) Общий порядок проведения сертификации СЗИ
25) Виды сертификационных испытаний

Примерные задания

Задание 1 Составить блок-схему общего порядка проведения сертификационных испытаний ПО СЗИ.

Задание 2. Подобрать СЗИ согласно модели угроз безопасности персональных данных заданной ИСПДн

7 Оценочные средства для проведения промежуточной аттестации

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

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий		
Знать:	– типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ – способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы;	1. Назначение и возможности аппаратно-программных средств защиты информации 2. Выбор мер защиты информации для реализации в информационной системе. 3. Защита информационной системы, ее средств, систем связи и передачи данных 4. Защита от вредоносного программного обеспечения 5. Программно-аппаратные комплексы средств защиты информации от НСД
Уметь:	– осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ; – применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы; – применять новые информационные технологии в сфере защиты данных.	Определить перечень СЗИ согласно требованиям к функциям подсистемы обеспечения безопасности информации типовой модели угроз безопасности персональных данных при их обработке в системе обеспечения вызова экстренных оперативных служб по единому номеру «112»

Владеть:	– методами исследования новых образцов программных, технических средств и информационных технологий, применяемых в области информационной безопасности	**Задание.** Провести тестирование работоспособности СЗИ «Страж NT».
ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать:	– понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем – основные принципы построения защищенных распределенных компьютерных систем – документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. современные принципы построения архитектуры ИС.	1. Понятие, виды и структура автоматизированных систем 2. Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения безопасности информации в АС. 3. Система и структура функциональных требований по защите от НСД в АС, группы и классы защищенности АС. 4. Общая структура требований безопасности к изделиям и системам ИТ, классы функциональных требований безопасности. 5. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении. 6. Анализ защищенности АС
Уметь:	– осуществлять анализ несложных процессов проектирования – применять государственные стандарты при проектировании автоматизированных систем в защищенном исполнении –разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	***Задание*** Составить техническое задание на создание системы защиты ПДн, обрабатываемых в распределенных информационных системах, имеющих подключение к сетям связи общего пользования.
Владеть:	– приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем – приемами разработки проектов нормативных документов,	***Задание.*** Разработать защиту объекта информатизации: Объект 2 категории. 3 здания, 50 помещений, наличие прилегающей территории, подлежащей контролю. Штат 100 человек. СВТ 150 ед., 5 серверов, распределенная сеть, выход в

	регламентирующих работу по защите информации навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	глобальные сети. Два выделенных помещения; 2 объекта вычислительной техники. Исходя из прикладного назначения ОИ следует обоснованно выбрать (рекомендовать к применению): - класс защищенности автоматизированной системы (АС), которая производит хранение и обработку конфиденциальной информации на объекте информатизации, - класс защищенности средств вычислительной техники (СВТ), составляющих аппаратно-программную поддержку автоматизированной системы, - класс межсетевых экранов (МЭ) по уровню защищенности от НСД, реализующих защиту внутренней вычислительной сети ОИ, - класс применяемых на ОИ антивирусных средств, - уровень контроля программного обеспечения средств защиты информации. В проекте защиты следует использовать сертифицированные средства и системы, прошедшие сертификацию не ниже выбранных классов.
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем		
Знать:	– уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; – требования к разработке и производству, проведению испытаний, поддержке безопасности СЗИ для определения уровня доверия; – положение о системе сертификации средств защиты информации; – продукцию, которую	1. Что понимают под сертификацией? 2. Основные отличия сертификации от лицензирования и аттестации. 3. Сколько участников входит в процесс сертификации ФСТЭК России? 4. Перечислите основные этапы сертификации. 5. Виды сертификационных испытаний. 6. Назовите основные отличия инспекционного контроля от

	необходимо сертифицировать; – состав участников системы сертификации и их основные функции; – этапы сертификации; – требования к защищенность информации в автоматизированных системах; – требования к проведению испытаний СЗИ; – порядок проведения сертификационных испытаний.	сертификационных испытаний. 7. Перечислите основные руководящие документы в области сертификации СЗИ. 8. Какие существуют этапы при отборе образца продукции при проведении сертификационных испытаний? 9. Основные положения руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». 10. Основные положения руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». 11. Основные положения руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации». 12. Основные положения руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». 13. Общий порядок проведения сертификации СЗИ. 14. Виды сертификационных испытаний.
Уметь:	– составлять техническое задание	**Задание**

	на выполнение работ по проведению сертификационных испытаний; – составлять акт отбора образца; – подать заявку на сертификацию; – оформить экспертное заключение и проект сертификата соответствия по результатам сертификации.	Составить заявку на сертификацию в федеральный орган по сертификации, которая должна включать: • наименование заявителя; • наименования продукции, которую Заявитель просит сертифицировать; • перечень нормативных и методических документов, на соответствие требованиям, которых Заявителю необходимо сертифицировать продукцию; • предложения Заявителя по выбору испытательной лаборатории, которая будет проводить сертификационные испытания; • дополнительные условия или сведения
Владеть:	– навыками проведения испытаний средств защиты информации, а также обеспечения безопасности средств защиты информации в ходе их применения	**Задание** 1. Выбрать любое свободное ПО. Найти всю возможную информацию о продукте (техническую и функциональную) необходимую для его дальнейшей сертификации. 2. Составить соглашение о неразглашении (NDA) между испытательной лабораторией и заявителем. 3. Определить используемую общественную лицензию, под которой распространяется выбранное ПО, и обозначить основные отличия от других существующих лицензий. 4. Определить достаточность найденных материалов для проведения сертификации. Описать какие входные данные дополнительно необходимы для проведения сертификационных работ.

Примерные темы курсовых работ:

1. Разработка концепции защищенной автоматизированной системы предприятия (по видам деятельности).

2. Разработка эффективных систем защиты информации в автоматизированных системах.

3. Разработка системы программно-аппаратной защиты автоматизированной системы объекта информатизации.

4. Разработка проекта СЗИ от НСД для АС учреждения.

5. Интеграция средств информационной безопасности в технологическую среду.

6. Формирование правил функционирования подразделений службы информационной безопасности.

7. Эксплуатация комплексной системы защиты информации на объекте защиты.

8. Выявление защищаемой информации и анализ структуры автоматизированной системы объекта информатизации.

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

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

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

Показатели и критерии оценивания экзамена:.

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

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

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

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

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

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

Показатели и критерии оценивания курсовой работы:

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

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

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

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

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. 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)

2. Зашита 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)

б) Дополнительная литература:

1. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true . - Макрообъект*. - ISBN 978-5-9967-1031-7.

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/441287 (дата обращения: 24.02.2020).

*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. Методические указания по выполнению практических работ. (Приложение 1.)
2. Методические указания по выполнению внеаудиторных самостоятельных работ. (Приложение 2.)

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 ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
MS Office Visio Prof 2019(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2016(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2013(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2010(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2007(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2003(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2002(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

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:
Лекционные аудитории:
- Мультимедийные средства хранения, передачи и представления информации.

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

Лаборатория программно-аппаратных средств защиты информации:
- Система защиты информации от несанкционированного доступа СТРАЖ NT(версия 3.0)

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

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

Рекомендации направлены на оказание методической помощи обучающимся при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение обучающимися умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности обучающийсяов к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ обучающиеся допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ обучающийся должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым обучающимся самостоятельно, согласно индивидуальному заданию.

Обучающиеся, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы обучающийся демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если обучающийся набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со обучающимися группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы проводятся в компьютерных классах или специализированных лабораториях с целью получения практических умений для формирования и развития профессиональных навыков и соответствующих компетенций по дисциплине. При подготовке к выполнению заданий лабораторной работы используйте лекции, справочный материал программного обеспечения, рекомендованную литературу и цифровые образовательные ресурсы соответствующих методических материалов, размещенных в сети Интернет или локальной сети университета. Перед выполнением лабораторной работы необходимо получить свой вариант индивидуального задания у преподавателя. Прежде чем приступить к выполнению лабораторной работы, внимательно прочтите рекомендации к ее выполнению. Ознакомьтесь с перечнем рекомендуемой литературы, повторите теоретический материал, относящийся к теме работы. Ответьте на контрольные вопросы, выполните задания для самостоятельного выполнения. По результатам лабораторной работы предоставляется отчет. Отчет к лабораторным работам должен содержать:

- название лабораторной работы;

- цель и задачи работы;

- краткие теоретические сведения;

- задания по лабораторной работе;

- ход работы - описание последовательности действий при выполнении работы;

- выводы или результаты.

Результаты выполнения лабораторной работы могут быть представлены в электронном варианте или распечатанные. Результаты выполнения заданий лабораторной работы можно сохранить на образовательном портале в личном кабинете и использовать при подготовке к экзамену.

Защита работы и результаты оценивания.

Защита проводится в два этапа:

1. Демонстрируются результаты выполнения задания. В случае выполнения лабораторной работы, предусматривающей разработку программы, при помощи тестового примера доказывается, что результат, получаемый при выполнении программы, является правильным.

2. Для защиты работы студенту необходимо ответить на дополнительные вопросы преподавателя. Каждая лабораторная работа оценивается определенным количеством баллов исходя из 5-бальной системы оценок.

Лабораторная работа считается выполненной и защищенной, если выполнены все задания и даны правильные ответы преподавателю на заданные вопросы. Лабораторная работа считается выполненной и незащищенной, если выполнены все задания, но полученные результаты являются неверными или не даны правильные ответы преподавателю на заданные вопросы и ответы были не полные. Обучающемуся, не выполнившим в полном объеме все задания лабораторной работы, или пропустившим по уважительной причине лабораторную работу, необходимо выполнить ее самостоятельно в компьютерном классе или специализированной лаборатории, результаты

выполненной работы сохранить на съемном накопителе или на образовательном портале. Результаты предоставить в сроки, указанные преподавателем вместе с отчетом, демонстрацией полученных результатов в компьютерном классе (или специализированной лаборатории) или предоставлением материалов на электронном образовательном ресурсе.

Правила по технике безопасности для обучающихся при проведении лабораторных работ:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности и противопожарным мерам.

2. Обучающийся должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах или специализированных лабораториях университета.