Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский государственный социальный университет»

УТВЕРЖДАЮ

Декан факультета

_____ /Крапивка С.В./

«06» июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ

Направление подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

Организация и технологии защиты информации

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ - *ПРОГРАММА БАКАЛАВРИАТА*

Форма обучения
Очная

Москва 2022

Рабочая программа дисциплины «Проектная деятельность» разработана на основании федерального государственного образовательного стандарта высшего образования – *бакалавриата* по направлению *10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
– *06.032 Специалист по безопасности компьютерных систем и сетей*
– *06.033 Специалист по защите информации в автоматизированных системах*
06.034 Специалист по технической защите информации.

Рабочая программа дисциплины «Проектная деятельность» разработана рабочей группой в составе: канд. пед. наук Крапивка С.В., канд. пед. наук, Мнацаканян О.Л. , канд. техн. наук Блинов А.О.

Руководитель основной образовательной программы канд. пед. Наук доцент — Н.Г. Витковская

(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на Ученом совете факультета информационных технологий. Протокол № 10 от «06» июня 2022 года.

Декан факультета кандидат педагогических наук, доцент — С.В. Крапивка

(подпись)

Рабочая программа дисциплины рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет» зам. ген. директора по науке, к.т.н., доцент — А.С. Мосолов

(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

д-р техн. наук, профессор, ФГБОУ ВО «Московский политехнический университет», НОЦ инфокогнитивных технологий — Н.И. Гданский

(подпись)

канд. техн. наук, доцент, ФГБОУ ВО «Российский государственный социальный университет», факультет информационных технологий — В.Л. Симонов

(подпись)

Согласовано
Научная библиотека, директор — И.Г. Маляр

(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1 Цель и задачи дисциплины

Цель дисциплины заключается в получении обучающимися теоретических знаний о проектной деятельности с последующим применением в профессиональной сфере и практических навыков (формирование) по связи, информационным и коммуникационным технологиям (в сфере индустриального производства программного обеспечения для информационно-вычислительных систем различного назначения).

Задачи дисциплины:

− изучение организации проектной деятельности для эффективного решения поставленных в практической деятельности задач различного уровня и сложности;

− изучение основ и методов планирования этапов будущего проекта;

− изучение основ тайм менеджмента в проектной деятельности;

− обретение навыков формирования и формулирования задач для индивидуальной и совместной (коллективной) проектной деятельности;

− применение и совершенствование профессиональных знаний, умений и навыков при работе над проектом;

− развитие навыков самостоятельной исследовательской работы;

− формирование навыков оформления и документального сопровождения проекта, в том числе, его презентации Заказчику.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования-программы *бакалавриата*

Дисциплина«Проектная деятельность» реализуется в *обязательной* части основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность *очной* формы обучения**.**

Изучение дисциплины «Проектная деятельность» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда дисциплин *«Математика», «Технологии самоорганизации и эффективного взаимодействия»***,** «Программирование».

Перечень последующих дисциплин, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной: «Комплексная защита объектов информатизации», «Анализ данных», «Организационное и правовое обеспечение информационной безопасности».

1.3 Планируемые результаты обучения по дисциплине в рамках планируемых результатов освоения основной профессиональной образовательной программы высшего образования – программы *бакалавриата*

Процесс освоения дисциплины «Проектная деятельность» направлен на формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций:УК-2; УК-3; ОПК-12; ПК-2; ПК-7 в соответствии с основной профессиональной образовательной программой высшего образования – программой бакалавриата по направлению подготовки *10.03.01 Информационная безопсность*.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты:

Категория компетенций	**Код компетенции**	**Формулировка компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения**
Разработка и реализация проектов	УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции УК-2.ИД-2. Планирует и выполняет практические действия в рамках компетенции УК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	*Знать:* необходимые для осуществления профессиональной деятельности правовые нормы *Уметь:* определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности *Владеть:* практическим опытом применения нормативной базы и решения задач в области избранных видов профессиональной деятельности.

Командная работа и лидерство	УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции УК-3.ИД-2. Планирует и выполняет практические действия в рамках компетенции УК-3.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	*Знать:* различные приемы и способы социализации личности и социального взаимодействия. *Уметь:* строить отношения с окружающими людьми, с коллегами. *Владеть:* практическим опытом участия в командной работе, в социальных проектах, распределения ролей в условиях командного взаимодействия.
	ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-8.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-8.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-8.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках	**Знать:** - принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода; - номенклатуру и основные параметры сертифицированных средств

			компетенции	обеспечения информационной безопасности.
				Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно-следственных связей.
				Владеть : - основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту информатизации; - методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования. - основными технологиями селективного информационного поиска и анализа результатов работы с информационными ресурсами по номенклатуре

				сертифицированных средств защиты объектов информатизации.
	ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-2.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ - основы администрирования вычислительных сетей - системы управления БД
				Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

				Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации
	ПК-7	Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-7.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-7.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода; - номенклатуру и основные параметры сертифицированных средств обеспечения информационной безопасности.
				Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и

				причинно-следственных связей.
				Владеть : - основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту информатизации; - методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования. - основными технологиями селективного информационного поиска и анализа результатов работы с информационными ресурсами по номенклатуре сертифицированных средств защиты объектов информатизации.

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Объем дисциплины, включая контактную работу обучающегося с педагогическими работниками и самостоятельную работу обучающегося

Общая трудоемкость дисциплины, изучаемой в 1,2,3,4,5,6 семестрах 12 зачетных единиц. По дисциплине предусмотрены: зачеты, которые проводятся в устной форме.

Очная форма обучения

Вид учебной работы	Всего часов	Семестры						
		1	2	3	4	5	6	
Контактная работа обучающихся с педагогическими работниками	**216**	**36**	**36**	**36**	**36**	**36**	**36**	
Учебные занятия лекционного типа								
из них: в форме практической подготовки								
Практические занятия	4	4						
из них: в форме практической подготовки	*4*	*4*						
Лабораторные занятия								
из них: в форме практической подготовки								
Иная контактная работа	212	32	36	36	36	36	36	
из них: в форме практической подготовки	*212*	*32*	*36*	*36*	*36*	*36*	*36*	
Самостоятельная работа обучающихся	**162**	**27**	**27**	**27**	**27**	**27**	**27**	
Контроль промежуточной аттестации	**54**	**9**	**9**	**9**	**9**	**9**	**9**	
Форма промежуточной аттестации		зачет	диф. зач	зачет	диф. зач	зачет	диф. зач	
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**432**	**72**	**72**	**72**	**72**	**72**	**72**	

2.2. Учебно-тематический план дисциплины

Очной формы обучения

Раздел, тема	Виды учебной работы, академических часов		
	Всего	тоятельная работ	Контактная работа обучающихся с педагогическими работниками

			Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*
Модуль 1 (семестр 1)												
Раздел 1.1. Введение в проектную деятельность	31	13	18	*18*			2	*2*			16	*16*
Раздел 1.2. Выполнение и защита учебного проекта	32	14	18	*18*			2	*2*			16	*16*
Контроль промежуточной аттестации (час)	**9**											
Общий объем, часов	**72**	**27**	**36**	***36***			**4**	***4***			**32**	***32***
Форма промежуточной аттестации	**зачет**											
Модуль 2 (семестр 2)												
Раздел 2.1. Планирование проектной деятельности на 2 семестр	18	7	9	*9*							9	*9*
Раздел 2.2. Техническое задание проекта	18	7	9	*9*							9	*9*
Раздел 2.3. Разработка проектного	18	7	9	*9*							9	*9*

решения												
Раздел 2.4. Документирование и защита проекта	18	6	9	*9*							9	*9*
Контроль промежуточной аттестации (час)	**9**											
Общий объем, часов	**72**	**27**	**36**	***36***							**36**	***36***
Форма промежуточной аттестации	**дифзачет**											
Модуль 3 (семестр 3)												
Раздел 3.1. Планирование проектной деятельности на 3 семестр	18	7	9	9							9	9
Раздел 3.2. Техническое задание проекта	18	7	9	9							9	9
Раздел 3.3. Разработка проектного решения	18	7	9	9							9	9
Раздел 3.4. Документирование и защита проекта	18	6	9	9							9	9
Контроль промежуточной аттестации (час)	**9**											
Общий объем, часов	**72**	**27**	**36**	***36***							**36**	***36***
Форма промежуточной аттестации	**зачет**											
Модуль 4 (семестр 4)												
Раздел 4.1. Планирование проектной деятельности на 4 семестр	18	7	9	9							9	9
Раздел 4.2. Техническое задание проекта	18	7	9	9							9	9

Раздел 4.3. Разработка проектного решения	18	7	9	9							9	9
Раздел 4.4. Документирование и защита проекта	18	6	9	9							9	9
Контроль промежуточной аттестации (час)	**9**											
Общий объем, часов	**72**	**27**	**36**	***36***							**36**	***36***
Форма промежуточной аттестации	**Диф. зачет**											
Модуль 5 (семестр 5)												
Раздел 5.1. Планирование проектной деятельности на 5 семестр	18	7	9	9							9	9
Раздел 5.2. Техническое задание проекта	18	7	9	9							9	9
Раздел 5.3. Разработка проектного решения	18	7	9	9							9	9
Раздел 5.4. Документирование и защита проекта	18	6	9	9							9	9
Контроль промежуточной аттестации (час)	**9**											
Общий объем, часов	**72**	**27**	**36**	***36***							**36**	***36***
Форма промежуточной аттестации	**зачет**											
Модуль 6 (семестр 6)												
Раздел 6.1. Планирование проектной деятельности на 6 семестр	18	7	9	9							9	9

Раздел 6.2. Техническое задание проекта	18	7	9	9							9	9
Раздел 6.3. Разработка проектного решения	18	7	9	9							9	9
Раздел 6.4. Документирование и защита проекта	18	6	9	9							9	9
Контроль промежуточной аттестации (час)	**9**											
Общий объем, часов	**72**	**27**	**36**	***36***							**36**	***36***
Форма промежуточной аттестации	**Диф. зачет**											
Общий объем, часов	**432**	**162**	**216**	***216***			**4**	***4***			**212**	***212***

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

3.1. Виды самостоятельной работы обучающихся по дисциплине

Очной формы обучения

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**
Модуль 1 (семестр 1)							
Раздел 1.1. Введение в проектную деятельность	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	Реферат	2	Компьютерное тестирование/защита реферата

Раздел 1.2. Выполнение и защита учебного проекта	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	Разработка проектного решения	2	Компьютерное тестирование/защита проекта
Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Модуль 2 (семестр 2)							
Раздел 2.1. Планирование проектной деятельности на 2 семестр	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка плана проекта	1	Защита плана проекта
Раздел 2.2. Техническое задание проекта	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Согласование технического задания	1	Защита технического задания проекта
Раздел 2.3. Разработка проектного решения	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка проектного решения	1	Компьютерное тестирование по тематике проекта
Раздел 2.4. Документирование и защита проекта	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Документирование проекта	1	Защита проекта
Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Модуль 3 (семестр 3)							
Раздел 3.1. Планирование проектной деятельности на 3 семестр	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка плана проекта	1	Защита плана проекта
Раздел 3.2. Техническое задание проекта	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Согласование технического задания	1	Защита технического задания проекта

Раздел 3.3. Разработка проектного решения	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка проектного решения	1	Компьютерное тестирование по тематике проекта
Раздел 3.4. Документирование и защита проекта	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Документирование проекта	1	Защита проекта
Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Модуль 4 (семестр 4)							
Раздел 4.1. Планирование проектной деятельности на 4 семестр	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка плана проекта	1	Защита плана проекта
Раздел 4.2. Техническое задание проекта	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Согласование технического задания	1	Защита технического задания проекта
Раздел 4.3. Разработка проектного решения	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка проектного решения	1	Компьютерное тестирование по тематике проекта
Раздел 4.4. Документирование и защита проекта	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Документирование проекта	1	Защита проекта
Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Модуль 5 (семестр 5)							
Раздел 5.1. Планирование проектной деятельности на 5 семестр	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка плана проекта	1	Защита плана проекта

Раздел 5.2. Техническое задание проекта	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Согласование технического задания	1	Защита технического задания проекта
Раздел 5.3. Разработка проектного решения	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка проектного решения	1	Компьютерное тестирование по тематике проекта
Раздел 5.4. Документирование и защита проекта	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Документирование проекта	1	Защита проекта
Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Модуль 6 (семестр 6)							
Раздел 6.1. Планирование проектной деятельности на 6 семестр	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка плана проекта	1	Защита плана проекта
Раздел 6.2. Техническое задание проекта	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Согласование технического задания	1	Защита технического задания проекта
Раздел 6.3. Разработка проектного решения	7	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Разработка проектного решения	1	Компьютерное тестирование по тематике проекта
Раздел 6.4. Документирование и защита проекта	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	3	Документирование проекта	1	Защита проекта
Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Общий объем по дисциплине (модулю), часов	**162**	**66**		**72**		**24**	

3.2 Методические указания к самостоятельной работе по дисциплине

РАЗДЕЛ 1.1. ВВЕДЕНИЕ В ПРОЕКТНУЮ ДЕЯТЕЛЬНОСТЬ

Цель: сформировать у студентов систему знаний о теоретических основах проектной деятельности.

Перечень изучаемых элементов содержания

Проектный подход. Введение в управление проектами. Содержание проектной деятельности. Проект как объект управления. Субъекты управления проектами. Процессы и функции управления проектами. Инициация и старт проекта.

Формирование целей проекта. Планирование проекта. Управление расписанием проекта. Организационное планирование и логистика проекта. Организационная структура проекта. Управление персоналом проекта. Управление коммуникациями проекта. Управление рисками проекта. Идентификация и обработка рисков проекта. Контроль проекта. Исполнение и завершение проекта.

Вопросы для самоподготовки:

1. Признаки проекта. Основные отличия проектов от операционной деятельности.
2. Проекты и программы.
3. Особенности управления различными типами проектов.
4. Причины неудач и критические факторы успеха проекта.
5. Современные методологии управления проектами.
6. Каскадный подход и гибкие методы.
7. Содержание и этапы проектной деятельности.
8. Особенности проекта как объекта управления.
9. Классификация проектов. «Открытые» и традиционные проекты.
10. Жизненный цикл проекта.
11. Принципы организации управления проектом.
12. Анализ стейкхолдеров проекта.
13. Рамки проекта: временные, функциональные, стоимостные.
14. Анализ заинтересованных сторон. Учет интересов участников проекта.
15. Выбор стратегии реализации проекта.

Практическое задание к разделу 1.1

Форма практического задания: реферат.

Перечень тем рефератов к разделу 1.1:

1. Особенности управления различными типами проектов.
2. Международные стандарты проектной деятельности.
3. Сравнительный анализ подходов IPMA, PMI, PRINCE-2.
4. Проектные роли. Организационная структура проекта.
5. Взаимосвязь системы стратегического управления и системы сбалансированных показателей.
6. Разработка структурных схем организации проектов.
7. Календарное планирование проекта.
8. Общий алгоритм создания календарного графика проекта.
9. Модели оптимизации расписания отдельного проекта и группы проектов.
10. Проектные роли.

Рубежный контроль к разделу 1.1

Форма рубежного контроля – защита реферата

РАЗДЕЛ 1.2.ВЫПОЛНЕНИЕ И ЗАЩИТА УЧЕБНОГО ПРОЕКТА

Цель: сформировать у студентов начальные практические умения разработки проекта.

Перечень изучаемых элементов содержания

Выбор темы проекта (базовый список текущих проектов размещается на корпоративном портале https://corp.rgsu.net и отображается в личном кабинете обучающегося на портале https://portfolio.rgsu.net).

Определение целей проекта, планирование этапов выполнения проекта. Разработка проектного решения. Подготовка презентации по проекту.

Вопросы для самоподготовки:

1. Анализ инструментальных средств реализации проекта.
2. Временная диаграмма проекта.
3. Команда проекта. Роли участников команды.
4. Проектная документация.

Практическое задание к разделу 1.2
Форма практического задания: разработка проектного решения.

Рубежный контроль к разделу 1.2
Форма рубежного контроля – защита проекта

РАЗДЕЛ 2.1.ПЛАНИРОВАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ НА 2 СЕМЕСТР

Цель: сформировать у студентов практические умения формулировки целей и задач проектов, начальные умения разработки календарного плана проекта.

Перечень изучаемых элементов содержания

Выбор темы проекта (базовый список текущих проектов размещается на корпоративном портале https://corp.rgsu.net и отображается в личном кабинете обучающегося на портале https://portfolio.rgsu.net; альтернативный список формируется преподавателем на основе текущих заявок от организаций-партнеров).

Определение целей проекта, этапов выполнения проекта. Календарное планирование проекта. Определение команды проекта. Роли участников проекта. Анализ существующих решений по тематике проекта.

Вопросы для самоподготовки:

1. Обзор инструментальных средств разработки календарного плана проекта.
2. Обзор альтернативных решений по тематике выбранного проекта.

Практическое задание к разделу 2.1
Форма практического задания: разработка плана проекта.

Рубежный контроль к разделу 2.1
Форма рубежного контроля – защита плана проекта.

РАЗДЕЛ 2.2. ТЕХНИЧЕСКОЕ ЗАДАНИЕ ПРОЕКТА

Цель: сформировать у студентов начальные практические умения работы с техническим заданием проекта.

Перечень изучаемых элементов содержания

Назначение технического задания. Типовая структура технического задания проекта. Стандарты для технического задания. Принципы формирования технического задания. Взаимодействие с заказчиком проекта.

Вопросы для самоподготовки:

1. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
2. ГОСТ 19.201-78 Единая система программной документации (ЕСПД). Техническое задание. Требования к содержанию и оформлению (с Изменением N 1).

Практическое задание к разделу 2.2
Форма практического задания: согласование технического задания.

Рубежный контроль к разделу 2.2
Форма рубежного контроля – защита технического задания проекта.

РАЗДЕЛ 2.3.РАЗРАБОТКА ПРОЕКТНОГО РЕШЕНИЯ

Цель: сформировать у студентов начальные практические умения разработки проектного решения, регламентированного техническим заданием.

Перечень изучаемых элементов содержания

Описание бизнес-процессов проекта. Проектирование архитектуры программного продукта. Проектирование систем хранения данных (при необходимости). Проектирование интерфесов (при необходимости). Кодирование и тестирование программного решения.

Вопросы для самоподготовки:

1. Обзор средств описания бизнес-процессов.
2. Архитектуры информационных систем.
3. Системы хранения данных.
4. Обзор систем и языков программирования по тематике проекта.

Практическое задание к разделу 2.3
Форма практического задания: разработка проектного решения.

Рубежный контроль к разделу 2.3
Форма рубежного контроля – компьютерное тестирование по тематике проекта.

РАЗДЕЛ 2.4. ДОКУМЕНТИРОВАНИЕ И ЗАЩИТА ПРОЕКТА

Цель: сформировать у студентов начальные практические умения документационного сопровождения и защиты проекта.

Перечень изучаемых элементов содержания

Требования к технической документации. Оформление документации по проекту. Инструментальные средства презентации проекта. Защита проекта.

Вопросы для самоподготовки:

1. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы (раздел «Требования к документированию»).
2. ГОСТ 19.201-78 Единая система программной документации (ЕСПД). Техническое задание. Требования к содержанию и оформлению (с Изменением N 1) (раздел «Требования к технической документации»).

Практическое задание к разделу 2.4
Форма практического задания: документирование проекта.

Рубежный контроль к разделу 2.4
Форма рубежного контроля – защита проекта.

РАЗДЕЛ 3.1. ПЛАНИРОВАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ НА 3 СЕМЕСТР

Цель: сформировать у студентов практические умения разработки календарного плана проекта.

Перечень изучаемых элементов содержания

Выбор темы проекта (базовый список текущих проектов размещается на корпоративном портале https://corp.rgsu.net и отображается в личном кабинете обучающегося

на портале https://portfolio.rgsu.net; альтернативный список формируется преподавателем на основе текущих заявок от организаций-партнеров).

Формулировка целей проекта, этапов выполнения проекта. Календарное планирование проекта. Общий алгоритмсоздания календарного графика проекта.Иерархическая структура работ проекта.

Определение команды проекта. Роли участников проекта. Анализ существующих решений по тематике проекта.

Вопросы для самоподготовки:

1. Автоматизация разработки календарного плана проекта.
2. Обзор альтернативных решений по тематике выбранного проекта.

Практическое задание к разделу 3.1
Форма практического задания: разработка плана проекта.

Рубежный контроль к разделу 3.1
Форма рубежного контроля – защита плана проекта.

РАЗДЕЛ 3.2. ТЕХНИЧЕСКОЕ ЗАДАНИЕ ПРОЕКТА

Цель: формировать у студентов практические умения работы с техническим заданием проекта.

Перечень изучаемых элементов содержания

Анализ структуры технического задания, полученного от заказчика. Взаимодействие с заказчиком проекта. Согласование технического задания.

Вопросы для самоподготовки:

1. Типовая структура технического задания проекта.
2. Стандарты для технического задания.
3. Принципы формирования технического задания.

Практическое задание к разделу 3.2
Форма практического задания: согласование технического задания.

Рубежный контроль к разделу 3.2
Форма рубежного контроля – защита технического задания проекта.

РАЗДЕЛ 3.3.РАЗРАБОТКА ПРОЕКТНОГО РЕШЕНИЯ

Цель: формировать у студентов начальные практические умения разработки проектного решения, регламентированного техническим заданием.

Перечень изучаемых элементов содержания

Описание бизнес-процессов выбранного проекта. Проектирование архитектуры программного продукта, соответствующей требованиям технического задания. Проектирование систем хранения данных (при необходимости). Проектирование интерфесов (при необходимости). Кодирование и тестирование программного решения.

Вопросы для самоподготовки:

1. Функционал средств описания бизнес-процессов.
2. Клиент-серверная архитектура информационных систем.
3. Обзор систем управления базами данных.
4. Описание систем и языков программирования по тематике проекта.

Практическое задание к разделу 3.3
Форма практического задания: разработка проектного решения.

Рубежный контроль к разделу 3.3
Форма рубежного контроля – компьютерное тестирование по тематике проекта.

РАЗДЕЛ 3.4. ДОКУМЕНТИРОВАНИЕ И ЗАЩИТА ПРОЕКТА

Цель: продолжить формирование у студентов начальных практических умений документационного сопровождения и защиты проекта.

Перечень изучаемых элементов содержания

Оформление документации по разработанному проекту. Инструментальные средства презентации проекта. Защита проекта.

Вопросы для самоподготовки:

1. Требования к технической документации.
2. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы (раздел «Требования к документированию»).
3. ГОСТ 19.201-78 Единая система программной документации (ЕСПД). Техническое задание. Требования к содержанию и оформлению (с Изменением N 1) (раздел «Требования к технической документации»).

Практическое задание к разделу 3.4
Форма практического задания: документирование проекта.

Рубежный контроль к разделу 3.4
Форма рубежного контроля – защита проекта.

РАЗДЕЛ 4.1.ПЛАНИРОВАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ НА 4 СЕМЕСТР

Цель: формировать у студентов практические умения разработки плана проекта в условиях командной работы над проектом.

Перечень изучаемых элементов содержания

Выбор темы проекта (базовый список текущих проектов размещается на корпоративном портале https://corp.rgsu.net и отображается в личном кабинете обучающегося на портале https://portfolio.rgsu.net; альтернативный список формируется преподавателем на основе текущих заявок от организаций-партнеров).

Формулировка целей проекта, этапов выполнения проекта. Составление календарного плана проекта.

Определение команды проекта. Распределение ролей участников проекта. Распределение ответственности в проекте. Виды и степень делегируемой ответственности. Матрица ответственности.

Анализ существующих решений по тематике выбранного проекта.

Вопросы для самоподготовки:

1. Проектные роли.
2. Заказчик проекта.
3. Функциональный (технический) заказчик.
4. Куратор (спонсор) проекта.
5. Администратор проекта.
6. Другие проектные роли.

Практическое задание к разделу 4.1
Форма практического задания: разработка плана проекта.

Рубежный контроль к разделу 4.1
Форма рубежного контроля – защита плана проекта.

РАЗДЕЛ 4.2.ТЕХНИЧЕСКОЕ ЗАДАНИЕ ПРОЕКТА

Цель: формировать у студентов практические умения работы с техническим заданием проекта.

Перечень изучаемых элементов содержания

Анализ структуры технического задания, полученного от заказчика (командная работа). Взаимодействие с заказчиком проекта. Согласование технического задания.

Вопросы для самоподготовки:

1. Типовая структура технического задания проекта.
2. Стандарты для технического задания.
3. Принципы формирования технического задания.

Практическое задание к разделу 4.2
Форма практического задания: согласование технического задания.

Рубежный контроль к разделу 4.2
Форма рубежного контроля – защита технического задания проекта.

РАЗДЕЛ 4.3. РАЗРАБОТКА ПРОЕКТНОГО РЕШЕНИЯ

Цель: продолжить формирование у студентов начальных практических умений разработки проектного решения, регламентированного техническим заданием.

Перечень изучаемых элементов содержания

Описание бизнес-процессов выбранного проекта. Проектирование архитектуры программного продукта, соответствующей требованиям технического задания (командная работа). Проектирование систем хранения данных (при необходимости). Проектирование интерфейсов (при необходимости). Кодирование и тестирование программного решения.

Вопросы для самоподготовки:

1. Функционал средств описания бизнес-процессов.
2. Клиент-серверная архитектура информационных систем: описание инструментальных средств реализации.
3. Реляционные базы данных.
4. Описание систем и языков программирования по тематике проекта.

Практическое задание к разделу 4.3
Форма практического задания: разработка проектного решения.

Рубежный контроль к разделу 4.3
Форма рубежного контроля – компьютерное тестирование по тематике проекта.

РАЗДЕЛ 4.4. ДОКУМЕНТИРОВАНИЕ И ЗАЩИТА ПРОЕКТА

Цель: продолжить формирование у студентов начальных практических умений документационного сопровождения и защиты проекта.

Перечень изучаемых элементов содержания

Оформление документации по разработанному проекту. Инструментальные средства презентации проекта. Защита проекта.

Вопросы для самоподготовки:

1. Требования к технической документации.
2. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы (раздел «Требования к документированию»).
3. ГОСТ 19.201-78 Единая система программной документации (ЕСПД). Техническое задание. Требования к содержанию и оформлению (с Изменением N 1) (раздел «Требования к технической документации»).

Практическое задание к разделу 4.4
Форма практического задания: документирование проекта.

Рубежный контроль к разделу 4.4
Форма рубежного контроля – защита проекта.

РАЗДЕЛ 5.1. ПЛАНИРОВАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ НА 5 СЕМЕСТР

Цель: продолжить формирование у студентов практических умений разработки плана проекта в условиях командной работы над проектом.

Перечень изучаемых элементов содержания

Выбор темы проекта (базовый список текущих проектов размещается на корпоративном портале https://corp.rgsu.net и отображается в личном кабинете обучающегося на портале https://portfolio.rgsu.net; альтернативный список формируется преподавателем на основе текущих заявок от организаций-партнеров).

Формулировка целей проекта, этапов выполнения проекта. Составление календарного плана проекта.

Формирование команды проекта. Распределение ролей участников проекта. Стадии развития проектной команды. Лидерство в проекте. Установочное совещание по проекту.

Анализ существующих решений по тематике выбранного проекта.

Вопросы для самоподготовки:

1. Концепция T.E.A.M.
2. Развитие проектной команды.
3. Установочное совещание по проекту.
4. Распределение ролей в совещании.

Практическое задание к разделу 5.1
Форма практического задания: разработка плана проекта.

Рубежный контроль к разделу 5.1
Форма рубежного контроля – защита плана проекта.

РАЗДЕЛ 5.2.ТЕХНИЧЕСКОЕ ЗАДАНИЕ ПРОЕКТА

Цель: продолжить формирование у студентов практических умений работы с техническим заданием проекта (командная работа).

Перечень изучаемых элементов содержания

Анализ структуры технического задания, полученного от заказчика (командная работа). Взаимодействие с заказчиком проекта. Согласование технического задания.

Вопросы для самоподготовки:

1. Типовая структура технического задания проекта.
2. Стандарты для технического задания.
3. Принципы формирования технического задания.

Практическое задание к разделу 5.2
Форма практического задания: согласование технического задания.

Рубежный контроль к разделу 5.2
Форма рубежного контроля – защита технического задания проекта.

РАЗДЕЛ 5.3. РАЗРАБОТКА ПРОЕКТНОГО РЕШЕНИЯ

Цель: продолжить формирование у студентов практических умений разработки проектного решения, регламентированного техническим заданием.

Перечень изучаемых элементов содержания

Описание бизнес-процессов выбранного проекта. Проектирование архитектуры программного продукта, соответствующей требованиям технического задания (командная работа). Проектирование систем хранения данных (при необходимости). Проектирование интерфейсов (при необходимости). Кодирование и тестирование программного решения. Предпроектный этап разработки мобильной версии проектного решения (при необходимости).

Вопросы для самоподготовки:

1. Методологии описания бизнес-процессов.
2. Функциональное проектирование.
3. Типовые клиент-серверные архитектуры.
4. Реляционные базы данных (язык SQL).
5. Описание систем и языков программирования по тематике проекта.

Практическое задание к разделу 5.3
Форма практического задания: разработка проектного решения.

Рубежный контроль к разделу 5.3
Форма рубежного контроля – компьютерное тестирование по тематике проекта.

РАЗДЕЛ 5.4.ДОКУМЕНТИРОВАНИЕ И ЗАЩИТА ПРОЕКТА

Цель: продолжить формирование у студентов практических умений документационного сопровождения и защиты проекта.

Перечень изучаемых элементов содержания

Оформление документации по разработанному проекту. Инструментальные средства презентации проекта. Защита проекта.

Вопросы для самоподготовки:

1. Требования к технической документации.
2. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы (раздел «Требования к документированию»).
3. ГОСТ 19.201-78 Единая система программной документации (ЕСПД). Техническое задание. Требования к содержанию и оформлению (с Изменением N 1) (раздел «Требования к технической документации»).

Практическое задание к разделу 5.4
Форма практического задания: документирование проекта.

Рубежный контроль к разделу 5.4
Форма рубежного контроля – защита проекта.

РАЗДЕЛ 6.1.ПЛАНИРОВАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ НА 6 СЕМЕСТР

Цель: формирование у студентов практических навыков разработки плана проекта в условиях командной работы над проектом.

Перечень изучаемых элементов содержания

Выбор темы проекта (базовый список текущих проектов размещается на корпоративном портале https://corp.rgsu.net и отображается в личном кабинете обучающегося на портале https://portfolio.rgsu.net; альтернативный список формируется преподавателем на основе текущих заявок от организаций-партнеров).

Формулировка целей проекта, этапов выполнения проекта. Составление календарного плана проекта.

Формирование команды проекта. Распределение ролей участников проекта.

Вербальные и невербальные коммуникации. Управление формальными и неформальными коммуникациями. План управления коммуникациями. Совещания на проекте. Оптимальная периодичность совещаний на проекте. Организация эффективного совещания. Процессы управления рисками.

Анализ существующих решений по тематике выбранного проекта.

Вопросы для самоподготовки:

1. План (политика) управления рисками.
2. Идентификация рисков
3. Методы идентификации рисков.
4. Метод Дельфи.

5. Диаграмма Исикавы.
6. Опросные листы.

Практическое задание к разделу 6.1
Форма практического задания: разработка плана проекта.

Рубежный контроль к разделу 6.1
Форма рубежного контроля – защита плана проекта.

РАЗДЕЛ 6.2. ТЕХНИЧЕСКОЕ ЗАДАНИЕ ПРОЕКТА

Цель: формирование у студентов практических навыков работы с техническим заданием проекта (командная работа).

Перечень изучаемых элементов содержания

Анализ структуры технического задания, полученного от заказчика (командная работа). Взаимодействие с заказчиком проекта. Согласование технического задания.

Вопросы для самоподготовки:

1. Типовая структура технического задания проекта.
2. Стандарты для технического задания.
3. Принципы формирования технического задания.

Практическое задание к разделу 6.2
Форма практического задания: согласование технического задания.

Рубежный контроль к разделу 6.2
Форма рубежного контроля – защита технического задания проекта.

РАЗДЕЛ 6.3. РАЗРАБОТКА ПРОЕКТНОГО РЕШЕНИЯ

Цель: формирование у студентов практических навыков разработки проектного решения, регламентированного техническим заданием.

Перечень изучаемых элементов содержания

Описание бизнес-процессов выбранного проекта. Проектирование архитектуры программного продукта, соответствующей требованиям технического задания (командная работа). Инфологическое и даталогическое проектирование систем хранения данных (при необходимости). Проектирование интерфейсов (при необходимости). Кодирование и тестирование программного решения. Разработка мобильной версии проектного решения (при необходимости).

Вопросы для самоподготовки:

1. Методологии описания бизнес-процессов (UML).
2. Трехзвенная архитектура информационных систем.
3. Тонкий клиент.
4. Сервер баз данных.
5. Сервер приложений.
6. Проектирование реляционных баз данных.
7. Описание систем и языков программирования по тематике проекта.

Практическое задание к разделу 6.3
Форма практического задания: разработка проектного решения.

Рубежный контроль к разделу 6.3
Форма рубежного контроля – компьютерное тестирование по тематике проекта.

РАЗДЕЛ 6.4. ДОКУМЕНТИРОВАНИЕ И ЗАЩИТА ПРОЕКТА

Цель: формирование у студентов практических навыков документационного сопровождения и защиты проекта.

Перечень изучаемых элементов содержания

Оформление документации по разработанному проекту. Инструментальные средства презентации проекта. Защита проекта.

Вопросы для самоподготовки:

4. Требования к технической документации.
5. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы (раздел «Требования к документированию»).
6. ГОСТ 19.201-78 Единая система программной документации (ЕСПД). Техническое задание. Требования к содержанию и оформлению (с Изменением N 1) (раздел «Требования к технической документации»).

Практическое задание к разделу 6.4

Форма практического задания: документирование проекта.

Рубежный контроль к разделу 6.4

Форма рубежного контроля – защита проекта.

РАЗДЕЛ 7.1. ПЛАНИРОВАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ НА 7 СЕМЕСТР

Цель: продолжить формирование у студентов практических навыков разработки плана проекта в условиях командной работы над проектом.

Перечень изучаемых элементов содержания

Выбор темы проекта (базовый список текущих проектов размещается на корпоративном портале https://corp.rgsu.net и отображается в личном кабинете обучающегося на портале https://portfolio.rgsu.net; альтернативный список формируется преподавателем на основе текущих заявок от организаций-партнеров).

Формулировка целей проекта, этапов выполнения проекта. Составление календарного плана проекта.

Формирование команды проекта. Распределение ролей участников проекта.

Принципы построения системы контроля проекта. Система отчетности. Методы и виды контроля. Учетная и прогнозная функции контроля. «Приборная панель» проекта. Управление изменениями. Уровни принятия решений.

Анализ существующих решений по тематике выбранного проекта.

Вопросы для самоподготовки:

1. Простой и детальный контроль проекта.
2. Запросы на изменения
3. Архив изменений.

Практическое задание к разделу 7.1

Форма практического задания: разработка плана проекта.

Рубежный контроль к разделу 7.1

Форма рубежного контроля – защита плана проекта.

РАЗДЕЛ 7.2. ТЕХНИЧЕСКОЕ ЗАДАНИЕ ПРОЕКТА

Цель: продолжить формирование у студентов практических навыков работы с техническим заданием проекта (командная работа).

Перечень изучаемых элементов содержания

Анализ структуры технического задания, полученного от заказчика (командная работа). Взаимодействие с заказчиком проекта. Согласование технического задания.

Вопросы для самоподготовки:

1. Типовая структура технического задания проекта.

2. Стандарты для технического задания.
3. Принципы формирования технического задания.

Практическое задание к разделу 7.2
Форма практического задания: согласование технического задания.

Рубежный контроль к разделу 7.2
Форма рубежного контроля – защита технического задания проекта.

РАЗДЕЛ 7.3. РАЗРАБОТКА ПРОЕКТНОГО РЕШЕНИЯ

Цель: продолжить формирование у студентов практических навыков разработки проектного решения, регламентированного техническим заданием.

Перечень изучаемых элементов содержания

Описание бизнес-процессов выбранного проекта. Проектирование архитектуры программного продукта, соответствующей требованиям технического задания (командная работа). Инфологическое и даталогическое проектирование систем хранения данных (при необходимости). Проектирование интерфейсов (при необходимости). Кодирование и тестирование программного решения. Разработка мобильной версии проектного решения (при необходимости).

Вопросы для самоподготовки:

1. Функциональное проектирование.
2. Средства разработки мобильных приложений.
3. Принцип разделения кода и данных (на примере выбранного проекта).
4. Описание систем и языков программирования по тематике проекта.

Практическое задание к разделу 7.3
Форма практического задания: разработка проектного решения.

Рубежный контроль к разделу 7.3
Форма рубежного контроля – компьютерное тестирование по тематике проекта.

РАЗДЕЛ 7.4. ДОКУМЕНТИРОВАНИЕ И ЗАЩИТА ПРОЕКТА

Цель: формирование у студентов практических навыков документационного сопровождения и защиты проекта.

Перечень изучаемых элементов содержания

Оформление документации по разработанному проекту. Инструментальные средства презентации проекта.

Завершение действий по проекту. Административное закрытие. Контрактное закрытие проекта.

Защита проекта.

Вопросы для самоподготовки:

1. Назначение, структура и состав корпоративной системы управления проектами (КСУП).
2. Основные функциональные блоки КСУП.
3. Проект внедрения КСУП.
4. Проектный офис. Типы проектных офисов.
5. Функции проектного офиса.
6. Требования к технической документации.

Практическое задание к разделу 7.4
Форма практического задания: документирование проекта.

Рубежный контроль к разделу 7.4
Форма рубежного контроля – защита проекта.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

4.1. Форма промежуточной аттестации обучающегося по дисциплине

Контрольным мероприятием промежуточной аттестации обучающихся по учебной дисциплине является: **зачет в 1,2,3 семестрах, дифференцированный зачет в 4,5,6,7 семестрах,** которые проводятся в **устной** форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	*Знать:* необходимые для осуществления профессиональной деятельности правовые нормы	Этап формирования знаний
		Уметь: определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности	Этап формирования умений
		Владеть: практическим опытом применения нормативной базы и решения задач в области избранных видов профессиональной деятельности.	Этап формирования навыков и получения опыта
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	*Знать:* различные приемы и способы социализации личности и социального взаимодействия.	Этап формирования знаний
		Уметь: строить отношения с окружающими людьми, с коллегами.	Этап формирования умений
		Владеть: практическим опытом участия в командной работе, в социальных проектах, распределения ролей в условиях командного взаимодействия.	Этап формирования навыков и получения опыта
ОПК-12	Способен проводить	Знать: принципы построения подсистем и средств	Этап формирования

	подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно-следственных связей. Владеть: • основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту информатизации; методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования	знаний Этап формирования умений Этап формирования навыков и опыта
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать:** - математический аппарат для решения профессиональных задач (ОПК-2) - инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап формирования знаний
		Уметь: применять соответствующий математический аппарат для решения профессиональных задач	Этап формирования умений
		Владеть: способностью применять соответствующий математический аппарат для решения профессиональных задач способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап формирования навыков и получения опыта
ПК-7	способностью проводить анализ	**Знать:**	Этап формирования знаний

	исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений	- принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода; - номенклатуру и основные параметры сертифицированных средств обеспечения информационной безопасности.	
		Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно-следственных связей.	Этап формирования умений
		Владеть : - основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту информатизации; - методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования. - основными технологиями селективного информационного поиска и анализа результатов работы с информационными ресурсами по номенклатуре сертифицированных средств защиты объектов информатизации.	Этап формирования навыков и получения опыта

4.3 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Этапы формирования компетенций	Показатель оценивания компетенции	Критерии и шкалы оценивания
УК-2; УК-3;	Этап	Теоретический блок	1) обучающийся глубоко и

ОПК-12; ПК-2; ПК-7	формирования знаний.	вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок: (9-10] баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения: [8-9) баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала: (6-8) баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки: [0-6] баллов.

УК-2; УК-3; ОПК-12; ПК-2; ПК-7	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией: (9-10] баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании: [8-9) баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению: (6-8) баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания: [0-6] баллов.
УК-2; УК-3; ОПК-12; ПК-2; ПК-7	Этап формирования навыков и получения опыта.	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

4.4 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине

СЕМЕСТР 1

Теоретический блок вопросов

1. Проектный подход.
2. Содержание проектной деятельности.
3. Этапы проектной деятельности.
4. Жизненный цикл проекта.
5. Признаки проекта. Основные отличия проектов от операционной деятельности.
6. Проект как объект управления.
7. Субъекты управления проектами.
8. Процессы и функции управления проектами.
9. Инициация и старт проекта.

10. Планирование проекта.
11. Организационная структура проекта.
12. Особенности управления различными типами проектов.
13. Причины неудач и критические факторы успеха проекта.
14. Рамки проекта: временные, функциональные, стоимостные.
15. Учет интересов участников проекта.

Аналитическое задание

1. Разработка структурных схем реализации проекта (по вариантам)

СЕМЕСТР 2

Теоретический блок вопросов

1. Определение целей проекта.
2. Этапы выполнения проекта.
3. Календарное планирование проекта.
4. Определение команды проекта.
5. Роли участников проекта.
6. Назначение технического задания.
7. Типовая структура технического задания проекта.
8. Понятие о стандартах для технического задания (ГОСТ 34.602-89).
9. Понятие о стандартах для технического задания (ГОСТ 19.201-78).
10. Понятие об описании бизнес-процессов.

Аналитическое задание

1. Составление плана реализации проекта (по вариантам).
2. Анализ существующих решений по проекту (по вариантам).

СЕМЕСТР 3

Теоретический блок вопросов

1. Календарное планирование проекта.
2. Общий алгоритм создания календарного графика проекта.
3. Иерархическая структура работ проекта.
4. Определение команды проекта.
5. Роли участников проекта.
6. Принципы формирования технического задания.
7. Взаимодействие с заказчиком проекта.
8. Формализация описания бизнес-процессов.
9. Принципы проектирования архитектуры информационных систем.
10. Клиент-серверная архитектура информационных систем

Аналитическое задание

1. Разработка структуры технического задания (по вариантам).
2. Автоматизированная разработка календарного плана проекта.

СЕМЕСТР 4

Теоретический блок вопросов

1. Распределение ролей участников проекта.
2. Распределение ответственности в проекте.
3. Виды и степень делегируемой ответственности.
4. Матрица ответственности.
5. Проектные роли.
6. Заказчик проекта.
7. Функциональный (технический) заказчик.
8. Куратор (спонсор) проекта.
9. Администратор проекта.

10. Клиент-серверная архитектура информационных систем: описание инструментальных средств реализации.

Аналитическое задание

1. Разработка технического задания (по вариантам).
2. Разработка решения в рамках защищаемого проекта.

СЕМЕСТР 5

Теоретический блок вопросов

1. Распределение ролей участников проекта.
2. Стадии развития проектной команды.
3. Лидерство в проекте.
4. Установочное совещание по проекту.
5. Концепция T.E.A.M.
6. Методологии описания бизнес-процессов.
7. Функциональное проектирование.
8. Методология IDEFx, DFD.
9. Типовые клиент-серверные архитектуры.
10. Реляционные базы данных.
11. Операции с данными.
12. Основные понятия SQL.

Аналитическое задание

1. Функциональное проектирование (по вариантам).
2. Решение задач по обработке данных с применением SQL.
3. Разработка решения в рамках защищаемого проекта.

СЕМЕСТР 6

Теоретический блок вопросов

1. Вербальные и невербальные коммуникации при работе над проектом.
2. Управление формальными и неформальными коммуникациями.
3. План управления коммуникациями.
4. Совещания на проекте.
5. Оптимальная периодичность совещаний на проекте.
6. Организация эффективного совещания.
7. Процессы управления рисками.
8. План (политика) управления рисками.
9. Идентификация рисков
10. Методы идентификации рисков.
11. Метод Дельфи.
12. Диаграмма Исикавы.
13. Опросные листы.
14. Инфологическое и даталогическое проектирование систем хранения данных.
15. Принципы разработки интерфейсов.
16. Методологии описания бизнес-процессов (UML).
17. Трехзвенная архитектура информационных систем.
18. Тонкий клиент.
19. Сервер баз данных.
20. Сервер приложений.

Аналитическое задание

1. Проектирование систем хранения данных (по вариантам).
2. Описание бизнес-процессов с применением UML (по вариантам).
3. Разработка решения в рамках защищаемого проекта.

СЕМЕСТР 7

Теоретический блок вопросов

1. Принципы построения системы контроля проекта.
2. Система отчетности.
3. Методы и виды контроля.
4. Простой и детальный контроль проекта.
5. Учетная и прогнозная функции контроля.
6. «Приборная панель» проекта.
7. Управление изменениями.
8. Архив изменений.
9. Уровни принятия решений.
10. Назначение, структура и состав корпоративной системы управления проектами (КСУП).
11. Основные функциональные блоки КСУП.
12. Проект внедрения КСУП.
13. Проектный офис. Типы проектных офисов.
14. Функции проектного офиса.
15. Завершение действий по проекту.
16. Административное закрытие проекта.
17. Контрактное закрытие проекта.
18. Документационное сопровождение проекта.
19. Средства разработки мобильных приложений.
20. Принцип разделения кода и данных.

Аналитическое задание

1. Комплексное задание в рамках защищаемого проекта.

4.5Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация по дисциплине «Проектная деятельность»проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам высшего образования – программ бакалаврита/магистратуры/специалитета в Российском государственном социальном университете и Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по дисциплине выставляется по пятибалльной системе для дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины

5.1.1. Основная литература

1. *Зуб, А. Т.* Управление проектами : учебник и практикум для среднего профессионального образования / А. Т. Зуб. — Москва : Издательство Юрайт, 2022. — 422 с. — (Профессиональное образование). — ISBN 978-5-534-01505-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491468

2. *Чекмарев, А. В.* Управление ИТ-проектами и процессами : учебник для вузов / А. В. Чекмарев. — Москва : Издательство Юрайт, 2022. — 228 с. — (Высшее образование). — ISBN 978-5-534-11191-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493916

3. Проектирование информационных систем : учебник и практикум для вузов / под общей редакцией Д. В. Чистова. — Москва : Издательство Юрайт, 2022. — 258 с. — (Высшее образование). — ISBN 978-5-534-00492-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489307

5.1.2. Дополнительная литература

1. Астапчук, В. А. Корпоративные информационные системы: требования при проектировании : учебное пособие для вузов / В. А. Астапчук, П. В. Терещенко. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 113 с. — (Высшее образование). — ISBN 978-5-534-08546-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453261

2. Гутгарц, Р. Д. Проектирование автоматизированных систем обработки информации и управления : учебное пособие для вузов / Р. Д. Гутгарц. — Москва : Издательство Юрайт, 2020. — 304 с. — (Высшее образование). — ISBN 978-5-534-07961-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455707

3. Григорьев, М. В. Проектирование информационных систем : учебное пособие для вузов / М. В. Григорьев, И. И. Григорьева. — Москва : Издательство Юрайт, 2020. — 318 с. — (Высшее образование). — ISBN 978-5-534-01305-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451794

4. Грекул, В. И. Проектирование информационных систем : учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — Москва : Издательство Юрайт, 2020. — 385 с. — (Высшее образование). — ISBN 978-5-9916-8764-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450997

5. Зараменских, Е. П. Управление жизненным циклом информационных систем : учебник и практикум для вузов / Е. П. Зараменских. — Москва : Издательство Юрайт, 2020. — 431 с. — (Высшее образование). — ISBN 978-5-9916-9200-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451064

6. Колошкина, И. Е. Автоматизация проектирования технологической документации : учебник и практикум для вузов / И. Е. Колошкина. — Москва : Издательство Юрайт, 2020. — 371 с. — (Высшее образование). — ISBN 978-5-534-14010-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467467

7. Поляков, Н. А. Управление инновационными проектами : учебник и практикум для вузов / Н. А. Поляков, О. В. Мотовилов, Н. В. Лукашов. — Москва : Издательство Юрайт, 2020. — 330 с. — (Высшее образование). — ISBN 978-5-534-00952-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450564

8. Тузовский, А. Ф. Проектирование и разработка web-приложений : учебное пособие для вузов / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2020. — 218 с. — (Высшее образование). — ISBN 978-5-534-00515-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451207

9. Черткова, Е. А. Программная инженерия. Визуальное моделирование программных систем : учебник для вузов / Е. А. Черткова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 147 с. — (Высшее образование). — ISBN 978-5-534-09172-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452749

10. Лаврищева, Е. М. Программная инженерия и технологии программирования сложных систем : учебник для вузов / Е. М. Лаврищева. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 432 с. — (Высшее образование). — ISBN 978-5-534-07604-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452137

11. Стружкин, Н. П. Базы данных: проектирование. Практикум : учебное пособие для вузов / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2020. — 291 с. — (Высшее образование). — ISBN 978-5-534-00739-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451246

12. Соколова, В. В. Вычислительная техника и информационные технологии. Разработка мобильных приложений : учебное пособие для вузов / В. В. Соколова. — Москва : Издательство Юрайт, 2020. — 175 с. — (Высшее образование). — ISBN 978-5-9916-6525-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451366

13. Казанский, А. А. Программирование на Visual C# : учебное пособие для вузов / А. А. Казанский. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 192 с. — (Высшее образование). — ISBN 978-5-534-12338-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451467

14. Федоров, Д. Ю. Программирование на языке высокого уровня Python : учебное пособие для вузов / Д. Ю. Федоров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-10971-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454100

15. Скороход, С.В. Программирование на платформе 1С: предприятие 8.3 : [16+] / С.В. Скороход ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 136 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=577921

16. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

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

18. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368

5.2 Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3 Методические указания для обучающихся по освоению дисциплины

Освоение обучающимся дисциплины «Проектная деятельность» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с рабочей программой дисциплины, доступной в электронной информационно-образовательной среде РГСУ.

Следует обратить внимание на списки основной и дополнительной литературы, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к занятию семинарского типа

При подготовке и работе во время занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач практического занятия, техники безопасности при работе с компьютерной техникой.

Работа во время проведения учебного занятия семинарского типа включает:

− консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

− самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Успешное выполнение заданий является необходимым условием при проведении рубежного контроля и допуска к зачету и дифференцированному зачету. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине», «Методические указания к самостоятельной работе по дисциплине»).

5.4 Информационно-технологическое обеспечение образовательного процесса по дисциплины

5.4.1. Средства информационных технологий

1. Персональные компьютеры;
2. Средства доступа к Интернет;
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.4.3. Информационные справочные системы и профессиональные базы данных

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная	Крупнейший российский информационно-	http://elibrary.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	электронная библиотека eLIBRARY.ru	аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.5 Материально-техническое обеспечение образовательного процесса по дисциплине

Для изучения дисциплины«Проектная деятельность» в рамках реализации основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность используются:

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть Интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.6 Образовательные технологии

При реализации дисциплины «Проектная деятельность» применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины«Проектная деятельность» предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме деловых и ролевых игр, разбора конкретных ситуаций в сочетании с внеаудиторной работой с целью формирования и развития **универсальных, общепрофессиональных, профессиональных** навыков обучающихся.

Учебные часы дисциплины«Проектная деятельность предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках дисциплины «Проектная деятельность» предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с *направленностью* реализуемой основной профессиональной образовательной программы высшего образования – программы бакалавриата

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский государственный социальный университет»

УТВЕРЖДАЮ
Декан факультета информационных технологий
/ Крапивка С.В./
06 июня 2022г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МАТЕМАТИКА

Направление подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

Организация и технологии защиты информации

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ - *ПРОГРАММА БАКАЛАВРИАТА*

Форма обучения
Очная

Москва 2022

Рабочая программа дисциплины (модуля) «Математика» разработана на основании федерального государственного образовательного стандарта высшего образования – *бакалавриата* по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
– *06.032 Специалист по безопасности компьютерных систем и сетей*
– *06.033 Специалист по защите информации в автоматизированных системах*

06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля) «Математика» разработана рабочей группой в составе: к. ф.-м. наук, доцент М.В.Фаминская

Руководитель основной образовательной программы канд. пед. Наук доцент _____ Н.Г. Витковская
(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на Ученом совете факультета информационных технологий. Протокол № 10 от «06» июня 2022 года.

Декан факультета кандидат педагогических наук, доцент _____ С.В. Крапивка
(подпись)

Рабочая программа дисциплины рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет» зам. ген. директора по науке, к.т.н., доцент _____ А.С. Мосолов
(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

д-р техн. наук, профессор, ФГБОУ ВО «Московский политехнический университет», НОЦ инфокогнитивных технологий _____ Н.И. Гданский
(подпись)

канд. техн. наук, доцент, ФГБОУ ВО «Российский государственный социальный университет», факультет информационных технологий _____ В.Л. Симонов
(подпись)

Согласовано
Научная библиотека, директор _____ И.Г. Маляр
(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1 Цель и задачи дисциплины (модуля)

Цель учебной дисциплины заключается в получении обучающимися теоретических знаний о линейной алгебре и аналитической геометрии; дифференциальном и интегральном исчислениях функции одной переменной; теоретико-вероятностном подходе при составлении и анализе математических моделей реальных ситуаций; методах математической обработки статистической информации и статистического оценивания с последующим применением в профессиональной сфере и практических навыков по профессиональной области деятельности:

научно-исследовательские и вычислительные центры;

научно-производственные объединения;

образовательные организации среднего профессионального и высшего образования;

органы государственной власти;

организации, осуществляющие разработку и использование информационных систем, научных достижений, продуктов и сервисов в области социальных наук.

Задачи учебной дисциплины:

1. Развитие логических и абстрактных форм мышления;
2. Понимание формального представления сущностей реальной действительности;
3. Приобретение научных и профессиональных знаний, используя современные образовательные и информационные технологии, а также учебную и профессиональную литературу;
4. Применение математических методов для обработки информации в профессиональной деятельности;
5. Выявление разных способов решения исследовательских задач.

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы высшего образования-программы *бакалавриата*

Дисциплина (модуль) *«Математика»* реализуется в *обязательной* части основной образовательной программы по направлению подготовки *10.03.01 Информационная безопасность. Очной формы обучения.*

Изучение дисциплины (модуля) *«Математика»* базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала дисциплины (модуля): *«Информатика и основы информационно-коммуникационных технологий»*.

Перечень последующих дисциплин (модулей), для которых необходимы знания, умения и навыки, формируемые данной дисциплиной (модулем): : *«Программирование», «Физика»,* «П*роектирование баз данных».*

1.3 Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основнойпрофессиональной образовательной программы высшего образования – программы *бакалавриата*

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих общепрофессиональной компетенции: ОПК-1, в соответствии с основной профессиональной образовательной программой высшего образования – программой бакалавриата по направлению подготовки *09.03.04 Программная инженерия*.

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
	ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-3.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-3.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - основные понятия и методы алгебры и аналитической геометрии: числовые множества, уравнения прямых, плоскостей, кривых второго порядка в декартовой системе координат, матрицы и операции над ними, определители матриц и методы их вычисления, системы линейных алгебраических уравнений и методы их решения, конечномерные линейные пространства, базис, линейная зависимость и независимость векторов, матрицы перехода; -основные понятия и методы математического анализа; основные понятия теории чисел; основные положения теории пределов и непрерывных функций; основы дифференциального и интегрального исчисления функции одной и нескольких переменных.

				Уметь: - применять математические методы для решения практических задач;
				Владеть: - способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии, а также учебную и профессиональную литературу; - навыками применения современного математического инструментария для решения сложных профессиональных задач.

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1 Объем дисциплины (модуля), включая контактную работу обучающегося с педагогическими работниками и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля), изучаемой в 1, 2, 3, 4 семестрах, составляет 17 зачетных единиц. По дисциплине (модулю) предусмотрены *экзамены*.

Очная форма обучения

Вид учебной работы	**Всего часов**	**Семестры**				
		1	2	3	4	
Контактная работа обучающихся с педагогическими работниками	**306**	**54**	**90**	**72**	**90**	
Учебные занятия лекционного типа	62	14	16	16	16	
из них: в форме практической подготовки						
Практические занятия	92	16	34	24	18	

из них: в форме практической подготовки						
Лабораторные занятия	16				16	
из них: в форме практической подготовки						
Иная контактная работа	136	24	40	32	40	
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**162**	**18**	**54**	**36**	**54**	
Контроль промежуточной аттестации	**144**	**36**	**36**	**36**	**36**	
Форма промежуточной аттестации		экзам	экзам	экзам	экзам	
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**612**	**108**	**180**	**144**	**180**	

2.2. Учебно-тематический план дисциплины (модуля)

Очной формы обучения

Раздел, тема	**Виды учебной работы, академических часов**										
	Всего	**Самостоятельная работа**	**Контактная работа обучающихся с педагогическими работниками**								
			Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*
Модуль 1. Алгебра и геометрия (семестр 1)												
Раздел 1.1 Комплексные числа. Рациональные дроби. Матрицы и определители. Системы линейных алгебраических уравнений.	24	6	18		6		4				8	
Раздел 1.2 Собственные значения и	24	6	18		4		6				8	

собственные векторы матрицы. Конечномерные линейные пространства. Евклидовы пространства.												
Раздел 1.3 Векторы на плоскости. Векторы в пространстве.	24	6	18		4		6				8	
Контроль промежуточной аттестации (час)	**36**											
Общий объем, часов	**108**	**18**	**54**		**14**		**16**				**24**	
Форма промежуточной аттестации	**экзамен**											
Модуль 2. Дифференциальное и интегральное исчисление функции одной переменной (семестр 2)												
Раздел 2.1 Последовательность. Функция одной переменной. Пределы. Непрерывность. Исследование функции с помощью производных.	28	10	18		4		6				8	
Раздел 2.2 Функции нескольких переменных. Производные функции нескольких переменных. Экстремумы функции. нескольких переменных.	29	11	18		4		6				8	
Раздел 2.3 Первообразная. Методы интегрирования. Определенный интеграл. Несобственные интегралы.	29	11	18		4		6				8	
Раздел 2.4 Интегральное исчисление функции нескольких переменных. Тройной интеграл. Криволинейные	29	11	18		2		8				8	

интегралы												
Раздел 2.5 Тройной интеграл. Криволинейные интегралы	29	11	18		2		8				8	
Контроль промежуточной аттестации (час)	**36**											
Общий объем, часов	**180**	**54**	**90**		**16**		**34**				**40**	
Форма промежуточной аттестации	**экзамен**											
Модуль 3. Теория вероятностей и математическая статистика (семестр 3)												
Раздел 3.1 Элементы комбинаторики. Алгебра событий. Классическое определение вероятности.	27	9	18		4		6				8	
Раздел 3.2 Теоремы сложения и умножения вероятностей. Формулы полной вероятности и Байеса.	27	9	18		4		6				8	
Раздел 3.3 Первичная обработка статистических данных. Интервальные статистические оценки параметров нормального распределения. Проверка статистических гипотез.	27	9	18		4		6				8	
Раздел 3.4 Критерий согласия Пирсона. Основные понятия теории корреляции.	27	9	18		4		6				8	
Контроль промежуточной аттестации (час)	**36**											
Общий объем, часов	**144**	**36**	**72**		**16**		**24**				**32**	
Форма промежуточной аттестации	**экзамен**											

Модуль 4. Дифференциальное и интегральное исчисление функции нескольких переменных (семестр 4)												
Раздел 4.1 Дифференциальные уравнения первого порядка	26	10	16		4		2		2		8	
Раздел 4.2 Дифференциальные уравнения высших порядков.	29	11	18		4		4		2		8	
Раздел 4.3 Последовательность. Числовые ряды.	31	11	20		4		4		4		8	
Раздел 4.4 Степенные ряды. Функциональные ряды.	29	11	18		2		4		4		8	
Раздел 4.5 Ряды Фурье.	29	11	18		2		4		4		8	
Контроль промежуточной аттестации (час)	**36**											
Общий объем, часов	**180**	**54**	**90**		**16**		**18**		**16**		**40**	
Форма промежуточной аттестации	**экзамен**											
Общий объем, часов	**612**	**162**	**306**		**62**		**92**		**16**		**136**	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1. Виды самостоятельной работы обучающихся по дисциплине (модулю)

Очной формы обучения

Раздел, тема	Всего	Виды самостоятельной работы обучающихся					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**

Модуль 1. Алгебра и геометрия (семестр 1)							
Раздел 1.1 Комплексные числа. Рациональные дроби. Матрицы и определители. Системы линейных алгебраических уравнений.	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2 Собственные значения и собственные векторы матрицы. Конечномерные линейные пространства. Евклидовы пространства.	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3 Векторы на плоскости. Векторы в пространстве.	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**18**	**6**		**6**		**6**	
Модуль 2. Дифференциальное и интегральное исчисление функции одной переменной (семестр 2)							
Раздел 2.1 Последовательность. Функция одной переменной. Пределы. Непрерывность. Исследование функции с помощью производных.	10	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2 Функции нескольких переменных. Производные функции нескольких переменных. Экстремумы функции. нескольких переменных.	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 2.3 Первообразная. Методы интегрирования. Определенный интеграл. Несобственные интегралы.	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.4 Интегральное исчисление функции нескольких переменных. Тройной интеграл. Криволинейные интегралы	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.5 Тройной интеграл. Криволинейные интегралы	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**54**	**20**		**24**		**10**	
Модуль 3. Теория вероятностей и математическая статистика (семестр 3)							
Раздел 3.1 Элементы комбинаторики. Алгебра событий. Классическое определение вероятности.	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.2 Теоремы сложения и умножения вероятностей. Формулы полной вероятности и Байеса.	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.3 Первичная обработка статистических данных. Интервальные статистические оценки параметров нормального распределения. Проверка статистических гипотез.	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 3.4 Критерий согласия Пирсона. Основные понятия теории корреляции.	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**36**	**12**		**16**		**8**	
Модуль 4. Дифференциальное и интегральное исчисление функции нескольких переменных (семестр 4)							
Раздел 4.1 Дифференциальные уравнения первого порядка	10	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.2 Дифференциальные уравнения высших порядков.	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.3 Последовательность. Числовые ряды.	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.4 Степенные ряды. Функциональные ряды.	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.5 Ряды Фурье.	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	Расчетно-графическая работа	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**54**	**20**		**24**		**10**	
Общий объем по дисциплине (модулю), часов	**162**	**58**		**70**		**34**	

3.2 Методические указания к самостоятельной работе по дисциплине (модулю)

Модуль 1. Алгебра и геометрия

Цель:

Целями освоения модуля «Алгебра и геометрия» являются приобретение студентами знаний теоретических основ линейной алгебры и аналитической геометрии с последующим применением навыков на практике, а также применение знаний по дисциплине в научно-исследовательской и профессиональной деятельности ОПК-1.

Перечень изучаемых элементов содержания

Элементы линейной алгебры и аналитической геометрии		
Раздел 1.1.	Комплексные числа	Числовые множества. Множество комплексных чисел. Алгебраическая, тригонометрическая и показательная форма комплексного числа. Операции над комплексными числами. Формула Эйлера.
	Рациональные дроби	Рациональные дроби. Разложение рациональной дроби на сумму простейших дробей.
	Матрицы и определители	Матрицы, операции над матрицами. Элементарные преобразования строк матрицы. Приведение матрицы к ступенчатому виду и виду Гаусса. Ранг матрицы. Определитель квадратной матрицы, его свойства. Методы вычисления определителей. Обратная матрица: свойства, способы построения.
	Системы линейных алгебраических уравнений	Совместность и определенность системы линейных алгебраических уравнений. Теорема Кронекера-Капелли. Решение систем линейных алгебраических уравнений с помощью обратной матрицы и правила Крамера. Решение систем линейных алгебраических уравнений методом Гаусса. Линейная однородная система алгебраических уравнений, ее фундаментальная система решений. Связь решений линейных однородных и неоднородных систем.
Раздел 1.2.	Собственные значения и собственные векторы матрицы	Собственные значения, собственные векторы матрицы. Присоединенные векторы матрицы. Спектр матрицы.
	Конечномерные линейные пространства	Линейные пространства. Линейная зависимость и независимость векторов. Базис и размерность пространства. Координаты вектора в заданном

		базисе. Преобразование координат при переходе к новому базису.
	Евклидовы пространства	Евклидовы пространства. Норма и ее свойства. Скалярное произведение. Ортогональный и ортонормированный базисы. Процесс ортогонализации Грамма-Шмидта.

Раздел 1.3.	Векторы на плоскости	
		Векторы: координаты, проекция вектора на ось, направляющие косинусы, линейные операции над векторами. Скалярное произведение двух векторов и его свойства. Векторное произведение двух векторов, его свойства.
	Векторы в пространстве	Смешанное произведение трех векторов и его свойства. Способы вычисления векторного и смешанного произведения. Взаимное расположение векторов. Приложения.
Раздел 1.4.	Уравнение прямой на плоскости	Вывод уравнения прямой на плоскости с помощью направляющего вектора, в параметрическом виде, каноническое уравнение прямой и уравнение прямой с угловым коэффициентом.
	Кривые второго порядка	Кривые второго порядка, их канонические уравнения. Приведение уравнений кривых второго порядка к каноническому виду.
	Прямая и плоскость	Уравнение плоскости. Уравнение прямой в пространстве. Взаимное расположение прямой и плоскости.

Вопросы для самоподготовки:

Векторы: координаты, проекция вектора на ось, направляющие косинусы.

Линейные операции над векторами.

Скалярное произведение двух векторов и его свойства.

Векторное произведение двух векторов, его свойства.

Смешанное произведение трех векторов и его свойства.

Взаимное расположение векторов.

Множества. Операции над множествами, свойства.

Декартова система координат. Преобразование координат на плоскости.

Прямая на плоскости. Различные виды уравнения прямой на плоскости.

Кривые второго порядка.

Уравнение плоскости.

Уравнение прямой в пространстве.

Взаимное расположение прямой и плоскости.

Поверхности второго порядка.

Понятие дифференциальной геометрии кривых и поверхностей.

Элементы топологии.

Линейные пространства. Линейная зависимость и независимость векторов.

Базис и размерность пространства.

Координаты вектора в заданном базисе. Преобразование координат при переходе к новому базису.

Линейный оператор, его матрица.

Преобразование матрицы линейного оператора при смене базиса.

Евклидовы пространства. Норма и ее свойства.

Ортогональный и ортонормированный базисы.

Процесс ортогонализации Грамма-Шмидта.

Квадратичные формы.

Понятие алгебраической структуры.

Комплексные числа, действия с комплексными числами.

Многочлены. Основная теорема алгебры.

Теорема Безу. Разложение многочлена на множители.

Рациональные дроби. Разложение рациональной дроби на сумму простейших дробей.

Матрицы, операции над матрицами.

Элементарные преобразования строк матрицы.

Приведение матрицы к ступенчатому виду и виду Гаусса.

Ранг матрицы. Ранг системы векторов.

Определитель квадратной матрицы, его свойства. Методы вычисления определителей.

Обратная матрица: свойства, способы построения.

Совместность и определенность системы линейных алгебраических уравнений. Теорема Кронекера-Капелли.

Решение систем линейных алгебраических уравнений с помощью обратной матрицы.

Решение систем линейных алгебраических уравнений с помощью правила Крамера.

Решение систем линейных алгебраических уравнений методом Гаусса.

Линейная однородная система алгебраических уравнений, ее фундаментальная система решений.

Связь решений линейных однородных и неоднородных систем.

Собственные значения, собственные векторы матрицы.

Присоединенные векторы матрицы.

Модуль 2. Дифференциальное и интегральное исчисление функции одной переменной

Цель:

Целями освоения модуля «Дифференциальное и интегральное исчисление функции одной переменной» являются приобретение студентами знаний теоретических основ дифференциальное исчисления функций одной переменной с последующим применением навыков на практике, а также применение знаний по дисциплине в научно-исследовательской и профессиональной деятельностиОПК-1.

Перечень изучаемых элементов содержания

Дифференциальное и интегральное исчисление функции одной переменной		
Раздел 2.1.	Последовательность. Функция.Пределы. Непрерывность	Последовательность. Функция. Способы задания функции. Основные элементарные функции. График. Предел функции. Непрерывность.
Раздел 2.2.	Производные Производная функции.	Собственные значения, собственные векторы матрицы. Присоединенные векторы матрицы. Спектр матрицы. Производная функции. Правила

		вычисления производной. Производная сложной функции. Производные высших порядков. Дифференцируемость функции.
	Исследование функции с помощью производных.	Теоремы о связи дифференцируемости с непрерывностью и с существованием производной. Дифференциал функции. Исследование функции с помощью производных.
Раздел 2.3.	Первообразная.	Первообразная. Неопределенный интеграл: определение, свойства, таблица основных интегралов.
	Методы интегрирования	Методы интегрирования: табличный, разложения. Интегрирование подведением под знак дифференциала. Интегрирование с помощью замены переменной.
Раздел 2.4.	Определенный интеграл	Определенный интеграл, интеграл Римана: определение, свойства, формула Ньютона-Лейбница, методы интегрирования, приложения.
	Несобственные интегралы	Интегралы с переменным верхним пределом. Интегралы с бесконечными пределами: определения, свойства. Признаки сходимости. Методы вычисления несобственных интегралов Интегралы от разрывных функций. Главное значение несобственного интеграла

Вопросы для самоподготовки:

Последовательность. Предел числовой последовательности.

Функция. Способы задания функции.

Предел функции в точке. Односторонние пределы. Предел функции на бесконечности.

Непрерывность функции. Точки разрыва функции и их классификация.

Производная функции: определение, геометрический смысл.

Правила вычисления производной.

Производная сложной функции.

Производные высших порядков.

Дифференцируемость функции.

Теоремы о связи дифференцируемости с непрерывностью и с существованием производной.

Дифференциал функции и его геометрический смысл.

Инвариантность формы первого дифференциала.

Раскрытие неопределенностей (правило Лопиталя).

Исследование функции: область определения, четность (нечетность), точки пересечения с координатными осями, промежутки знакопостоянства, непрерывность, точки разрыва.

Асимптоты графика функции.

Достаточные условия монотонности функции.

Достаточные условия экстремумов функции.

Достаточные условия выпуклости, вогнутости, точки перегиба графика функции.

Общая схема исследования функции и построение графика.

Первообразная. Неопределенный интеграл: определение. Теорема об общем виде первообразных.

Основные свойства неопределенного интеграла.

Таблица основных интегралов.

Методы интегрирования: табличный, разложения.

Интегрирование подведением под знак дифференциала.

Интегрирование с помощью замены переменной.

Определенный интеграл: определение, свойства.

Формула Ньютона- Лейбница.

Вычисление определенного интеграла с помощью замены переменной.

Некоторые приложения определенного интеграла.

Интегралы с бесконечными пределами: определения, свойства.

Модуль 3. Теория вероятностей и математическая статистика

Цель:

Целью учебного модуля «Теория вероятностей и математическая статистика » является знакомство с теоретико-вероятностным подходом при составлении и анализе математических моделей реальных ситуаций, изучение основных методов математической обработки статистической информации, имеющих применение в практической деятельности будущего выпускникаОПК-1.

Перечень изучаемых элементов содержания

№ п/п	Наименование разделов и тем дисциплины	Содержание темы
РАЗДЕЛ 3.1.	Элементы комбинаторики	Элементы комбинаторики. Формулы для вычисления количества перестановок, размещений и сочетаний.
	Алгебра событий. Классическое определение вероятности	Случайные события, их классификация. Алгебра событий. Классическое и статистическое определения вероятности события.
РАЗДЕЛ 3.2.	Теоремы сложения и умножения вероятностей	Теоремы сложения и умножения вероятностей. Понятия несовместности и независимости событий. Повторные испытания, схема Бернулли.
	Формулы полной вероятности и Байеса.	Формула полной вероятности. Формула Байеса. Решение задач на вычисление вероятности события с применением всех изученных методов.
РАЗДЕЛ 3.3.	Первичная обработка статистических данных	Основные понятия математической статистики – генеральная совокупность, выборка и ее характеристики, частота и относительная частота, статистический ряд, интервальный ряд. Построение полигона и гистограммы. Точечные оценки математического ожидания, дисперсии и среднего квадратического отклонения. Метод условных вариант.
	Интервальные статистические оценки параметров нормального распределения	Построение доверительных интервалов для математического ожидания и дисперсии, среднего квадратического отклонения для нормального распределения.
	Проверка статистических гипотез	Понятие статистической гипотезы. Критическая область и область принятия гипотезы. Ошибки первого и второго рода. Схема проверки

		гипотезы на примере сравнения двух и нескольких дисперсий нормальных генеральных совокупностей. Проверка гипотезы о равенстве двух средних нормальных генеральных совокупностей в случаях известной и неизвестной дисперсии. Сравнение выборочной средней с гипотетической генеральной средней нормальной генеральной совокупности.
РАЗДЕЛ 3.4.	Критерий согласия Пирсона	Проверка гипотезы о нормальном распределении на основе критерия согласия Пирсона.
	Основные понятия теории корреляции	Ковариация, корреляция. Выборочный коэффициент корреляции, проверка гипотезы о его значимости. Построение линии регрессии.

Вопросы для самоподготовки:

Перестановки, сочетания и размещения с повторениями и без повторений. Комбинаторные формулы для подсчета их количества.

Классическое определение вероятности события. Понятия эксперимента, элементарных исходов, вычисление вероятности события в простейших случаях. Примеры.

Теорема о сложении вероятностей. Пример применения.

Теорема об умножении вероятностей. Пример применения.

Схема Бернулли. Вычисление вероятности наступления k успехов в n испытаниях. Пример.

Зависимые события. Формула условной вероятности. Пример применения.

Полная группа событий. Формула полной вероятности. Пример применения.

Формула Байеса. Пример применения.

Дискретная случайная величина. Закон распределения. Пример составления закона распределения для дискретной случайной величины.

Функция распределения дискретной случайной величины. Пример вычисления и построения графика.

Биномиально распределенная случайная величина. Определение, пример.

Числовые характеристики дискретных случайных величин. Физический смысл и правила вычисления.

Непрерывная случайная величина. Определение и пример. Функция плотности непрерывной случайной величины. Свойства функции плотности.

Функция распределения непрерывной случайной величины, ее свойства.

Равномерно распределенная случайная величина. Пример. Вид функции распределения. Числовые характеристики равномерно распределенной случайной величины.

Нормально распределенная случайная величина. Вид функции распределения. Числовые характеристики нормально распределенной случайной величины. Вероятность попадания нормально распределенной случайной величины в заданный интервал.

Дискретная двумерная случайная величина. Безусловный и условные законы распределения. Зависимость и независимость компонент.

Понятие ковариации двух случайных величин. Свойства ковариации. Коэффициент корреляции, его свойства.

Модуль 4. Дифференциальное и интегральное исчисление функции нескольких переменных

Цель:

приобретение студентами знаний теоретических основ дифференциального и интегрального исчисления функции нескольких переменных с последующим применением навыков на практике, а также применение знаний по дисциплине в научно-исследовательской и профессиональной деятельности ОПК-1.

Перечень изучаемых элементов содержания

Дифференциальное и интегральное исчисление функции одной переменной		
Раздел 4.1.	Функции нескольких переменных	Функции нескольких переменных: определение, геометрическая интерпретация, линии уровня, предел функции в точке, частные производные первого и второго порядков. Полный дифференциал. Производная сложной функции. Производная функции по направлению.

Раздел 4.2.	Производные Производная функции.	Градиент функции и его свойства. Ротор, дивергенция векторного поля.
	Экстремумы функции нескольких переменных	Экстремумы функции двух переменных: необходимое и достаточное условия экстремума. Условный экстремум (метод множителей Лагранжа). Наибольшее и наименьшее значения функции в замкнутой области.
Раздел 4.3.	Интегральное исчисление функции нескольких переменных	Двойной интеграл, его свойства, вычисление, применение. Геометрический смысл двойного интеграла. Вычисление двойного интеграла в декартовой системе координат
	Тройной интеграл	Тройной интеграл, его свойства, вычисление, применение.
Раздел 4.4.	Криволинейные интегралы	Криволинейный интеграл, его свойства, вычисление, применение.
		Формула Грина

Вопросы для самоподготовки:

Функции нескольких переменных: область определения, линии уровня, геометрическая интерпретация.

Предел функции в точке, частные производные первого и второго порядков функции нескольких переменных.

Частные производные первого порядка.

Частные производные второго порядка.

Полный дифференциал (для функции двух переменных).

Производная сложной функции.

Производная функции по направлению.

Градиент функции и его свойства.

Экстремумы функции двух переменных: необходимое и достаточное условия экстремума.

Условный экстремум (метод множителей Лагранжа).

Наибольшее и наименьшее значения функции в замкнутой области.

Двойной интеграл, его свойства, вычисление, применение.

Тройной интеграл, его свойства, вычисление, применение.

Криволинейный интеграл, его свойства, вычисление, применение.

Формула Грина.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.1

Форма практического задания: расчетно-графические работы.

1. Выполнить действия: а) $\frac{(2+5i)\cdot(-3+i)}{4-3i}$; б) $\sqrt[3]{-8}$;

в) $3z_1 \cdot z_2 - 4\cdot(z_1 - 2z_2) + \frac{z_1}{z_1 + z_2}$, если $z_1 = -2 - i$, $z_2 = -3 - 2i$.

2. Разложить многочлен на множители

$$f(x) = x^4 - 2x^3 + 5x^2 - 8x + 4.$$

3. Разложить рациональную дробь на сумму простейших дробей:

а) $\frac{x^2 + 2x + 3}{(x-1)\cdot(x^3 - 1)}$; б) $\frac{3x^3 - x^2 - 8x + 13}{x^2 + x - 2}$.

4. Вычислить матрицу $3A - 2B$, если

$$A = \begin{pmatrix} 0 & 1 & 2 \\ -1 & 7 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 4 & 3 & -1 \\ 0 & 5 & 6 \end{pmatrix}.$$

5. Выполнить действия и найти ранг полученной матрицы:

$$\begin{pmatrix} 0 & 1 & 2 \\ -1 & 7 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -3 & 0 \\ 2 & -1 \end{pmatrix}.$$

6. Решить матричное уравнение $B \cdot X = A$,

где $A=\begin{pmatrix}-13 & 24\\ 18 & 6\end{pmatrix}$, $B=\begin{pmatrix}-1 & 5\\ 6 & 0\end{pmatrix}$.

7. Решить систему по правилу Крамера:

$$\begin{cases}2x-3y+z=-7\\ x+4y+2z=-1\\ x-4y=-5.\end{cases}$$

8. Исследовать систему на совместность, найти методом Гаусса общее решение, а затем одно частное решение:

$$\begin{cases}5x_1+12x_2+5x_3+3x_4=10\\ 4x_1+x_3=2-3x_2-3x_4\\ 11\cdot(x_1+x_2)+4\cdot(x_3+x_4)=8-4x_4\end{cases}$$

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.2

форма рубежного контроля – контрольная работа.

1. Решить систему методом Крамера и с помощью обратной матрицы

$$\begin{cases}x+y+z=1\\ 2x+2y+z=1\\ x+3y+2z=3\end{cases}$$

2. Решить систему уравнений методом Гаусса

$$\begin{cases}2x-y-z=-3\\ x+y-8z=33\\ y-5z=23\end{cases}$$

3. Найти собственные значения и собственные векторы матрицы

$$\begin{pmatrix} 5 & -6 & 6 \\ 1 & 0 & 1 \\ -2 & 4 & -3 \end{pmatrix}$$

4. Найти матрицу перехода от нового базиса f_1, f_2, f_3 к старому базису e_1, e_2, e_3.

$$\overrightarrow{e_1} = (1;0;1);\ \overrightarrow{e_2} = (1;1;0);\ \overrightarrow{e_3} = (0;1;1);$$
$$\overrightarrow{f_1} = (1;-1;0);\ \overrightarrow{f_2} = (1;0;-1);\ \overrightarrow{f_3} = (0;1;-1)$$

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.3

Форма практического задания: расчетно-графические работы.

1. Построить радиус-вектор данной точки А. Найти расстояние от точки А(1;-2;3) до оси ОХ. Найти расстояние от точки А(0;-2;-3) до плоскости XOY.

2. Из начала координат построить вектор АВ. Найти направляющие косинусы этого вектора . Отметить на чертеже углы α, β, γ. А(1;3;-2); В(3;5;0).

3. Найти вектор DE+FE, если D(2;3;-4); E(1;6;4); F(0;-3;5).Найти косинус угла ВСА в треугольнике АВС и площадь этого треугольника, если А(3;6;-2); В(1;8;1) и С(-1;5;-3).

4. Найти объём пирамиды ABCD и длину высоты, опущенной из вершины D, если А(3;6;-2); В(1;8;1); С(-1;5;-3); D(0;-3;2).

5.В треугольнике АВС найти точку пересечения стороны АС с высотой, опущенной из вершины В. Задание выполнить графически и аналитически. А(6;-2); В(8;1) и С(5;-3).

6. Написать уравнение плоскости, проходящей через точку А перпендикулярно вектору АВ. А(1;3;-2); В(3;5;0).

7. Написать канонические уравнения прямой DE, где D(2;3;-4); E(1;6;4).

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1. 4

форма рубежного контроля – контрольная работа.

1. Найти уравнение прямой, проходящей через точку $M(-2;6)$

а) параллельно прямой $5x+3y-7=0$;

б) перпендикулярно прямой $5x+3y-7=0$.

2. Написать уравнение плоскости, проходящей через три точки:

$$M_1(1;2;3),\ M_2(3;0;1)\ \text{и}\ M_3(1;-2;-3).$$

3. Найти угол между прямой, заданной уравнениями

$$\begin{cases} x=2z-1 \\ y=-2z+1, \end{cases}$$

и прямой, проходящей через начало координат и точку $(1;2;-2)$.

4.Векторы $\bar{a}$ и $\bar{b}$ образуют угол $\varphi=\frac{\pi}{6}$. Зная, что $|\bar{a}|=3$ и $|\bar{b}|=2$, вычислить

$$\left|(3\bar{a}-\bar{b})\times(\bar{a}-2\bar{b})\right|.$$

5. Найти объем пирамиды *ABCD*, если

$$A(3;10;-1),\quad B(-2;3;-5),\quad C(-6;0;-3),\quad D(1;-1;2).$$

6. Определить тип кривой:

$$2x^2-3x+7y^2+2y=9.$$

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.1

Форма практического задания: расчетно-графические работы.

1. Вычислить пределы:

а) $\lim\limits_{n\to\infty}\frac{(n-2)\cdot(n-4)\cdot(n-6)}{n^3}$, б) $\lim\limits_{x\to\infty}\frac{x^2-3x+2}{4x^2+5}$, в) $\lim\limits_{x\to 0}\frac{\sqrt{x+4}-2}{x}$.

2. Используя 1-й и 2-й замечательные пределы, найти пределы:

а) $\lim\limits_{x\to 0}\frac{\sin 4x+3x^2}{5x}$, б) $\lim\limits_{x\to\infty}\left(\frac{4+x}{5-x}\right)^{2x}$.

3. Для данной функции $y=f(x)$ найти точки разрыва, если они существуют. Дать их классификацию. Сделать эскиз графика функции.

$$y=\begin{cases}3^x, & x\le 0,\\ \sin x, & 0<x<\pi,\\ 0, & x\ge\pi.\end{cases}$$

4. В точке $x=3$ найти значение производной функции

$$y=\frac{1}{(x-1)^2}+\sqrt{x+1}\,.$$

5. Найти производные функций:

а) $y=\sin \operatorname{arcctg}^3\frac{\sqrt[3]{2x^2}}{5-2x^3}$, б) $y=3^{\cos 2x}\cdot \operatorname{tg}x^3$.

6. Раскрыть неопределенность, используя правило Лопиталя:

а) $\lim\limits_{x\to 0}\frac{2^{x^2}-1}{\cos 2x-1}$; б) $\lim\limits_{x\to+0}(\ln 2x\cdot \operatorname{tg}3x)$; в) $\lim\limits_{x\to+0}\left(\operatorname{arcctg}2x-\pi/2\right)\cdot\ln\sin 3x\right)$.

7. Найти асимптоты графика функции

$$f(x)=\frac{x^2+5}{x-3}.$$

8. Найти точки перегиба, промежутки выпуклости и вогнутости графика функции

$$f(x)=\frac{2x^2}{1+x^2}.$$

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.2

форма рубежного контроля – контрольная работа.

1.Вычислить пределы:

а) $\lim\limits_{n\to\infty}\frac{(n+1)\cdot(n+2)\cdot(n+3)}{n^3}$, б) $\lim\limits_{x\to\infty}\frac{x^2-5x+1}{3x^2+7}$, в) $\lim\limits_{x\to 0}\frac{\sqrt{x+9}-3}{x}$.

2.Используя 1-й и 2-й замечательные пределы, найти пределы:

а) $\lim\limits_{x\to 0}\frac{\sin 5x+4x^2}{2x}$, б) $\lim\limits_{x\to\infty}\left(\frac{2+x}{3-x}\right)^x$.

3. Исследовать на непрерывность данную функцию, определить тип точек разрыва, если они есть, сделать эскиз графика функции:

$$f(x)=\begin{cases}\sin 2x, & \text{если } x\le \pi/4,\\ \cos 2x, & \text{если } \pi/4<x<\pi,\\ 1, & \text{если } x\ge \pi.\end{cases}$$

4.Найти производные функций:

а) $y=\log_2{}^3(tg3x)$, б) $y=\left(1+e^{-x}\right)^{\cos x}$.

5.Раскрыть неопределенность, используя правило Лопиталя:

а) $\lim\limits_{x\to 0}\dfrac{\sin 5x+4x^2}{2x}$; б) $\lim\limits_{x\to+\infty}\dfrac{3e^x+8+\ln x}{x^3-2x}$; в) $\lim\limits_{x\to\infty}\dfrac{\frac{\pi}{2}-arctgx}{e^{3/x}-1}$.

6. Вычислить

$$y''(0), \text{ если } y=x^2\cdot e^{x^2}.$$

7.Найти асимптоты графика функции

$$y=\frac{x^3-8}{x^2-4}.$$

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.3

Форма практического задания: расчетно-графические работы.

1. Найти неопределенные интегралы:

а $\int\left(6+\dfrac{1}{x^3}-\dfrac{2}{\sin^2(3x-5)}-\dfrac{3}{x^2+4x+7}\right)dx$, б) $\int\dfrac{5^{1/x^2}}{x^3}dx$, в) $\int\dfrac{3x+1}{x(x-1)}\mathrm{d}x$.

2. Вычислить определенные интегралы:

а) $\int\limits_0^{3\pi/2}\cos\dfrac{x}{3}dx$, б) $\int\limits_0^4\dfrac{dx}{1+\sqrt{x}}$.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.4: форма рубежного контроля – контрольная работа.

1. Найти неопределенные интегралы:

а) $\int\left(4x^2+3x+11\right)\mathrm{d}\,x$, б) $\int\frac{2x+7}{x^2+7x+1}\mathrm{d}\,x$,

в) $\int\frac{3x+1}{x(x-1)}\mathrm{d}\,x$, г) $\int(2x+7)\sin(3x)dx$

2. Вычислить определенные интегралы:

а) $\int\limits_0^{\pi/2}\frac{dx}{2+\cos x}$, б) $\int\limits_4^9\frac{\sqrt{x}}{\sqrt{x}-1}dx$.

3. Вычислить несобственный интеграл

$$\int\limits_e^{+\infty}\frac{dx}{x\sqrt{\ln x}}$$

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3.1

Форма практического задания: расчетно-графические работы.

1. В магазин поступило 30 новых телевизоров, среди которых 5 имеют скрытые дефекты. Наудачу отбирается один телевизор. Какова вероятность того, что он не имеет скрытых дефектов?

2. Из партии, содержащей 10 изделий, среди которых 3 бракованных, наудачу извлекают 3 изделия. Найти вероятность того, что ровно одно из них бракованное.

3. Для сигнализации об аварии установлены два независимо работающих сигнализатора. Вероятность того, что при аварии сигнализатор сработает, равна 0,99 для первого сигнализатора и 0,95 для второго. Найти вероятность того, что при аварии сработает только один сигнализатор.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3.2: форма рубежного контроля – контрольная работа.

1. Найти вероятность выпадения одинаковых чисел при однократном подкидывании двух игральных кубиков.

2. В коллекции 10 монет, из которых 4 имеют дефекты. Коллекционер выбирает наугад 7 монет. Найти вероятность, что 2 из них будут с дефектами.

3. В зимний период вероятность задержки авиарейса составляет 0.45. Найти вероятность, что из трех рейсов хотя бы один задержат.

4. В среднем пять человек из 100 готовы сменить работу на менее оплачиваемую, но находящуюся недалеко от места проживания. Приближенно вычислить вероятность, что из 300 опрошенных людей 80 согласятся на такую смену работы.

5. Три автомобильных концерна поставляют на продажу автомобили в соотношении 40%, 30% и 30%. Вероятность того, что автомобиль, поставленный первым концерном, не будет бракованным, равна 0.7, для второго концерна такая вероятность 0.8, для третьего – 0.85. Куплен бракованный автомобиль. Найти вероятность, что он поставлен первым концерном.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3.3

Форма практического задания: расчетно-графические работы.

1. Дискретная случайная величина X задана рядом распределения. Найти:

1) функцию распределения $F(X)$ и её график;

2) математическое ожидание $M[X]$;

3) дисперсию $D[X]$.

X	1	3	4	7	8
P	0,1	0,2	0,25	0,3	0,15

2. Задана непрерывная случайная величина X с помощью плотности распределения вероятностей $f(x)$, сосредоточенная на отрезке $[a;b]$.

а) Найти функцию распределения $F(X)$ и ее график.

б) Найти математическое ожидание $M[X]$.

в) Найти дисперсию $D[X]$.

г) Найти вероятность попадания в интервал $\left(\frac{a+b}{2};\frac{3b-a}{2}\right)$.

$$f(x)=\begin{cases}0;\ x\le 0\\ 3x^2-2x+1;\ 0<x\le 1\\ 0;\ x>1.\end{cases}$$

3.Провести полную обработку экспериментальных данных по заданной выборке объема n, взятой из генеральной совокупности нормально распределенной случайной величины X с заданной доверительной вероятностью $\gamma=0,9$.:

6,28; 6,31; 6,23; 6,35; 6,32; 6,36; 6,33; 6,31; 6,26; 6,21; 6,31; 6,38; 6,34; 6,25; 6,28; 6,39; 6,27; 6,32; 6,9; 6,30; 6,24; 6,32; 6,26; 6,35; 6,32; 6,31; 6,29; 6,28; 6,33; 6,36.

а). Найти вариационный ряд, полигон частот.

б) Составить интервальную таблицу по данным выборки (взять 7-10 интервалов), построить гистограмму частот.

в) Методом условных вариант найти выборочное среднее $\overline{X}$ и выборочную дисперсию S^2:

$$\overline{X}=\frac{1}{n}\sum_{i=1}^{n}x_i,\quad S^2=\frac{1}{n-1}\sum_{i=1}^{n}(x_i-\overline{X})^2.$$

.

г). Найти доверительный интервал для $m=M[x]$:

в случае известной σ ($\sigma=S$),

в случае неизвестной σ.

д) Найти доверительный интервал для среднеквадратичного отклонения $\sigma=\sqrt{D[x]}$.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3.4

форма рубежного контроля – контрольная работа.

1. Согласно многолетним исследованиям, можно утверждать, что в среднем один человек из шести мечтает полностью изменить свое окружение. Случайная величина равна количеству таких «мечтателей» среди пяти опрошенных людей. Составить закон распределения данной случайной величины и вычислить ее математическое ожидание.

2. Дискретная случайная величина задана своим законом распределения:

	2		.25	.5	.5
		.15	.05	.2	.25

Вычислить математическое ожидание, дисперсию, среднее квадратическое отклонение данной случайной величины. Задать функцию распределения аналитически и с помощью графика. Вычислить вероятность того, что случайная величина примет значение, не меньшее 1.

3. Рассматривается нормально распределенная случайная величина с параметрами $a = 2, \quad \sigma = 8$. Найти вероятность того, что

а) случайная величина примет значение из интервала $(-1;10)$.

б) значение случайной величины будет больше чем 7.

4. Дискретная двумерная случайная величина задана законом распределения:

X \ Y				
-2	.05		.25	.15
2	.15	.15	.05	.1

а) Зависимы ли компоненты?

б) Выписать закон распределения с.в. X+Y и условный закон распределения с.в. X при условии, что Y=0.

в) Найти $\mathrm{cov}(5X - 2Y; 3X + Y)$.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4.1

Форма практического задания: расчетно-графические работы.

1. Найти частные производные функции

$$u = \frac{1}{2} z x^{-2y} - \operatorname{arctg}^3 2y \cdot \lg(5y^2 - x).$$

2. Найти дифференциал функции

$$z = xy \cos xy.$$

3. Исследовать на локальные экстремумы функцию

$$z = 3xy - 5x^2 - 2y^2 + 1.$$

4. Найти наибольшее и наименьшее значения функции

$$z = x^2 + y^2 - 2x + 3y \text{ в области } x^2 + y^2 \le 13.$$

5. Указать направление и величину наибольшего роста функции

$$z = x^2 - 2x + y^2 - 4 \text{ в точке } M_0(-2; 0).$$

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4.2

форма рубежного контроля – контрольная работа.

1. Найти частные производные первого порядка функции

$$z = x^2 + 2x + y^2 - 3 \text{ в точке } M_0(-1;2).$$

2. Найти полный дифференциал функции

$$z = arctg(xy) - \sqrt{x^3 + y^3}.$$

3. Найти градиент функции

$$z = \ln\left(2x^4 + 4y^2\right) \text{ в точке } M_0(4;-2).$$

4. Найти экстремумы функции двух переменных:

$$z = x^2 - xy + y^2 + 9x - 6y + 20.$$

5. Найти условные экстремумы функции

$$z = 4y^2 - 10x^2, \text{ если } 5x + y = 16.$$

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4.3

Форма практического задания: расчетно-графические работы.

1. Изменить пределы интегрирования в двойном интеграле

$$\int_{-2}^{-1} dy \int_{-(2+y)}^{0} f\ dx + \int_{-1}^{0} dy \int_{\sqrt[3]{y}}^{0} f\ dx$$

2. Вычислить объём тела, ограниченного поверхностями:

$$x + y = 6,\ \ y = \sqrt{3x},$$
$$z = 4y,\ \ z = 0.$$

3. Вычислить

$$\iint_D 3y^2 \sin\frac{xy}{2}\ dxdy;$$
$$D:\ x = 0,\ y = \sqrt{\frac{4\pi}{3}},\ y = \frac{2}{3}x.$$

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4.4:

форма рубежного контроля – контрольная работа.

1.Вычислить двойной интеграл

$$\iint_D (1 - x - 2y)dxdy$$

по области D, ограниченной следующими линиями

$$x = 2y^2,\ \ x = 2,\ \ y = 4.$$

2.Вычислить следующий криволинейный интеграл

$$\int_{(0,1)}^{(3,-4)} x\,dx + y\,dy.$$

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по учебной дисциплине (модулю) является **экзамен,** который проводится в **письменной** форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	**Знать:** - основные понятия и методы алгебры и аналитической геометрии: числовые множества, уравнения прямых, плоскостей, кривых второго порядка в декартовой системе координат, матрицы и операции над ними, определители матриц и методы их вычисления, системы линейных алгебраических уравнений и методы их решения, конечномерные линейные пространства, базис, линейная зависимость и независимость векторов, матрицы перехода; -основные понятия и методы математического анализа; основные понятия теории чисел; основные положения теории пределов и непрерывных функций; основы дифференциального и интегрального исчисления функции одной и	Этап формирования знаний

		нескольких переменных.	
		Уметь: - применять математические методы для решения практических задач;	Этап формирования умений
		Владеть: - способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии, а также учебную и профессиональную литературу; - навыками применения современного математического инструментария для решения сложных профессиональных задач.	Этап формирования навыков и получения опыта

4.3 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Этапы формирования компетенций	Показатель оценивания компетенции	Критерии и шкалы оценивания
ОПК-3	Этап формирования знаний.	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок: (9-10] баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в

			ответе на вопрос, может правильно применять теоретические положения: [8-9) баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала: (6-8) баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки: [0-6] баллов.
ОПК-3	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией: (9-10] баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании: [8-9) баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению: (6-8) баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания: [0-6] баллов.
ОПК-3	Этап формирования навыков и получения опыта.	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

4.4 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

1 семестр. Модуль «Алгебра» и модуль «Геометрия»

Теоретический блок вопросов:

1. Понятие алгебраической структуры.
2. Комплексные числа, действия с комплексными числами.
3. Многочлены. Основная теорема алгебры.
4. Теорема Безу. Разложение многочлена на множители.
5. Рациональные дроби. Разложение рациональной дроби на сумму простейших дробей.
6. Матрицы, операции над матрицами.
7. Элементарные преобразования строк матрицы.
8. Приведение матрицы к ступенчатому виду и виду Гаусса.
9. Ранг матрицы. Ранг системы векторов.
10. Определитель квадратной матрицы, его свойства. Методы вычисления определителей.
11. Обратная матрица: свойства, способы построения.
12. Совместность и определенность системы линейных алгебраических уравнений. Теорема Кронекера-Капелли.
13. Решение систем линейных алгебраических уравнений с помощью обратной матрицы.
14. Решение систем линейных алгебраических уравнений с помощью правила Крамера.
15. Решение систем линейных алгебраических уравнений методом Гаусса.
16. Линейная однородная система алгебраических уравнений, ее фундаментальная система решений. Связь решений линейных однородных и неоднородных систем.
17. Собственные значения, собственные векторы матрицы.
18. Присоединенные векторы матрицы.
19. Векторы: координаты, проекция вектора на ось, направляющие косинусы.
20. Линейные операции над векторами.
21. Скалярное произведение двух векторов и его свойства.
22. Векторное произведение двух векторов, его свойства.
23. Смешанное произведение трех векторов и его свойства.
24. Взаимное расположение векторов.
25. Множества. Операции над множествами, свойства.
26. Декартова система координат. Преобразование координат на плоскости.
27. Прямая на плоскости. Различные виды уравнения прямой на плоскости.
28. Кривые второго порядка.
29. Уравнение плоскости.
30. Уравнение прямой в пространстве.
31. Взаимное расположение прямой и плоскости.
32. Поверхности второго порядка.
33. Понятие дифференциальной геометрии кривых и поверхностей.
34. Элементы топологии.

35. Линейные пространства. Линейная зависимость и независимость векторов.
36. Базис и размерность пространства.
37. Координаты вектора в заданном базисе. Преобразование координат при переходе к новому базису.
38. Линейный оператор, его матрица.
39. Преобразование матрицы линейного оператора при смене базиса.
40. Евклидовы пространства. Норма и ее свойства.
41. Ортогональный и ортонормированный базисы.
42. Процесс ортогонализации Грамма-Шмидта.
43. Квадратичные формы.

Аналитическое задание:

Задачи, которые могут быть включены в экзаменационный билет, приведены в примерных вариантах контрольных работ и в расчетно-графических работах.

2 семестр.Модуль «Дифференциальное исчисление функции одной переменной» и модуль «Интегральное исчисление функции одной переменной»

Теоретический блок вопросов:

1. Последовательность. Предел числовой последовательности.
2. Функция. Способы задания функции.
3. Предел функции в точке. Односторонние пределы. Предел функции на бесконечности.
4. Непрерывность функции. Точки разрыва функции и их классификация.
5. Производная функции: определение, геометрический смысл.
6. Правила вычисления производной.
7. Производная сложной функции.
8. Производные высших порядков.
9. Дифференцируемость функции. Теоремы о связи дифференцируемости с непрерывностью и с существованием производной.
10. Дифференциал функции и его геометрический смысл. Инвариантность формы первого дифференциала.
11. Раскрытие неопределенностей (правило Лопиталя).
12. Исследование функции: область определения, четность (нечетность), точки пересечения с координатными осями, промежутки знакопостоянства, непрерывность, точки разрыва.
13. Асимптоты графика функции.
14. Достаточные условия монотонности функции.
15. Достаточные условия экстремумов функции.
16. Достаточные условия выпуклости, вогнутости, точки перегиба графика функции.
17. Общая схема исследования функции и построение графика.
18. Первообразная. Неопределенный интеграл: определение. Теорема об общем виде первообразных.
19. Основные свойства неопределенного интеграла.
20. Таблица основных интегралов.
21. Методы интегрирования: табличный, разложения.
22. Интегрирование подведением под знак дифференциала.
23. Интегрирование с помощью замены переменной.
24. Определенный интеграл: определение, свойства.
25. Формула Ньютона- Лейбница.
26. Вычисление определенного интеграла с помощью замены переменной.
27. Некоторые приложения определенного интеграла.
28. Интегралы с бесконечными пределами: определения, свойства.

Аналитическое задание:

Задачи, которые могут быть включены в экзаменационный билет, приведены в примерных вариантах контрольных работ и в расчетно-графических работах.

3 семестр.Модуль «Теория вероятностей» и модуль «Математическая статистика»

Теоретический блок вопросов:

1. Перестановки, сочетания и размещения с повторениями и без повторений. Комбинаторные формулы для подсчета их количества.
2. Классическое определение вероятности события. Понятия эксперимента, элементарных исходов, вычисление вероятности события в простейших случаях. Примеры.
3. Теорема о сложении вероятностей. Пример применения.
4. Теорема об умножении вероятностей. Пример применения.
5. Схема Бернулли. Вычисление вероятности наступления k успехов в n испытаниях. Пример.
6. Зависимые события. Формула условной вероятности. Пример применения.
7. Полная группа событий. Формула полной вероятности. Пример применения.
8. Формула Байеса. Пример применения.
9. Дискретная случайная величина. Закон распределения. Пример составления закона распределения для дискретной случайной величины.
10. Функция распределения дискретной случайной величины. Пример вычисления и построения графика.
11. Биномиально распределенная случайная величина. Определение, пример.
12. Числовые характеристики дискретных случайных величин. Физический смысл и правила вычисления.
13. Непрерывная случайная величина. Определение и пример. Функция плотности непрерывной случайной величины. Свойства функции плотности.
14. Функция распределения непрерывной случайной величины, ее свойства.
15. Равномерно распределенная случайная величина. Пример. Вид функции распределения. Числовые характеристики равномерно распределенной случайной величины.
16. Нормально распределенная случайная величина. Вид функции распределения. Числовые характеристики нормально распределенной случайной величины. Вероятность попадания нормально распределенной случайной величины в заданный интервал.
17. Дискретная двумерная случайная величина. Безусловный и условные законы распределения. Зависимость и независимость компонент.
18. Понятие ковариации двух случайных величин. Свойства ковариации. Коэффициент корреляции, его свойства.

Аналитическое задание:

Задачи, которые могут быть включены в экзаменационный билет, приведены в примерных вариантах контрольных работ и в расчетно-графических работах.

4 семестр.Модуль «Дифференциальное исчисление функции нескольких переменных» и модуль «Интегральное исчисление функции нескольких переменных»

Теоретический блок вопросов:

1. Функции нескольких переменных: область определения, линии уровня, геометрическая интерпретация.
2. Предел функции в точке, частные производные первого и второго порядков

функции нескольких переменных.
3. Частные производные первого порядка.
4. Частные производные второго порядка.
5. Полный дифференциал (для функции двух переменных).
6. Производная сложной функции.
7. Производная функции по направлению.
8. Градиент функции и его свойства.
9. Экстремумы функции двух переменных: необходимое и достаточное условия экстремума.
10. Условный экстремум (метод множителей Лагранжа).
11. Наибольшее и наименьшее значения функции в замкнутой области.
12. Первообразная. Неопределенный интеграл: определение. Теорема об общем виде первообразных.
13. Основные свойства неопределенного интеграла.
14. Таблица основных интегралов.
15. Методы интегрирования: табличный, разложения.
16. Интегрирование подведением под знак дифференциала.
17. Интегрирование с помощью замены переменной.
18. Определенный интеграл: определение, свойства.
19. Формула Ньютона- Лейбница.
20. Вычисление определенного интеграла с помощью замены переменной.
21. Некоторые приложения определенного интеграла.
22. Интегралы с бесконечными пределами: определения, свойства.

Аналитическое задание:

Задачи, которые могут быть включены в экзаменационный билет, приведены в примерных вариантах контрольных работ и в расчетно-графических работах.

4.5 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам высшего образования – программ бакалавриата/магистратуры/специалитета в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по дисциплине (модулю) выставляется по пятибалльной системе.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля)

5.1.1. Основная литература

1. *Богомолов, Н. В.* Математика : учебник для вузов / Н. В. Богомолов, П. И. Самойленко. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 401 с. — (Высшее образование). — ISBN 978-5-534-07001-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488864
2. *Бугров, Я. С.* Высшая математика в 3 т. Т. 1. Дифференциальное и интегральное исчисление в 2 кн. Книга 1 : учебник для вузов / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-02148-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491315
3. *Бугров, Я. С.* Высшая математика в 3 т. Т. 1. Дифференциальное и интегральное исчисление в 2 кн. Книга 2 : учебник для вузов / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-02150-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491316

5.1.2. Дополнительная литература

1. *Богомолов, Н. В.* Математика. Задачи с решениями в 2 ч. Часть 1 : учебное пособие для среднего профессионального образования / Н. В. Богомолов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 439 с. — (Профессиональное образование). — ISBN 978-5-534-09108-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490794
2. *Богомолов, Н. В.* Математика. Задачи с решениями в 2 ч. Часть 2 : учебное пособие для среднего профессионального образования / Н. В. Богомолов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 320 с. — (Профессиональное образование). — ISBN 978-5-534-09135-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490795
3. *Андрухаев, Х. М.* Теория вероятностей и математическая статистика. Сборник задач : учебное пособие для вузов / Х. М. Андрухаев. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 177 с. — (Высшее образование). — ISBN 978-5-9916-8599-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491173
4. *Ильин, В. А.* Математический анализ в 2 ч. Часть 1 в 2 кн. Книга 1 : учебник для вузов / В. А. Ильин, В. А. Садовничий, Б. Х. Сендов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 324 с. — (Высшее образование). — ISBN 978-5-534-07067-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491294
5. *Ильин, В. А.* Математический анализ в 2 ч. Часть 1 в 2 кн. Книга 2 : учебник для вузов / В. А. Ильин, В. А. Садовничий, Б. Х. Сендов. — 4-е изд., перераб. и

доп. — Москва : Издательство Юрайт, 2022. — 315 с. — (Высшее образование). — ISBN 978-5-534-07069-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491295

5.2 Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3 Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) «*Математика*» предполагает изучение материалов дисциплины (модуля) на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с рабочей программойдисциплины (модуля), доступной в электронной информационно-образовательной среде РГСУ.

Следует обратить внимание на списки основной и дополнительной литературы, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе.

С этой целью:

- внимательно прочитайте материал предыдущей лекции;
- ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;
- внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;
- запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;
- постарайтесь уяснить место изучаемой темы в своей подготовке;
- узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу.

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает:

- консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач;
- самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Обработка, обобщение полученных результатов практической работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

5.4 Информационно-технологическое обеспечение образовательного процесса по дисциплины (модуля)

5.4.1. Средства информационных технологий

1. Персональные компьютеры;
2. Средства доступа к Интернет;
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.4.3. Информационные справочные системы и профессиональные базы данных

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к	https://urait.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
		учебникам, учебной и методической литературе по различным дисциплинам.	
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.5 Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) «Математика» в рамках реализации основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет),

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть Интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.6 Образовательные технологии

При реализации дисциплины (модуля) *«Математика»* применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины (модуля) *«Математика»* предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме разбор конкретных ситуаций, практические тренинги в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

При освоении дисциплины (модуля) *«Математика»* предусмотрено применение электронного обучения.

Учебные часы дисциплины (модуля) *«Математика»* предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках дисциплины (модуля) *«Математика»* предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с

направленностью реализуемой основной профессиональной образовательной программы высшего образования – программы бакалавриата.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/

«06» __июня__2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль):
Организация и технология защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ – УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Форма обучения очная

Москва 2022 г.

Рабочая программа дисциплины (модуля) «Основы информационной безопасности» разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность **(уровень бакалавриата)**, утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– 06.030 Специалист по защите информации в телекоммуникационных системах и сетях

– 06.032 Специалист по безопасности компьютерных систем и сетей

– 06.033 Специалист по защите информации в автоматизированных системах

- 06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля)разработана рабочей группой в составе: канд. пед. наук, доцента Мнацаканян О.Л, канд.тех.наук Малиничев Д.М., канд. экн. наук, доцент Кучмезов Х.Х.

Руководитель основной профессиональной образовательной программы к.п.н., доцент — Н.Г. Витковская

(подпись)

Рабочая программа дисциплины (модуля)обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года
Декан факультета
К.п.н., доцент — С.В. Крапивка

(подпись)

Рабочая программа дисциплины (модуля)рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет»
зам. ген. директора по науке, к.т.н., доцент — А.С. Мосолов

(подпись)

Рабочая программа дисциплины (модуля)рецензирована и рекомендована к утверждению:

.д.т.н. , доцент, профессор кафедры информационных технологий , ГБОУВО Академия ГПС МЧС России) — С.Ю. Бутузов

(подпись)

к.ф.-м.н, доцент
кафедра прикладной математики и информатики РГСУ — Н.П. Третьяков

(подпись)

Согласовано
Научная библиотека, директор — И.Г. Маляр

(подпись)

СОДЕРЖАНИЕ

Ошибка! Закладка не определена.

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) изучение принципов обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности.

Задачи дисциплины:

В результате изучения курса выпускник должен решать следующие *профессиональные задачи* (в сфере организационно и правового обеспечения информационной безопасности, управления информационной безопасностью, технической защиты информации):

1. развитие системного мышления в области обеспечения информационной безопасности государства;
2. изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
3. оценки защищенности и обеспечения информационной безопасности объектов информатизации.

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы

Учебная дисциплина «Основы информационной безопасности» реализуется в базовой части основной профессиональной образовательной программы «Информационная безопасность» по направлению подготовки 10.03.01 Информационная безопасность очной формы обучения.

Изучение дисциплины (модуля)**«Основы информационной безопасности»** базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Правоведение», «Информатика и информационные технологии».

Изучение дисциплины (модуля)**«Основы информационной безопасности»** является базовым для последующего освоения программного материала учебных дисциплин: «Основы управления информационной безопасностью», «Криптографические методы защиты информации», «Контроль безопасности в компьютерных сетях».

1.3. Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основной профессиональной образовательной программы

Процесс освоения дисциплины (модуля)направлен на формирование у обучающихся следующих общекультурных и общепрофессиональные компетенций: ОПК-1, ОПК-8, ОПК-2.1 в соответствии с основной профессиональной образовательной программой «Информационная безопасность» по направлению подготовки 10.03.01 Информационная безопасность.

В результате освоения дисциплины (модуля)обучающийся должен демонстрировать следующие результаты:

Категория компетенций	**Код компетенции**	**Формулировка компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения**
	ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-1.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-1.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	*Знать:* сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства
				Уметь: Умеет применять основные методы обеспечения информационной безопасности
				Владеть: базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества и государства
	ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и	ОПК-8.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения

		методических документов в целях решения задач профессиональной деятельности;	действий в рамках компетенции ОПК-8.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-8.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	информационной безопасности, так и работающих в пограничных сферах. **Уметь:** проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации **Владеть:** современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации

	ОПК-2.1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-2.1.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-2.1.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-2.1.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Знать: глобальные и локальные проблемы обеспечения информационно-психологической и информационно-технической безопасности личности , общества и государства в информационном пространстве, в том числе с учетом современных угроз со стороны иностранных технических разведок, субъектов как промышленного шпионажа и технологического терроризма, так и представителей криминальной сферы.
				Уметь: самостоятельно анализировать и дифференцированно оценивать угрозы информационной безопасности, обоснованно представлять себе значение инженерно-технических и гуманитарных

				научных направлений для эффективного противодействия субъектам угроз и экономически обоснованному применению методов и средств управления системой комплексного обеспечения информационной безопасности.
				Владеть: основными знаниями в вопросах мирового динамического процесса исторического развития методов и средств обеспечения информационной безопасности, с учетом социального и научно-технического развития общества.

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем дисциплины (модуля), включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 8 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		2				
Контактная работа обучающихся с педагогическими работниками	144	144				
Учебные занятия лекционного типа	32	32				
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	48	48				
из них: в форме практической подготовки						
Иная контактная работа	64	64				
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	108	108				
Контроль промежуточной аттестации	36	36				
Форма промежуточной аттестации		экзам				
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	288	288				

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	Виды учебной работы, академических часов		
	Всего	оятельная	Контактная работа обучающихся с педагогическими работниками

			Всего	из них: в форме практической подготовки	Лекционные занятия	из них: в форме практической подготовки	Семинарские/практические занятия	из них: в форме практической подготовки	Лабораторные занятия	из них: в форме практической подготовки	Иная контактная работа	из них: в форме практической подготовки
Модуль 1 (семестр 2)												
Раздел 1.1	31	13	18		4				6		8	
Раздел 1.2	31	13	18		4				6		8	
Раздел 1.3	31	13	18		4				6		8	
Раздел 1.4	31	13	18		4				6		8	
Раздел 1.5	32	14	18		4				6		8	
Раздел 1.6	32	14	18		4				6		8	
Раздел 1.7	32	14	18		4				6		8	
Раздел 1.8	32	14	18		4				6		8	
Контроль промежуточной аттестации (час)	36											
Общий объем, часов	288	108	144		32				48		64	
Форма промежуточной аттестации	экзамен											
Общий объем, часов	288	108	144		32				48		64	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1. Виды самостоятельной работы обучающихся по дисциплине (модулю)

Раздел, тема	Всего	Виды самостоятельной работы обучающихся					
		Академическая активность, час	Форма академической активности	Выполнение практ. заданий, час	Форма практического задания	Рубежный текущий контроль, час	Форма рубежного текущего контроля
Модуль 1 (семестр 2)							
Раздел 1.1	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 1.4	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.5	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.6	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.7	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.8	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру,	108	44		48		16	

часов							
Общий объем по дисциплине (модулю), часов	108	44		48		16	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю)

МОДУЛЬ «ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РФ. ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАРУБЕЖНЫХ СТРАНАХ. НОРМАТИВНАЯ БАЗА, РОССИЙСКИЕ И МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИБ»

РАЗДЕЛ 1 ИСТОРИЯ РАЗВИТИЯ ПРОБЛЕМ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Цель: Осветить историческое развитие проблемы защиты информации со времен Древней Руси и средневековья до наших дней.

Перечень изучаемых элементов содержания

Криптография. Государственные интересы. Система безопасности.

Вопросы для самоподготовки:

1. Защита государственных интересов в XII–XIV вв.
2. Криптография Древней Руси.
3. Криптография в годы гражданской войны.
4. Криптография в России накануне и в период Русско-японской войны.
5. Защита государственных интересов в период создания советской власти.
6. Защита государственных интересов в период НЭПА.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторный практикум.

Цель:

Изучить историю развитие проблемы защиты информации в Древней Руси и до наших дней.

Контрольные вопросы:

1. Защита государственных интересов в период образования русского централизованного государства (вторая половина XIV в. - первая половина XVI в.).
2. Защита государственных интересов в период сословно-представительной монархии (середина XVI в. - середина XVII в.).
3. Защита государственных интересов во второй половине XVII–XVIII вв.
4. Российская криптография XIV–XVIII вв. Русская криптография в эпоху Петра Великого.
5. Защита государственных интересов во второй половине XIX в.
6. «Черные кабинеты» России. Русская криптографии в период войны Наполеона против России.
7. Защита государственных интересов в первой половине XIX в.
8. Методы криптографической защиты информации России в XIX в.

9. Криптографическая деятельность революционеров в 20-х – 70-х годах XIX в.: успехи и неудачи.
10. Защита государственных интересов с 1900 по 1917 гг.
11. Криптографическая деятельность СССР накануне и во время Второй мировой войны.
12. Защита государственных интересов в 1928–1941 гг.
13. Защита государственных интересов в период Великой отечественной войны.
14. Тайные операции в криптографии. Агентурные действия в период между Первой и Второй мировыми войнами.
15. Развитие систем защиты информации в период холодной войны.
16. Система безопасности СССР во второй половине 40-х -первой половине 50-х гг. XX в.
17. Организация защиты государственных секретов и система безопасности во второй половине 50-х–80 -х гг. XX в.
18. Тайные операции в криптографии. Агентурные действия после Второй мировой войны.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 2. ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАРУБЕЖНЫХ СТРАНАХ

Цель: Осветить историческое развитие проблемы защиты информации со времен античности и средневековья до наших дней

Перечень изучаемых элементов содержания

Тайные операции. Проблем информационной безопасности. Определение требований к разработке.

Вопросы для самоподготовки:

1. «Черные кабинеты» Франции. Французская криптографии в период войны Наполеона против России.
2. Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы XVIII- начале XX вв.
3. Криптографическая деятельность Германии накануне и во время Второй мировой войны.
4. Формирование особенностей политики защиты государственных секретов и коммерческой тайны в США XVIII- начале XX вв.
5. Тайные операции Великобритании в криптографии. Агентурные действия в период между Первой и Второй мировыми войнами.
6. Становление систем, формирование основных понятий, выработка принципов, методов, основных подходов и направлений защиты информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторный практикум.

Цель:

Изучить историю развитие нормативно - правовых актов защиты информации в зарубежных государствах

Контрольные вопросы:

1. Развитие криптографии в древние времена.
2. Развитие криптографии в Античную эпоху.
3. На какой период приходится наиболее интенсивное решение проблем информационной безопасности?

4. Становление и развитие систем защиты информации в ведущих зарубежных странах в период конца XIX и начала XX века.

5. Прогресс методов и систем защиты информации в период первой мировой войны и межвоенного периода.

6. Охота за «Энигмой».

7. Развитие систем защиты информации в период холодной войны.

8. Задачи построения систем защиты информации во второй половине XX века.

9. Формирование особенностей политики защиты государственных секретов и коммерческой тайны в Японии XVIII- начале XX вв.

10. Криптографическая деятельность накануне и во время Второй мировой войны.

11. Проведите историческую ретроспективу становления систем защиты информации в ведущих зарубежных странах?

12. Опишите создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии)?

13. Какие можно отметить особенности опыта организации защиты информации на Древнем Востоке?

14. Какие обнаруживаются исторические истоки разделения и классификации видов тайн?

15. Проведите историческую ретроспективу формирования основных понятий защиты информации в ведущих зарубежных странах?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 3 ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В СИСТЕМЕ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ СОВРЕМЕННОГО ОБЩЕСТВА

Цель: Дать краткий обзор понятия *информационной войны в системе международных отношений*

Перечень изучаемых элементов содержания

Информационное противоборство. **Информационная война. Практические аспекты ведения информационных войн. Государственная информационная политика.**

Вопросы для самоподготовки:

1. Охарактеризуйте причины, вызвавшие появление информационных войн.2. Принцип простоты

2. Психологическая защита личности как основной способ обеспечения информационно-психологической безопасности.

3. Основные сферы деятельности человечества, в которых возможно применение технологии информационных войн для достижения поставленных задач.

4. «Информационно-психологическая безопасность»: определение, угрозы информационно-психологической безопасности личности и их основные источники.6. Принцип повторного использования

5. Охарактеризуйте картину политических отношений в современном мире.

6. Информационно-психологическая война как средство достижения политических целей.

7. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторный практикум.
Цель:
Изучение подходов к введению информационных войн, виды информационных войн

Контрольные вопросы:
1. Понятие «информационное оружие», основные виды информационного оружия.
2. Основные этапы развития методов и средств ЗИ в процессе эволюции человечества.
3. Охарактеризуйте современное состояние проблемы защиты информации в мире.
4. На какой период приходится наиболее интенсивное решение проблем информационной безопасности?
5. Основные элементы типовой системы защиты информации.
6. Приоритеты геополитической конкуренции в информационном пространстве.
7. Объекты Информационного доминирование.
8. Объекты информационного противоборства.
9. Субъекты информационного противоборства.
10. Внешнее управление информационно-психологическими процессами.
11. Информационно-психологическая экспансия, агрессия.
12. Информационно-психологические операции как организационная форма реализации концепции информационно-психологической войны.
13. Организация защита информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др.
14. Порядок предоставления защищаемой информации другим странам при международном сотрудничестве?
15. Значение промышленного шпионажа для формирования систем защиты информации
16. Международная защита интеллектуальной собственности.
17. Реалии информационной войны.
18. Защита гражданского общества от информационного оружия в XXI веке.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 4 МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Цель:
является создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, обеспечение защиты интересов РФ при международном информационном обмене.

Перечень изучаемых элементов содержания

Обострения международной конкуренции за обладание информационными ресурсами. Информационное оружие. Международное сотрудничество между компаниями.

Вопросы для самоподготовки:
1. Современные тенденции международного сотрудничества в области ИБ.
2. Деятельность Ассоциации аудита и контроля информационных систем.

3. Назовите основные международные стандарты ИБ.
4. Порядок предоставления защищаемой информации другим странам.
5. Критерии определяющие степень доверия в стандарте «Оранжевая книга».
6. Особенности международно-правовых документов в области информационной безопасности и защиты информации.
7. Организационно-правовые основы международного сотрудничества в области защиты информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: лабораторный практикум.
Цель:
Создание условий для эффективного участия России в международном сотрудничестве в области защиты информации.

Контрольные вопросы:

1. Международный опыт в сфере защиты коммерчески ценной информации в законодательстве зарубежных стран.
2. Международный опыт нормативного регулирования информационной безопасности.
3. Основные направления международной деятельности по правовому регулированию сети Интернет.
4. Порядок выезда персонала, осведомленного в сведениях, составляющих государственную тайну, за границу.
5. Подготовка к передаче другим государствам сведений, составляющих государственную тайну.
6. Обеспечение информационной безопасности коммерческой деятельности в сети Интернет.
7. Основные соглашения в области международного сотрудничества в области защиты информации.
8. Особенности построения межгосударственных систем защиты информации.
9. Охарактеризуйте деятельность Ассоциации аудита и контроля информационных систем.
10. Определите назначения и виды классов безопасности в «Оранжевой книге».
11. Почему Британский стандарт BS 7799 используется наиболее часто.
13. В чем отличие применения международных стандартов ISO15408 и ISO17799.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 5. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В США

Цель: является рассмотрение систем защиты информации в США, особенности их современной организации и функционирования, перспектив развития и возможностей использования опыта в России.

Перечень изучаемых элементов содержания

Концепция информационной войны в США. Кибернетическая война. Психологическая война. Правовое регулирование информационной безопасности в США.

Вопросы для самоподготовки:

1. Нормативно-правовые акты, регулирующие правовое обеспечение ИБ в США.

2. Для чего в структуре МО США созданы силы быстрого реагирования в СМИ и каковы их задачи?

3. Основные принципы ИВ, реализуемые на военном уровне концепции ИВ США.

4. Современные концепции информационной безопасности США.

5. Основная цель Закона «Об информационной безопасности» в США?

6. Роль ФБР в решении задач обеспечения информационной безопасности США?

7. Правовое регулирование информационной безопасности в США.

8. Современные концепции информационной безопасности США.

9. Классификация защищаемой информации в США.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5

Форма практического задания: лабораторный практикум.

Цель:

Формирование и развитие навыков системы защиты информации в соответствии с современными принципами организации систем защиты информации.

Контрольные вопросы:

1. Основные функции службы надзора по защите информации в США.

2. Совершенствование системы органов защиты информации после событий 11 сентября 2001 г.

3. Организация защиты коммерческой тайны в США.

4. Организация защиты служебной тайны в США.

5. Организация защиты персональных данных в США.

6. Подбор, проверка и юридическая защита кадров, принимаемых на работу в охранно-сыскные агентства в США.

7. Характер и масштабы рынка услуг, предоставляемых частными правоохранительными организациями США юридическим и физическим лицам.

8. Приоритеты исследований в области защиты американской информационной инфраструктуры.

9. Состав и основные направления деятельности органов, осуществляющих защиту информации по национальной безопасности в США.

10. Особенности функционирования национальной системы защиты информации в США.

11. Организация защиты коммерческой тайны в США. Правовые документы, регламентирующие эту деятельность

12. Степени секретности сведений и грифы секретности информации, составляющей государственную тайну в США.

13. Особенности функционирования американских систем защиты информации в негосударственных структурах.

14. Расскажите основные документы, касающиеся аспектов ведения ИВ США. Каково их содержание?

15. Организация доступа в США к грифованной информации.

16. Организация защиты информации в США по национальной безопасности.

17. Основные направления деятельности служб безопасности фирм в США.

18. Государственная политика США в области защиты информации.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 5: форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 6. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СТРАНАХ ЕВРОСОЮЗА

Цель: является рассмотрение систем защиты информации в Европейском союзе, особенности их современной организации и функционирования, перспектив развития и возможностей использования опыта в России.

Перечень изучаемых элементов содержания

Организационно-правовые основы построения системы защиты информации в Европейском союзе. Правовое регулирование информационной безопасности в Европейском союзе. Особенности функционирования систем защиты информации в негосударственных структурах.

Вопросы для самоподготовки:

1. Порядок отнесения информации к государственной и коммерческой тайне
2. Степени секретности сведений и грифы секретности носителей

3. Организационно-правовые основы построения системы защиты информации в Великобритании, Франции и Германии.
4. Характеристика систем защиты информации в западноевропейских странах.
5. Ответственность за компьютерные преступления в Европейском Союзе.
6. Роль ЕС и международных организации в регулировании международного информационного обмена.
7. Основные направления совершенствования деятельности служб безопасности Европейского Союза.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 6

Форма практического задания: лабораторный практикум.

Цель:

Формирование и развитие навыков системы защиты информации в соответствии с современными принципами организации систем защиты информации в Европейском Союзе.

Контрольные вопросы:

1. Современный этап развития систем защиты информации в ведущих зарубежных странах.
2. Особенности функционирования системы защиты информации в Соединённом Королевстве Великобритании и Северной Ирландии.
3. Особенности функционирования системы защиты информации во Французской Республике.
4. Особенности функционирования системы защиты информации в Федеративной Республике Германия.
5. Цели и задачи, связанные с обеспечением информационной безопасности в крупных европейских компаниях.
6. Общий подход к учету требований безопасности в крупных европейских компаниях
7. Какие основные проблемы решают специалисты стран Евросоюза в условиях возможности применения информационного оружия.
8. Характеристика современной системы защиты информации в Европейском Союзе.
9. Охарактеризуйте нормативно-правовую базу Европейского Союза в сфере информационной безопасности.
10. Состояние проблемы информационной безопасности в странах Евросоюза.
11. Системы защиты информации в Соединённом Королевстве Великобритании и Северной Ирландии.

12. Системы защиты информации в Федеративной Республике Германия.
13. Системы защиты информации во Французской Республике.
14. Международные организации в области информационной безопасности.
15. Основные проблемы решают специалисты стран Евросоюза в условиях возможности применения информационного оружия?
16. Основные положения конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных».
17. Органы Европейского Союза, обеспечивающих реализацию европейской политики информационного общества.
18. Какие цели преследует идея создания системы коллективного контроля и обеспечения ИБ европейских стран?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 6: форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 7. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ

Цель: является рассмотрение систем защиты информации в Китайской Народной Республике, особенности их современной организации и функционирования, перспектив развития и возможностей использования опыта в России.

Перечень изучаемых элементов содержания

Организационно-правовые основы построения системы защиты информации в Китайской Народной Республике. Правовое регулирование информационной безопасности в Китайской Народной Республике. Особенности функционирования систем защиты информации в негосударственных структурах.

Вопросы для самоподготовки:

1. Порядок отнесения информации к государственной и коммерческой тайне
2. Степени секретности сведений и грифы секретности носителей
3. Организационно-правовые основы построения системы защиты информации в Китайской Народной Республике.
4. Ответственность за компьютерные преступления в Китайской Народной Республике.
5. Основные направления совершенствования деятельности служб безопасности в Китайской Народной Республике**.**
6. Классификация секретной информации в Китайской Народной Республике
7. Организационная структура спецслужб в Китайской Народной Республике
8. «Великая стена» информационной безопасности Китая.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 7

Форма практического задания: лабораторный практикум.

1. Цель работы

Формирование и развитие навыков системы защиты информации в соответствии с современными принципами организации систем защиты информации в Китайской Народной Республике.

2. Содержание работы

1. В чём состоит сущность проводимых КНР кибернетических атак на ресурсы МО США и России?

2. Государственная политика КНР в области защиты информации.

3. Основные мероприятия по обеспечению ИБ КНР, осуществляемые в процессе интеграции в глобальную сеть Интернет?

4. Каковы основные элементы правовой системы ИБ КНР?

5. Основная цель Закона КНР от 01.11.2014 «О контрразведке»?

6. Основные мероприятия, осуществляемые руководством Китая, направленные на повышение ИБ страны.

7. Особенности функционирования систем защиты информации в коммерческих структурах КНР.

8. Охарактеризуйте нормативно-правовую базу КНР в сфере ИБ и ответственность за компьютерные преступления в Китае.

9. Расскажите основные документы, касающиеся аспектов ведения ИВ КНР. Каково их содержание?

10. Роль РЭБ генштаба НОАК в решении задач обеспечения информационной безопасности в компьютерных сетях?

11. Современные концепции информационной безопасности КНР.

12. Состав и основные направления деятельности органов, осуществляющих защиту информации по национальной безопасности в КНР.

13. Степени секретности сведений и грифы секретности информации, составляющей правительственную тайну в КНР.

14. Что представляет собой концепция ИВ КНР?

15. Что такое «Великая стена» информационной безопасности КНР? Какие задачи ей присущи?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 7: форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 8. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Цель: является рассмотрение систем защиты информации в Российской Федерации, особенности их современной организации и функционирования, перспектив развития и возможностей использования.

Перечень изучаемых элементов содержания

Организационно-правовые основы построения системы защиты информации в Российской Федерации. Правовое регулирование информационной безопасности Российской Федерации. Особенности функционирования систем защиты информации в негосударственных структурах.

Вопросы для самоподготовки:

1. Нормативное правовое обеспечение функционирования системы обеспечения информационной безопасности Российской Федерации.

2. Нормативное правовое обеспечение безопасности конституционных прав и свобод человека и гражданина в области получения и использования информации.

3. Нормативное правовое обеспечение защиты информационных ресурсов от несанкционированного доступа, безопасности информационных и телекоммуникационных систем.

4. Нормативное правовое обеспечение безопасности информационного обеспечения государственной политики Российской Федерации.

5. Первоочередные меры по совершенствованию нормативного правового обеспечения информационной безопасности Российской Федерации.

6. Информационные угрозы безопасности РФ. Доктрина информационной безопасности РФ.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 8

Форма практического задания: лабораторный практикум.

3. Цель работы

Формирование и развитие навыков системы защиты информации в соответствии с современными принципами организации систем защиты информации в Российской Федерации.

4. Содержание работы

1.Нормативное правовое обеспечение безопасности развития современных информационных технологий, отечественной индустрии информации.

2. Каков порядок распоряжения сведениями, составляющими государственную тайну?

3. Порядок обращение с документами, содержащими сведения составляющие государственную тайну.

4. Что такое «правовое обеспечение информационной безопасности», раскройте содержание правового обеспечения безопасности сведений.

5. Правовая защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации.

6. Правовое обеспечение защиты государственной тайны в Российской Федерации.

7. Государственная тайна. Порядок допуска должностных лиц и граждан Российской Федерации к государственной тайны?

8. Состояния информационной безопасности РФ и основные задачи по ее обеспечению.

9. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные).

10. Тайна государственной охранной деятельности в Российской Федерации.

11. В чем заключается сущность информационной безопасности организаций и государства?

12. Перечислите принципы обеспечения информационной безопасности Российской Федерации и раскройте их содержание.

13. Раскройте содержание прав и обязанностей обладателя информации, составляющей коммерческую тайну.

14. В чем заключается порядок предоставления информации, составляющей коммерческую тайну?

15. В чем заключается ответственность за нарушение законодательства?

16. Какова цель ранжирования должностей по степени риска управления бизнес-процессами?

17. Особенности обработки персональных данных осуществляемой без использования средств автоматизации

18. Правовой режим обеспечения безопасности государственных и муниципальных систем в Российской Федерации.

19. Управление рисками информационной безопасности. Методы обработки рисков информационной безопасности.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 8: форма рубежного контроля – Отчет по лабораторной работе.

Модуль: Основы информационной безопасности

Раздел 1. Информационная безопасность и уровни ее обеспечения

Цель: ознакомиться с основными подходами к определению понятия "информационная безопасность

Перечень изучаемых элементов содержания

различные подходы к определению понятия "информационная безопасность" и отличие "компьютерной безопасности" от "информационной безопасности".

Тема 1.1. Понятие "информационная безопасность"

Цель: Определение понятия "информационная безопасность"

Перечень изучаемых элементов содержания

определения "информационной безопасности" приводимые в руководящих документах.

Вопросы для самоподготовки:

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию "информационная безопасность".
3. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?
4. Что понимается под "компьютерной безопасностью"?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.1

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Понятие информационной безопасности».

Контрольные вопросы:

1. Информационная безопасность.
2. Защита информации.
3. Основные составляющие информационной безопасности
4. Доступность, целостность и конфиденциальность информационных ресурсов.
5. Важность и сложность проблемы информационной безопасности
6. Доктрина информационной безопасности Российской Федерации.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.1: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.2. Составляющие информационной безопасности

Цель: изучить составляющие информационной безопасности и их характеристику.

Перечень изучаемых элементов содержания

- составляющие понятия "информационная безопасность";
- определение целостности информации;
- определения конфиденциальности и доступности информации.

Вопросы для самоподготовки:

1. Приведите определение доступности информации.
2. Приведите определение целостности информации.
3. Приведите определение конфиденциальности информации.
4. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.2.

Форма практического задания: лабораторный практикум.
Лабораторная работа 2. «Составляющие информационной безопасности».

Контрольные вопросы:
1. Основные составляющие. Важность проблемы.
2. Понятие информационной безопасности.
3. Защита информации.
4. Основные составляющие информационной безопасности.
5. Основные определения и критерии классификации угроз.
6. Основные угрозы конфиденциальности.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.2.: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.3. Система формирования режима информационной безопасности
Цель: получить представление о системном подходе, обеспечивающем информационную безопасность.

Перечень изучаемых элементов содержания

- уровни формирования режима информационной безопасности;
- особенности законодательно-правового и административного уровней;
- подуровни программно-технического уровня.

Вопросы для самоподготовки:

1. Назовите основные документы, которыми руководствуется на организационном уровне.
2. Приведите примеры реализации технической защиты информации компании.
3. Приведите примеры реализации физической защиты информации компании.
4. Назовите известные вам криптографические средства защиты информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.3.

Форма практического задания: лабораторный практикум.
Лабораторная работа 3. «Система формирования режима информационной безопасности».

Контрольные вопросы:
1. Перечислите задачи информационной безопасности общества.
2. Перечислите уровни формирования режима информационной безопасности.
3. Дайте краткую характеристику законодательно-правового уровня.
4. Какие подуровни включает программно-технический уровень?
5. Что включает административный уровень?
6. В чем особенность морально-этического подуровня?

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.3: форма рубежного контроля – отчет по лабораторной работе.

Раздел 2. Стандарты информационной безопасности

Цель: изучить основные положения стандартов информационной безопасности

Перечень изучаемых элементов содержания

- использовать стандарт для оценки защищенности информационных систем.

- выбирать механизмы безопасности для защиты распределенных систем.

Тема 2.1. Стандарты информационной безопасности: "Общие критерии"

Цель: изучить основные положения международного стандарта ISO/IEC 15408 по оценке защищенности информационных систем.

Перечень изучаемых элементов содержания

- основное содержание оценочного стандарта ISO/IEC 15408;
- отличия функциональных требований от требований доверия;
- классы функциональных требований и требований доверия;
- использовать стандарт для оценки защищенности информационных систем.

Вопросы для самоподготовки:

1. Какие виды требований включает стандарт ISO/IEC 15408?
2. Чем отличаются функциональные требования от требований доверия?
3. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
4. Перечислите существующие критерии оценки безопасности АС, согласно стандарту, ISO 15408?
5. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
6. Какова цель требований по отказоустойчивости информационных систем?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.1

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Стандарты информационной безопасности».

Контрольные вопросы:

1. Понятие безопасности информации
2. Международный стандарт информационной безопасности
3. Особенности процесса стандартизации в Интернете
4. Стандарты безопасности в Интернете: SSL (TLS), SET, IPSec
5. Особенности российского рынка
6. Государственные стандарты

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.1: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.2. Стандарты информационной безопасности распределенных систем

Цель: ознакомиться с основными положениями стандартов по обеспечению информационной безопасности в распределенных вычислительных сетях.

Перечень изучаемых элементов содержания

- основное содержание стандартов по информационной безопасности распределенных систем;
- основные сервисы безопасности в вычислительных сетях;
- наиболее эффективные механизмы безопасности;
- задачи администрирования средств безопасности.

Вопросы для самоподготовки:

1. Какие существуют активные сетевые атаки? Дайте краткое описание каждой атаки?
2. Какие механизмы безопасности используются для обеспечения конфиденциальности трафика?
3. Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
4. Дайте определение понятию средство безопасности?

5. Что понимается под администрированием средств безопасности?
6. Какие виды избыточности могут использоваться в вычислительных сетях?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.2

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «Стандарты информационной безопасности распределенных систем».

Контрольные вопросы:

1. Информационная безопасность распределенных систем. Рекомендации X.800
2. Сетевые сервисы безопасности
3. Аутентификация партнеров по общению
4. Управление доступом.
5. Конфиденциальность данных.
6. Аутентификация источника данных.
7. Семиуровневая модель OSI
8. Сетевые механизмы безопасности
9. Шифрование.
10. Электронная цифровая подпись.
11. Администрирование средств безопасности.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.2.: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.3. Стандарты информационной безопасности в РФ

Цель: ознакомиться с основными стандартами и спецификациями по оценке защищенности информационных систем в РФ.

Перечень изучаемых элементов содержания

- о роли Гостехкомиссии в обеспечении информационной безопасности в РФ;
- о документах по оценке защищенности автоматизированных систем в РФ.

Вопросы для самоподготовки:

1. Перечислить показатели защищённости межсетевых экранов.
2. Перечислить классы защищённости АС от НСД и необходимые требования по защите информации.
3. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
4. Перечислить основные полномочия ФСТЭК.
5. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
6. Показатели защищенности межсетевых экранов.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.3.

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «Стандарты информационной безопасности в РФ».

Контрольные вопросы:

1. Необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских организаций.
2. Доминирование аппаратно-программных продуктов зарубежного производства.
3. Доктрина информационной безопасности Российской Федерации

4. Согласование отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения;
5. Разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности
6. Разработка методов и средств обеспечения информационной
7. Классификация стандартов в области информационной безопасности
8. Руководящие документы ФСТЭК
9. Криптографические стандарты.
10. Управленческие стандарты

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.3.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 3. Административный уровень обеспечения информационной безопасности

Цель: изучить содержание административного уровня обеспечения информационной безопасности.

Перечень изучаемых элементов содержания

- цели и задачи административного уровня обеспечения информационной безопасности;
- содержание административного уровня;
- направления разработки политики безопасности.

Тема 3.1. Цели, задачи и содержание административного уровня

Цель: изучить цели, задачи и содержание административного уровня обеспечения информационной безопасности.

Перечень изучаемых элементов содержания

- цели и задачи административного уровня обеспечения информационной безопасности;
- содержание административного уровня.

Вопросы для самоподготовки:
1. Содержание административного уровня.
2. Дайте определение политики безопасности.
3. Направления разработки политики безопасности.
4. Перечислите составные элементы автоматизированных систем.
5. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 3.1.

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Административный уровень обеспечения информационной безопасности».

Контрольные вопросы:
1. Цели, задачи и содержание административного уровня
2. Разработка политики информационной безопасности
3. Определение объема и требуемого уровня защиты данных;
4. Определение ролей субъектов информационных отношений.
5. Основные положения информационной безопасности организации;
6. Область применения политики безопасности;
7. Цели и задачи обеспечения информационной безопасности организации;

8. Распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 3.1: форма рубежного контроля – отчет по лабораторной работе.

Тема 3.2. Разработка политики информационной безопасности

Цель: изучить цели, задачи и содержание разработки политики информационной безопасности

Перечень изучаемых элементов содержания

- цели и задачи политики информационной безопасности;
- направления разработки политики безопасности.

Вопросы для самоподготовки:

1. Основная цель разработки политики безопасности на предприятии.
2. Субъекты и объекты информационных систем и их классификация.
3. Цели и задачи административного уровня обеспечения информационной безопасности.
4. Место политики безопасности в структуре ВНД (внутренней нормативной документации) предприятия.
5. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 3.2.

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «Разработка политики информационной безопасности».

Контрольные вопросы:

1. Политика безопасности
2. Основные направления разработки политики безопасности:
3. Определение объема и требуемого уровня защиты данных;
4. Определение ролей субъектов информационных отношений.
5. Оранжевая книга
6. Состав автоматизированной информационной системы

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 3.2.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 4. Классификация угроз "информационной безопасности"

Тема 4.1. Классы угроз информационной безопасности

Цель: изучить классы угроз информационной безопасности.

Перечень изучаемых элементов содержания

- классы угроз информационной безопасности;
- причины и источники случайных воздействий на информационные системы.

Вопросы для самоподготовки:

1. Перечислите классы угроз информационной безопасности.
2. Назовите причины и источники случайных воздействий на информационные системы.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 4.1

Форма практического задания: лабораторный практикум.
Лабораторная работа 1. «Классы угроз информационной безопасности».

Контрольные вопросы:
1. Составляющие информационной безопасности .
2. Компоненты информационных систем.
3. Характер воздействия .
4. Расположение источника угроз .
5. Внутренние угрозы.
6. Внешние угрозы.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 4.1: форма рубежного контроля – отчет по лабораторной работе.

Тема 4.2. Каналы несанкционированного доступа к информации

Цель: изучить каналы несанкционированного доступа к информации.

Перечень изучаемых элементов содержания

- каналы несанкционированного доступа к информации.

Вопросы для самоподготовки:
1. Перечислите каналы несанкционированного доступа.
2. В чем особенность "упреждающей" защиты в информационных системах.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 4.2.

Форма практического задания: лабораторный практикум.
Лабораторная работа 2. «Каналы несанкционированного доступа к информации».

Контрольные вопросы:
1. Основные каналы НСД.
2. Отсутствует система разграничения доступа.
3. Сбой или отказ в компьютерных системах.
4. Ошибочные действия пользователей или обслуживающего персонала компьютерных систем.
5. Ошибки в системе разграничения доступа.
6. Фальсификация полномочий.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 4.2.: форма рубежного контроля – отчет по лабораторной работе.

Модуль: Компьютерные вирусы и антивирусные средства

Раздел 1. Компьютерные вирусы

Цель: ознакомиться с угрозами информационной безопасности, создаваемыми компьютерными вирусами.

Перечень изучаемых элементов содержания

- *компьютерные вирусы,*
- *антивирусное ПО.*

Тема 1.1. Вирусы как угроза информационной безопасности

Цель: изучить особенности угроз и характерные черты компьютерных вирусов.

Перечень изучаемых элементов содержания

- характерные черты компьютерных вирусов;
- проблемы при определении компьютерного вируса.

Вопросы для самоподготовки:

1. Чем опасны вирусы для информационных систем?
2. Какие трудности возникают при определении компьютерного вируса?
3. В чем опасность 0-day вирусов?
4. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
5. В чем особенность компьютерного вируса "Чернобыль"?
6. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.1

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Изучение вредоносных вирусов и их действий».

Контрольные вопросы:

1. Признаки, характерные для зараженных компьютеров.
2. Явные, косвенные и скрытые проявления вредоносных программ.
3. Способы поиска проявлений вредоносных программ.
4. Признаки заражения сайтов вредоносным ПО.
5. Заражение с помощью методов простой переадресации.
6. Технологии сигнатурного анализа (реактивной защиты);
7. Технологии вероятностного анализа (или проактивной защиты).
8. Эвристический анализ; Метод контроля активности HIPS - размещаемая система предотвращения вторжений.
9. Виртуальные технологии. VIPS – метод контроля активности
10. Методы контроля целостности ПО и ОС.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.1: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.2. Классификация компьютерных вирусов

Цель: изучить классы компьютерных вирусов и их характеристику.

Перечень изучаемых элементов содержания

- классы компьютерных вирусов;
- характеристику различных компьютерных вирусов.

Вопросы для самоподготовки:

1. Классифицируйте компьютерные вирусы.
2. Охарактеризуйте файловый и загрузочный вирусы.
3. Перечислите деструктивные возможности компьютерных вирусов.
4. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.2

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «Противодействие вредоносных программ обнаружению».

Контрольные вопросы:

1. Противодействие вредоносных программ обнаружению.
2. Защита от обнаружения и снятия перехватов.
3. Поведенческое противодействие. Антируткиты.
4. Использование ловушек для антируткитов.
5. Технологии блокировки работы антивирусных продуктов.
6. Основные методы защиты вредоносных программ от удаления: watchdog, метод троянского потока, блокировка доступа к файлу, пересоздание ключей реестра.
7. Профилактика и обнаружение вирусов в системе.
8. Периодическое сканирование при запуске.
9. Выборочное или полное сканирование. Сканирование с помощью резидентного модуля.
10. Классификации антивирусных средств.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.2: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.3. Характеристика "вирусоподобных" программ

Цель: изучить характерные черты и деструктивные возможности "вирусоподобных" программ.

Перечень изучаемых элементов содержания

- виды "вирусоподобных" программ;
- деструктивные возможности "вирусоподобных" программ.

Вопросы для самоподготовки:

1. Перечислите виды "вирусоподобных" программ.
2. Поясните механизм функционирования "троянской программы" (логической бомбы).
3. В чем заключаются деструктивные свойства логических бомб?
4. Как используются утилиты скрытого администрирования и их деструктивные возможности?
5. Для создания каких вирусов используются полиморфик-генераторы?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.3

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «Общие характеристики компьютерных вирусов».

Контрольные вопросы:

1. Понятие компьютерные вирусы. Классификация компьютерных вирусов.
2. Программы-агенты.
3. Сетевые вирусы. «Черви», «трояны».
4. Макровирусы.
5. Файловые вирусы.
6. Загрузочные вирусы.
7. Пути проникновения вируса в компьютер.

8. Вредоносные действия вирусов. Ущерб и угрозы безопасности, связанные с вредоносными программами.

9. Примеры вредоносных вирусов и их действий: вирусы Zero-day, руткиты, работающие в user-mode , Kernel-mode руткит, Boot-рутикты, атаки на GUI.

10.DDoS атаки, перегрузка каналов связи, атака с помощью переполнения пакетами SYN.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.3.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 2. Антивирусное программное обеспечение

Тема 2.1. Классификация антивирусных программ

Цель: изучить основные понятия по борьбе с вирусами, виды антивирусных программ и их характеристику.

Перечень изучаемых элементов содержания

- виды антивирусных программ;
- принципы функционирования антивирусных программ;
- факторы, определяющие качество антивирусной программы.

Вопросы для самоподготовки:

1. Дайте определения понятию «Эвристическое сканирование»
2. Дайте определение понятия «Сканирование по сигнатурам»
3. Каким базовым функционалом должна обладать современная антивирусная программа?
4. Что такое антивирусная база сигнатур?
5. Какие факторы определяют качество антивирусной программы?

Форма практического задания: лабораторный практикум.

Лабораторная работа 4. «Антивирусные средства и системы».

Контрольные вопросы:

1. Препятствие проникновению вредоносного ПО в систему. Устранение вирусов из компьютерной системы.
2. Пример защитных экранов антивируса Avast .
3. Антивирусные программы: антивирусные блокировщики; ревизоры; полифаги; полифаги-мониторы.
4. Антивирусные комплексы: комплекс для защиты рабочих станций; комплекс для защиты файловых серверов; комплекс для защиты почтовых систем; комплекс для защиты шлюзов.
5. Основные функции антивирусных средств: обнаружение вирусов, дезактивация вируса, лечение, прививка. Примеры антивирусных средств.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.1.: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.2. Профилактика компьютерных вирусов

Цель: изучить основы профилактики компьютерных вирусов, пути проникновения вирусов в компьютеры и основные правила защиты от компьютерных вирусов.

Перечень изучаемых элементов содержания

- наиболее распространенные пути заражения компьютеров вирусами;
- правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.

Вопросы для самоподготовки:

1. Какие особенности заражения вирусами при использовании электронной почты?
2. Особенности заражения компьютеров локальных сетей.
3. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
4. Как ограничить заражение макровирусом при работе с офисными приложениями?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.2.

Форма практического задания: лабораторный практикум.

Лабораторная работа 5. «Комплексная система антивирусной защиты».

Контрольные вопросы:

1. Какие способы применения политик на клиентских компьютерах существуют в Kaspersky Administration Kit? В чем различие этих способов?
2. Перечислите, какие уровни важности могут иметь события в Kaspersky Administration Kit?
3. Какие задачи не наследуются подчиненным Сервером администрирования?
4. Каким образом можно внести изменения в настройки унаследованной задачи?
5. В каких качествах может использоваться лицензионный ключ в приложениях Лаборатории Касперского?
6. Объясните в чем разница между шифрованным и полиморфным вирусом?
7. Достаточно ли для защиты от заражения вредоносной программой установить файлам разрешения только для чтения?
8. Объясните в чем отличие понятий вирус и вредоносная программа.
9. Назначение, содержание Комплексной Системы Антивирусной Защиты. Уровень защиты шлюзов.
10. Защита почтовых систем. Уровень защиты серверов и рабочих станций.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.2.: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.3. Обнаружение неизвестного вируса

Цель: изучить характерные черты неизвестных вирусов и методики их обнаружения.

Перечень изучаемых элементов содержания

- общий алгоритм обнаружения неизвестного вируса.

Вопросы для самоподготовки:

1. Перечислите основные этапы алгоритма обнаружения вируса.
2. Как обнаружить загрузочный вирус?
3. Как обнаружить резидентный вирус?
4. Характерные черты макровируса.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.3.

Форма практического задания: лабораторный практикум.

Лабораторная работа 6. «Антивирус Касперского для Microsoft ISA Server».

Контрольные вопросы:

1. Какие фильтры будут установлены Антивирусом Касперского для Microsoft *ISA Server* при установке последнего на Microsoft *ISA Server*, работающий в режиме Proxy?
2. Каким образом буду проверяться архивы при отключенном механизме распаковки архивов в Антивирусе Касперского для Microsoft *ISA Server*?
3. По протоколу HTTP идет загрузка архива, содержащего инфицированный объект, поддающийся лечению и чистый файл. Что произойдет с таким архивом?
4. В каком случае не формируется уведомление пользователю при обнаружении вредоносного объекта?
5. Какие пути доставки уведомлений существуют в Антивирус Касперского 5.5 для MS Exchange Server?
6. Почему рекомендуется не отсылать уведомления о найденном вирусе отправителю инфицированного сообщения?
7. Куда и в каком виде по умолчанию сохраняются файлы отчета?
8. Что произойдет с Антивирусом Касперского для MS Exchange Server при нарушении целостности файлов антивирусных баз?

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.3.: форма рубежного контроля – отчет по лабораторной работе.

Модуль: Экономика защиты информации

Раздел 1. Экономическая эффективность защиты информации

Цель: ознакомиться с основными понятиями экономической эффективности защиты информации и предпринимательского риска

Перечень изучаемых элементов содержания

различные подходы к определению понятия «добывание информации», основы предпринимательства и их возможные риски.

Тема 1.1. Основные методики определения затрат на информационную безопасность

Цель: изучить основные методики определения затрат на информационную безопасность.

Перечень изучаемых элементов содержания

- понятие коммерческой и государственной тайн,
- ценность информации,
- требуемый уровень защиты информации,
- затраты на защиту засекреченной информации.

Вопросы для самоподготовки:

1. Основные методики определения затрат на информационную безопасность
2. Определение коммерческой и государственной тайн
3. Каковы затраты на защиту засекреченной информации
4. Чем определяется требуемый уровень защиты информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.1

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Изучение методик определения затрат на информационную безопасность».

Контрольные вопросы:

1. Затраты на формирование звена управления системой защиты ин- формации и другие организационные затраты;
2. Затрат на приобретение и установку средств защиты
3. Затраты на обслуживание системы информационной безопасности:
4. Затраты на контроль работы системы безопасности
5. Затраты на обеспечение должного качества информационных технологий и их соответствия требованиям стандартов
6. Затраты на повышение квалификации персонала в вопросах ис- пользования имеющихся средств защиты, выявления и предотвращения угроз безопасности
7. Затраты, связанные с пересмотром политики информационной безопасности предприятия
8. Затраты на ликвидацию последствий нарушения режима информационной безопасности:
9. Затраты, возникающие в результате потери новаторства

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.1: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.2. Определение размера целесообразных затрат на обеспечение безопасности информации

Цель: изучить понятие размера целесообразных затрат на обеспечение безопасности информации.

Перечень изучаемых элементов содержания:

- платежная матрица производителя,
- критерий Лапласа,
- критерий Вальда,
- критерий Гурвица.

Вопросы для самоподготовки:

1. Понятие платежной матрицы производителя,
2. Государственная тайна
3. Коммерческая тайна

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.2

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «Определение размера целесообразных затрат на обеспечение безопасности информации».

Контрольные вопросы:

1. Платежная матрица производителя
2. Критерий Лапласа
3. Критерий Вальда

4. Критерий Сэвиджа
5. Критерий Гурвица

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.2: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.3. Модель определения зон защиты предприятия в условиях ограниченности средств

Цель: изучить модель определения зон защиты предприятия в условиях ограниченности средств

Перечень изучаемых элементов содержания:
- политика безопасности на предприятии,
- понятие количества защищаемых зон,
- ценность объекта.

Вопросы для самоподготовки:
1. Понятие политики безопасности на предприятии,
2. Количество защищаемых зон на предприятии,
3. Понятие ценности объекта.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.3

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «Модель определения зон защиты предприятия в условиях ограниченности средств».

Контрольные вопросы:
1. Количество защищаемых объектов на предприятии
2. Выделяемое финансирование
3. Определение математического ожидания ущерба на предприятии
4. Модель определения объектов защиты в условиях независимости ущербов

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.3: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.4. Модель распределения работы службы безопасности предприятия

Цель: изучить модель распределения работы службы безопасности предприятия

Перечень изучаемых элементов содержания:
- задачи службы безопасности на предприятии,
- криминальные структуры,
- оптимальное распределение групп службы безопасности на предприятии.

Вопросы для самоподготовки:
- обязанности службы безопасности на предприятии,
- стратегии проникновения на предприятие извне,
- количество работников службы безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.4

Форма практического задания: лабораторный практикум.

Лабораторная работа 4. «модель распределения работы службы безопасности предприятия».

Контрольные вопросы:
1. Задачи службы безопасности предприятия
2. Организация службой безопасности поиска и возможных вариантов нападений
3. Оптимальная численность подразделения
4. Стратегия криминальных структур по проникновению на предприятие

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.4: форма рубежного контроля – отчет по лабораторной работе.

Раздел 2. Предпринимательский риск
Цель: ознакомиться с понятием предпринимательский риск
Перечень изучаемых элементов содержания
Основные угрозы для экономической безопасности предприятия.

Тема 2.1. Понятие предпринимательского риска
Цель: изучить понятийный аппарат предпринимательского риска
Перечень изучаемых элементов содержания:
- понятие риска,
- понятие рискованной ситуации.

Вопросы для самоподготовки:
1. Обоснование уровня приемлемого риска при принятии управленческих решений.
2. Защита материальных, финансовых и информационных ресурсов.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.1

Форма практического задания: лабораторный практикум.
Лабораторная работа 5. «Понятие предпринимательского риска».

Контрольные вопросы:
1. Понятие риска
2. Определение рисковой ситуации
3. Обоснование уровня приемлемого риска при принятии управленческих решений.
4. Разработка стратегии и тактики ведения производственно- хозяйственной деятельности, позволяющих минимизировать хозяйственный риск и обеспечить экономическую безопасность.
5. Защита персонала.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.1: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.2. Классификация предпринимательского риска
Цель: изучить классификацию предпринимательского риска
Перечень изучаемых элементов содержания:
- внешние и внутренние риски,

- политические, технические, коммерческие и финансовые риски,
- частный и спекулятивный риски.

Вопросы для самоподготовки:

1. Определения внешних и внутренних рисков.
2. Определения политических, технических, коммерческих и финансовых рисков.
3. Определение частного и спекулятивного рисков.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.2

Форма практического задания: лабораторный практикум.
Лабораторная работа 6. «Классификация предпринимательского риска».

Контрольные вопросы:

1. Внешние факторы риска
2. Внутренние факторы риска
3. Кратковременные факторы риска
4. Постоянные факторы риска
5. Допустимые факторы риска
6. Политические факторы риска
7. Критические факторы риска
8. Катастрофические факторы риска

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.2: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.3. Анализ и оценки риска
Цель: изучить анализ и оценки рисков
Перечень изучаемых элементов содержания:
- целесообразность инвестиций,
- меры по защите от возможных потерь на предприятии.

Вопросы для самоподготовки:

1. Материальные потери.
2. Трудовые потери.
3. Финансовые потери.
4. Потери времени.
5. Специальные виды потерь.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.3

Форма практического задания: лабораторный практикум.
Лабораторная работа 7. «Анализ и оценки риска».

Контрольные вопросы:

1. Определение риска в абсолютном выражении
2. Определение риска в относительном выражении
3. Статистический способ анализа риска
4. Экспертный способ анализа риска
5. Расчетно-аналитический способ анализа риска
6. Способы анализа риска на основе аналогий.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.3: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.4. Способы минимизации риска
Цель: изучить возможности минимизации рисков на предприятии
Перечень изучаемых элементов содержания:
- методы снижения риска на предприятии,
- избежание риска,
- страхование риска.

Вопросы для самоподготовки:
1. Диверсификация производственной деятельности.
2. Хеджирование.
3. Опционы на закупку товаров и услуг.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.4

Форма практического задания: лабораторный практикум.
Лабораторная работа 8. «Способы минимизации риска».

Контрольные вопросы:
1. Методам снижения риска на предприятии
2. Страхование риска
3. Минимизация риска
4. Избежание риска
5. Самострахование риска

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.4: форма рубежного контроля – отчет по лабораторной работе.

Модуль: Разработка, конфигурирование и обеспечение безопасности КИС и ПО

Раздел 1. Понятия КИС и ПО

Цель: ознакомиться с основными понятиями корпоративных информационных систем и программного обеспечения

Перечень изучаемых элементов содержания
различные подходы к определению понятия КИС и ПО.

Тема 1.1. Общие сведения о КИС и ПО
Цель: изучить основные сведения о КИС и ПО.
Перечень изучаемых элементов содержания
- Понятие КИС и ПО,
- Контроль качества на предприятии,
- ИСО 9000 и информатизация предприятий,
- Общие требования к корпоративным информационным системам и ПО,
- Архитектура КИС и ПО,
- История развития КИС.

Вопросы для самоподготовки:

1. Определение КИС и ПО,
2. История развития КИС,
3. Архитектура КИС и ПО.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.1

Форма практического задания: лабораторный практикум.
Лабораторная работа 1. «Внедрение КИС и ПО. Методики внедрения».

Контрольные вопросы:
1. Метод «Большой взрыв»
2. Метод «Франчайзинговая стратегия»
3. Метод «Точный бросок»
4. Общая методика внедрения корпоративных информационных систем
5. Причины неудач при внедрении КИС

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.1.: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.2. Жизненный цикл КИС и ПО
Цель: изучить жизненный цикл КИС и ПО.
Перечень изучаемых элементов содержания
- Жизненный цикл программного обеспечения. Модели жизненного цикла.
- Подготовка к внедрению или разработке системы. Процесс внедрения.
- Разработка стратегии автоматизации
- Анализ деятельности предприятия
- Реорганизация деятельности
- Методика BSP.

Вопросы для самоподготовки:
1. Жизненный цикл программного обеспечения.
2. Модели жизненного цикла.
3. Анализ деятельности предприятия
4. Реорганизация деятельности
5. Методика BSP.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.2.

Форма практического задания: лабораторный практикум.
Лабораторная работа 2. «Жизненный цикл КИС и ПО».

Контрольные вопросы:
1. Модели жизненного цикла КИС: каскадная, спиральная.
2. Этапы проектирования КИС.
3. Реинжиниринг бизнес-процессов.
4. Моделирование бизнес-процессов.
5. Системы автоматизированного проектирования КИС.
6. CASE-технологии.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.2.: форма рубежного контроля – отчет по лабораторной работе.

Тема 1.3. Внедрение КИС и ПО

Цель: изучить особенности внедрения КИС и ПО на предприятиях.

Перечень изучаемых элементов содержания

- Выбор системы
- Внедрение системы
- Эксплуатация системы
- Типичные проблемы при внедрении КИС
- Сравнение затрат на этапы цепочки выбора и возможных потерь
- Разработка стратегии развития предприятия
- Разработка стратегии автоматизации.

Вопросы для самоподготовки:

1. Выбор системы
2. Внедрение и эксплуатация системы
3. Разработка стратегии развития предприятия
4. Разработка стратегии автоматизации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 1.3.

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «Внедрение КИС и ПО на предприятиях».

Контрольные вопросы:

1. Основные причины внедрения КИС.
2. Этапы проектирования КИС.
3. Основные проблемы, связанные с внедрением КИС.
4. Минимизация ресурсов при внедрении КИС.
5. Основные особенности выбора КИС.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 1.3.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 2. Разработка КИС и ПО

Цель: ознакомиться с основами разработки корпоративных информационных систем и программного обеспечения

Перечень изучаемых элементов содержания

различные подходы к разработке КИС и ПО.

Тема 2.1. Разработки информационных систем

Цель: изучить возможности разработки КИС и ПО.

Перечень изучаемых элементов содержания

- Основные компоненты.
- Принципы создания информационных систем.
- Понятия проекта и проектирования информационной системы.
- Методы проектирования информационных систем.
- Краткая характеристика применяемых технологий проектирования

- Требования к технологии проектирования информационных систем
- Технология и стандарты проектирования.
- Выбор средств проектирования информационных систем.

Вопросы для самоподготовки:
1. Принципы создания информационных систем.
2. Методы проектирования информационных систем.
3. Технология и стандарты проектирования.
4. Выбор средств проектирования информационных систем.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.1

Форма практического задания: лабораторный практикум.
Лабораторная работа 1. «Разработка информационных систем».

Контрольные вопросы:
1. Модели информационной системы
2. Стадии разработки программного обеспечения.
3. Этапы разработки информационной системы.
4. Общие сведения о моделях информационной системы.
5. Подходы к разработке информационных систем.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.1.: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.2. Разработки информационных систем, работающих с использованием Internet
Цель: изучить возможности разработки КИС с использованием Internet.
Перечень изучаемых элементов содержания
- Разработка сценариев
- Использование интернет-приложений при разработке корпоративных информационных систем
- Использование web-приложений в сети интранет
- Доступ к базам данных из интернет-приложений. Интерфейсы cgi, api, fastcgi.
- Создания сайта электронного магазина в среде asp.
- Особенности работы с asp-файлами.
- Объекты доступа к базе данных в asp.

Вопросы для самоподготовки:

1. Использование интернет-приложений при разработке корпоративных информационных систем
2. Использование web-приложений в сети интранет
3. Интерфейсы cgi, api, fastcgi
4. Особенности работы с asp-файлами.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.2.

Форма практического задания: лабораторный практикум.
Лабораторная работа 2. «Информационные системы, работающие с использованием Internet».

Контрольные вопросы:
1. Составляющие информационных технологий

2. Классификация информационных технологий.
3. Роль сетей Internet (Wide Area Network)/ Intranet (Local Area Network) в информационных технологиях
4. Основные свойства информационных технологий

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.2.: форма рубежного контроля – отчет по лабораторной работе.

Тема 2.3. Разработка интегрированных информационных систем

Цель: изучить различные виды КИС.

Перечень изучаемых элементов содержания

- Проектирование клиент-серверных корпоративных информационных систем.
- Принципы и особенности проектирования интегрированных информационных систем
- Основные понятия и особенности проектирования клиент-серверных информационных систем (КИС)
- Стандартные методы совместного доступа к базам и программам в сложных информационных системах (драйверы odbc, dcom и corba технологии)
- Разработка информационной системы с трехзвенной (трехуровневой) архитектурой.
- Проектирование систем оперативной обработки транзакций
- Использование систем управления рабочими потоками
-Использование интернет-приложений
- Проектирование систем оперативного анализа данных.

Вопросы для самоподготовки:

1. Проектирование клиент-серверных корпоративных информационных систем.
2. Разработка информационной системы с трехзвенной (трехуровневой) архитектурой.
3. Использование систем управления рабочими потоками.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 2.3.

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «Разработки интегрированных информационных систем».

Контрольные вопросы:

1. Классификация информационных систем
2. Базовые методологии разработки информационных систем.
3. Уровень функциональности ИС.
4. Обзор интегрированных КИС.
5. Концепция ИКИС «Галактика».

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 2.3.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 3. Конфигурирование КИС и ПО

Цель: ознакомиться с основами конфигурирования корпоративных информационных систем и программного обеспечения

Перечень изучаемых элементов содержания

различные технические подходы при конфигурировании КИС и ПО.

Тема 3.1. Цели и задачи сопровождения и конфигурационного управления версиями программных средств.

Цель: изучить возможности сопровождения и конфигурационного управления версиями ПО.

Перечень изучаемых элементов содержания

- Цели и основные понятия сопровождения и конфигурационного управления версиями программных средств.
- Основные объекты КИС.

Вопросы для самоподготовки:

1. Цели и основные понятия сопровождения и конфигурационного управления версиями программных средств.
2. Основные объекты КИС.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 3.1.

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Сопровождение конфигурационного управления версиями программных средств».

Контрольные вопросы:

1.Ресурсы, необходимые для обеспечения сопровождения и управления конфигурацией программных средств.
2. Организация специалистов для сопровождения и управления конфигурацией программных средств.
3. Характеристика качества процессов сопровождения программных средств.
4. Верификация и тестирование модификаций при сопровождении программных средств.
5. Инструментальные системы для управления конфигурацией программных средств.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 3.1.: форма рубежного контроля – отчет по лабораторной работе.

Тема 3.2. Особенности тестирования и отладки программных компонент.

Цель: изучить особенности тестирования и отладки программных компонент.

Перечень изучаемых элементов содержания

- Методы и стратегии тестирования программных компонентов.
- Этапы и задачи тестирования программных компонент.
- Принципы работы с метаданными КИС.
- Принципы работа со справочником КИС.
- Принципы работы с документами КИС.

Вопросы для самоподготовки:

1. Методы и стратегии тестирования программных компонентов.
2. Принципы работы с метаданными КИС.
3. Принципы работа со справочником и документами КИС.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 3.2.

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «Особенности тестирования и отладки программных компонент».

Контрольные вопросы:

1. Принципы построения компонент для обеспечения надежности функционирования программных средств.

2. Особенности тестирования и отладки программных компонент.
3. Методы и стратегии тестирования программных компонент.
4. Этапы и задачи тестирования программных компонент.
5. Принципы тестирования структуры программных модулей.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 3.2.: форма рубежного контроля – отчет по лабораторной работе.

Тема 3.3. Требования к технологии и средствам автоматизации разработки сложных программных средств.

Цель: изучить требования к технологии и средствам автоматизации разработки сложных программных средств.

Перечень изучаемых элементов содержания

- Планирование и управление обеспечением качества и надежности программ.
- Перечень стандартов, обеспечивающих надежность программных средств.
- Принципы администрирования КИС.
- Технология сохранения и восстановления данных КИС.

Вопросы для самоподготовки:

1. Перечень стандартов, обеспечивающих надежность программных средств.
2. Принципы администрирования КИС.
3. Технология сохранения и восстановления данных КИС.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 3.3.

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «Средства автоматизации разработки сложных программных средств».

Контрольные вопросы:

1. Требования к объекту разработки
2. Требования к процессу, технологии и организации выполнения совокупности работ и документов.
3. Требования к методам и характеристикам средств автоматизации выполнения работ.
4. Требования к методам и средствам контроля, измерения и документирования качества процессов и результатов выполненных работ.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 3.3.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 4. Обеспечение безопасности КИС и ПО

Цель: ознакомиться с основами обеспечения безопасности корпоративных информационных систем и программного обеспечения на предприятии

Перечень изучаемых элементов содержания

различные подходы к обеспечению безопасности КИС и ПО.

Тема 4.1. Основные цели и задачи аудита безопасности и анализа рисков компании

Цель: изучить основные цели и задачи аудита безопасности и анализа рисков.

Перечень изучаемых элементов содержания

- Актуальность аудита безопасности и анализа рисков компании
- Оценка уровня безопасности КИС
- Возможные виды аудита безопасности КИС.

Вопросы для самоподготовки:

1. Оценка уровня безопасности КИС
2. Возможные виды аудита безопасности КИС.
3. Актуальность аудита безопасности и анализа рисков компании.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 4.1.

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Цели и задачи аудита безопасности и анализа рисков компании».

Контрольные вопросы:

1. Понятие аудита информационной безопасности.
2. Основные направления аудита информационной безопасности.
3. Когда возникает необходимость проведения аудита.
4. Виды аудита.
5. Классификация видов аудита.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 4.1.: форма рубежного контроля – отчет по лабораторной работе.

Тема 4.2. Возможные методики аудита безопасности КИС

Цель: изучить основные цели и задачи аудита безопасности и анализа рисков.

Перечень изучаемых элементов содержания:

- Новое поколение стандартов информационной безопасности
- Стандарты ISO/IEC 17799:2000 (BS 7799-1:2000) и BS 7799-2:2000
- Стандарт COBIT 3rd Edition
- Стандарт ISO/IEC 15408

Вопросы для самоподготовки:

1. Стандарты информационной безопасности,
2. Особенности стандарта ISO/IEC,
3. Особенности стандарта COBIT,
4. Особенности стандарта ISO/IEC 15408.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 4.2.

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «Методики аудита безопасности КИС».

Контрольные вопросы:

1.Новое поколение стандартов информационной безопасности
2.Анализ информационных рисков компании.
3.Методы оценивания информационных рисков компании.
4.Табличные методы оценки рисков.
5.Пример методики анализа рисков на качественном уровне (матрица рисков.)
6.Роль анализа рисков в процессе создания корпоративной системы информационной безопасности (на примере модели LifeCycle Security).
7.Возможная методика реорганизации корпоративной системы безопасности.
8.Проектирование системы обеспечения безопасности объекта.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 4.2.: форма рубежного контроля – отчет по лабораторной работе.

Тема 4.3. Аналитический обзор инструментальных средств для анализа рисков и защищенности корпоративных систем Intranet/Internet

Цель: изучить основные инструментальные средства для анализа рисков и защищенности корпоративных систем.

Перечень изучаемых элементов содержания:

- Инструментальные проверки уровня безопасности компании
- Internet Scanner и System Security Scanner
- Сканер уязвимости Symantec NetRecon
- Система централизованного управления безопасностью Enterprise Security Manager
- Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar)
- Сканер Retina
- Сканер Xspider

-Пример использования средств активного аудита.

- Инструментальные средства анализа рисков
- Использование "матрицы рисков" (MS IT Advisor for Risk Management)
- Количественный подход к анализу рисков на примере RiskWatch
- Выбор оптимальной стратегии защиты компании.

Вопросы для самоподготовки:

1. Инструментальные проверки уровня безопасности компании
2. Сравнение Internet Scanner и System Security Scanner
3. Инструментальные средства анализа рисков.
4. Выбор оптимальной стратегии защиты компании.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ТЕМЕ 4.3.

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «Инструментальные средства для анализа рисков и защищенности корпоративных систем Intranet/Internet».

Контрольные вопросы:

1. Internet Scanner и System Security Scanner
2. Сканер уязвимости Symantec NetRecon
3. Система централизованного управления безопасностью Enterprise Security Manager
4. Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar)
5. Сканер Retina
6. Сканер Xspider
7. Пример использования средств активного аудита.
8. Использование "матрицы рисков" (MS IT Advisor for Risk Management)
9. CRAMM
10. Количественный подход к анализу рисков на примере RiskWatch
11. Выбор оптимальной стратегии защиты компании.

РУБЕЖНЫЙ КОНТРОЛЬ К ТЕМЕ 4.3.: форма рубежного контроля – отчет по лабораторной работе.

Оформление работ, выполняемых в рамках самостоятельной работы осуществляется в соответствии с Методическими указаниями по оформлению письменных работ обучающихся в

рамках самостоятельной работы, утвержденными Учебно-методическим советом РГСУ, Протокол № 2 от 25 июня 2015 года.

Конкретные практические задания и задания для рубежного контроля определяются в учебно-методических материалах по работе обучающихся в электронной информационно-образовательной среде РГСУ с применением технологий электронного обучения по данной дисциплине, утверждаемых ежегодно.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по дисциплине является **экзамен,** которые проводятся в **устной** форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	*Знать:* сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства	Этап формирования знаний
		Уметь: Умеет применять основные методы обеспечения информационной безопасности	Этап формирования умений
		Владеть: базовой терминологией и гуманитарными аспектами в области информационной безопасности личности,	Этап формирования навыков и получения опыта

		общества и государства	
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах. **Уметь:** проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации **Владеть:** современными технологиями информационного поиска и дифференцированного анализа	Этап формирования знаний Этап формирования умений

			Этап формирования навыков и получения опыта
ОПК-2.1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Знать: глобальные и локальные проблемы обеспечения информационно-психологической и информационно-технической безопасности личности , общества и государства в информационном пространстве, в том числе с учетом современных угроз со стороны иностранных технических разведок, субъектов как промышленного шпионажа и технологического терроризма, так и представителей криминальной сферы. Уметь: самостоятельно анализировать и дифференцированно оценивать угрозы информационной безопасности, обоснованно представлять себе значение инженерно- технических и гуманитарных научных направлений для эффективного противодействия субъектам угроз и экономически обоснованному применению методов и средств	Этап формирования знаний
			Этап формирования умений

		управления системой комплексного обеспечения информационной безопасности. Владеть: основными знаниями в вопросах мирового динамического процесса исторического развития методов и средств обеспечения информационной безопасности, с учетом социального и научно-технического развития общества.	 Этап формирования навыков и получения опыта

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Этапы формирования компетенций	Показатель оценивания компетенции	Критерии и шкалы оценивания
ОПК-1, ОПК-8, ОПК-2.1		Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных

			неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.
ОПК-1, ОПК-8, ОПК-2.1		Аналитическое задание (задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.) Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией - 9-10 баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании -7-8 баллов; 3) испытывает затруднения в выполнении практических

			заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению5-6 баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания - 0-4 баллов.
ОПК-1, ОПК-8, ОПК-2.1		Аналитическое задание (задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.) Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

4.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Теоретический блок вопросов:

1. В чем отличие применения международных стандартов ISO15408 и ISO17799.
2. Защита государственных интересов в период образования русского централизованного государства (вторая половина XIV в. -первая половина XVI в.).
3. Информационно-психологические операции как организационная форма реализации концепции информационно-психологической войны инфраструктуры.

4. Какие можно отметить особенности опыта организации защиты информации на Древнем Востоке?
5. Каков порядок распоряжения сведениями, составляющими государственную тайну?
6. Криптографическая деятельность СССР накануне и во время Второй мировой войны.
7. Особенности построения межгосударственных систем защиты информации.
8. Охарактеризуйте нормативно-правовую базу Европейского Союза в сфере информационной безопасности.
9. Порядок обращение с документами, содержащими сведения составляющие государственную тайну.
10. Правовой режим обеспечения безопасности персональных данных.
11. Приоритеты исследований в области защиты американской информационной инфраструктуры.
12. Раскройте содержание правового режима электронной цифровой подписи.
13. Системы защиты информации в Федеративной Республике Германия.
14. Состав и основные направления деятельности органов, осуществляющих защиту информации по национальной безопасности в США.
15. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности.
16. Тайные операции в криптографии. Агентурные действия в период между Первой и Второй мировыми войнами.
17. Характеристика современной системы защиты информации в Европейском Союзе.
18. Что является нормативно-правовой основой для введения дополнительных ограничений по контролю над деятельностью персонала?
19. Что такое «правовое обеспечение информационной безопасности», раскройте содержание правового обеспечения безопасности сведений.
20. Что такое «сертификат ключа электронной цифровой подписи» и зачем он нужен?
21. Перечислите службы образующие государственную систему защиты информации.
22. Правовая защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации.
23. Основные положения конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных».
24. Роль ЕС и международных организации в регулировании международного информационного обмена.
25. Национальные интересы РФ в информационной сфере и их обеспечения.
26. Административный уровень информационной безопасности
27. Администрирование средств безопасности
28. Вредоносное программное обеспечение
29. Действия, приводящие к неправомерному овладении конфиденциальной информацией: разглашение
30. Действия, приводящие к неправомерному овладении конфиденциальной информацией: утечка
31. Действия, приводящие к неправомерному овладении конфиденциальной информацией: несанкционированный доступ
32. Документы по оценке защищенности автоматизированных систем в РФ

33. Достоверность информации. Юридическая значимость информации. Доступность данных. Доступ к информации. Субъект доступа к информации. Оперативность доступа к информации. Собственник информации.
34. Закон "Об информации, информатизации и защите информации"
35. Законодательный уровень информационной безопасности

36. Защита информации от утечки. Защита информации от разглашения. Защита информации от НСД. Система защиты информации. Информационная безопасность.
37. Основные понятия программно-технического уровня информационной безопасности
38. Основные принципы информационной безопасности

39. Особенности обеспечения информационной безопасности в компьютерных сетях
40. Особенности современных информационных систем, существенные с точки зрения безопасности
41. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт
42. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

43. Правовые основы информационной безопасности общества
44. Понятие КИС и ПО
45. Контроль качества на предприятии
46. ИСО 9000 и информатизация предприятий.
47. Общие требования к корпоративным информационным системам и ПО
48. Архитектура КИС и ПО
49. История развития КИС
50. Жизненный цикл программного обеспечения. Модели жизненного цикла.
51. Подготовка к внедрению или разработке системы. Процесс внедрения.
52. Разработка стратегии автоматизации предприятия
53. Анализ деятельности предприятия
54. Реорганизация деятельности предприятия
55. Методика BSP
56. Подход TQM/CPI
57. BPR – реинжиниринг по Хаммеру и Чампи
58. Выбор КИС
59. Внедрение КИС
60. Эксплуатация КИС
61. Типичные проблемы при внедрении КИС
62. Сравнение затрат на этапы цепочки выбора и возможных потерь
63. Основные компоненты ИС.
64. Принципы создания информационных систем.
65. Понятия проекта и проектирования информационной системы.
66. Методы проектирования информационных систем.
67. Краткая характеристика применяемых технологий проектирования ИС
68. Требования к технологии проектирования информационных систем
69. Технология и стандарты проектирования ИС.
70. Выбор средств проектирования информационных систем
71. Case-средства разработки информационных систем. Общая характеристика

72. Функционально-ориентированный и объектно-ориентированный подходы к проектированию ИС
73. Функционально-ориентированное проектирование ИС
74. Объектно-ориентированное проектирование ИС
75. Содержание RAD-технологии прототипного создания приложений
76. Прототипное проектирование ИС (RAD-технология)
77. Методология IDEF0
78. Типы диаграмм в IDEF0
79. Работы в IDEF0
80. Стрелки IDEF0. Типы стрелок
81. Среда BPWIN
82. Применение методологии IDEF0
83. Применение методологии DFD
84. Применение методологии IDEF3
85. Проведение экспертизы и создание отчетов в BPWIN
86. Создание логической и физической модели данных в ERWIN
87. Концептуальное моделирование фактографических баз данных
88. Создание логической модели данных в ERWIN
89. Уровни логической модели в ERWIN
90. Методология IDEF1X
91. Построение модели данных в ERWIN
92. Типы сущностей и иерархия наследования в ERWIN
93. Архитектуры фактографических баз данных
94. Создание физической модели данных
95. Соответствие логической модели ERWIN и модели процессов BPWIN
96. Базы данных с файл-серверной архитектурой
97. Пример создания базы данных архитектуры клиент-сервер с помощью DELPHI
98. Проектирование клиент-серверных корпоративных информационных систем.
99. Принципы и особенности проектирования интегрированных информационных систем
100. Основные понятия и особенности проектирования клиент-серверных информационных систем (КИС)
101. Стандартные методы совместного доступа к базам и программам в сложных информационных системах (драйверы odbc, dcom и corba технологии)
102. Разработка информационной системы с трехзвенной (трехуровневой) архитектурой.
103. Проектирование систем оперативной обработки транзакций
104. Использование систем управления рабочими потоками
105. Использование интернет-приложений
106. Проектирование систем оперативного анализа данных.
107. Разработка сценариев
108. Использование интернет-приложений при разработке корпоративных информационных систем
109. Использование web-приложений в сети интранет
110. Доступ к базам данных из интернет-приложений. Интерфейсы cgi, api, fastcgi.
111. Особенности работы с asp-файлами.
112. Объекты доступа к базе данных в asp.
113. Диаграмма прецедентов использования UML.

114. Диаграммы классов объектов UML.
115. Диаграммы состояний UML
116. Диаграмма взаимодействия объектов UML.
117. Диаграмма деятельностей UML.
118. Диаграммы пакетов UML.
119. Диаграммы компонентов и размещения UML.
120. Актуальность аудита безопасности и анализа рисков компании
121. Оценка уровня безопасности КИС
122. Возможные виды аудита безопасности КИС
123. Новое поколение стандартов информационной безопасности
124. Стандарты ISO/IEC 17799:2000 (BS 7799-1:2000) и BS 7799-2:2000
125. Стандарт COBIT 3rd Edition
126. Стандарт ISO/IEC 15408
127. Анализ информационных рисков компании
128. Методы оценивания информационных рисков компании
129. Табличные методы оценки рисков
130. Пример методики анализа рисков на качественном уровне (матрица рисков)
131. Роль анализа рисков в процессе создания корпоративной системы информационной безопасности (на примере модели LifeCycle Security)
132. Возможная методика реорганизации корпоративной системы безопасности
133. Проектирование системы обеспечения безопасности объекта
134. Инструментальные проверки уровня безопасности компании
135. Internet Scanner и System Security Scanner
136. Сканер уязвимости Symantec NetRecon
137. Система централизованного управления безопасностью Enterprise Security Manager
138. Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar)
139. Сканер Retina
140. Сканер Xspider
141. Пример использования средств активного аудита.
142. Инструментальные средства анализа рисков
143. Использование "матрицы рисков" (MS IT Advisor for Risk Management)
144. Количественный подход к анализу рисков на примере RiskWatch
145. Выбор оптимальной стратегии защиты компании.
146. Разработка концепции, эскизного проекта, руководящих и специальных нормативных документов
147. Структура концепции информационной безопасности
148. Предложения по структуре эскизного проекта

Аналитическое задание*:*

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Брачное агентство).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (1) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

2. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Диспетчерская служба такси).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (1) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

3. Сформировать электронно-цифровую подпись к сообщению «M» и произвести проверку целостности принятого сообщения.

p	q	e	d	M
13	7	5	29	2652

4. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Железнодорожная касса).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (4) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

5. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Брачное агентство).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (1) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

6. Сформировать электронно-цифровую подпись к сообщению «M» и произвести проверку целостности принятого сообщения.

p	q	e	d	M
115	113	302	450	4123

7. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Научно проектное предприятие).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (1) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

8. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Центр оказания государственных услуг).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (4) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

9. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Туристическое агентство).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (2) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

10. Сформировать электронно-цифровую подпись к сообщению «M» и произвести проверку целостности принятого сообщения.

p	q	e	d	M
15	13	7	29	4132

11. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Издательство).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (1) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

12. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Офис благотворительного фонда).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (1) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

13. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Компания по разработке ПО для сторонних организаций).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (4) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

14. Сформировать электронно-цифровую подпись к сообщению «M» и произвести проверку целостности принятого сообщения.

p	q	e	d	M
7	11	37	9	256

15. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Офис интернет-провайдера).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «С» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (1) предложенных в Приложении «Е» ГОСТа произведите оценку рисков информационной безопасности.

16. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «С, D и Е» ГОСТа.

2. Выберите три различных информационных актива организации (Дизайнерская фирма).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «С» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (2) предложенных в Приложении «Е» ГОСТа произведите оценку рисков информационной безопасности.

17. Сформировать электронно-цифровую подпись к сообщению «М» и произвести проверку целостности принятого сообщения.

p	q	e	d	M
11	6	4	9	255

18. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «С, D и Е» ГОСТа.

2. Выберите три различных информационных актива организации (Брачное агентство).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (2) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

19. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Отделение полиции).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (3) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

20. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Рекрутинговое агентство).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (2) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

21. Сформировать электронно-цифровую подпись к сообщению «M» и произвести проверку целостности принятого сообщения.

p	q	e	d	M
3	11	2	9	1220

22. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Центр оказания государственных услуг).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (4) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

23. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Интернет-магазин).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (3) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

24. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Офис страховой компании).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (2) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

25. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»:

1. Ознакомьтесь с Приложениями «C, D и E» ГОСТа.

2. Выберите три различных информационных актива организации (Поликлиника).

3. Из Приложения «D» ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

4. Пользуясь Приложением «C» ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

6. Пользуясь одним из методов (2) предложенных в Приложении «E» ГОСТа произведите оценку рисков информационной безопасности.

5.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестации по дисциплине проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным

программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по дисциплине выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1.1. Основная литература

1. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741
2. *Внуков, А. А.* Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

5.1.2. Дополнительная литература

1. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469866
2. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/473348

5.2. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Сайт антивирусной компании «Avast!». [Электронный ресурс]: офиц. сайт – Режим доступа: http://www.avast.com/ru-ru/index
2. Сайт антивирусной компании ESET NOD32. [Электронный ресурс]: офиц. сайт – Режим доступа: http://www.esetnod32.ru/

3. Сайт антивирусной компании «Dr. Web». [Электронный ресурс]: офиц. сайт – Режим доступа: http://www.drweb.com/
4. Сайт антивирусной компании «Лаборатория Касперского». [Электронный ресурс]: офиц. сайт – Режим доступа: http://www.kaspersky.ru/

№№	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины

Освоение обучающимся дисциплины (модуля)«Основы информационной безопасности» предполагает изучение материалов дисциплины (модуля)на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины. Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с

инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю)»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине (модулю).

5.4.Информационно-технологическое обеспечение образовательного процесса по дисциплине

5.4.1. Информационные технологии

1. Персональные компьютеры;
2. Доступ к Интернет
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.4.3. Информационные справочные системы и профессиональные базы данных

Обучающиеся по программе **«Информационная безопасность»** в университете имеют доступ к следующим современным профессиональным базам данных, информационным справочникам:

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных	Полнотекстовая база данных	http://ebiblioteka.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	«EastView»	периодических изданий	
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.5. Материально-техническое обеспечение образовательного процесса по дисциплине

Для изучения дисциплины (модуля) **«Основы информационной безопасности»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки **10.03.01 Информационная безопасность** используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

По всем темам проводятся лабораторные занятия в лаборатории, оснащенной специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет), а также специализированным лабораторным оборудованием (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением)

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.6. Образовательные технологии

Освоение дисциплины (модуля)**«Основы информационной безопасности»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме компьютерных симуляций в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

В рамках дисциплины (модуля)**«Основы информационной безопасности»** предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/
«06» _июня___2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технология защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ – УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022

Рабочая программа дисциплины (модуля) **«Программно-аппаратные средства защиты информации»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" **(уровень бакалавриата)**, утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
– *06.032 Специалист по безопасности компьютерных систем и сетей*
– *06.033 Специалист по защите информации в автоматизированных системах*

06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля) разработана рабочей группой в составе: к.п.н. Алейников В.В., к.т.н., доц. Сиротский А.А.

Руководитель основной профессиональной образовательной программы к.п.н., доц., доц. _____ Н.Г. Витковская

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года

Декан факультета, _____ С.В. Крапивка
К.п.н., доцент
(подпись)

Рабочая программа дисциплины (модуля) рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет»
зам. ген. директора по науке, _____ А.С. Мосолов
к.т.н., доцент
(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

.д.т.н. , доцент, профессор кафедры информационных технологий , _____ С.Ю. Бутузов
ГБОУВО Академия ГПС МЧС России)
(подпись)

к.ф.-м.н, доцент
кафедра прикладной математики и информатики РГСУ _____ Н.П. Третьяков
(подпись)

Согласовано
Научная библиотека, директор _____ И.Г. Маляр
(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1 Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) заключается в получении обучающимися теоретических знаний о программно-аппаратной защите информации, структуре требований предъявляемых к программно-аппаратным средствам защиты информации, изучении основ практического применения средств обеспечения информационной безопасности, а также в формировании теоретической базы для последующих дисциплин, связанных с процедурами обеспечения информационной безопасности с последующим применением в профессиональной сфере и практических навыков (формирование) по **обеспечению безопасности информации.**

Задачи дисциплины (модуля) :

1. Изучение информационной безопасности корпоративных информационных систем.
2. Защита информации в компьютерных сетях.
3. Аудит качества и надежности защиты информационных систем.
4. Управление информационной безопасностью.

1.1. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы

Учебная дисциплина «**Программно-аппаратные средства защиты информации**» реализуется в **базовой** части основной профессиональной образовательной программы «Информационная безопасность» по направлению подготовки / специальности **«10.03.01 «Информационная безопасность»» очной формы обучения.**

Изучение дисциплины (модуля) «Программно-аппаратные средства защиты информации» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Программирование», «Математика».

Изучение дисциплины (модуля) «Программно-аппаратные средства защиты информации» является базовым для последующего освоения программного материала учебных дисциплин: «Криптографические методы защиты информации», «Основы управления информационной безопасности».

1.2. Планируемые результаты обучения по дисциплине (модулю)в рамках планируемых результатов освоения основной профессиональной образовательной программы.

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих **общепрофессиональных, профессиональных и профессионально-специализированных компетенций**: ОПК-3, ПК-1, ПК-2, ПК-9, ПК-15 в соответствии с основной профессиональной образовательной программой «Организация и технология защиты информации» по направлению подготовки «10.03.01 «Информационная безопасность»».

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	**Код компетенции**	**Формулировка компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения**

	ОПК-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-2.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	*Знать:* современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. *Уметь:* выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. *Владеть:* навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.

	ПК-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-1.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-1.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности - основные направления политик защиты информации на предприятии (организации) **Уметь**: выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации **Владеть:** Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

	ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-2.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** -нормативные документы , связанные с лицензированием видов деятельности, связанных с защитой информации и информационных систем; -нормативные документы, связанные с сертификации средств защиты информации и информационных систем; -факторы, воздействующие на информацию и информационные системы, подлежащие защите, критерии их защищенности, средства и методы обеспечения их защиты. **Уметь:** осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности объекта;

				Владеть: методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; навыками практического применения регламентирующих и методических документов по программно- аппаратной защите информации и информационных систем; - методами и средствами выявления угроз безопасности автоматизированным системам.
	ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной	ПК-9.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах.

		безопасности по профилю своей профессиональной деятельности	ПК-9.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-9.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Уметь:** проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации. **Владеть:** современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации.
	ПК-15	Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и	ПК-15.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции	**Знать:** основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области

		экспортному контролю	ПК-15.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-15.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Уметь:** - организовывать технологические процессы организации в том числе на основе локальной и комплексной автоматизации процессов обработки документов в документационной службе в соответствии с нормативными актами и нормативными методическими документами
				Владеть: - навыками работы с нормативными правовыми актами в области защиты информации - методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем дисциплины (модуля), включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 15 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		5	6			
Контактная работа обучающихся с педагогическими работниками	**270**	**144**	**126**			
Учебные занятия лекционного типа	58	32	26			
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	92	48	44			
из них: в форме практической подготовки						
Иная контактная работа	120	64	56			
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**198**	**108**	**90**			
из них: в форме практической подготовки	39	21	18			
Контроль промежуточной аттестации	**72**	**36**	**36**			
Форма промежуточной аттестации		экзам	экзам			

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**540**	**288**	**252**			

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	**Виды учебной работы, академических часов**												
	Всего	**Самостоятельная работа**	*из них: в форме практической подготовки*	**Контактная работа обучающихся с педагогическими работниками**									
				Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*
Модуль 1 (семестр 5)													
Раздел 1.1	31	13	*3*	18		4				6		8	
Раздел 1.2	31	13	*3*	18		4				6		8	
Раздел 1.3	31	13	*3*	18		4				6		8	
Раздел 1.4	31	13	*3*	18		4				6		8	
Раздел 1.5	32	14	*3*	18		4				6		8	
Раздел 1.6	32	14	*2*	18		4				6		8	
Раздел 1.7	32	14	*2*	18		4				6		8	
Раздел 1.8	32	14	*2*	18		4				6		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**288**	**108**	***21***	**144**		**32**				**48**		**64**	
Форма промежуточной аттестации	**экзамен**												
Модуль 2 (семестр 6)													

Раздел 2.1	30	12	*3*	18		4				6		8	
Раздел 2.2	31	13	*3*	18		4				6		8	
Раздел 2.3	31	13	*3*	18		4				6		8	
Раздел 2.4	31	13	*3*	18		4				6		8	
Раздел 2.5	31	13	*2*	18		4				6		8	
Раздел 2.6	31	13	*2*	18		4				6		8	
Раздел 2.7	31	13	*2*	18		2				8		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**252**	**90**	***18***	**126**		**26**				**44**		**56**	
Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**540**	**198**	***39***	**270**		**58**				**92**		**120**	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1 Виды самостоятельной работы обучающихся по дисциплине

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**
Модуль 1 (семестр 5)							
Раздел 1.1	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 1.3	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.4	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.5	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.6	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.7	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.8	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**108**	**44**		**48**		**16**	
Модуль 2 (семестр 6)							
Раздел 2.1	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 2.3	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.4	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.5	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.6	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.7	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**90**	**35**		**41**		**14**	
Общий объем по дисциплине (модулю), часов	**198**	**79**		**89**		**30**	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю»)

МОДУЛЬ «ПРЕДМЕТ И ЗАДАЧИ КУРСА. НЕСАНКЦИОНИРОВАННОЕ КОПИРОВАНИЕ ИНФОРМАЦИИ.»

РАЗДЕЛ 1.1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ ПРОГРАММНО-АППАРАТНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Цель: Изучить основные термины и определения в области программно-аппаратной защиты информации.

Перечень изучаемых элементов содержания

Тема 1. Информация, как фактор производства.

Вопросы для самоподготовки:

1. Ценность информации.
2. Дезинформация.
3. Коммерческая тайна.
4. Государственная тайна.

Тема 2. Объект и субъект защиты информации.

Вопросы для самоподготовки:

1. АСОД (Автоматизированная система обработки данных).
2. ЭВМ (Электронно- вычислительная машина).
3. Вычислительные системы и сети.

Тема 3. Программно-аппаратные средства защиты информации.

Вопросы для самоподготовки:

1.Программные средства защиты информации.
2. Аппаратные средства защиты информации.
3. Комплексный подход к защите информации от НСД.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.1

Форма практического задания: реферат

Примерный перечень тем рефератов к разделу 1.1:

1. Политика информационной безопасности предприятия.
2. Нормативно-правовая база обеспечения информационной безопасности предприятия.
3. Содержание основных законов Российской Федерации в сфере компьютерного права.
4.Законодательная база РФ по вопросам защиты информации.
5.Комплексный подход к обеспечению информационной безопасности.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.1: форма рубежного контроля – реферат.

РАЗДЕЛ 1.2. НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ, РЕГЛАМЕНТИРУЮЩИЕ ПРИМЕНЕНИЕ ПРОГРАММНО-АППАРАТНОЙ ЗАЩИТЫ ИНФОРМАЦИИ. ПРЕДМЕТ И ЗАДАЧИ КУРСА

Цель: Изучить нормативно-правовые документы, регламентирующие применение программно-аппаратной защиты информации, а также предмет и основные задачи курса.

Перечень изучаемых элементов содержания

Политика информационной безопасности.

Тема 1. Нормативно-правовые документы, регламентирующие применение ПАСЗИ.

Вопросы для самоподготовки:

1. Политика информационной безопасности
2. Доктрина информационной безопасности РФ.

Тема 2. Предмет и задачи курса.

Вопросы для самоподготовки:

1. Методы обеспечения информационной безопасности
2. Средства обеспечения информационной безопасности
3. Цель ПАСЗИ.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.2

Форма практического задания: практическое задание.

Примерный перечень тем рефератов к разделу 1.2:

1. Органы (подразделения), обеспечивающие информационную безопасность.
2. Технология защиты информационной системы.
3. Информационное право.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.2: форма рубежного контроля – реферат.

РАЗДЕЛ 1.3. МЕТОДЫ И СРЕДСТВА ПРОГРАММНО-АППАРАТНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Цель: Изучить основные методы и средства программно-аппаратной защиты информации.

Перечень изучаемых элементов содержания

Спектр – Z. Криптон-Вето.

Тема 1. Методы и средства программно-аппаратной защиты информации.

Вопросы для самоподготовки:

1. Классификация программно-аппаратных средств защиты информации.
2. Примеры ПАСЗИ.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.3

Форма практического задания: практическое задание.

Примерный перечень тем рефератов к разделу 1.3:

1. Программно-аппаратный комплекс защиты **DAALLAS LOCK**
2. Система криптографической защиты «Верба»

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.3: форма рубежного контроля – реферат.

РАЗДЕЛ 1.4. НАСТРОЙКИ ЗАЩИЩАЕМОГО ПО НА ХАРАКТЕРИСТИКИ КОМПЬЮТЕРА

*Цель: освоение методов настройки защищаемого программного продукта на характеристики компьютера и пользователя***.**

Перечень изучаемых элементов содержания

Защита информации. Копирование информации. Несанкционированное копирование.

Вопросы для самоподготовки:

1. Функции Windows API.
2. Структура реестра Windows.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.4

Форма практического задания: практическое задание

Примерный перечень тем рефератов к разделу 1.4:

1. Использование функций Windows API для получения индивидуальных характеристик аппаратных средств компьютера (в соответствии с индивидуальным заданием).
2. Использование функций Windows API для получения индивидуальных характеристик операционной системы (в соответствии с индивидуальным заданием).

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.4: форма рубежного контроля – реферат.

РАЗДЕЛ 1.5. ЗАЩИТА ПО ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

*Цель: освоение средств защиты программ от несанкционированного копирования***.**

Перечень изучаемых элементов содержания

Программное обеспечение. Копирование информации. Несанкционированное копирование.

Вопросы для самоподготовки:

1. Инсталляция.
2. Программирование.
3. Характеристики компьютера.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.5

Форма практического задания: практическое задание

Примерный перечень тем рефератов к разделу 1.5:

1. Функции проверки легальности среды запуска.
2. Модифицированные программы.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.5: форма рубежного контроля – реферат.

РАЗДЕЛ 1.6. ИНТЕРФЕЙСЫ WINDOWS ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Цель: Изучить интерфейсы Windows.

Перечень изучаемых элементов содержания

Интерфейс. Защита информации. Операционная система.

Вопросы для самоподготовки:

1. Тестирование модифицированной программы.
2. Программные средства.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.6

Форма практического задания: практическое задание

Примерный перечень тем рефератов к разделу 1.6:

1. Методы и средства криптографического интерфейса ОС Windows.
2. Средства для разграничения доступа к конфиденциальной компьютерной информации.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.6: форма рубежного контроля – реферат.

РАЗДЕЛ 1.7 ЗАЩИЩЕННЫЕ ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ

Цель: Изучить защищенные программно-аппаратные комплексы.

Перечень изучаемых элементов содержания

Secret Net. Тонкий клиент.

Тема 1. Сертифицированные программно-аппаратные средства защиты информации.

Вопросы для самоподготовки:

1. Программно-аппаратный комплекс SecretNet.
2. Реализация основных защитных механизмов средствами SecretNet.
3. Настройка комплекса SecretNet.

Тема 2. Программно-аппаратные комплексы на базе «тонких клиентов».

Вопросы для самоподготовки:

1. Основные достоинства комплексов на базе «тонких клиентов».
2. Администрирование комплексов на базе «тонких клиентов».
3. Реализация основных защитных механизмов на базе «тонких клиентов».

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.7

Форма практического задания: практическое задание.

Примерный перечень тем рефератов к разделу 1.7:

1. Разработка инструкций по эксплуатации программно-аппаратных комплексов.
2. Разработка должностных инструкций администраторов информационной безопасности программно-аппаратных комплексов.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.7: форма рубежного контроля – реферат.

МОДУЛЬ «МЕХАНИЗМЫ ЗАЩИЩЕННОГО ДОСТУПА. ОБЛАЧНЫЕ РЕШЕНИЯ.»

РАЗДЕЛ 2.1. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.

Цель: Изучить базовые механизмы защиты информации.

Перечень изучаемых элементов содержания
Идентификация. Аутентификация. Биометрическая аутентификация. Авторизация.

Тема 1. Идентификация.

Вопросы для самоподготовки:
1. Идентификаторы.
2. Технология идентификации.

Тема 2. Аутентификация.

Вопросы для самоподготовки:
1.Аутентифицируемый и аутентифицирующий.
2. Аутентификаторы.
3. Односторонняя аутентификация.
4. Двусторонняя аутентификация.
5. Авторизация.
6. Технология аутентификации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.1

Форма практического задания: практическое задание

Примерный перечень тем рефератов к разделу 2.1:
1Исследование стойкости паролей.
2.Алгоритмы генерации стойких паролей.
3.Свойства хэш-функции.
4.Алгоритмы хэш – преобразований.
5.Российский стандарт вычисления хэш-функции.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.1: форма рубежного контроля – реферат.

РАЗДЕЛ 2.2. УПРАВЛЕНИЕ И РАЗГРАНИЧЕНИЕ ДОСТУПА

Цель: Изучить иерархический доступ к файлу, защиту сетевого файлового ресурса, фиксацию доступа к файлам; доступ к данным со стороны процесса.

Перечень изучаемых элементов содержания
Шифрование. Контроль доступа. Разграничение доступа. Управление доступом. Основные методы управления и разграничения доступом.

Тема 1. Управление доступом.

Вопросы для самоподготовки:
1. Организация доступа к файлам.
2. Понятие атрибутов доступа.
3.Защита сетевого файлового ресурса.

Тема 2. Разграничение доступа.

Вопросы для самоподготовки:

1. Фиксация доступа к файлам.
2. Способы фиксации файлов доступа.
3. Журналы доступа.
4. Выявление следов НСД к файлам.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.2

Форма практического задания: практическое задание.

Примерный перечень тем рефератов к разделу 2.2:

1. Доступ к данным со стороны процесса.
2. Способы фиксации факта доступа.
3. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа.
4. Надежность систем ограничения доступа.
5. Защита файлов от изменения.
6. Организация защиты сетевых ресурсов с использованием СЗИ «Secret Net».
7. Особенности защиты данных от изменения.
8. Защита массивов информации от изменения (имитозащита).
9. Криптографическая постановка защиты от изменения данных.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.2: форма рубежного контроля – реферат.

РАЗДЕЛ 2.3. ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Цель: Изучить понятие и технологию электронно-цифровой подписи.

Перечень изучаемых элементов содержания

Электронно-цифровая подпись.

Тема 1. Электронно-цифровая подпись.

Вопросы для самоподготовки:

1. История возникновения ЭЦП.
2. Схемы построения ЭЦП.
3. Подделка ЭЦП.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.3

Форма практического задания: практическое задание.

Примерный перечень тем рефератов к разделу 2.3:

1. Федеральные законы об ЭЦП.
2. ЭЦП в России.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.3: форма рубежного контроля – реферат.

РАЗДЕЛ 2.4. ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ: SaaS

Цель: Изучить облачные технологии, программное обеспечение как сервис.

Перечень изучаемых элементов содержания

Облачные технологии. SaaS.

Вопросы для самоподготовки:
1. Достоинства и недостатки SaaS.
2. Защита информации.
3. Бизнес приложения (CRM, поддержка сервисов, свои приложения).

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.4

Форма практического задания: практическое задание

Примерный перечень тем рефератов к разделу 2.4:
1. Соответствие аппратно-программных комплексов облачным технологиям на примере SaaS
2.Сравнение SaaS, IaaS, PaaS.
3. BPaaS.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.4: форма рубежного контроля – реферат.

РАЗДЕЛ 2.5. ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ: IaaS
Цель: Изучить облачные технологии, инфраструктура как сервис.

Перечень изучаемых элементов содержания
Облачные технологии. IaaS.

Вопросы для самоподготовки:
1. Достоинства и недостатки IaaS.
2. Защита информации.
3. Инфраструктура (безопасность, скорость, доступ).

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.5

Форма практического задания: практическое задание

Примерный перечень тем рефератов к разделу 2.5:
1. Соответствие аппратно-программных комплексов облачным технологиям на примере IaaS
2. Сравнение SaaS, IaaS, PaaS.
3. BPaaS.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.5: форма рубежного контроля – реферат.

РАЗДЕЛ 2.6. ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ: PaaS
Цель: Изучить облачные технологии, платформа как сервис.

Перечень изучаемых элементов содержания
Облачные технологии. PaaS.

Вопросы для самоподготовки:

1. Достоинства и недостатки PaaS.
2. Защита информации.
3. Платформа (настройка экранов, отчетов, интерфейсов, бизнес-процессов).

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.6

Форма практического задания: практическое задание

Примерный перечень тем рефератов к разделу 2.6:
1. Соответствие аппратно-программных комплексов облачным технологиям на примере PaaS
2. Сравнение SaaS, IaaS, PaaS.
3. BPaaS.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.6: форма рубежного контроля – реферат.

РАЗДЕЛ 2.7. КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА

Цель: Изучить целостность программного обеспечения, получить навыки контроля над целостностью ПО. Ознакомиться с замкнутой программной средой.

Перечень изучаемых элементов содержания
Целостность ПО. Замкнутая программная среда.

Тема 1. Контроль целостности ПО.

Вопросы для самоподготовки:
1. Программные средства контроля целостности программного обеспечения (ПО).
2. Эталонные образы ПО.
3. Механизмы ограничения прав пользователей при нарушении целостности ПО.

Тема 2. Замкнутая программная среда.

Вопросы для самоподготовки:
1. Программные средства организации замкнутой программной среды.
2. Списки разрешённых программ для пользователей.
3. Механизмы ограничения прав пользователей при запуске ПО.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.7

Форма практического задания: практическое задание.

Примерный перечень тем рефератов к разделу 2.7:
1. Формирование списков разрешённых программ пользователей.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.7: форма рубежного контроля – реферат.

РАЗДЕЛ 2.8 ЗАЩИТА ОТ УДАЛЕННЫХ АТАК.

Цель: Ознакомиться с удаленными атаками, получить навыки противостояния им

Перечень изучаемых элементов содержания
Удаленные атаки. Межсетевые экраны.

Тема 1. Удаленные атаки на сетевые службы.

Вопросы для самоподготовки:
1. Классификация атак.
2. Механизмы удалённых атак.
3. Модели удалённых атак.

Тема 2. Межсетевые экраны.

Вопросы для самоподготовки:
1. Классификация и разновидности МСЭ.
2. Фильтрующие маршрутизаторы.
3. Шлюзы сетевого уровня.
4. Шлюзы прикладного уровня.
5. Системы обнаружения и предотвращения вторжений.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.8

Форма практического задания: практическое задание.

Примерный перечень тем рефератов к разделу 2.8:
3. Механизмы возникновения уязвимостей инфокоммуникационных систем.
4. Алгоритмы атак на уязвимости инфокоммуникационных систем.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.8: форма рубежного контроля – реферат.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

4.1. Форма промежуточной аттестации обучающегося по учебной дисциплине

Контрольным мероприятием промежуточной аттестации обучающихся по учебной дисциплине является **экзамен,** который проводится в **устной** форме.

В случае применения электронного обучения, дистанционных образовательных технологий указывается форма промежуточной аттестации, а также дается краткая инструкция по проведению.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-2	Способен	*Знать:* современные	Этап формирования знаний

	применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	
		Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Этап формирования умений
		Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Этап формирования навыков и получения опыта
ПК-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать:** методы установки, настройки и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации и информационных систем.	Этап формирования знаний
		Уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации и информационных систем.	Этап формирования умений
		Владеть: способностью выполнять работы по установке, настройке и обслуживанию	Этап формирования навыков и получения опыта

		программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации и информационных систем.	
ПК-2	Способен применять технические и программно-аппаратные средства обработки и защиты информации	**Знать:** -нормативные документы , связанные с лицензированием видов деятельности, связанных с защитой информации и информационных систем; -нормативные документы, связанные с сертификации средств защиты информации и информационных систем; -факторы, воздействующие на информацию и информационные системы, подлежащие защите, критерии их защищенности, средства и методы обеспечения их защиты.	Этап формирования знаний
		Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности объекта;	Этап формирования умений
		Владеть: методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; навыками практического применения	Этап формирования навыков и получения опыта

		регламентирующих и методических документов по программно- аппаратной защите информации и информационных систем; - методами и средствами выявления угроз безопасности автоматизированным системам.	
ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах.	Этап формирования знаний
		Уметь: проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации	Этап формирования умений
		Владеть: современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов	Этап формирования навыков и получения опыта

		информатизации	
ПК-15	Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Этап формирования знаний
		Уметь: - организовывать технологические процессы организации в том числе на основе локальной и комплексной автоматизации процессов обработки документов в документационной службе в соответствии с нормативными актами и нормативными методическими документами	Этап формирования умений
		Владеть: - навыками работы с нормативными правовыми актами в области защиты информации - методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной	Этап формирования навыков и получения опыта

		безопасности	

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	**Этапы формирования компетенций**	**Показатель оценивания компетенции**	**Критерии и шкалы оценивания**
ОПК-2, ПК-1, ПК-2, ПК-9, ПК-15	Этап формирования знаний.	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.

ОПК-2, ПК-1, ПК-2, ПК-9, ПК-15	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией - 9-10 баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании -7-8 баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению5-6 баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания - 0-4 баллов.
ОПК-2, ПК-1, ПК-2, ПК-9, ПК-15	Этап формирования навыков и получения опыта	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

4.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Теоретический блок вопросов:

1. Виды систем идентификации и аутентификации.
2. Парольные подсистемы идентификации и аутентификации. Количественная оценка стойкости парольной защиты.
3. Хранение аутентифицирующей информации в открытых компьютерных системах. Типовые схемы хранения ключевой информации. Защита БД аутентификации.
4. Политики безопасности операционных систем.
5. Защита баз данных аутентификации операционных систем класса Windows.
6. Понятие Хеш-функций.
7. Алгоритмы вычисления хеш-значений.
8. Протокол CHAP.
9. Протокол S/KEY.
10. Протокол Kerberos.
11. Удаленная аутентификация в Windows с использованием хэша LANMAN.
12. Технические устройства идентификации и аутентификации.
13. Устройства iButton (Touch Memory), архитектура, разновидности и параметры.
14. Бесконтактные радиочастотные карты Proximity. Архитектура и принцип работы.
15. Смарт-карты. Устройство и принцип работы.
16. Электронные ключи e-Token. Устройство и принцип работы. Программный комплекс (ПК) eToken PKI.
17. Архитектура SMART-карт.
18. Идентификация и аутентификация пользователей с помощью биометрических устройств.
19. Архитектура биометрических устройств идентификации и аутентификации.
20. Системы контроля доступа (СКД) и Системы контроля и управления доступом (СКУД):
функции, разновидности.
21. Архитектура сетевых СКД, СКУД.
22. Защита программного обеспечения от несанкционированного использования.
23. Защита программного обеспечения от несанкционированного копирования.
24. Модульная архитектура и требования к системам защиты программного обеспечения от несанкционированного использования и копирования.
25. Электронные ключи. Защита программ с помощью электронных ключей HASP.
26. Механизм защиты структурного кода Pattern Code Security.
27. Защита программного обеспечения от исследования.
28. Классификация средств атаки на средства защиты программного обеспечения.
29. Защита от разрушающих программных воздействий (РПВ).
30. Компьютерные вирусы как класс разрушающих программных воздействий (РПВ). Отличительные особенности класса, функции, основные разновидности.
31. Методы борьбы с разрушающими программными воздействиями (РПВ).
32. Сертификация программного обеспечения по уровню контроля отсутствия не декларируемых возможностей (НДВ).
33. Требования РД ФСТЭК 1998 г. «Защита от НСД. Часть 1. ПО средств защиты. Классификация по уровню контроля отсутствия НДВ».
34. Статический анализ исходных текстов программ.
35. Типовые дефекты программного обеспечения.
36. Классификация угроз безопасности ОС.
37. Защищённые операционные системы.
38. Аппаратное обеспечение средств защиты ОС.
39. Аудит безопасности в ОС.
40. Облачные технологии: достоинства и недостатки.
41. SaaS
42. IaaS.
42. PaaS.

5.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестации по учебной дисциплине проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по учебной дисциплине выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля)

5.1.1. Основная литература

1. *Нестеров, С. А.* Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/434171
2. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249

5.1.2. Дополнительная литература

1. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262

5.2. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) «**Программно-аппаратные средства защиты информации**» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины (модуля) . Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

5.4.Информационно-технологическое обеспечение образовательного процесса по учебной дисциплине

5.4.1. Информационные технологии

1. Персональные компьютеры;
2. Средства доступа к Интернет
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.4.3. Информационные справочные системы и профессиональные базы данных

Обучающиеся по программе **«Информационная безопасность»** в университете имеют доступ к следующим современным профессиональным базам данных, информационным справочникам:

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.5. Материально-техническое обеспечение образовательного процесса по дисциплине

Для изучения дисциплины (модуля) «**Программно-аппаратные средства защиты информации**» в рамках реализации основной профессиональной образовательной программы по направлению подготовки **«10.03.01 «Информационная безопасность»»** используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.6. Образовательные технологии

Освоение дисциплины (модуля) **«Программно-аппаратные средства защиты информации»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме (решение и разбор конкретных криптографических шифров) в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

Учебные часы дисциплины «**Программно-аппаратные средства защиты информации**» предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках дисциплины (модуля) **«Программно-аппаратные средства защиты информации»** предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/

«06» __июня__2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технология защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ – УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022 г.

Рабочая программа дисциплины (модуля) **«Методы и средства криптографической защиты информации»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" **(уровень бакалавриата)**, утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

- *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
- *06.032 Специалист по безопасности компьютерных систем и сетей*
- *06.033 Специалист по защите информации в автоматизированных системах*
- *06.034 Специалист по технической защите информации.*

Рабочая программа дисциплины (модуля) разработана рабочей группой в составе: д.т.н. проф. Семина В.Г., ст. пр. Елисеева Д.Ю.

Руководитель основной профессиональной образовательной программы
к.п.н., доцент _____ Н.Г. Витковская
(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года

Декан
К.п.н., доцент _____ С.В. Крапивка
(подпись)

Рабочая программа дисциплины (модуля) рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет»
зам. ген. директора по науке, к.т.н., доцент _____ А.С. Мосолов
(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

.д.т.н. , доцент, профессор кафедры информационных технологий , ГБОУВО Академия ГПС МЧС России) _____ С.Ю. Бутузов
(подпись)

к.ф.-м.н, доцент
кафедра прикладной математики и информатики РГСУ _____ Н.П. Третьяков
(подпись)

Согласовано
Научная библиотека, директор _____ И.Г. Маляр
(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) заключается в получении обучающимися теоретических знаний о математических и алгоритмических аспектах современной криптографии, а также практических навыков по применению криптографических методов защиты информации для решения широкого класса задач проблемы обеспечения информационной безопасности государства и общества**.**

Задачи дисциплины (модуля)

1. Получение обучающимися знаний об основных криптографических алгоритмах защиты информации в системах обеспечения информационной безопасности современных вычислительных архитектур.
2. Формирование навыков разработки программного обеспечение средств и систем криптографической защиты информации.
3. Формирование способностей к организации исследовательской и проектной деятельности на основе понимания математической и информационной сущности криптографических методов для решения задач построения систем обеспечения информационной безопасности сетевых информационных технологий.

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы

Учебная дисциплина «Методы и средства криптографической защиты информации» реализуется в базовой части основной профессиональной образовательной программы «Информационная безопасность» по направлению подготовки 10.03.01 «Информационная безопасность» очной формы обучения. Изучение дисциплины (модуля) «Методы и средства криптографической защиты информации» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Математика», «Программирование», «Основы информационной безопасности». Изучение дисциплины (модуля) «Методы и средства криптографической защиты информации» является одной из полезных составляющих для успешного выполнения выпускной квалификационной работы.

1.3. Планируемые результаты обучения по учебной дисциплине в рамках планируемых результатов освоения основной профессиональной образовательной программы

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих **профессиональных** компетенций: ОПК-9, ПК-1, ПК-2, ПК-5, ПК-9 в соответствии с основной профессиональной образовательной программой **«**Информационная безопасность**»** по направлению подготовки 10.03.01 "Информационная безопасность**».**

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	**Код компетенции**	**Формулировка компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения**

	ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-9.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-9.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Знать: методы установки, настройки и обслуживанию технических и криптографических средств защиты информации Уметь: выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации Владеть: способностью выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации
	ПК-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-1.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-1.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Знать: - эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности - основные направления политик защиты информации на предприятии (организации) Уметь: выполнять работы по установке, конфигурированию и эксплуатации технических и программных

				средств обеспечения информационной безопасности и защиты информации Владеть: Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
	ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-2.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Знать: - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ - основы администрирования вычислительных сетей - системы управления БД
				Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействия нарушениям

				сетевой безопасности с использованием различных программных и аппаратных средств защиты
				Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации
	ПК-5	Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-5.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-5.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** термины и понятия, применительно к процессам управления информационной безопасностью **Уметь:** Оценивать наличие и опасность технических каналов утечки информации **Владеть:** Методологией теоретического и инструментального анализа выявления и предотвращения образования технических каналов утечки информации

ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-9.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-9.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-9.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах. **Уметь:** проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации. **Владеть:** современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации.

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем дисциплины (модуля), включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 15 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		5	6	7		
Контактная работа обучающихся с педагогическими работниками	**270**	**90**	**72**	**108**		
Учебные занятия лекционного типа	58	18	16	24		
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	92	32	24	36		
из них: в форме практической подготовки						
Иная контактная работа	120	40	32	48		
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**216**	**81**	**63**	**72**		
из них: в форме практической подготовки	*44*	*16*	*14*	*14*		
Контроль промежуточной аттестации	**54**	**9**	**9**	**36**		
Форма промежуточной аттестации		зачет	диф. зач	экзам		
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**540**	**180**	**144**	**216**		

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	**Виды учебной работы, академических часов**											
	Всего	**Самостоятельная работа**	*из них: в форме практической подготовки*	**Контактная работа обучающихся с педагогическими работниками**								
				Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*

Модуль 1 (семестр 5)													
Раздел 1.1	34	16	*4*	18		4				6		8	
Раздел 1.2	34	16	*3*	18		4				6		8	
Раздел 1.3	34	16	*3*	18		4				6		8	
Раздел 1.4	34	16	*3*	18		4				6		8	
Раздел 1.5	35	17	*3*	18		2				8		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**180**	**81**	***16***	**90**		**18**				**32**		**40**	
Форма промежуточной аттестации	**зачет**												
Модуль 2 (семестр 6)													
Раздел 2.1	33	15	*4*	18		4				6		8	
Раздел 2.2	34	16	*4*	18		4				6		8	
Раздел 2.3	34	16	*3*	18		4				6		8	
Раздел 2.4	34	16	*3*	18		4				6		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**144**	**63**	***14***	**72**		**16**				**24**		**32**	
Форма промежуточной аттестации	**дифференцированный зачет**												
Модуль 3 (семестр 7)													
Раздел 3.1	30	12	*3*	18		4				6		8	
Раздел 3.2	30	12	*3*	18		4				6		8	
Раздел 3.3	30	12	*2*	18		4				6		8	
Раздел 3.4	30	12	*2*	18		4				6		8	
Раздел 3.5	30	12	*2*	18		4				6		8	
Раздел 3.6	30	12	*2*	18		4				6		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**216**	**72**	***14***	**108**		**24**				**36**		**48**	

Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**540**	**216**	***44***	**270**		**58**				**92**		**120**	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1. Виды самостоятельной работы обучающихся по дисциплине (модулю)

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**
Модуль 1 (семестр 5)							
Раздел 1.1	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.4	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 1.5	17	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**81**	**35**		**36**		**10**	
Модуль 2 (семестр 6)							
Раздел 2.1	15	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.3	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.4	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**63**	**27**		**28**		**8**	
Модуль 3 (семестр 7)							
Раздел 3.1	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.2	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 3.3	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.4	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.5	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.6	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**72**	**30**		**30**		**12**	
Общий объем по дисциплине (модулю), часов	**216**	**92**		**94**		**30**	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю)

МОДУЛЬ 1 ТЕОРИЯ ИНФОРМАЦИИ.

РАЗДЕЛ 1. Основы информационной безопасности и защита информации. История криптографии. Основные термины и определения.

Цель: заключается в получении обучающимися теоретических знаний об основных составляющих информационной безопасности, объектах защиты, категориях и носителях информации, средствах защиты информации, основных терминах и определениях, основных требованиях к криптосистемам, классификации криптографических систем.

Перечень изучаемых элементов содержания

Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации. Наивная криптография, формальная криптография, математическая криптография. Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем.

Вопросы для самоподготовки:

1. Понятия "информационная безопасность" и "защита информации". Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Средства защиты информации.
2. Криптография. Основные термины и определения.
3. Классификация криптографических систем.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – реферат.

РАЗДЕЛ 2. Классификация шифров. Шифры замены. Шифры перестановки.

Цель: заключается в получении обучающимися теоретических знаний об основах шифрования, шифрах.

Перечень изучаемых элементов содержания

Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Основы шифрования, шифры одинарной и множественной перестановки.

Вопросы для самоподготовки:

1. Понятия "информационная безопасность" и "защита информации". Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Шифры замены. Основные методы шифрования.
2. Шифры перестановки. Основные методы шифрования

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – реферат.

РАЗДЕЛ 3. Шифры гаммирования. Комбинированные шифры. Шифрование с открытым ключом. Хеш-функции. Криптографические протоколы. Протоколы обмена ключами.

Цель: заключается в получении обучающимися теоретических знаний о шифровании по модулю N и 2, генерация гаммы, генераторы гамм, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамаля, алгоритм на основе эллиптических кривых.

Перечень изучаемых элементов содержания

Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамаля, алгоритм на основе эллиптических кривых. Основные понятия, MD5, применение шифрования для получения хеш-образа. Основные сведения о криптографических протоколах, протоколы обмена ключами.

Вопросы для самоподготовки:

1. Шифры гаммирования. Основные методы шифрования.
2. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Схема режима шифрования DES-ECB.
2. Схема режима шифрования DES-CBC.
3. Схема режима шифрования DES-CPB и DES-OFB.
4. Тройной DES. Сферы применения различных режимов DES.
5. Схема режима шифрования простой замены ГОСТ 28147-89.
6. Шифрование с открытым ключом. Основные понятия.
7. Алгоритм шифрования RSA.
8. Алгоритм шифрования Эль-Гамаля.
9. Алгоритм шифрования на основе задачи об укладке ранца.
10. Эллиптические кривые. Основные понятия. Сложение и умножение точки.
11. Алгоритм шифрования на основе эллиптических кривых.
12. Хэш-функции. Основные понятия и разновидности.
13. Хэш-функция. MD5.
14. Криптографические протоколы. Основные понятия.
15. Протоколы обмена ключами.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – реферат.

РАЗДЕЛ 4. Протоколы аутентификации (идентификации). Протоколы электронной цифровой подписи. Протоколы контроля целостности. Протоколы электронных платежей. Протоколы голосования. Другие протоколы.

Цель: заключается в получении обучающимися теоретических знаний о парольной идентификации / аутентификации, протоколе на базе алгоритма RSA, алгоритме цифровой подписи ГОСТ 34.10-94, алгоритме цифровой подписи ГОСТ 34.10-2001, разновидностях ЭЦП.

Перечень изучаемых элементов содержания

Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи. Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП. Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми

карточками в Internet, электронные кошелки в Internet, цифровые деньги. Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления.

Вопросы для самоподготовки:

1. Протоколы аутентификации. Разновидности и краткая характеристика.
2. Парольная идентификация/аутентификация.
3. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Сервер аутентификации Kerberos.
2. Идентификация/аутентификация с помощью биометрических данных.
3. Идентификационные карты (ID-cards) и электронные ключи.
4. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
5. ЭЦП на базе алгоритма RSA.
6. Алгоритм цифровой подписи ГОСТ 34.10-94.
7. Алгоритм цифровой подписи ГОСТ 34.10-2001.
8. Протоколы контроля целостности.
9. Электронные платежи.
10. Классическое ("бумажное") голосования.
11. Российский опыт электронного голосования.
12. Протокол разделения секрета.
13. Протокол подбрасывания монеты по телефону.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – реферат.

РАЗДЕЛ 5. Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа. Стеганография. Кодирование информации.

Цель: заключается в получении обучающимися знаний о теории алгоритмов и чисел, основах криптоанализа, стеганографии, кодировании информации.

Перечень изучаемых элементов содержания

Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя. Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы. Общие сведения, классическая стеганография, компьютерная стеганография. Общие сведения, общедоступные и секретные кодовые системы, номенклаторы.

Вопросы для самоподготовки:

1. Тайные многосторонние вычисления.
2. Сложность алгоритмов.
3. Простые числа.
4. Разложение числа на простые сомножители.
5. Нахождение начального списка простых чисел.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Секретные кодовые системы.

2. Понятие наибольшего общего делителя.
3. Основные сведения о криптоанализе и атаки на криптосистемы.
4. Классическая стеганография.
5. Компьютерная стеганография.
6. Общие сведения о кодировании.
7. Общедоступные кодовые системы.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 5: форма рубежного контроля – реферат.

МОДУЛЬ 2 ЭЛЕМЕНТЫ ТЕОРИИ КОДИРОВАНИЯ.

РАЗДЕЛ 1. АЛФАВИТНОЕ КОДИРОВАНИЕ. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ. ПРОБЛЕМА РАСПОЗНАВАНИЯ ВЗАИМНОЙ ОДНОЗНАЧНОСТИ АЛФАВИТНОГО КОДИРОВАНИЯ

Цель: Изучение основных понятий теории кодирования
Перечень изучаемых элементов содержания
Шифры, алфавит, стандарты, основные алгоритмы

Вопросы для самоподготовки:

1. Буквы, префикс, алфавит.
2. М-ичное кодирование.
3. Таблица кодов.
4. Множество элементарных кодов.
5. Двоично-десятичное кодирование.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Основные понятия теории кодирования.
2. Задача теории кодирования. Объект теории кодирования
3. Кодирование и декодирование информации .
4. Алфавитное кодирование.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – реферат.

Раздел 2. АЛГОРИТМ ПОСТРОЕНИЯ ПРЕФИКСНОГО КОДА ПО НАБОРУ ДЛИН ЭЛЕМЕНТАРНЫХ КОДОВ.

Цель: Изучение алгоритмов построения префиксного кода

Перечень изучаемых элементов содержания
Символ, код, алгоритмы, Хаффман.

Вопросы для самоподготовки

1. Области применения асимметричные методов шифрования.
2. Схема шифрования Эль-Гамаля.
3. Криптосистема, основанная на проблеме Диффи -Хеллмана.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Алгоритм Хаффмана
2. Адаптивное сжатие
3. Описание множество префиксных кодов

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – реферат.

Раздел 3. АЛГОРИТМЫ ЭКОНОМНОГО АЛФАВИТНОГО КОДИРОВАНИЯ

Цель: Изучение различных алгоритмов алфавитного кодирования информации
Перечень изучаемых элементов содержания
Методы, алгоритмы, схемы экономного алфавитного кодирования

Вопросы для самоподготовки

1. Области применения асимметричные методов шифрования.
2. Схема шифрования Эль-Гамаля.
3. Криптосистема, основанная на проблеме Диффи -Хеллмана.
4. Схема шифрования Ривеста-Шамира-Адлемана.
5. Схема шифрования Меркля-Хеллмана и Хора-Ривеста.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Алгоритм Хаффмана
2. Алгоритм Фано
3. Алгоритм Шеннона
4. Энтропия и ее связь со стоимостью оптимального алфавитного кодирования

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – реферат.

РАЗДЕЛ 4. СЖАТИЯ ПРИ АЛФАВИТНОМ КОДИРОВАНИИ

Цель: Изучение необходимости сжатия информации
Перечень изучаемых элементов содержания
Алфавит, кодирование, сжатие информации

Вопросы для самоподготовки:

1. Пересылка электронных документов.

2. Сжатие электронных документов.
3. Дисковое пространство.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Универсальные методы сжатия с потерями.
2. Универсальные методы сжатия без потерь.
3. Общие принципы, на которых построено сжатие.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – реферат.

РАЗДЕЛ 5. КОДИРОВАНИЕ ВЕРОЯТНОСТНЫХ ИСТОЧНИКОВ С КОНЕЧНЫМ ЧИСЛОМ СОСТОЯНИЙ

Цель: Изучение кодирования вероятностных источников информации.
Перечень изучаемых элементов содержания
Кодирование, теорема, алгоритм, граф, дискретный источник.

Вопросы для самоподготовки:

1. Экономное кодирование.
2. Теорема Шеннона.
3. Марковский процесс.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Вероятностные свойства сообщений.
2. Алгоритмы блочного кодирования.
3. Кодирование для эргодических источников с двумя состояниями.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 5: форма рубежного контроля – реферат.

РАЗДЕЛ 6. ВОПРОСЫ КОДИРОВАНИЯ СТОХАСТИЧЕСКИХ ЯЗЫКОВ. СООТНОШЕНИЕ МЕЖДУ СТОИМОСТЬЮ ОПТИМАЛЬНОГО КОДИРОВАНИЯ И ЭНТРОПИЕЙ СТОХАСТИЧЕСКОГО ЯЗЫКА

Цель: Изучение возможностей кодирования стохастических языков.
Перечень изучаемых элементов содержания
Двоичное кодирование, стохастические языки, энтропия.

Вопросы для самоподготовки:

1. Теорема Шеннона.
2. Оптимальное кодирование.
3. Длинные и короткие сообщения.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 6

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Основные определения, относящиеся к кодированию стохастических языков
2. Соотношение между стоимостью оптимального кодирования и энтропией для произвольного стохастического языка
3. Понятие нижней оценкой стоимости кодирования
4. Понятие верхней оценкой стоимости кодирования

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 6: форма рубежного контроля – реферат.

РАЗДЕЛ 7. ВОПРОСЫ КОДИРОВАНИЯ КОНТЕКСТНО-СВОБОДНЫХ ЯЗЫКОВ

Цель: Изучение вопросов кодирования КС-языков.

Перечень изучаемых элементов содержания

Кодирование, декодирование, Шеннон, теорема.

Вопросы для самоподготовки:

1. Вероятностные свойства сообщений.
2. Эргодические источники.
3. Теория кодирования.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 7

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Развитие методов теории кодирования, относящихся к алгоритмам построения экономных кодов.
2. Исследование зависимости эффективности кодирования от структурных и вероятностных свойств стохастического КС-языка.
3. Стоимость оптимального кодирования и энтропия стохастического КС-языка.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 7: форма рубежного контроля – реферат.

МОДУЛЬ 3
МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.

РАЗДЕЛ 1. СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Цель: Изучение структур поточных и блочных алгоритмов и режимов использования поточных и блочных шифров

Перечень изучаемых элементов содержания

Блочные шифры, поточные шифры, стандарты, основные алгоритмы

Вопросы для самоподготовки:

6. 1. Общие сведения о блочных шифрах.
7. 5. Генерирование блочных шифров.
8. 6. Алгоритмы блочного шифрования.
9. 7 Алгоритм DES и его модификации.
10. 8. Стандарт AES. Алгоритм Rijndael.
11. 9. Алгоритм RC6.
12. 10 Российский стандарт шифрования ГОСТ 28147-89.
13. 11 Алгоритмы SAFER+, SAFER++.
14. Общие сведения о потоковых шифрах.
15. 12. Режимы применения блочных шифров.
16. 13.Примеры потоковых шифров
17. 14. Потоковые шифры.
18. 15. Общие сведения о потоковых шифр.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: реферат.

Примерный перечень тем рефератов:

19. Самосинхронизирующиеся шифры.
20. Синхронные шифры.
21. Примеры потоковых шифров.
22. Алгоритм RC4.
23. Алгоритм SEAL.
24. Алгоритм WAKE.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – реферат.

Раздел 2. АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Цель: Изучение криптографических методов шифрования сообщений в открытых каналах связи

Перечень изучаемых элементов содержания

Методы, алгоритмы, схемы ассиметричного шифрования

Вопросы для самоподготовки

6. Области применения асимметричные методов шифрования.
7. Схема шифрования Эль-Гамаля.
8. Криптосистема, основанная на проблеме Диффи -Хеллмана.
9. Схема шифрования Ривеста-Шамира-Адлемана.
10. Схема шифрования Меркля-Хеллмана и Хора-Ривеста.

11. Криптосистемы, основанные на эллиптических кривых.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Роль методов ассиметричного шифрования в развитии прикладных открытых информационных система
2. Области применения асимметричные методов шифрования.
3. Односторонние функции и функции-ловушки.
4. Модель схемы ассиметричного шифрования.
5. Понятие открытого ключа.
6. Криптосистемы Эль-Гамаля.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – реферат.

Раздел 3. ЭЛЕКТРОННЫЕ ЦИФРОВЫЕ ПОДПИСИ

Цель: Изучение схем ЭЦП, основанных на ассиметричных и симметричных криптосистемах

Перечень изучаемых элементов содержания

Схема, процедуры выработки и верификации, национальный стандарт ЭЦП

Вопросы для самоподготовки:

1. Постановка задачи ЭЦП.
2. Криптосистемы, основанные на эллиптических кривых.
3. Алгоритмы электронной цифровой подписи .
4. Цифровые подписи, основанные на асимметричных криптосистемах
5. Стандарт цифровой подписи DSS.
6. Стандарт цифровой подписи ГОСТ Р 34.10-94 96
7. Стандарт цифровой подписи ГОСТ Р 34.10-2001 99.
8. Цифровые подписи, основанные на симметричных криптосистемах

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Функции хэширования
2. Функция хэширования SHA
3. Функции хэширования SHA-256, SHA-512 и SHA-384
4. Функция хэширования ГОСТ Р 34.11-94
5. Функция хэширования MD5

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – реферат.

РАЗДЕЛ 4. УПРАВЛЕНИЕ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ

Цель: Изучение систем управления и механизмов обмена ключами
Перечень изучаемых элементов содержания
Генерация ключей, накопление ключей, распределение ключей, смена и уничтожение

Вопросы для самоподготовки:

1. Обычная система управления ключами.
2. Управление ключами, основанное на системах с открытым
Ключом.
3. Протокол обмена секретным ключом.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: реферат.

Примерный перечень тем рефератов:

4. Использование сертификатов.
5. Протоколы аутентификации.
6. Анонимное распределение ключей.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – реферат.

РАЗДЕЛ 5. МОДУЛЯРНАЯ АРИФМЕТИКА

Цель: Изучение модулярной арифметики, базирующейся на «Китайской теореме об остатках».
Перечень изучаемых элементов содержания
Непозиционные системы счисления, разряды, числа.

Вопросы для самоподготовки:

4. Прямое преобразование.
5. Арифметические операции.
6. Обратное преобразование.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5

Форма практического задания: реферат.

Примерный перечень тем рефератов:

4. Круговая система обозначений.
5. Протоколы аутентификации.
6. Анонимное распределение ключей.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 5: форма рубежного контроля – реферат.

РАЗДЕЛ 6. ГЕНЕРАЦИЯ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Цель: Изучение возможностей генерации псевдослучайных последовательностей.
Перечень изучаемых элементов содержания

Шифрование, генераторы случайных чисел, случайные последовательности, неслучайные последовательности.

Вопросы для самоподготовки:

4. Генераторы случайных чисел.
5. Шифрование.
6. Генератор паролей.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 6

Форма практического задания: реферат.

Примерный перечень тем рефератов:

5. Отличие генератора псевдослучайных чисел (ГПСЧ) от генератора случайных чисел (ГСЧ).
6. Уязвимости ГПСЧ.
7. Области для взлома.
8. Шумоподобные сложные сигналы.
9. Отличие случайной последовательности чисел от неслучайной.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 6: форма рубежного контроля – реферат.

Оформление работ, выполняемых в рамках самостоятельной работы осуществляется в соответствии с Методическими указаниями по оформлению письменных работ обучающихся в рамках самостоятельной работы, утвержденными Учебно-методическим советом РГСУ, Протокол № 2 от 25 июня 2015 года.

Конкретные практические задания и задания для рубежного контроля определяются в учебно-методических материалах по работе обучающихся в электронной информационно-образовательной среде РГСУ с применением технологий электронного обучения по данной дисциплине, утверждаемых ежегодно кафедрой.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по учебной дисциплине являются: **зачет, диф.зачет, экзамен.**

.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-9	Способен применять средства криптографической и технической	**Знать:** методы установки, настройки и обслуживанию технических и криптографических средств защиты информации	Этап формирования знаний

	защиты информации для решения задач профессиональной деятельности		
		Уметь: выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации	Этап формирования умений
		Владеть: способностью выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации	Этап формирования навыков и опыта
ПК-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать:** методы установки, настройки и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Этап формирования знаний
		Уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	Этап формирования умений
		Владеть: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	Этап формирования навыков и получения опыта
ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения	Знать: основные программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап формирования знаний

	профессиональных задач		
		Уметь: применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап формирования умений
		Владеть: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап формирования навыков и получения опыта
ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	**Знать:** нормативные документы для обоснования безопасности информационных систем, отечественные и зарубежные стандарты оценки защищенности информационных систем, источники информации по проблематике информационной безопасности	Этап формирования знаний
		Уметь: собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и	Этап формирования умений

		прочих отечественных и зарубежных источниках	
		Владеть: - навыками работы с нормативными правовыми актами; навыками сбора и обработки необходимых данных - навыками анализа и интерпретации информации, содержащейся в различных отечественных и зарубежных источниках, в том числе с использованием электронных журналов и библиотек	Этап формирования навыков и получения опыта

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	**Этапы формирования компетенций**	**Показатель оценивания компетенции**	**Критерии и шкалы оценивания**
ОПК-9, ПК-1, ПК-2, ПК-5, ПК-9	Этап формирования знаний	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных

			неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.
ОПК-9, ПК-1, ПК-2, ПК-5, ПК-9	Этап формирования умений	Аналитическое задание *(задачи,)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией - 9-10 баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании -7-8 баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению5-6 баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет
ОПК-9, ПК-1, ПК-2, ПК-5, ПК-9	Этап формирования навыков и получения опыта	Аналитическое задание *(задачи,)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

			четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания - 0-4 баллов.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Теоретический блок вопросов:

1.Определение алгебраической операции подстановки.
2.Определение операции гаммирования. Понятие гаммы шифра и датчика псевдослучайной последовательности.
3 Основные классы симметричных криптосистем.
4. Общие сведения о блочных шифрах.
5. Генерирование блочных шифров.
6. Алгоритмы блочного шифрования.
7 Алгоритм DES и его модификации.
8. Стандарт AES. Алгоритм Rijndael .
9. Алгоритм RC6.
10 Российский стандарт шифрования ГОСТ 28147-89.
11 Алгоритмы SAFER+, SAFER++.
12. Режимы применения блочных шифров.
13. Потоковые шифры.
14. Общие сведения о потоковых шифрах.
15. Самосинхронизирующиеся шифры.
16. Синхронные шифры.
17. Примеры потоковых шифров.
18.Алгоритм RC4.
19.Алгоритм SEAL.
20.Алгоритм WAKE.
21. Общие положения.
22. Односторонние функции и функции-ловушки.
23. Асимметричные системы шифрования.
24. Криптосистема Эль-Гамаля.
25. Криптосистема, основанная на проблеме Диффи-Хеллмана.
26. Криптосистема Ривеста-Шамира-Адлемана.
27. Криптосистемы Меркля-Хеллмана и Хора-Ривеста.
28. Криптосистемы, основанные на эллиптических кривых.
29. Постановка задачи ЭЦП.
30. Алгоритмы электронной цифровой подписи.
31. Цифровые подписи, основанные на асимметричных криптосистемах .
32. Стандарт цифровой подписи DSS.

33. Стандарт цифровой подписи ГОСТ Р 34.10-94.
34. Стандарт цифровой подписи ГОСТ Р 34.10-2001.
35. Цифровые подписи, основанные на симметричных криптосистемах.
36. Функции хэширования.
37. Функция хэширования SHA.
38. Функции хэширования SHA-256, SHA-512 и SHA-381.
39. Функция хэширования ГОСТ Р 34.11-94.
40. Функция хэширования MD5.
41. УПРАВЛЕНИЕ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ.
42. Обычная система управления ключами.
43. Управление ключами, основанное на системах с открытым ключом.
44. Протокол обмена секретным ключом.
45. Использование сертификатов.
46. Протоколы аутентификации.
47. Анонимное распределение ключей

Аналитическое задание ***(задачи)***

1. Моноалфавитная подстановка. Пример простейшей подстановки.
2.Общая формула моноалфавитной подстановки.
4.Моноалфавитная подстановка Вижинера.
5. Моноалфавитная подстановка для шифра Бофора.
6.Гомофоническая замена. Пример.
7. Полиалфавитная подстановка, Пример.
8.Полиграммная замена. Пример (Шифр Плейфера).
9.Шифрование с автоключом. Пример схемы.
10.Схема шифрования с автоключом при использовании криптограммы.
11.Метод перестановки с ключом (правило перестановки. Пример
12 Метод перестановки с ключом записи по строкам и ключом чтения по столбцам матрицы. Пример.
13.Метод перестановки с использованием гамильтонова пути на графе.
14.Процедура шифрования методом гаммирования.
15.Метод гаммирования. Пример реализации для русского алфавита по mod 33

5.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестации по учебной дисциплине проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по учебной дисциплине выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам

бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля)

5.1.1. Основная литература

1. *Лось, А. Б.* Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242
2. *Запечников, С. В.* Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487

5.1.2. Дополнительная литература

1. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489745
2. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490421
3. *Васильева, И. Н.* Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489919

5.2. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная	Крупнейший российский информационно-аналитический портал в области науки,	http://elibrary.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	библиотека eLIBRARY.ru	технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) «**Методы и средства криптографической защиты информации**» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины (модуля). Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

5.4. Информационно-технологическое обеспечение образовательного процесса по учебной дисциплине

5.4.1. Информационные технологии

1. Персональные компьютеры;
2. Доступ к Интернет
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.5. Информационные справочные системы и профессиональные базы данных

Обучающиеся по программе **«Информационная безопасность»** в университете имеют доступ к следующим современным профессиональным базам данных, информационным справочникам:

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.6. Материально-техническое обеспечение образовательного процесса по учебной дисциплине

Для изучения дисциплины (модуля) **«Методы и средства криптографической защиты информации»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки 10.03.01 "Информационная безопасность» используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими

средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет.

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.7. Образовательные технологии

Освоение дисциплины (модуля) **«Методы и средства криптографической защиты информации»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме (решение и разбор конкретных криптографических шифров) в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

Учебные часы дисциплины «**Методы и средства криптографической защиты информации**» предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках дисциплины (модуля) **«Методы и средства криптографической защиты информации»** предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/

«06» __июня___2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технология защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022 г.

Рабочая программа дисциплины (модуля) **«Защита информации от утечки по техническим каналам»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки **10.03.01 Информационная безопасность (уровень бакалавриата)**, утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
– *06.032 Специалист по безопасности компьютерных систем и сетей*
– *06.033 Специалист по защите информации в автоматизированных системах*
- 06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля) разработана рабочей группой в составе:
к.т.н, доцент Сиротский А.А. , старший преподаватель Мальцев Н.В.

Руководитель основной профессиональной образовательной программы
к.п.н., доцент _____ Н.Г. Витковская
(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года

Декан факультета
К.п.н., доцент _____ С.В. Крапивка
(подпись)

Рабочая программа дисциплины (модуля) рекомендована к утверждению представителями организаций-работодателей:
АО ПВП «Амулет»
зам. ген. директора по науке, _____ А.С. Мосолов
к.т.н., доцент
(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

.д.т.н. , доцент, профессор кафедры информационных технологий , _____ С.Ю. Бутузов
ГБОУВО Академия ГПС МЧС России)
(подпись)

к.ф.-м.н, доцент
кафедра прикладной математики и информатики РГСУ _____ Н.П. Третьяков
(подпись)

Согласовано
Научная библиотека, директор _____ И.Г. Маляр
(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля)

Целями изучения дисциплины «Защита информации от утечки по техническим каналам» являются:

1. *Формирование* профессиональных навыков, связанных с инженерно- техническими принципами обеспечения информационной безопасности, основаны на знании потенциальных возможностей нарушителя по добыванию информации по техническим каналам утечки и несанкционированному проникновению к объекту защиты, с методами и средствами инженерно-технической защиты и охраны информации, с принципом действия, характеристиками и функциональными возможностями технических средств защиты и охраны информации, с подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты и охраны информации; базовых теоретических понятий, лежащих в основе инженерно-технической защиты и охраны информации;
2. *Формирование* представления о факторах, влияющих на возможность образования технических каналов утечки информации и последствий преднамеренных деструктивных воздействий на объекты информатизации.
3. *Формирование* представления о методах и средствах объективного контроля за эффективностью реализации комплексного подхода к обеспечению информационной безопасности объекта информатизации.
4. *Развитие* способностей к логическому и алгоритмическому мышлению, навыков использования методов и средств обеспечения информационной безопасности; использования современных технических средств для защиты объектов информатизации от утечки по техническим каналам и преднамеренному воздействию.

Задачи дисциплины (модуля) :

1. Усвоение основных понятий об условиях и физических принципах возникновения технических каналов утечки информации, а также преднамеренных воздействий на объекты информатизации;
2. Формирование знаний о принципах, методах и средствах организационной и инженерно-технической защиты объектов информатизации от преднамеренных воздействий и утечки информации по техническим каналам.
3. Изучение основных принципов построения и функциональных особенностей, современных инженерно- технических средств защиты информации и охраны объектов информатизации;
4. Формирование теоретических знаний и практических навыков по анализу и инструментальной оценки реальной защищенности объекта информатизации;

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы.

Учебная дисциплина «Защита информации от утечки по техническим каналам» реализуется в базовой части основной профессиональной образовательной программы «Информационная безопасность» по направлению подготовки «10.03.01 Информационная безопасность», направленность программы "Организация и технологии защиты информации", очной формы обучения.

Изучение дисциплины (модуля) **«Защита информации от утечки по техническим каналам»** базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Математика», «Физика», «Информатика и информационные технологии».

Изучение дисциплины (модуля) **«Защита информации от утечки по техническим каналам»** является базовым для последующего освоения программного материала учебных дисциплин: «Основы управления информационной безопасностью», «Контроль безопасности в компьютерных сетях», « Методы противодействия социальной инженерии».

1.3. Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основной профессиональной образовательной программы .

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих профессиональных компетенций: ОПК-7, ОПК-9, ПК-6, ПК-7, ПК-8, ПК-9, ПК-11, ПК-12, ПК-15 в соответствии с основной профессиональной программой по направлению подготовки бакалавров **10.03.01 Информационная безопасность .**

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	**Код компетенции**	**Формулировка компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения**
	ОПК-7	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-7.ИД-2. Планирует и выполняет практические действия в рамках компетенции	*Знать:* основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий.
			ОПК-7.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	*Уметь:* применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для

				автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ.
				Владеть: навыками программирования, отладки и тестирования прототипов программно-технических комплексов задач.
	ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-9.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-9.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** методы установки, настройки и обслуживанию технических и криптографических средств защиты информации
				Уметь: выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации
				Владеть: способностью выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации
	ПК-6	Способен принимать участие в организации и проведении	ПК-6.ИД-1. Сформирован понятийный аппарат и теоретическая	**Знать:** - основные принципы оценки работоспособности и тестирования

		контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	основа для выполнения практических действий в рамках компетенции ПК-6.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-6.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	оборудования обработки и передачи данных - критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
				Уметь: - использовать возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации - составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности
				Владеть: - навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий - навыками использования методов тестирования коммуникационног

				о оборудования и аппаратуры обработки данных, криптографических систем
	ПК-7	Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-7.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-7.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода; - номенклатуру и основные параметры сертифицированных средств обеспечения информационной безопасности.
				Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно-следственных связей.
				Владеть : - основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту

				информатизации; - методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования. - основными технологиями селективного информационного поиска и анализа результатов работы с информационными ресурсами по номенклатуре сертифицированных средств защиты объектов информатизации.
	ПК-8	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-8.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-8.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** критерии защищенности объекта информатизации, состав оборудования и методологию контроля, изложенных в нормативно-методических документах, федерального, ведомственного и производственного уровней. **Уметь:** при оформлении отчетных материалов четко формулировать цель проведенных работ, объект и предмет работ,

				результаты инструментальных исследований, выводы и рекомендации по результатам проведенных работ, в понятной, как техническому специалисту, так и специалисту в сфере управления форме.
				Владеть: навыками написания отчетных материалов, в том числе технически и экономически обоснованных выводов и рекомендаций, в понятной как техническому специалисту, так и специалисту в сфере управления форме.
	ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-9.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-9.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-9.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах.

			компетенции	
				Уметь: проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации.
				Владеть: современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации.
	ПК-11	Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных

			ПК-11.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-11.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	сферах. **Уметь:** проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации. **Владеть:** теоретическими знаниями и практическими навыками по проведению инструментальных исследований объектов информатизации, на их соответствие их защищенности требуемым критериям.
	ПК-12	Способен принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-12.ИД-2. Планирует и выполняет	**Знать:** функциональное назначение, технические и конструктивные особенности применения, общие принципы построения и работы исследуемой системы защиты информации. **Уметь:** применять сведения,

			практические действия в рамках компетенции ПК-12.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	изложенные в соответствующих нормативно-методических, технических и эксплуатационных документах, а так же соответствующее специализированное оборудование и измерительные приборы для проведении экспериментальных исследований системы защиты информации. **Владеть:** теоретическими знаниями и навыками по практическому применению соответствующего специализированного оборудования и измерительных приборов для проведении экспериментальных исследований системы защиты информации мероприятий
	ПК-15	Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности	ПК-15.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-15.ИД-2. Планирует и	**Знать:** основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области **Уметь:**

		Российской Федерации, Федеральной службы по техническому и экспортному контролю	выполняет практические действия в рамках компетенции ПК-15.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	- организовывать технологические процессы организации в том числе на основе локальной и комплексной автоматизации процессов обработки документов в документационной службе в соответствии с нормативными актами и нормативными методическими документами
				Владеть: - навыками работы с нормативными правовыми актами в области защиты информации - методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2. Объем дисциплины (модуля) , включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 12 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		3	4	5		
Контактная работа обучающихся с педагогическими работниками	**216**	**72**	**36**	**108**		
Учебные занятия лекционного типа	48	16	8	24		
из них: в форме практической подготовки						

Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	72	24	12	36		
из них: в форме практической подготовки						
Иная контактная работа	96	32	16	48		
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**162**	**63**	**27**	**72**		
из них: в форме практической подготовки	*33*	*12*	*7*	*14*		
Контроль промежуточной аттестации	**54**	**9**	**9**	**36**		
Форма промежуточной аттестации		зачет	диф. зач	экзам		
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**432**	**144**	**72**	**216**		

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	**Виды учебной работы, академических часов**												
	Всего	**Самостоятельная работа**	*из них: в форме практической подготовки*	**Контактная работа обучающихся с педагогическими работниками**									
				Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*
Модуль 1 (семестр 3)													
Раздел 1.1	33	15	*3*	18		4				6		8	
Раздел 1.2	34	16	*3*	18		4				6		8	
Раздел 1.3	34	16	*3*	18		4				6		8	
Раздел 1.4	34	16	*3*	18		4				6		8	
Контроль промежуточной аттестации (час)	**9**												

Общий объем, часов	**144**	**63**	***12***	**72**		**16**				**24**		**32**	
Форма промежуточной аттестации	**зачет**												
Модуль 2 (семестр 4)													
Раздел 2.1	31	13	*4*	18		4				6		8	
Раздел 2.2	32	14	*3*	18		4				6		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**72**	**27**	***7***	**36**		**8**				**12**		**16**	
Форма промежуточной аттестации	**дифференцированный зачет**												
Модуль 3 (семестр 5)													
Раздел 3.1	30	12	*3*	18		4				6		8	
Раздел 3.2	30	12	*3*	18		4				6		8	
Раздел 3.3	30	12	*2*	18		4				6		8	
Раздел 3.4	30	12	*2*	18		4				6		8	
Раздел 3.5	30	12	*2*	18		4				6		8	
Раздел 3.6	30	12	*2*	18		4				6		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**216**	**72**	***14***	**108**		**24**				**36**		**48**	
Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**432**	**162**	***33***	**216**		**48**				**72**		**96**	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1. Виды самостоятельной работы обучающихся по дисциплине

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**

		Академическая активность, час	Форма академической активности	Выполнение практ. заданий, час	Форма практического задания	Рубежный текущий контроль, час	Форма рубежного текущего контроля
Модуль 1 (семестр 3)							
Раздел 1.1	15	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.4	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**63**	**27**		**28**		**8**	
Модуль 2 (семестр 4)							
Раздел 2.1	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	14	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Модуль 3 (семестр 5)							
Раздел 3.1	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.2	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.3	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.4	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.5	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.6	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**72**	**30**		**30**		**12**	
Общий объем по дисциплине (модулю), часов	**162**	**68**		**70**		**24**	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю»)

МОДУЛЬ 1 «Концепция технической защиты информации

Раздел 1. Демаскирующие признаки, электро и радио технических процессов, возникающих в радиоэлектронной аппаратуре и характеризующих технические каналы утечки информации, а так же критерии защищенности объектов информатизации.

Цель: Изучение характеристик информации, видов, источников и носителей защищаемой информации, классификации демаскирующих признаков, особенности их свойств и анализ их значения для технических разведок и специалистов по защите информации.

Перечень изучаемых элементов содержания

Свойства информации, как объекта защиты. Классификация, видов, источников и носителей защищаемой информации, Классификация демаскирующих признаков. Свойства видовых, сигнальных и вещественных признаков. Классификация основных видов технических разведок, с точки зрения среды распространения информации и совокупности свойств демаскирующих признаков. Устранение до заданного уровня (минимизация) демаскирующих признаков, как одна из основных задача технической защиты информации.

Вопросы для самоподготовки:

1. Составляющие информации, как объекта защиты.
2. Основные свойства и формы существования информации, определяющие методы и критерии её защиты.
3. Носители защищаемой информации.
4. Классификация и основные свойства демаскирующих признаков объекта.
5. Специфические свойства видовых признаков, которые реализуются в процессе защиты от несанкционированного наблюдения**.**
6. Сигнальные демаскирующие признаки, влияющие на защищенность объектов информатизации.
7. Виды технической разведки и их связь с формами существования информации и демаскирующими признаками.
8. Демаскирующие признаки естественных и искусственно создаваемых каналов утечки информации.

Практическое задание к разделу 1.

Формы контроля самостоятельной работы обучающихся:

Лабораторная работа 1.

«Исследование физических параметров видовых и сигнальных демаскирующих признаков, влияющих на защищенность объектов информатизации».

Контрольные вопросы:

1. Причины необходимости выявления демаскирующих признаков присущих конкретному объекту информатизации нарушителем и специалистом по защите информации.
2. Какие ограничения на объективное обнаружение видовых демаскирующих признаков накладывают условия реализации визуально- оптического канала и как этот процесс используется для защиты видовой информации. Привести примеры.
3. Какие параметры электрического и электромагнитного сигнала могут источниками образования сигнальных демаскирующих признаков.
4. Связь между видами демаскирующих признаков и направлениями образования каналов утечки информации, характеризующих виды технической разведки.

Модуль 2. Основы электро и радио технических процессов в защищаемой радиоэлектронной аппаратуре

Раздел 1. Основы электротехники и построения электрических цепей.

Цель: Изучение физических процессов в электрических цепях, основных законов построения и функционирования электрических цепей постоянного и переменного тока.

Перечень изучаемых элементов содержания.

1. Основные законы электротехники.
2. Классификация элементной базы электротехники.
3. Пассивные элементы электрических цепей.
4. Электрические машины.
5. Цепи постоянного и переменного тока.
6. Расчёт цепей постоянного и переменного тока.

Вопросы для самоподготовки:

1. Основные виды и характеристики элементов электрических цепей.
2. Построение векторных диаграмм электрических цепей переменного тока.
3. Вольт-амперные характеристики.
4. Нагрузочные характеристики.
5. Режимы работы источников электроэнергии.
6. Сопротивление в электрических цепях.
7. Устройство и принцип работы электрических машин.
8. Мощность в электрических цепях.
9. Линейные, нелинейные, активные и реактивные элементы электрических цепей.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Форма практического задания лабораторные работы. (14 час.)

Лабораторная работа 1.
«Изучение соединений в электрических цепях». (4 часа)

Вопросы для самоподготовки:

1. **Последовательное соединение элементов.**
2. **Параллельное соединение элементов.**
3. **Смешанное соединение элементов.**

Контрольные вопросы:

1. **Рассчитать схему из смешанного соединения резисторов.**
2. **Рассчитать схему из смешанного соединения конденсаторов.**
3. **Рассчитать схему из смешанного соединения источников ЭДС.**
4. **Основные параметры элементов электрических цепей.**

Лабораторная работа 2.
***«Изучение электрической цепи постоянного тока»*. (4 часа)**

Вопросы для самоподготовки.

1. Физические процессы в замкнутых многоконтурных цепях постоянного тока.
2. Понятие ветвей, контуров и узлов в электрических цепях.
3. Генераторные (активные) и параметрические (пассивные) элементы электрических цепей.
4. Применение законов Ома и Кирхгофа для расчёта электрических цепей.

Контрольные вопросы:

1. Параметры и характеристики источников напряжения и источников ЭДС.
2. Нагрузочные характеристики источников электроэнергии.
3. Баланс в электрических цепях.
4. Мощность в электрических цепях постоянного тока.
5. Токи и напряжения в электрических цепях постоянного тока.
6. Измерение токов и напряжений в электрических цепях постоянного тока.

Лабораторная работа 3.
***«Изучение электрической цепи переменного тока»*. (6 часов)**

Вопросы для самоподготовки.

1. Физические процессы в замкнутых многоконтурных цепях переменного тока.
2. Понятие ветвей, контуров и узлов в электрических цепях переменного тока.
3. Понятие фаз токов и напряжений в электрических цепях переменного тока.
4. Применение законов Ома и Кирхгофа для расчёта электрических цепей переменного тока.

Контрольные вопросы:

1. Параметры и характеристики реактивных элементов.
2. Характеристики источников электроэнергии переменного тока.
3. Мощность в электрических цепях переменного тока.
4. Токи и напряжения в электрических цепях переменного тока.
5. Измерение токов и напряжений в электрических цепях переменного тока.
6. Построение векторных диаграмм токов и напряжений.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – отчеты по лабораторным работам.

Раздел 2. Основы полупроводниковых технологий и элементной базы электронной техники, применяемой на объектах информатизации.

Цель: Изучение элементной базы современной полупроводниковой техники, устройства и работы полупроводниковых приборов.

Перечень изучаемых элементов содержания.

1. **Полупроводниковые материалы.**
2. **Собственные и примесные полупроводники.**
3. **Зонная теория.**
4. **Полупроводниковый переход.**
5. **Вольт-амперные характеристики идеального и реального полупроводникового перехода.**
6. **Полупроводниковые диоды, Вольт-амперные характеристики диодов.**
7. **Стабилитроны, Вольт-амперные характеристики стабилитронов.**
8. **Варикапы, вольт-фарадные характеристики варикапов.**

9. **Туннельные диоды, Вольт-амперные характеристики туннельных диодов.**
10. **Транзисторы и их разновидности.**
11. **Режимы работы транзисторов.**
12. **Классы усиления.**
13. **Биполярные транзисторы, вольт-амперные характеристики биполярных транзисторов.**
14. **Схемы включения биполярных транзисторов.**
15. **Свойства и характеристики биполярных транзисторов.**
16. **Полевые транзисторы, вольт-амперные характеристики полевых транзисторов.**
17. **Схемы включения полевых транзисторов.**
18. **Свойства и характеристики полевых транзисторов.**
19. **Тринисторы.**
20. **Вольт-амперные характеристики тринисторов.**
21. **Виды тринисторов.**
22. **Применение диодов, транзисторов, и тринисторов.**
23. **Операционный усилитель.**
24. **Базовые логические элементы.**
25. **Расчёт усилительного каскада на одном биполярном транзисторе по схеме с общим эмиттером.**

Вопросы для самоподготовки:

1. ***Основные виды и характеристики элементов электронной техники.***
2. ***Использование вольт-амперных характеристик для расчета и анализа электронных схем.***
3. ***Свойства и характеристики диодов.***
4. ***Свойства и характеристики транзисторов.***
5. ***Свойства и характеристики усилителей.***

Лабораторная работа 1.
«Изучение полупроводниковых диодов». (4 часа)

Вопросы для самоподготовки:

1. **Виды и классификация диодов.**
2. **Условные графические обозначения диодов.**
3. **Выпрямительные схемы.**

Контрольные вопросы:

1. **Как работает однополупериодный выпрямитель?**
2. **Как работает двухполупериодный выпрямитель?**
3. **Применение и схема включения стабилитронов.**
4. **Коэффициент стабилизации.**
5. **Фильтрация и сглаживание пульсаций в выпрямительных схемах.**
6. **Разновидности вторичных источников питания.**

Лабораторная работа 2.
***«Изучение полупроводниковых транзисторов».* (4 часа)**

Вопросы для самоподготовки.

1. Виды и классификация транзисторов.
2. Условные графические обозначения транзисторов.

3. Схемы включения транзисторов.
4. Питание транзисторных схем.
5. Режимы работы транзисторов.

Контрольные вопросы:

1. Как устроен и работает транзистор?
2. Структуры транзисторов.
3. Вольт-амперные характеристики транзисторов.
4. Справочные параметры и характеристики транзисторов.

Лабораторная работа 3.
«Расчет схемы усилителя на полупроводниковом транзисторе». **(6 часов)**

Вопросы для самоподготовки.

1. Свойства схемы с общим эмиттером.
2. Принцип работы транзисторного каскада.
3. Н-параметры транзистора.
4. Структуры транзисторов.
5. Вольт-амперные характеристики транзисторов.
6. Справочные параметры и характеристики транзисторов.

Контрольные вопросы:

1. Порядок расчета транзисторной схемы.
2. Неопределенности при расчётах электронных схем.
3. Построение линий нагрузки.
4. Построение кривых допустимой мощности.
5. Режимы работы транзистора на вольт-амперных характеристиках.
6. Рабочая точка схемы.
7. Классы усиления.

Раздел 3. Основы схемотехнического построения электронной аппаратуры.

Цель: Изучение схемотехнического построения современной электронной аппаратуры.

Перечень изучаемых элементов содержания.

1. **Интегральные схемы.**
2. **Операционные усилители.**
3. **Логические элементы.**
4. **Схемы на логических элементах.**
5. **Схемы на операционных усилителях.**
6. **Пассивные фильтры.**
7. **Амплитудно-частотные характеристики усилительных схем.**

Вопросы для самоподготовки:

1. ***Смысловое значение амплитудных характеристик.***
2. ***Смысловое значение амплитудно-частотных характеристик.***
3. ***Использование амплитудно-частотных характеристик для расчета и анализа свойств электронных схем.***
4. ***Аналоговые и дискретные сигналы.***
5. ***Цифровые сигналы.***
6. ***Особенности аналоговой и цифровой аппаратуры.***

Лабораторная работа 1.
«Изучение операционных усилителей». (4 часа)

Вопросы для самоподготовки:

1. **Свойства, виды и назначение операционных усилителей.**
2. **Основное уравнение операционного усилителя.**
3. **Схемы включения операционного усилителя.**
4. **Усилительные схемы.**
5. **Амплитудно-частотные характеристики усилительных схем.**

Контрольные вопросы:

1. **Как устроен операционный усилитель?**
2. **Для чего используется операционный усилитель?**
3. **Как обозначается операционный усилитель на схемах?**
4. **Основные схемы включения операционных усилителей.**

Лабораторная работа 2.
***«Изучение Логических схем».* (4 часа)**

Вопросы для самоподготовки.

1. Виды и классификация логических элементов.
2. Устройство логических элементов.
3. Комбинационные схемы на логических элементах.
4. Схемы элементарных ячеек памяти.
5. Триггеры.

Контрольные вопросы:

1. Что такое микросхема?
2. Как устроен и работает логический элемент?
3. Как устроен и работает триггер?
4. Основные виды логических элементов и триггеров.
5. Базовые логические элементы.
6. Принцип двойственности.
7. Виды логики: ТТЛ логика, электрические параметры элементов ТТЛ.

Лабораторная работа 3.
***«Расчёт и анализ фильтров».* (6 часов)**

Вопросы для самоподготовки.

1. Фильтрующие цепочки.
2. Виды пассивных фильтров.
3. Вывод дифференциального уравнения пассивной фильтрующей цепочки.
4. Получение комплексного коэффициента передачи пассивной фильтрующей цепочки.
5. Получение выражения для амплитудно-частотных и фазочастотных характеристики фильтрующих цепочек.

Контрольные вопросы:

1. Порядок анализа и расчета пассивных фильтров.
2. Построение амплитудно-частотных и фазочастотных характеристики фильтрующих цепочек.

Модуль3. Источники возникновения опасных сигналов, подлежащих защите.
Раздел 1. Утечка речевой информации за счет звуковых колебаний.

Цель: Изучение физических процессов характеризующих акустический сигнал, с учетом его влияния на разборчивость речи, как объективного информационного критерия оценки защищенности речевой информации от утечки .

Перечень изучаемых элементов содержания.

7. Основные физические характеристики звукового сигнала.
8. Особенности частотных, временных и энергетических составляющих звукового сигнала, влияющих на защищенность речевой информации от утечки.
9. Связь между смысловой (**с**емантической) составляющей речи и энергетическими характеристиками звукового сигнала , как физического носителя речевой информации**.**

Вопросы для самоподготовки:

10. Основные частотные, временные и энергетические составляющих звукового сигнала, влияющих на защищенность речевой информации от утечки.
11. Форманты речи и их влияние на разборчивость , как объективного критерия защищенность речевой информации от утечки.
12. Физические процессы, лежащие в основе образования акустических, виброакустических, акустоэлектрических и других подобных каналов утечки конфиденциальной речевой информации.
13. Влияние характеристик среды распространения акустического, виброакустического и акустоэлектрического и других подобных каналов утечки конфиденциальной речевой информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Форма практического задания лабораторные работы. (4 часа)

Лабораторная работа 1.

«Изучение влияния на информативность речи спектральных и энергетических составляющих звукового и маскирующего шумового сигнала в канале речевой утечки информации из защищаемого помещения. (2 часа)

Вопросы для самоподготовки*:*

4. Особенности распространения звуковых колебаний в различных средах.
5. Связь энергетических параметров речи с ее информативностью. Форманты. Разборчивость в октавных полосах.
6. Методы измерения энергетических параметров речевого сигнала. Децибелы.
7. Разборчивость речевого сигнала в октавных полоса.
8. Виды маскирующих сигналов, применяемых для защиты речевой информации.
9. Зависимость разборчивости речи от характеристик среды распространения речевого сигнала.

Контрольные вопросы:

5. Обосновать функциональную связь разборчивости речи и защищенности речевой информации от утечки.
6. Классификация и основные характеристики маскирующих сигналов, применяемых для защиты речевой информации от утечки.

7. Критерий защищенности речевой информации и его связь с параметрами речи и маскирующего сигнала.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – отчет по лабораторной работе.

Лабораторная работа 2.
Исследование информативности речи при виброакустических и акустоэлектрических преобразованиях в элементах инженерных коммуникация и ВТСС, расположенных в защищаемом помещении. (2 часа)

Вопросы для самоподготовки.

5. Физические процессы возникновения виброакустического канала утечки речевой информации.
6. Физические процессы возникновения акустоэлектрического канала утечки речевой информации.
7. Генераторные (активные) и параметрические (пассивные) акустоэлектрические преобразователи (АЭП).

Контрольные вопросы:

7. Принцип обратимости преобразователей, лежащий в основе образования канала утечки речевой информации за счет АЭП.
8. Привести примеры генераторных АЭП в конкретных технических средствах.
9. Привести примеры параметрических АЭП в конкретных технических средствах.
10. Привести примеры многомерности распространения виброакустического речевого сигнала в здании.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – отчеты по лабораторным работам.

Раздел 2. Утечка речевой и телекоммуникационной за счет ПЭМИН.

Цель:

Изучение физических процессов характеризующих канал утечки речевой и телекоммуникационной информации за счет побочных электромагнитных излучений и наводок (ПЭМИН) в эфире и в отходящих слаботочных линиях, а так же в системах электропитания и заземления технических средств.

Перечень изучаемых элементов содержания

1. Схемно-конструктивные условия и физические принципы образования канала утечки информации, за счет ПЭМИН в слаботочных и силовых линиях, выходящих за пределы защищаемого помещения..
2. Схемно-конструктивные условия и физические принципы образования канала утечки информации, за счет ПЭМИН в эфире, в условия ближней и дальней зон.

Вопросы для самоподготовки:

1. Физические процессы образования канала утечки информации за счет электромагнитных наводок на слаботочных и силовых линиях, выходящих за пределы защищаемого помещения.

2. Физические процессы возникновения в эфире технического канала утечки информации за счет электромагнитных излучений, в условия ближней и дальней зон.
3. Особенности схемно - конструктивного построения технических средств, приводящие к образованию каналов утечки информации за счет ПЭМИН.
4. Критерии защищенности технических средств по каналу ПЭМИН.
5. Естественные и искусственные процессы возникновения канала утечки информации за счет ПЭМИН.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.

Форма практического задания лабораторные работы. (4 часа)
Лабораторная работа 1.

Исследование технического канала утечки конфиденциальной информации возникающего за счет магнитного поля, создаваемого основными техническими средствами при обработке офисным оборудованием речевой информации.

Вопросы для самоподготовки:

1. Физические принципы образования технического канала утечки речевой информации по магнитному полю, при работе основных технических средств. Особенности данного канала и степень угрозы защищаемой информации.
2. Физические принципы образования канала утечки речевой информации за счет преобразования магнитного поля ОТСС в электрический сигнал в элементах ВТСС. Его особенности и степень угрозы защищаемой информации.

Контрольные вопросы:

1. Особенности распространения электромагнитного сигнала в ближней и дальней зонах.
2. Привести примеры возникновения подобного технического канала утечки для конкретного офисного оборудования.
3. Функциональное назначение понятий размер зоны R1и R2, с точки зрения обеспечения информационной безопасности объекта информатизации.

Лабораторная работа 2 (4 часа).

Изучение источников и условий образования канала утечки информации в эфире за счет ПЭМИН от цифрового и аналогового офисного оборудования.

Вопросы для самоподготовки:

1. Элементы технических средств являющиеся источниками образования ПЭМИН.
2. Мониторинг эфира, с целью выявления несанкционированных излучений.
3. Условия образования канала утечки информации за счет ПЭМИН.
4. Особенности ПЭМИН от цифрового и аналогового оборудования.
5. Особенности распространения ПЭМИН в ближней, промежуточной и дальней зонах.

Контрольные вопросы:

1. Источники возникновения канала утечки информации за счет ПЭМИН.
2. Классификация ПЭМИН по степени угрозы защищаемой информации.
3. Общая методология выявления опасного сигнала ПЭМИН, в зависимости от распространения сигнала в ближней, промежуточной и дальней зонах.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.: форма рубежного контроля – отчет по лабораторной работе.

Модуль 4.

Методы и средства защиты информации от утечки по техническим каналам

Раздел 1. Методы и средства защиты информатизации от утечки информации по техническим каналам в звуковом диапазоне частот.

Цель:

Изучение пассивных и активных инженерно-технических методов и средств защиты речевой конфиденциальной информации от утечки из защищаемых помещений.

Перечень изучаемых элементов содержания

Критерии защищенности речевой информации от несанкционированного прослушивания нарушителем за пределами защищаемого помещения. Пассивные методы и средства защиты помещений и слаботочного офисного оборудования, как субъектов утечки информации за счет несанкционированного подслушивания за пределами защищаемого помещения. Звукоизоляция помещений. Фильтрация и ограничение уровня опасного сигнала в слаботочных линиях, выходящих за пределы защищаемого помещения. Шумовая маскирующая помеха. Критерии выбора средств защиты. Защита функциональных каналов связи с помощью скремблеров. Выявление естественных и искусственных каналов утечки информации.

Вопросы для самоподготовки:

1. Разборчивость, как объективный критерий защищенности речи.
2. Конструктивные материалы, применяемые для повышения звукоизоляции помещения.
3. Виды и энергетические параметры маскирующих шумовых сигналов.
4. Ограничители малых амплитуд.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Форма практического задания лабораторные работы. (6 часов)

Лабораторная работа 1.

Исследование пассивных и активных методов защиты речевой информации от утечки по акустическому, виброакустическому каналам утечки и каналу ПЭМИН в низкочастотном диапазоне частот (4 часа)

Вопросы для самоподготовки*:*

1. Особенности распространения звуковых колебаний в различных средах.
2. Связь соотношения сигнал/помеха с разборчивостью речи.
3. Методы измерения энергетических параметров речевого сигнала. Децибелы.
4. Разборчивость речевого сигнала в октавных полоса.
5. Виды маскирующих сигналов, применяемых для защиты речевой информации.
6. Зависимость разборчивости речи от характеристик среды распространения речевого сигнала.

Контрольные вопросы:

1. Классификация и основные характеристики маскирующих сигналов, применяемых для защиты речевой информации от утечки.
2. Обосновать выбор вида маскирующих помех для защиты конфиденциальной речевой информации.
3. Критерий защищенности речевой информации и его связь с параметрами речи и различными видами маскирующего сигнала.

Лабораторная работа 2.

Исследование пассивных и активных методов защиты ВТСС от утечки речевой информации в слаботочные линии за счет АЭП (4 часа)

Вопросы для самоподготовки*:*

1. Функциональное устройство слаботочных (телефонные, оповещения), систем, являющихся физическими каналами утечки информации.
2. Принципы возникновения АЭП во ВТСС.
3. Системы пассивного подавления преобразованного сигнала. сигнала.
4. Принципы активной защиты преобразованного опасного сигнала. Виды маскирующих сигналов, применяемых для защиты АЭП.

Контрольные вопросы:

1. Фильтры и ограничители малых амплитуд, как средства пассивной защиты
2. Классификация и основные характеристики маскирующих сигналов, применяемых для защиты речевой информации от утечки.
3. Обосновать выбор вида маскирующих помех для защиты конфиденциальной речевой информации.
4. Критерий защищенности речевой информации и его связь с параметрами речи и различными видами маскирующего сигнала.

Раздел 2. Методы и средства защиты информации от утечки информации по каналу ПЭМИН.,

Перечень изучаемых элементов содержания

1. Критерии защищенности. Экранирование и фильтрация.
2. Средства и системы линейного и пространственного зашумления как пассивные методы и средства защиты ПЭМИН.
3. Критерии выбора средств защиты.
4. Выявление естественных и искусственных каналов утечки информации.
5. Проблемы защиты информации в условиях ближней и дальней зон распространения опасного сигнала

.

Вопросы для самоподготовки:

1. Современные технические средства линейного и пространственного зашумления в условиях ближней и дальней зон распространения опасного сигнала.
2. Критерии выбора оборудования.
3. Классификация средств экранирования.
4. Современная аппаратура и основные принципы выявления искусственных и естественных каналов утечки информации.

1. ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Форма практического задания лабораторные работы. (8 часов)

Лабораторная работа 1 (4 часа).

Изучение технических средств выявления искусственных каналов утечки информации в эфире. Радиомониторинг эфира.

Вопросы для самоподготовки*:*

1. Демаскирующие признаки искусственных каналов утечки информации.
2. Технические средства выявления искусственных каналов утечки информации.
3. Методология выявления искусственных каналов утечки информации

Контрольные вопросы:

1. Какие демаскирующие признаки излучающих и неизлучающих закладочных устройств.
2. Примеры технических средств выявления излучающих и неизлучающих устройств негласного добывания информации.

Лабораторная работа 2.

Исследование пассивных и активных методов защиты информации от утечки по каналу ПЭМИН. (4 часа)

Вопросы для самоподготовки*:*

1. Методы и средства пассивной защиты информации от утечки по каналу ПЭМИН.
2. Методы и средства линейного и пространственного зашумления.

Контрольные вопросы:

1. Перечислите методы и средства пассивной защиты информации от утечки по каналу ПЭМИН.
2. Средства линейного зашумления.
3. Средства пространственного зашумления.
4. Требования к маскирующей помехе.

Модуль 5. Методы и средства охраны объектов информатизации от несанкционированного проникновения и преднамеренного воздействия.

Раздел 1. Инженерно-технические средства охраны объектов информатизации, создающие физические препятствия несанкционированному проникновению нарушителя.

Цель:

Изучение средств и методов защиты объектов информатизации от постороннего проникновения на основе создания естественных и искусственных преград затрудняющих передвижение нарушителя и увеличивающих время, необходимое для несанкционированное проникновение к объекту защиты.

Перечень изучаемых элементов содержания

1. Назначение и классификация и конструктивное устройство средств инженерной укрепленности объектов информатизации.
2. Классификация по степени защиты дверей, замков, сейфов, и других подобных устройств.
3. Анализ конструктивных особенностей средств инженерной укрепленности с целью выбора наиболее эффективной конструкции для конкретных условий объекта.

Вопросы для самоподготовки:

1. Классификация замков.
2. Сувальдные и цилиндровые механические замки. Особенности конструкции современных запирающих устройств.
3. Современные металлические шкафы и сейфы. Особенности конструкции.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Форма практического задания: лабораторный практикум (8 часов).

Лабораторная работа 1 (4 часа).

Изучение конструктивных особенностей и защищенности к внешним воздействиям дверных конструкций сейфов и замковых устройств, как элементов средств инженерно- технической укрепленности объектов информатизации.

Цель: Практическое изучение конструктивных особенностей типовых механических замков и исследование с помощью виртуальных моделей их уязвимости к внешним воздействующим факторам и основных методов конструктивной защиты от антропогенных угроз.

Вопросы для самоподготовки:

1. Устройство сувальдных и цилиндровых механические замки. Особенности конструкции.
2. Конструкция входных дверей, как физической преграды и средства обеспечения звукоизоляции помещения.
3. Сейфы устойчивые ко взлому. Классификация.
4. Огнестойкие сейфы. Классификация.
5. Классификация замков и дверей по степени устойчивости ко взлому.

Контрольные вопросы:

1. Конструктивные отличия замков сувальдного и цилиндрового типа**.**
2. Классификация цилиндровых замков по конструктивному исполнению кодирующий элементов "механизма секрета". Привести примеры.
3. Классификация сейфов устойчивых ко взлому по функциональному назначению и конструктивному исполнению.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 2. Технические средства охраны объектов информатизации, обнаруживающие и контролирующие процесс несанкционированного проникновения нарушителя.

Цель: Изучение конструктивных особенностей и принципов построения технических средств обнаружения и контроля угроз несанкционированного проникновения нарушителя и возникновения пожара .

Перечень изучаемых элементов содержания

1. Классификация технические средства выявления и нейтрализации угроз по физическим принципам обнаружения и зонам контроля.
2. Изучение принципов построения и конструктивных особенностей применения систем охранной и пожарной сигнализации.
3. Изучение принципов построения и конструктивных особенностей применения систем охранного телевидения.
4. Изучение принципов построения и конструктивных особенностей применения систем контроля и управления доступом.
5. Изучение принципов построения и конструктивных особенностей применения систем электронной идентификации личности и контроля за логистикой грузов.
6. Изучение возможных направлений воздействия угрозы технологического (кибернетического и электромагнитного) терроризма на информационные системы и методов противодействия этим угрозам средствами физической защиты объектов информатизации.

Вопросы для самоподготовки:

1. Конструктивные особенности современных охранных и пожарных извещателей.
2. Функциональные возможности современных систем охранного телевидения.
3. Современные системы электронной идентификации и логистики на основе биометрических характеристик и RFID технологий.
4. Современные направления деструктивного воздействия на информационные системы
5. Нормативные документы регламентирующие направления обеспечения защиты информационных систем.

Лабораторная работа 1 (4 часа).

Исследование устройства и параметров видеокамеры системы охранного телевидения, влияющих на охранные свойства системы охранного телевидения (СОТ).

Цель: Практическое исследование влияния параметров видеокамеры на информативность видеоизображения, получаемого оператором системы охранного телевидения от наблюдаемого и контролируемого объекта (цели).

Перечень изучаемых элементов:

1. Измерение и расчет взаимной связи поля зрения, фокусного расстояния и размера ПЗС матрицы видеокамеры;
2. Измерение и расчет поля зрения типового человека и сравнение полученных результатов с соответствующими параметрами объективов видеокамер.
3. Исследование зависимости размера минимальная различимая деталь (изображения) МРД в зависимости от целевой задачи видеоконтроля.
4. Исследование влияния цветовых характеристик видеокамеры на эффективность реализации целевой задачи видеоконтроля наблюдаемого объекта (цели).
5. Практическое изучения применения «КРОП-ФАКТОРА», как коэффициента вычисления эквивалентного фокусного расстояния сменных объективов.

Вопросы для самоподготовки:

1. Терминология видеосистем.
2. Устройство видеокамеры.
3. Параметры объектива и ПЗС матрицы, влияющие на углы обзора видеокамеры.
4. "КРОП-ФАКТОР"

Контрольные вопросы:

1. Классификация объективов по конструкции.
2. Как влияет фокусное расстояние объектива на площадь кадра и детализацию объекта наблюдения(цели).
3. Как влияет размер ПЗС матрицы на площадь кадра и детализацию объекта наблюдения(цели).

Лабораторная работа 2 (4 часа).
Изучение технических (аппаратно-программных) средств обработки и отображения видеосигнала, поступающего от видеокамер.

Цель лабораторной работы является практическое изучения функциональных возможностей и методологии работы технических средств обработки и отображения видеосигнала, поступающего от видеокамер, на базе аппаратно- программного видеорегистратора.

Перечень изучаемых элементов:

1. Изучение разделителей экрана (квадратор).
2. Изучение детектора движения
3. Изучение системы архивирования информации.

Вопросы для самоподготовки:

1. Функциональной назначение мультиплексоров и разделителей экрана.
2. Аналоговые и цифровые детекторы движения.
3. Различие в способах выбора и отображения зон детектирования для аналоговых и цифровых детекторы движения.
4. Функциональные и потребительские отличия систем аналогового и цифрового детектирования движения в кадре.

5. Аналоговые и цифровые системы архивирования видеоинформации.

Контрольные вопросы:

1. Отличие функции обнаружения активности и обнаружения вторжения.
2. Отличие в установке зон детектирования в аналоговых и цифровых детекторах.
3. Функциональные разновидности современных детекторов движения.
4. Что дает оператору наличие в системе детекторов движения.
5. Эргономический принцип расположения средств отображения информации для повышения эффективности работы оператора.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.: форма рубежного контроля – отчеты по лабораторным работам.

Модуль 6. Контроль эффективности защиты объекта информатизации

Раздел 1. Основные цели, методы и требования к средствам проведения контроля защищенности объектов информатизации.

Цель:

Изучение вопросов, связанных с проведением аналитических и инструментальных работ по оценки первичной защищенности объектов информатизации и разработке требований на их организационную и техническую защиту.

Перечень изучаемых элементов содержания

1. Специсследование. Решаемые задачи. Конечная цель. Принцип выбора оборудования.
2. Спецобследование. Спецпроверка. Решаемые задачи. Конечная цель. Принцип выбора оборудования.
3. Метрологические требования к средствам инструментального контроля защищенности объекта информатизации.
4. Основные требования к тестовым сигналам.

Вопросы для самоподготовки:

1. Особенности проведения спецсследования основных и вспомогательных технических средств и систем.
2. Условия выбора тестовых сигналов при проведении специсследования.
3. Виды тестовых сигналов для проведения специсследования.
4. Условия выбора инструментальных средств контроля для проведения специсследований, с официальным оформлением результатов.
5. Выбор оборудования для "оценочных" исследований.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Лабораторных и семинарских занятий для данного раздела не предусмотрено.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – Устный опрос обучающихся.

Раздел 2. Классификация, основные принципы и особенности функционального и схемно-конструктивного построения средств инструментального контроля защищенности объектов информатизации.

Цель. Изучение видов и функционального назначения и особенностей построения измерительных приборов и специализированного оборудования, применяемого для проведения работ по контроля защищенности объектов информатизации

Перечень изучаемых элементов содержания

1. Функциональные возможности современных измерительных приборов и специализированных средств проведения контроля защищенности объектов информатизации.
2. Основные схемно- конструктивные принципы и функциональные возможности современных измерительных приборов и специализированных средств проведения контроля защищенности объектов информатизации.
3. Современные средства обнаружения технических устройств формирования искусственных каналов утечки информации.
4. Требования к источникам тестовых сигналов, применяемых для проведения специсследований современных технических средств.

Вопросы для самоподготовки:

1. Особенности построения и задачи, решаемые в процессе проведения специисследования селективными приборами измерения напряжения и токов. Примеры.
2. Особенности построения и задачи, решаемые в процессе проведения специисследования селективными приборами измерения и отображения временных характеристик исследуемого сигнала. Примеры.
3. Особенности построения и задачи, решаемые в процессе проведения специисследования селективными приборами измерения и отображения спектральных характеристик исследуемого сигнала. Примеры.
4. Особенности построения и задачи, решаемые специализированными средства обнаружения технических устройств формирования искусственных каналов утечки информации. Принципы обнаружения.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.
Лабораторных и семинарских занятий для данного раздела не предусмотрено.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.: форма рубежного контроля – Устный опрос обучающихся.

.

Раздел 3. Специализированные технические средства и измерительные приборы, применяемые для оценки и анализа защищенности объекта информатизации в инфразвуковом, звуковом и ультразвуковых диапазонах частот.

Цель. Изучение функционального возможностей и особенностей построения измерительных приборов и специализированного оборудования, применяемого для проведения работ по контроля защищенности объектов информатизации от утечки конфиденциальной речевой информации в инфразвуковом, звуковом и ультразвуковых диапазонах частот.

.

Перечень изучаемых элементов содержания.

1. Селективные нановольтметры. Особенности применения в процессе проведения специсследований.
2. Измерители шума и вибраций. Особенности применения в процессе проведения специсследований.
3. Анализаторы спектра реального времени. Особенности применения в процессе проведения специсследований.
4. Источники тестовых сигналов в инфразвуковом, звуковом и ультразвуковых диапазонах частот.

Вопросы для самоподготовки:

1. Устройство, технические характеристики, органы управления и отбражения информации селективного нановольтметров UNIPAN 233; UNIPAN 237. Методика измерения.
2. Устройство, технические характеристики, органы управления и отображения информации измерителей шума и вибраций ВШВ-003. Методика измерения.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.

Форма практического задания: лабораторный практикум (2 часа).

Лабораторная работа 1 (2 часа). Изучение измерительных приборов, применяемых в процессе проведения специальных исследований в инфразвуковом, звуковом и ультразвуковых диапазонах частот.

Цель: Получение практических навыков в работе с селективным нановольтметром *UNIPAN 233,* шумомером ххххх и измерителем шума и вибраций ВШВ 003.

Вопросы для самоподготовки:

1. Органы управления приборами.
2. Октавная селективность приборов.
3. Настройка приборов.
4. Считывание показаний.

Контрольные вопросы.

1. Что такое октавная селективность.
2. Как определяется полоса пропускания селективного устройства.
3. Как считываются показания стрелочного прибора.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 4. Специализированные технические средства и измерительные приборы, применяемые для оценки и анализа защищенности объекта информатизации в радиочастотном диапазоне.

Цель. Изучение функционального возможностей и особенностей построения измерительных приборов и специализированного оборудования, применяемого для проведения работ по контроля защищенности объектов информатизации от утечки конфиденциальной речевой информации в радиочастотном диапазоне.

Перечень изучаемых элементов содержания.

5. Селективные высокочастотные микровольтметры. Особенности применения в процессе проведения специсследований.
6. Высокочастотные анализаторы спектра последовательного анализа. Особенности применения в процессе проведения специсследований.
7. Источники тестовых сигналов в радиочастотном диапазоне**.**

Вопросы для самоподготовки:

1. Принцип построения радиоприемного устройства прямого усиления.
2. Принцип построения супергетеродинного радиоприемного устройства.
3. Устройство, технические характеристики, органы управления и отображения информации высокочастотных селективных микровольметров SMV-8, SMV-11. Методика измерения.

4. Устройство, технические характеристики, органы управления и отображения анализатора спектра радиосигнала ххххх Методика измерения.
5. Выбор тестовых сигналов.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4.

Форма практического задания: лабораторный практикум (2 часа).

Лабораторная работа 1 (2 часа). Изучение измерительных приборов, применяемых в процессе проведения специальных исследований в инфразвуковом, звуковом и ультразвуковых диапазонах частот.

Цель: Получение практических навыков в работе с измерительными приборами и специализированными устройствами радиодиапазона: SMV-8, SMV-11, хххх.

Вопросы для самоподготовки:

5. Органы управления приборами.
6. Селективность приборов.
7. Настройка приборов.
8. Считывание показаний.

Контрольные вопросы.

4. Что такое селективность по ПЧ и селективность по НЧ.
5. Как определяется полоса пропускания селективного устройства.
6. Как считываются показания прибора.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – отчет по лабораторной работе.

Раздел 5. Методология проведения мероприятий по контролю защищенности объектов информатизации от утечки конфиденциальной информации по техническим каналам.

Цель: Практическое изучения методов, программных и аппаратных средств контроля защищенности объектов информатизации от утечки конфиденциальной информации, анализа результатов и оформления протоколов проведенной работы.

Перечень изучаемых элементов содержания.

1. Практические навыки по анализу защищаемого помещения, в целях выявления источников образования технических каналов утечки информации.
2. Методологические основы проведения специсследований и спецобследования помещений.
3. Обоснование выбора оборудования для эффективного проведения работ..
4. Обоснование выбора источников тестовых сигналов для проверки конкретного оборудования.

Вопросы для самоподготовки:

1. Методология технического анализа оборудования, расположенного в защищаемом помещении, в целях выявления источников образования технических каналов утечки информации.
2. Методологии проведения технических мероприятий по контролю защищенности объектов информатизации от утечки конфиденциальной информации по техническим каналам.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5.

Форма практического задания: лабораторный практикум (4 часа).

Лабораторная работа 1 (4 часа).

Практическое изучение методологии проведения комплексных работ по контролю защищенности объектов информатизации, на примере оборудования типового офисного помещения.

Цель: Практическое освоение методологии и технических средств по обнаружению и локализации технических средств негласного получения информации, выявления естественных и искусственно созданных каналов утечки информации, а также инструментальной оценки защищенности объектов информатизации, на примере оборудования типового офисного помещения.

Вопросы для самоподготовки:

1. ОТСС. Технические каналы утечки информации.
2. ВТСС. Технические каналы утечки информации.
3. Критерии защищенности конфиденциальной информации на границе защищаемого помещения. для естественных технических каналов утечки.
4. Технические средства для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения информации, а также для выявления естественных и искусственно созданных каналов утечки информации.
5. Технические средства для инструментального контроля защищенности объектов информатизации.
6. Основные положения методик проведения контрольных мероприятий по оценки защищенности объектов информатизации от утечки конфиденциальной информации.

Контрольные вопросы.

1. Перечислить примеры ОТСС и ВТСС, являющихся возможными источниками образования технических каналов утечки конфиденциальной информации из типового офисного кабинета, на примере имеющегося в лаборатории учебного имитационного комплекса (УИК).
2. Перечислить наиболее опасные каналы утечки для конкретного состава оборудовании УИК.
3. Назначение и состав многофункционального поискового устройства ST 033 "Пиранья".
4. Перечислить состав оборудования, необходимого для инструментальной оценки защищенности УИК

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.: форма рубежного контроля – отчет по лабораторной работе в виде типового протокола о результатах проведенных исследований и предлагаемых рекомендациях по устранению выявленных угроз.

Оформление работ, выполняемых в рамках самостоятельной работы осуществляется в соответствии с Методическими указаниями по оформлению письменных работ обучающихся в рамках самостоятельной работы, утвержденными Учебно-методическим советом РГСУ. Конкретные практические задания и задания для рубежного контроля определяются в учебно-методических материалах по работе обучающихся в электронной информационно-образовательной среде РГСУ с применением технологий электронного обучения по данной дисциплине, утверждаемых ежегодно факультетом.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по дисциплине (модулю) является **экзамен / зачет / дифференцированный зачет,** который проводится в **устной / письменной** форме.

В случае применения электронного обучения, дистанционных образовательных технологий указывается форма промежуточной аттестации, а также дается краткая инструкция по проведению.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-7	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;	*Знать:* основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий.	Этап формирования знаний
		Уметь: применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ.	Этап формирования умений
		Владеть: навыками программирования, отладки и тестирования	Этап формирования навыков и получения опыта

		прототипов программно-технических комплексов задач.	
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	**Знать:** методы установки, настройки и обслуживанию технических и криптографических средств защиты информации	Этап формирования знаний
		Уметь: выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации	Этап формирования умений
		Владеть: способностью выполнять работы по установке, настройке и обслуживанию технических и криптографических средств защиты информации	Этап формирования навыков и получения опыта
ПК – 6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать:** функциональное назначение основные принципы построения средств защиты информации, а так же методы и средства проведения контрольных проверок, основываясь на официальных критериях обеспечения защищенности.	Этап формирования знаний
		Уметь: разработать программу и осуществить проведение необходимых контрольных проверок, с учетом дифференцированного и системного подхода, либо согласовать организационно-техническую составляющую данных работ со сторонней организацией, имеющей соответствующие лицензии на выполнение работ и сертификаты на устанавливаемые средства защиты.	Этап формирования умений
		Владеть: теоретическими знаниями и практическими навыками по проведению мероприятий по контролю средств защиты информации на основе критериев и методологии, изложенных в нормативно-методических документах, федерального, ведомственного и производственного уровней.	Этап формирования навыков и получения опыта

ПК – 7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.	**Знать:** • принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода; • номенклатуру и основные параметры сертифицированных средств обеспечения информационной безопасности.	Этап формирования знаний
		Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно- следственных связей.	Этап формирования умений
		Владеть : • основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту информатизации; • методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования. • основными технологиями селективного информационного поиска и анализа результатов работы с информационными ресурсами по номенклатуре сертифицированных средств защиты объектов информатизации.	Этап формирования навыков и получения опыта
ПК – 8	Способность оформлять рабочую техническую документацию, с учетом действующих нормативных и методических документов.	**Знать:** критерии защищенности объекта информатизации, состав оборудования и методологию контроля, изложенных в нормативно- методических документах, федерального, ведомственного и производственного уровней.	Этап формирования знаний
		Уметь: при оформлении отчетных материалов четко формулировать цель	Этап формирования умений

		проведенных работ, объект и предмет работ, результаты инструментальных исследований, выводы и рекомендации по результатам проведенных работ, в понятной, как техническому специалисту, так и специалисту в сфере управления форме.	
		Владеть: навыками написания отчетных материалов, в том числе технически и экономически обоснованных выводов и рекомендаций, в понятной как техническому специалисту, так и специалисту в сфере управления форме.	Этап формирования навыков и получения опыта
ПК – 9	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзоры по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах.	Этап формирования знаний
		Уметь: проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации.	Этап формирования умений
		Владеть: современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации.	Этап формирования навыков и получения опыта
ПК – 11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.	**Знать:** методологию и метрологию проведения инструментальных исследований, связанных с объективной оценкой защищенности объектов информатизации.	Этап формирования знаний
		Уметь: проводить: • измерения параметров, исследуемых процессов, с помощью существующих измерительных приборов, с возможностью обоснованного	Этап формирования умений

		выбора функциональных аналогов; • математическую обработку полученных результатов; • разработку обоснованных выводов и рекомендаций по результатам инструментальных исследований.	
		Владеть: теоретическими знаниями и практическими навыками по проведению инструментальных исследований объектов информатизации, на их соответствие их защищенности требуемым критериям.	Этап формирования навыков и получения опыта
ПК – 12	Способность принимать участие в проведении экспериментальных исследований системы защиты информации.	**Знать:** функциональное назначение**,** технические и конструктивные особенности применения, общие принципы построения и работы исследуемой системы защиты информации.	Этап формирования знаний
		Уметь: применять сведения, изложенные в соответствующих нормативно- методических, технических и эксплуатационных документах, а так же соответствующее специализированное оборудование и измерительные приборы для проведении экспериментальных исследований системы защиты информации.	Этап формирования умений
		Владеть: теоретическими знаниями и навыками по практическому применению соответствующего специализированного оборудования и измерительных приборов для проведении экспериментальных исследований системы защиты информации мероприятий	Этап формирования навыков и получения опыта
ПК-15	Способность организовывать технологический процесс защиты	**Знать:** нормативные правовые актами и нормативные методические документы ФСБ и ФСТЭК., МВД.	Этап формирования знаний

	информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по техническому и экспортному контролю (ФСТЭК).	**Уметь:** Разрабатывать политику безопасности предприятия.	Этап формирования умений
		Владеть: теоретическими знаниями и практическими навыками разработке и реализации политики безопасности предприятия, в плане анализа и оценке угроз, рисков и мероприятий по минимизации их последствий с учетом экономических факторов.	Этап формирования навыков и получения опыта

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	**Этапы формирования компетенций**	**Показатель оценивания компетенции**	**Критерии и шкалы оценивания**
ОПК-7; ОПК-9; ПК-6; ПК-7; ПК-8; ПК-9; ПК-11; ПК-12; ПК-15	Этап формирования знаний.	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает

			последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.
ОПК-7; ОПК-9; ПК-6; ПК-7; ПК-8; ПК-9; ПК-11; ПК-12; ПК-15	Этап формирования умений.	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией - 9-10 баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании -7-8 баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению5-6 баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания - 0-4 баллов.
ОПК-7; ОПК-9; ПК-6; ПК-7; ПК-8; ПК-9; ПК-11; ПК-12; ПК-15	Этап формирования навыков и получения опыта.	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

4.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Теоретический блок вопросов:

1. Информация. Информационная сфера. Информационная безопасность.
2. Автоматизированная система, как объект информационной защиты.
3. Акустические, виброакустические каналы утечки речевой информации.
4. Аакустоэлектрические каналы утечки речевой информации
5. Основные понятия в области акустики.
6. Классификация акустических каналов утечки информации
7. Звук, Звуковое давление, Сила (интенсивность) звука
8. Классификация технических каналов утечки акустической информации
9. Оптико-электронный канал утечки информации
10. Параметрические акустоэлектрические преобразователи
11. Генераторные акустоэлектрические преобразователи.
12. Классификация демаскирующих признаков.
13. Классификация технической разведки.
14. Технические средства акустической разведки. Возможности, Основные характеристики.
15. Методы и средства образования искуственных каналов утечки информации.
16. Физические основы образования естественных каналов утечки информации. Краткая характеристика.
17. Заходовые и беззаходовые способы и средства негласного конфиденциальной добывания информации.
18. Демаскирующие признаки технических средств негласного добывания информации, образующих
19. Классификация закладочных устройств по типу каналы передачи конфиденциальной информации из защищаемых помещений.
20. Классификация и физические процессы возникновения акустоэлектрического преобразования ("микрофонный эффект") в элементах технических средств.
21. Физические процессы формирования искусственного канала утечки информации, методом "высокочастотного навязывания".
22. Особенности схемно - конструктивного построения технических средств, приводящие к образованию канала утечки информации за счет ПЭМИН.
23. Критерии защищенности технических средств по каналу ПЭМИН.
24. Естественные и искусственные процессы возникновения канала утечки информации за счет ПЭМИН.
25. Пассивные и активные методы защиты речевой информации.
26. Экранирование технических средств
27. Фильтрация опасных сигналов
28. Помехоподавляющие фильтры
29. Зашумление.
30. Скремблеры. Назначение. Принципы построения.
31. Зоны и рубежи охраны.

32. Замки, запорные устройства. Классификация. Конструктивное исполнение. Требования руководящих документов и рекомендации по их выбору.
33. Сейфы и хранилища. Требования руководящих документов и рекомендации по их выбору.
34. Классификация сигнализационных систем.
35. Системы охранной сигнализации. Функциональные особенности.
36. Системы пожарной сигнализации. Функциональные особенности.
37. Системы тревожной сигнализации. Функциональные особенности.
38. Извещатели сигнализационных систем. Классификация.
39. Классификация телевизионных систем. Системы замкнутого телевидения (CCTV). Системы промышленного и охранного телевидения. Общность и различие.
40. Основные задачи, состав и структура системы охранного телевидения (СОТ).
41. Видеокамеры. Устройство. Основные характеристики и особенности практического применения в различных условиях.
42. Структура системы контроля и управления доступом.. Классификация средств и систем контроля и управления доступом.
43. Способы электронной идентификации и их характеристики.
44. Особенности функционирования считывающих и преграждающих устройств в условиях деструктивного воздействия антропогенных факторов.
45. Перспективы развития систем контроля и управления доступом.
46. Роль и место антитеррористических мероприятий в системе обеспечения комплексной безопасности предприятия, в том числе его информационной составляющей.
47. Технические средства антитеррористической защиты, их назначение и основные характеристики
48. Технологический терроризм. Классификация. Обобщенная характеристика методов и средств деструктивного воздействия. Примеры реализации, по материалам открытой печати.
49. Организационно- технические и инженерно- технические методы защиты объекта от субъектов технологического терроризма.
50. Классификация методов технической разведки по физическим принципам возникновения каналов утечки информации.
51. Основные демаскирующие признаки каналов утечки информации.
52. Физические принципы, заложенные в методологию выявления искусственно созданных и естественно образованных каналов утечки конфиденциальной речевой, телекоммуникационной текстовой и графической информации.
53. Нормативные документы, определяющие терминологию в сфере применения средств инструментального контроля.
54. Технические средства для проведения мероприятий по выявлению каналов утечки информации.
55. Классификация и функциональные особенности технических средств выявления каналов утечки информации.
56. Измерительные приборы и оборудование инструментальной оценки уязвимости технических средств с точки зрения утечки конфиденциальной информации. Классификация и функциональные особенности.
57. Измерительные приборы и оборудование инструментальной оценки уязвимости выделенных и защищаемых помещений с точки зрения утечки конфиденциальной информации. Классификация и функциональные особенности.
58. Приборы для исследования акустических и виброакустических сигналов. Структурная схема. Элементы управления и индикации. Методика работы.
59. Специализированные технические средства экспертной оценки защищенности технических средств и выделенные помещений. Назначение и методика работы.
60. Многофункциональные устройства «Пиранья»
61. Локаторы нелинейности.

62. Селективные нано и микровольтметры в НЧ и ВЧ диапазонах.

4.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестации по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по дисциплине (модулю) выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля)

5.1.1. Основная литература.

1. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019
2. *Внуков, А. А.* Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

5.1.2. Дополнительная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: ***https://www.biblio-online.ru/bcode/434171***

5.2. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Интернет-Университет информационных технологий – ИНТУИТ.РУ (http://www.intuit.ru)
2. Искусство управления информационной безопасностью (http://www.iso27000.ru)
3. Институт экономической безопасности (http://www.bre.ru/security)

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) ««**Защита информации от утечки по техническим каналам»** предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины (модуля) . Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

5.4.Информационно-технологическое обеспечение образовательного процесса по дисциплине (модулю)

5.4.1. Информационные технологии

1. Персональные компьютеры;
2. Доступ к интернет
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.4.3. Информационные справочные системы и профессиональные базы данных

Обучающиеся по программе **«Информационная безопасность»** в университете имеют доступ к следующим современным профессиональным базам данных, информационным справочникам:

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.4.4. Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) **«Защита информации от утечки по техническим каналам»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки **10.03.01 "Информационная безопасность"**используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет), демонстрационными материалами (презентации лекций), видеофильмами DVD

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

По теме «Защита информации от утечки по техническим каналам» проводятся лабораторный занятий в **лаборатории,** оснащенной специализированной мебелью: стол для преподавателя, парты, стулья, доска для написания мелом; техническими средствами обучения: видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет.

По теме «Защита информации от утечки по техническим каналам» проводятся лабораторный занятий в **Наименование лаборатории,** оснащенной специализированной мебелью: стол для преподавателя, парты, стулья, доска для написания мелом; техническими средствами обучения: видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет, а также лабораторным оборудованием.

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.4.5. Образовательные технологии

При реализации дисциплины (модуля) **«Защита информации от утечки по техническим каналам»** применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины (модуля) **«Защита информации от утечки по техническим каналам»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

При освоении дисциплины (модуля) «**Защита информации от утечки по техническим каналам»** предусмотрено применением электронного обучения.

Учебные часы дисциплины «**Защита информации от утечки по техническим каналам»** предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках дисциплины (модуля) **«Защита информации от утечки по техническим каналам»** предусмотрены встречи с руководителями и работниками организаций, деятельность

которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/
«06» __июня___2022г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направленность (профиль)
Организация и технологии защиты информации

Направление подготовки
10.03.01 Информационная безопасность

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022 г.

Рабочая программа дисциплины (модуля) **«Основы управления информационной безопасностью»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.04 "Информационная безопасность" (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
– *06.032 Специалист по безопасности компьютерных систем и сетей*
– *06.033 Специалист по защите информации в автоматизированных системах*
06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля) разработана рабочей группой в составе: д.т.н., профессор Неизвестный С.И., ст.пр. Елисеева Д.Ю.

Руководитель основной профессиональной образовательной программы к.п.н., доцент — Н.Г. Витковская

(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года

Декан факультета
К.п.н. доцент — С.В. Крапивка

(подпись)

Рабочая программа дисциплины (модуля) рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет»
зам. ген. директора по науке, к.т.н., доцент — А.С. Мосолов

(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

д.т.н., доцент, профессор кафедры информационных технологий, ГБОУВО Академия ГПС МЧС России) — С.Ю. Бутузов

(подпись)

к.ф.-м.н, доцент
кафедра прикладной математики и информатики РГСУ — Н.П. Третьяков

(подпись)

Согласовано
Научная библиотека, директор — И.Г. Маляр

(подпись)

СОДЕРЖАНИЕ:

1.1. РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) заключается в получении обучающимися теоретических знаний и практических навыков в организации и ведении системы менеджмента информационной безопасности в организациях; организационное планирование и управление объектами, субъектами и процессами обеспечения информационной безопасности, оценке информационных рисков; планировании мер по обработке рисков; реализации и внедрения соответствующих механизмов контроля, распределении ролей и ответственности, обучения и мотивации персонала, оперативной работы по осуществлению защитных мероприятий; мониторинге функционирования механизмов контроля, оценки их эффективности и выработке соответствующих корректирующих воздействий с последующим применением в профессиональных сферах информационной безопасности:

- эксплуатационной;
- проектно-технологической;
- экспериментально-исследовательской;
- организационно-управленческой.

Задачи дисциплины (модуля) : приобретение студентами теоретических знаний и практических навыков:

1. организации и ведения системы менеджмента информационной безопасности в организациях;
2. оценки информационных рисков; планирования мер по управлению рисками;
3. реализации и внедрения соответствующих механизмов контроля, распределения ролей и ответственности, обучения и мотивации персонала, оперативной работы по осуществлению защитных мероприятий;
4. мониторинга функционирования механизмов контроля, оценки их эффективности и выработке соответствующих корректирующих воздействий.

Эксплуатационная деятельность в области обеспечения информационной безопасности:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта;
- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

проектно-технологическая деятельность:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

- сбор, изучение научно-технической информации, отечественного и

зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;
- контроль эффективности реализации политики информационной безопасности объекта.

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы.

Учебная дисциплина **«Основы управления информационной безопасностью»** реализуется в базовой части основной профессиональной образовательной программы "Информационная безопасность" по направлению подготовки 10.03.01 "Информационная безопасность" очной формы обучения.

Изучение дисциплины (модуля) **«Основы управления информационной безопасностью»** базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Основы информационной безопасности».

Изучение дисциплины (модуля) **«Основы управления информационной безопасностью»** является одной из полезных составляющих для успешного выполнения выпускной квалификационной работы.

1.3. Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основной профессиональной образовательной программы.

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих общепрофессиональных и профессиональных компетенций ОПК-10, ПК-2.2, ПК-3, ПК-9, ПК-10, ПК-13, ПК-14, ПК-15 в соответствии с основной профессиональной образовательной программой "Информационная безопасность" по направлению подготовки 10.03.01 "Информационная безопасность" очной формы обучения.

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	**Код компетенции**	**Формулировка компетенции**	**Код и наименование индикатора достижения**	**Результаты обучения**

			компетенции	
	ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-10.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-10.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Знать: технические каналы утечки информации,организацию защиты информации от утечки по техническим каналам, основные характеристики и принципы построения средств защиты информации от утечки по техническим каналам *Уметь:* проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем *Владеть:* методами проектирования и навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности
	ОПК-2.2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения	ОПК-2.2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках	Знать: основные методы администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем

		их устойчивости к деструктивным воздействиям на информационные ресурсы	компетенции ОПК-2.2.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-2.2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Уметь: администрировать средства и системы защиты информации автоматизированных систем
				Владеть: навыками контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем
	ПК-3	Способен администрировать подсистемы информационной безопасности объекта защиты	ПК-3.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-3.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-3.ИД-3.	**Знать:** - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ - основы администрирования вычислительных сетей - системы управления БД - эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности - основные направления политик защиты информации на предприятии (организации) - возможные угрозы информационной безопасности, связанные с аспектами деятельности предприятия (организации),

			Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	особенностями технологических процессов, организационной структуры и др.
				Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействиия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты - выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации

				Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации
	ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-9.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-9.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-9.ИД-3. Применяет методы анализа	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах.
				Уметь: проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации.

			практической деятельности и ее результатов в рамках компетенции	**Владеть:** современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации.
	ПК-10	Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-10.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-10.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - методы планировании и проведении аудитов информационной безопасности - методику планирования мероприятий по информационной безопасности и расстановку приоритетов - основные подходы к формированию и обоснованию бюджета на информационную безопасность - сущность процессов обеспечения информационной безопасности
				Уметь: - оценивать экономическую эффективность и целесообразность реализации защитных мероприятий - внедрять системы управления информационной безопасностью и/или готовится к сертификации по современным международным стандартам
				Владеть: - методикой оценки и управления рисками в организации - методикой контроля рисков информационной безопасности во всех сферах деятельности

	ПК-13	Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-13.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-13.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации; - понятие системы управления, основные виды структур, принципы системного подхода к анализу структур
				Уметь: - реализовывать на практике принципы политики безопасности - использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности
				Владеть: - навыками анализа, обработки и интерпретации результатов решения прикладных задач управления - навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью - навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации
	ПК-14	Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	ПК-14.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-14.ИД-2. Планирует и	**Знать:** - сущность и содержание работы исполнителей - виды управленческих решений в области организации работ по проекту и нормированию труда - особенности процесса организации работы исполнителей
				Уметь: - анализировать содержание работы исполнителей - разрабатывать, анализировать и оценивать необходимость применения различных форм работы - разрабатывать план по реализации управленческих решений в области организации работ по проекту и нормированию труда навыками

			выполняет практические действия в рамках компетенции ПК-14.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Владеть:** - навыками анализа и установления форм и направлений деятельности в работе исполнителей - навыками оценки труда исполнителей - навыками разработки плана реализации управленческих решений в области организации работ по проекту и нормированию труда
	ПК-15	Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-15.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-15.ИД-3. Применяет методы анализа	**Знать:** основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области **Уметь:** - организовывать технологические процессы организации в том числе на основе локальной и комплексной автоматизации процессов обработки документов в документационной службе в соответствии с нормативными актами и нормативными методическими документами

			практической деятельности и ее результатов в рамках компетенции	**Владеть:** - навыками работы с нормативными правовыми актами в области защиты информации - методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем дисциплины (модуля), включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 17 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		5	6	7	8	
Контактная работа обучающихся с педагогическими работниками	**306**	**72**	**54**	**90**	**90**	
Учебные занятия лекционного типа	64	16	12	18	18	
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	106	24	18	32	32	
из них: в форме практической подготовки						
Иная контактная работа	136	32	24	40	40	
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**216**	**63**	**18**	**81**	**54**	
из них: в форме практической подготовки	*41*	*12*	*3*	*16*	*10*	
Контроль промежуточной аттестации	**90**	**9**	**36**	**9**	**36**	
Форма промежуточной аттестации		зачет	экзам	зачет	экзам	
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**612**	**144**	**108**	**180**	**180**	

2.1. Учебно-тематический план дисциплины (модуля)

Раздел, тема	Виды учебной работы, академических часов

	Всего	**Самостоятельная работа**	*из них: в форме практической подготовки*	**Контактная работа обучающихся с педагогическими работниками**									
				Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*
Модуль 1 (семестр 5)													
Раздел 1.1	33	15	*3*	18		4				6		8	
Раздел 1.2	34	16	*3*	18		4				6		8	
Раздел 1.3	34	16	*3*	18		4				6		8	
Раздел 1.4	34	16	*3*	18		4				6		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**144**	**63**	***12***	**72**		**16**				**24**		**32**	
Форма промежуточной аттестации	**зачет**												
Модуль 2 (семестр 6)													
Раздел 2.1	24	6	*1*	18		4				6		8	
Раздел 2.2	24	6	*1*	18		4				6		8	
Раздел 2.3	24	6	*1*	18		4				6		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**108**	**18**	***3***	**54**		**12**				**18**		**24**	
Форма промежуточной аттестации	**экзамен**												

Модуль 3 (семестр 7)													
Раздел 3.1	34	16	*4*	18		4				6		8	
Раздел 3.2	34	16	*3*	18		4				6		8	
Раздел 3.3	34	16	*3*	18		4				6		8	
Раздел 3.4	34	16	*3*	18		4				6		8	
Раздел 3.5	35	17	*3*	18		2				8		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**180**	**81**	***16***	**90**		**18**				**32**		**40**	
Форма промежуточной аттестации	**зачет**												
Модуль 4 (семестр 8)													
Раздел 4.1	28	10	*2*	18		4				6		8	
Раздел 4.2	29	11	*2*	18		4				6		8	
Раздел 4.3	29	11	*2*	18		4				6		8	
Раздел 4.4	29	11	*2*	18		4				6		8	
Раздел 4.5	29	11	*2*	18		2				8		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**180**	**54**	***10***	**90**		**18**				**32**		**40**	
Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**612**	**216**	***41***	**306**		**64**				**106**		**136**	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Виды самостоятельной работы обучающихся по дисциплине

Раздел, тема	Всего	Виды самостоятельной работы обучающихся

		Академическая активность, час	Форма академической активности	Выполнение практ. заданий, час	Форма практического задания	Рубежный текущий контроль, час	Форма рубежного текущего контроля
Модуль 1 (семестр 5)							
Раздел 1.1	15	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.4	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**63**	**27**		**28**		**8**	
Модуль 2 (семестр 6)							
Раздел 2.1	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 2.3	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**18**	**6**		**6**		**6**	
Модуль 3 (семестр 7)							
Раздел 3.1	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.2	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.3	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.4	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.5	17	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**81**	**35**		**36**		**10**	
Модуль 4 (семестр 8)							
Раздел 4.1	10	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 4.2	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.3	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.4	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.5	11	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**54**	**20**		**24**		**10**	
Общий объем по дисциплине (модулю), часов	**216**	**88**		**94**		**34**	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю)

МОДУЛЬ 1. БАЗОВЫЕ ПОНЯТИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

РАЗДЕЛ 1. Основные понятия системы управления информационной безопасностью

Цель: изучить основные понятия системы управления информационной безопасностью.

Перечень изучаемых элементов содержания

Основы управления информационной безопасностью как это циклический процесс.
Стандарт ISO 27001.
Создание и эксплуатация Системы Управления Информационной Безопасностью (СУИБ).
Процессная модель: планирование, реализация, проверка, действие (ПРПД).

Вопросы для самоподготовки:

1. Понятие СУИБ.

2. Структура СУИБ.
3. Стандарт ISO 27001.
4. Создание и эксплуатация СУИБ.
5. Процессная модель: планирование, реализация, проверка, действие (ПРПД).

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Основы управления информационной безопасностью как циклический процесс.
2. Стандарт ISO 27001. Создание и эксплуатация СУИБ. Процессная модель: планирование, реализация, проверка, действие (ПРПД).
3. Политики безопасности, управление непрерывностью бизнеса и управление безопасностью. Структура СУИБ.
4. Внедрение стандартов ISO 27001/17799 в организации.
5. Принцип приверженности руководства. Вовлечение в процесс обеспечения ИБ всех сотрудников организации.
6. Создание и эксплуатация Системы управления информационной безопасностью (СУИБ) предприятия.
7. Системный принцип.
8. Иерархический принцип.
9. SMART принцип.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – реферат.

РАЗДЕЛ 2. Основные элементы системы управления информационной безопасностью
Цель: дать знания обучающимся по базовым принципам создания системы управления информационной безопасностью.

Перечень изучаемых элементов содержания

Политики безопасности, управление непрерывностью бизнеса и управление безопасностью. Структура СУИБ.
Внедрение стандартов ISO 27001/17799 в организации.
Принцип приверженности руководства.
Вовлечение в процесс обеспечения ИБ всех сотрудников организации.
Оценка рисков. Привлечение внешних консультантов.

Вопросы для самоподготовки:
- Основы управления информационной безопасностью как циклический процесс.
- Стандарт ISO 27001. Создание и эксплуатация СУИБ. Процессная модель: планирование, реализация, проверка, действие (ПРПД).
- Политики безопасности, управление непрерывностью бизнеса и управление безопасностью. Структура СУИБ.
- Внедрение стандартов ISO 27001/17799 в организации.

- Принцип приверженности руководства. Вовлечение в процесс обеспечения ИБ всех сотрудников организации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания:

Лабораторная работа (в форме индивидуальной работы) «Схема элементов системы управления информационной безопасностью». Работа выполняется с применением MS Visio.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – сдача Лабораторной работы.

РАЗДЕЛ 3. Сетевая модель и сетевое планирование управлением информационной безопасности

Цель: дать знания обучающимся и сформировать у них навыки по разработке сетевой модели и сетевого планирования управлением информационной безопасности.

Перечень изучаемых элементов содержания

Сущность и специфика сетевой модели, сетевого графика, сетевого плана, календарно-сетевого плана.
Жизненный цикл в сетевой модели.
Метод прямого планирования в сетевой модели.
Метод обратного планирования в сетевой модели.
Раннее и позднее начало работ, окончание работ.
Определение длительности процесса ИБ. Критический путь сетевой модели.
Индивидуальный и общий резервы.
Планирование логических связей.
Планирование ресурсов сетевой модели.

Вопросы для самоподготовки:
1. Модель СУИБ.
2. Особенности сетевых моделей СУИБ.
3. Назначение и область применения СУИБ.
4. Цели разработки, организации и внедрения СУИБ.
5. Планирование разработки, организации и внедрения СУИБ.
6. Задачи разработки, организации и внедрения СУИБ.
7. Критический путь сетевой модели.
8. Этап реализации разработки, организации и внедрения СУИБ.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: Лабораторная работа 3 (в форме индивидуальной работы) «Разработка Сетевой модели управления информационной безопасностью».

Работа выполняется с применением MS Visio.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – сдача Лабораторной работы.

РАЗДЕЛ 4. Разработка документов управления информационной безопасности

Цель: дать знания обучающимся и сформировать у них навыки по разработке документов управления информационной безопасности.

Перечень изучаемых элементов содержания

Иерархическая структура Внутренней нормативной документации предприятия по обеспечению информационной безопасности.
Состав Внутренней нормативной документации предприятия по обеспечению информационной безопасности.
Типовые регламенты и процедуры по обеспечению информационной безопасности.
Требования к Внутренней нормативной документации предприятия по обеспечению информационной безопасности со стороны бизнеса.
Требования к Внутренней нормативной документации предприятия по обеспечению информационной безопасности со стороны государственных регулирующих органов.

Вопросы для самоподготовки:

1. Разработка политик информационной безопасности.
2. «Политика управления паролями».
3. «Политика управления доступом к ресурсам корпоративной сети».
4. «Политика обеспечения ИБ при взаимодействии с сетью Интернет».
5. Международные стандарты ИБ ISO 17799, ISO 15408, ISO 13335, COBIT, ITIL, руководящие документы и рекомендации ФСТЭК и ФСБ.
6. Разработка планов обеспечения непрерывности бизнеса.
7. Меры, методы и средства сохранения (поддержания) работоспособности информационных систем организации при возникновении аварийных ситуаций.
8. Порядок работ по восстановлению процессов обработки информации в случае нарушения работоспособности информационных систем и их основных компонентов.
9. Стандарты BS 25999-1:2006, BS 25999-2:2007, BS 25999.
10. Разработка профилей защиты и заданий по безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: Лабораторная работа (в форме индивидуальной работы) «Разработка орг.структуры подразделения управления информационной безопасностью».

Работа выполняется с применением MS Visio.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – сдача Лабораторной работы.

МОДУЛЬ 2 ПРИНЦИПЫ СОЗДАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Раздел 1 Политики безопасности, управление непрерывностью бизнеса

Цель: Дать знания обучающимся по базовым принципам создания системы управления информационной безопасностью.

Перечень изучаемых элементов содержания Раздела 1

Политики безопасности, управление непрерывностью бизнеса и управление безопасностью. Структура СУИБ.
Внедрение стандартов ISO 27001/17799 в организации.
Принцип приверженности руководства.
Вовлечение в процесс обеспечения ИБ всех сотрудников организации.
Оценка рисков. Привлечение внешних консультантов.

Вопросы для самоподготовки:

1. Основы управления информационной безопасностью как циклический процесс.
2. Стандарт ISO 27001. Создание и эксплуатация СУИБ. Процессная модель: планирование, реализация, проверка, действие (ПРПД).
3. Политики безопасности, управление непрерывностью бизнеса и управление безопасностью. Структура СУИБ.
4. Внедрение стандартов ISO 27001/17799 в организации.
5. Принцип приверженности руководства. Вовлечение в процесс обеспечения ИБ всех сотрудников организации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: Лабораторная работа (в форме индивидуальной работы)
Лабораторная работа (в форме индивидуальной работы) «Разработка структуры политики информационной безопасности предприятия»

Работа выполняется с применением MS Visio.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – сдача лабораторной работы.

Раздел 2 Принципы построения системы управления информационной безопасности

Цель: Дать знания обучающимся по принципам построения системы управления информационной безопасностью.

Перечень изучаемых элементов содержания Раздела 2

- Принципы построения системы управления информационной безопасностью.
- Процессный и проектный принципы.
- Принцип синергии.
- Конвергентный подход.
- Подход ITIL\ITSM.
- Подход IBM\Rational.
- SWOT-анализ.
- Международные стандарты защиты информации (стандарты ISO).
- Национальные стандарты РФ (ГОСТы).

Вопросы для самоподготовки:

- Перечислите основные принципы построения системы управления информационной безопасностью.
- Что такое процессный принцип?
- Что такое проектный принцип?
- В чем сущность принципа синергии?
- Что такое конвергентный подход?
- Основная стратегия создания СУИБ в подходе ITIL\ITSM.
- Основная стратегия создания СУИБ в подходе IBM\Rational.

Форма практического задания: реферат.

Примерный перечень тем рефератов:

- Процессный и проектный принципы.
- Принцип синергии.
- Конвергентный подход.
- Подход ITIL\ITSM.
- Подход IBM\Rational.
- SWOT-анализ.
- Международные стандарты защиты информации (стандарты ISO).
- Национальные стандарты РФ (ГОСТы).

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – реферат.

Раздел 3 Вовлечение в процесс обеспечения ИБ всех сотрудников организации.

Цель: Дать знания обучающимся по процессу вовлечения и мотивации сотрудников предприятия на эффективное Основы управления информационной безопасностью.

Перечень изучаемых элементов содержания Раздела 3

- Основы согласования целеполагания стратегии бизнеса и стратегии информационной безопасностью.
- Роль Этического кодекса предприятия в эффективности управления информационной безопасностью.
- Отличие влияния вертикальных и горизонтальных связей в обеспечении управления информационной безопасностью.
- Процесс мотивации сотрудников на эффективное Основы управления информационной безопасностью.
- Плюсы и минусы систем DLP.
- Мероприятия по предотвращению внутренних (инсайдерских) инцидентов нарушения информационной безопасности.

Формы контроля самостоятельной работы обучающихся по Разделу 3:

Лабораторная работа (в форме индивидуальной работы) «Разработка Этического кодекса обеспечения информационной безопасности ИТ-предприятия»

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – сдача лабораторной работы.

Раздел 4. Оценка рисков.

Цель: знакомство слушателей с ролью и содержанием управления рисками информационной безопасности.

Перечень изучаемых элементов содержания

- Определение рисков информационной безопасности.
- Факторы рисков информационной безопасности.
- Переход рисков в проблемы (инциденты информационной безопасности).
- Отождествление рисков информационной безопасности.
- Качественная оценка рисков информационной безопасности.
- Перевод качественной в количественную оценку рисков информационной безопасности.
- Ранжирование рисков информационной безопасности.
- Определение стратегии реагирования на риски информационной безопасности.
- Разработка мероприятий реагирования на риски информационной безопасности.
- Мотивация персонала на упреждение инцидентов информационной безопасности и управление рисками.

Вопросы для самоподготовки:

- Что такое риски информационной безопасности?
- Что важнее управление инцидентами или управление рисками?
- В чем состоит качественная оценка рисков информационной безопасности?
- Примеры перевода качественной в количественную оценку рисков информационной безопасности.

- Метрики ранжирования рисков информационной безопасности.
- Примеры стратегий реагирования на риски информационной безопасности.
- Мероприятий минимизации отрицательных последствий рисков информационной безопасности.
- Источники финансирования управления рисков информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: реферат.

Примерный перечень тем рефератов:

- Методы оценки вероятности рисков.
- Зависимость величины рисков от фаз жизненного цикла процесса управления информационной безопасности.
- Основные функции риск-менеджера.
- Роль технологий эмпатии в предотвращении инцидентов и рисков информационной безопасности.
- DLP и управление рисками информационной безопасности.
- Оценка рисков и TQM.
- Метод Делфи.
- Технологии «Оценка-270» и «Оценка-360» в управлении рисками информационной безопасности..
- Диаграмма Ишикава анализа рисков.
- Метод Паретто.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – реферат.

МОДУЛЬ 3 РАЗРАБОТКА ДОКУМЕНТОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Раздел 1 Состав внутренней нормативной документации предприятия

Цель: Дать знания обучающимся знания и сформировать у них навыки по разработке документов управления информационной безопасности.

Перечень изучаемых элементов содержания Раздела 1.

Внутренняя нормативная документация предприятия по обеспечению информационной безопасности:

- Стратегия обеспечения информационной безопасности.
- Структура процесса обеспечения информационной безопасности.
- Положение о подсистеме управления доступом к информационным ресурсам.
- Положение о подсистеме правления паролями.
- АСКД.

- Положение о подсистеме обеспечения отражения внешних атак.
- Положение о подсистеме обеспечения защиты от внутренних инцидентов.
- Положение о подсистеме антивирусной защиты.
- Положение о подсистеме защиты ЛВС.
- Положение о подсистеме защиты аппаратно-программных комплексов.
- Положение о подсистеме вибро-акустической защиты.
- Положение о подсистеме межсетевых экранов.
- Положение о подсистеме защиты персональных данных.
- Положение о подсистеме обнаружения недекларированных свойств аппаратуры и ПО.

Вопросы для самоподготовки:

- Сущность и назначение управления доступом к информационным ресурсам.
- Сущность и назначение правления паролями.
- Сущность и назначение АСКД.
- Сущность и назначение обеспечения отражения внешних атак.
- Сущность и назначение обеспечения защиты от внутренних инцидентов.
- Сущность и назначение антивирусной защиты.
- Сущность и назначение защиты ЛВС.
- Сущность и назначение защиты аппаратно-программных комплексов.
- Сущность и назначение вибро-акустической защиты.
- Сущность и назначение межсетевых экранов.
- Сущность и назначение защиты персональных данных.
- Сущность и назначение обнаружения недекларированных свойств аппаратуры и ПО.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: Лабораторная работа (в форме индивидуальной работы) «Разработка структуры внутренней норм. документации управления информационной безопасностью».

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – сдача лабораторной работы.

Раздел 2. Типовые регламенты и процедуры по обеспечению информационной безопасности

Цель: Дать знания обучающимся по разработке типовых регламентов управления информационной безопасности.

Перечень изучаемых элементов содержания Раздела 2.

- Структура типового регламента обеспечения информационной безопасности.
- Назначение типового регламента обеспечения информационной безопасности.
- Область применения типового регламента обеспечения информационной безопасности.
- Нормативная база типового регламента обеспечения информационной безопасности.

- Ограничения и границы типового регламента обеспечения информационной безопасности.
- Содержание типового регламента обеспечения информационной безопасности.
- Ресурсы обеспечения действия типового регламента обеспечения информационной безопасности.
- Порядок внесения изменений и дополнений в регламент обеспечения информационной безопасности.

Вопросы для самоподготовки:

1. Краткое содержание общей политики информационной безопасности.
2. Структура политики управления доступом к информационным ресурсам.
3. Структура политики управления паролями.
4. «Политика управления доступом к ресурсам корпоративной сети».
5. «Политика обеспечения ИБ при взаимодействии с сетью Интернет».
6. Что такое профили защиты информационных ресурсов?
7. Назначение регламента обеспечения конфиденциальности информации на предприятии.
8. Назначение регламента обеспечения целостности информации на предприятии.
9. Назначение регламента обеспечения доступности информации на предприятии.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: Лабораторная работа (в форме индивидуальной работы) «Разработка частных политик управления информационной безопасностью».

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – сдача лабораторной работы.

Раздел 3. Иерархическая структура внутренней нормативной документации по информационной безопасности

Цель: Дать знания обучающимся по разработке структуры внутренней нормативной документации по информационной безопасности.

Перечень изучаемых элементов содержания Раздела 3:

- Введение в таксономию. Применение таксономии при разработке структуры внутренней нормативной документации по информационной безопасности.
- Стратегия обеспечения информационной безопасности предприятия и определение приоритетов защиты информации.
- Определение иерархической подчиненности регламентов и процедур обеспечения информационной безопасности, предъявляемое бизнес-процессами предприятия.
- Миссия предприятия и обеспечение информационной безопасности.
- Этический кодекс.

- Политика обеспечения информационной безопасности.
- Частные политики обеспечения информационной безопасности.
- Процессы обеспечения информационной безопасности.
- Рабочие регламенты обеспечения информационной безопасности.
- Процедуры обеспечения информационной безопасности.

Вопросы для самоподготовки:

1. Чем определяется вертикальная субординация во внутренней нормативной документации по информационной безопасности?
2. Какова связь между основными бизнес-процессами предприятия и приоритетом во внутренней нормативной документации по информационной безопасности?
3. Что такое таксономия?
4. Принципы применения таксономии в разработке структуры внутренней нормативной документации по информационной безопасности.
5. Чем определяется глубина проработки регламентов и процедур внутренней нормативной документации по информационной безопасности?
6. Приведите пример иерархической структуры внутренней нормативной документации по информационной безопасности.
7. Какова роль этического кодекса и разработке структуры внутренней нормативной документации по информационной безопасности?
8. Кто разрабатывает структуру внутренней нормативной документации по информационной безопасности?
9. Приведите пример горизонтальной структуры внутренней нормативной документации по информационной безопасности.
10. Почему в инновационной деятельности горизонтальные структуры управления информационной безопасности доминируют над вертикальными?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: Лабораторная работа (в форме индивидуальной работы) «Разработка таксономии внутренней норм. документации управления информационной безопасностью».

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – сдача лабораторной работы.

Раздел 4. Требования к внутренней нормативной документации предприятия

Цель: Дать знания обучающимся по требованиям к внутренней нормативной документации по информационной безопасности.

Перечень изучаемых элементов содержания Раздела 4:

- Требования к внутренней нормативной документации предприятия по обеспечению информационной безопасности со стороны бизнеса.
- Требования к внутренней нормативной документации предприятия по обеспечению информационной безопасности со стороны государственных регулирующих органов.
- Учет статей Конституции РФ при разработке внутренней нормативной документации по информационной безопасности (ч.1 ст. 15, ст.18, ч.3 ст.15, ч.4 ст.15, ст. 18, ст. 123, 125, ст. 19, 22, 45-54).
- Требования актов федерального законодательства, международные договоры РФ;
- Требования законов федерального уровня (включая федеральные конституционные законы, кодексы);
- Требования указов Президента РФ;
- Требования постановлений правительства РФ;
- Требования нормативные правовых актов федеральных министерств и ведомств;
- Требования нормативных правовых актов субъектов РФ, органов местного самоуправления.
- Требования международных стандартов информационной безопасности – государственные (национальные) стандарты РФ; рекомендации по стандартизации; методические указания.
- Техническое задание как документ тактических требований к системе информационной безопасности.

Вопросы для самоподготовки:

1. Какие вопросы информационной безопасности входят в сферу деятельности Комитета государственной думы по безопасности?
2. Какие вопросы информационной безопасности входят в сферу деятельности Совета безопасности России?
3. Какие вопросы информационной безопасности входят в сферу деятельности Федеральной службы по техническому и экспортному контролю (ФСТЭК)?
4. Какие вопросы информационной безопасности входят в сферу деятельности Федеральной службы безопасности России (ФСБ России)?
5. Какие вопросы информационной безопасности входят в сферу деятельности Министерства внутренних дел Российской Федерации (МВД России)?
6. Какие вопросы информационной безопасности входят в сферу деятельности Федеральной службы надзора в сфере информационных технологий и массовых коммуникаций (Роскомнадзор)?
7. Приведите пример структуры Технических требований к системе информационной безопасности.
8. Для чего применяются Технические условия в Техническом задании на систему информационной безопасности?
9. Кратное содержание ГОСТ 34.601-90, ГОСТ 34.602-90.
10. Кратное содержание ГОСТ 19.403.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: Лабораторная работа (в форме индивидуальной работы) «Разработка технического задания на систему управления информационной безопасностью».

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – сдача лабораторной работы.

МОДУЛЬ 4 ИНЖИНИРИНГ В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.

РАЗДЕЛ 1. Процедура внедрения системы управления информационной безопасностью

Цель: дать знания обучающимся и сформировать у них навыки по разработке процедуры внедрения системы управления информационной безопасностью.

Перечень изучаемых элементов содержания

Планирование внедрения системы управления информационной безопасностью.
Реализация внедрения системы управления информационной безопасностью.
Контроль и регулирование внедрения системы управления информационной безопасностью.
Анализ и завершение внедрения системы управления информационной безопасностью.
Регламенты и процедуры по внедрения системы управления информационной безопасностью.
Этапы внедрения системы управления информационной безопасностью.
Разработка Технического задания системы управления информационной безопасностью.
Разработка Эскизного проекта системы управления информационной безопасностью.
Разработка Технического проекта системы управления информационной безопасностью.
Разработка Рабочего проекта системы управления информационной безопасностью.
Разработка Интегрированного плана внедрения системы управления информационной безопасностью.
Отладка системы управления информационной безопасностью.
Пробная эксплуатация системы управления информационной безопасностью.
Доработка системы управления информационной безопасностью.
Ввод системы управления информационной безопасностью в пром.эксплуатацию.
Передача системы управления информационной безопасностью группе сопровождения.

Вопросы для самоподготовки:

1. Этапы внедрения системы управления информационной безопасностью.
2. Предварительный аудит СУИБ
3. Детальный план мероприятий по подготовке к сертификации, оценка информационных рисков, анализ расхождений с требованиями стандарта
4. Планирование и внедрение недостающих механизмов контроля, разработка стратегии и плана внедрения.
5. Работы по внедрению механизмов контроля: подготовка сотрудников организации, обучение, тренинги, повышение осведомленности;
6. Подготовка документации СУИБ: политики, стандарты, процедуры, регламенты, инструкции, планы;

7. Подготовка свидетельств функционирования СУИБ: отчеты, протоколы, приказы, записи, журналы событий.
8. Международные стандарты ИБ ISO 17799, ISO 15408, ISO 13335, COBIT, ITIL
9. Руководящие документы и рекомендации ФСТЭК и ФСБ.
10. Что представляет собой «Акт сдачи-приемки системы управления информационной безопасностью в эксплуатацию»?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторная работа (в форме индивидуальной работы) «Разработка Плана процедуры внедрения системы управления информационной безопасностью».

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – сдача лабораторной работы.

РАЗДЕЛ 2. Инжиниринг внутренних нормативных документов и процесса управления информационной безопасностью

Цель: дать знания обучающимся в области инжиниринга управления информационной безопасностью.

Перечень изучаемых элементов содержания
Планирование инжиниринга управления информационной безопасностью.
Реализация инжиниринга управления информационной безопасностью.
Контроль и регулирование инжиниринга управления информационной безопасностью.
Анализ и завершение инжиниринга управления информационной безопасностью.

Вопросы для самоподготовки:
1. Что такое инжиниринг в информационной безопасности?
2. Сущность и отличие технологий инжиниринга EPC и EPCM (Engineering, Procurement, Construction, Management).
3. Инжиниринг в пробной эксплуатации, анализе и доработке СУИБ.
4. Сдача в пром. эксплуатацию СУИБ как этап инжиниринга.
5. Что такое PDRI CII?
6. Каковы основные уровни зрелости системы управления информационной безопасностью по стандарту CMMI ESI?
7. На каких уровнях зрелости системы управления информационной безопасностью применение стандартов вредно?
8. Что является основой капитализации системы управления информационной безопасностью?
9. Чем отличается инжиниринг систем от реинжиниринга?
10. В каких случаях эффективно применение реинжиниринга системы управления информационной безопасностью?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: Лабораторная работа (в форме индивидуальной работы) «Разработка внутренней норм. документации управления информационной безопасностью».

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – сдача лабораторной работы.

РАЗДЕЛ 3. Инжиниринг организационных структур управления информационной безопасности.

Цель: дать знания обучающимся в области инжиниринга организационных структур управления информационной безопасностью.

Перечень изучаемых элементов содержания
Регламенты и процедуры инжиниринга управления информационной безопасностью.
Организация технологического процесса защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Вопросы для самоподготовки:

1. Основные нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
2. Интегральный отчет по разработке, организации и внедрения СУИБ.
3. Извлечённые уроки инжиниринга информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: Лабораторная работа (в форме индивидуальной работы) «Разработка структуры подразделения управления информационной безопасностью».

Примерный перечень тем рефератов:

1. Пример исследования эффективности СЗИ с использованием морфологической матрицы.
2. Модель процесса защиты информации предприятия.
3. Оценка альтернативных проектов организации СЗИ с использованием критериального метода.
4. Оценка альтернативных проектов организации СЗИ с использованием метода парных сравнений.
5. Перспективные направления в организации и управлении системой защиты информации на предприятии.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – сдача лабораторной работы.

Оформление работ, выполняемых в рамках самостоятельной работы осуществляется в соответствии с Методическими указаниями по оформлению письменных работ обучающихся в рамках самостоятельной работы, утвержденными Учебно-методическим советом РГСУ, Протокол № 2 от 25 июня 2015 года.

Конкретные практические задания и задания для рубежного контроля определяются в учебно-методических материалах по работе обучающихся в электронной информационно-образовательной среде РГСУ с применением технологий электронного обучения по данной дисциплине, утверждаемых ежегодно.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по дисциплине (модулю) является **зачет / экзамен,** которые проводятся в **устной** форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	Знать: технические каналы утечки информации,организацию защиты информации от утечки по техническим каналам, основные характеристики и принципы построения средств защиты информации от утечки по техническим каналам	Этап формирования знаний
		Уметь: проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем	Этап формирования умений
		Владеть: методами проектирования и	Этап формирования навыков и получения опыта

		навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности	
ОПК-2.2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	Знать: основные методы администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем	Этап формирования знаний
		Уметь: администрировать средства и системы защиты информации автоматизированных систем	Этап формирования умений
		Владеть: навыками контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем	Этап формирования навыков и получения опыта
ПК-3	Способен администрировать подсистемы информационной безопасности объекта защиты	**Знать:** - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ - основы администрирования вычислительных сетей - системы управления БД - эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности - основные направления политик защиты информации на предприятии (организации) - возможные угрозы	Этап формирования знаний

		информационной безопасности, связанные с аспектами деятельности предприятия (организации), особенностями технологических процессов, организационной структуры и др.	
		Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействиия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты - выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Этап формирования умений
		Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Этап формирования навыков и получения опыта
ПК-9	способностью осуществлять	**Знать:**	Этап формирования

	подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	нормативные документы для обоснования безопасности информационных систем, отечественные и зарубежные стандарты оценки защищенности информационных систем, источники информации по проблематике информационной безопасности	знаний
		Уметь: -осуществлять информационный поиск и дифференцированный анализ -собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источниках	Этап формирования умений
		Владеть: - навыками работы с нормативными правовыми актами; навыками сбора и обработки необходимых данных - навыками анализа и интерпретации информации, содержащейся в различных отечественных и зарубежных источниках, в том числе с использованием электронных журналов и библиотек	Этап формирования навыков и получения опыта
ПК-10	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать:** требования к оформлению рабочей технической документации с учетом действующих нормативных и методических документов	Этап формирования знаний
		Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Этап формирования умений
		Владеть: инструментами и технологиями оформления рабочей технической	Этап формирования навыков и получения опыта

		документации	
ПК-13	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	**Знать:** методы проведения экспериментов в области защиты информации	Этап формирования знаний
		Уметь: проводить обработку, оценку погрешности и достоверности их результатов экспериментов в области защиты информации	Этап формирования умений
		Владеть: организационными и техническими навыками по проведению экспериментов в области защиты информации	Этап формирования навыков и получения опыта
ПК-14	способность принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать:** проведение экспериментальных исследований системы защиты информации	Этап формирования знаний
		Уметь: принимать участие в проведении экспериментальных исследований системы защиты информации	Этап формирования умений
		Владеть: проведение экспериментальных исследований системы защиты информации	Этап формирования навыков и получения опыта
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю России.	Этап формирования знаний
		Уметь: организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной	Этап формирования умений

		службы по техническому и экспортному контролю	
		Владеть: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Этап формирования навыков и получения опыта

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	**Этапы формирования компетенций**	**Показатель оценивания компетенции**	**Критерии и шкалы оценивания**
ОПК-10, ОПК-2.2, ПК-3, ПК-9, ПК-10, ПК-13, ПК-14, ПК-15	Этап формирования знаний	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в

			изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.
ОПК-10, ОПК-2.2, ПК-3, ПК-9, ПК-10, ПК-13, ПК-14, ПК-15	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией - 9-10 баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании -7-8 баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению5-6 баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания - 0-4 баллов.
ОПК-10, ОПК-2.2, ПК-3, ПК-9, ПК-10, ПК-13, ПК-14, ПК-15	Этап формирования навыков и получения опыта	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

4.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Теоретический блок вопросов:

1. Основы управления информационной безопасностью как циклический процесс.
2. Стандарт ISO 27001. Создание и эксплуатация СУИБ. Процессная модель: планирование, реализация, проверка, действие (ПРПД).
3. Политики безопасности, управление непрерывностью бизнеса и управление безопасностью. Структура СУИБ.
4. Внедрение стандартов ISO 27001/17799 в организации.
5. Принцип приверженности руководства. Вовлечение в процесс обеспечения ИБ всех сотрудников организации.
6. Создание и эксплуатация Системы управления информационной безопасностью (СУИБ) предприятия.
7. Системный принцип.
8. Иерархический принцип.
9. SMART принцип.
10. Процессный принцип.
11. Проектный принцип.
12. Принцип синергии.
13. Конвергентный подход.
14. Подход ITIL\ITSM.
15. Подход IBM\Rational.
16. SWOT-анализ.
17. Международные стандарты защиты информации (стандарты ISO).
18. Национальные стандарты РФ (ГОСТы).
19. Руководящие документы ГосТех Комиссии РФ, ФСТЭК, ФСБ, Совета Безопасности РФ.
20. Плюсы и минусы применения стандартов.
21. Внутренняя нормативная документация предприятия в области защиты информации.
22. Политики управления информационной безопасности как составная часть Политики безопасности управления бизнесом и управления безопасностью предприятия.
23. Подготовительный этап разработки, организации и внедрения СУИБ.
24. Назначение и область применения СУИБ.
25. Цели разработки, организации и внедрения СУИБ.
26. Планирование разработки, организации и внедрения СУИБ.
27. Задачи разработки, организации и внедрения СУИБ.
28. Этап реализации разработки, организации и внедрения СУИБ.
29. Пробная эксплуатация, анализ и доработка СУИБ.
30. Сдача в пром. Эксплуатацию СУИБ.
31. Интегральный отчет по разработке, организации и внедрения СУИБ. Извлечённые уроки.
32. Управление содержанием защиты информации на предприятии.
33. Управление интеграцией защиты информации на предприятии.
34. Управление рисками.
35. Управление коммуникациями.
36. Управление затратами.
37. Управление информационными ресурсами.
38. Управление временем и документооборотом.
39. Управление качеством.
40. Общая модель Системы управления информационной безопасностью предприятия.
41. Объекты защиты.

42. Субъекты защиты.
43. Процесс защиты.
44. Методологии, онтологии и инструменты моделирования СУИБ.
45. Сетевая модель.
46. Календарно-сетевое планирование.
47. Диаграмма Гантта.
48. Политика безопасности предприятия.
49. Особенности моделирования сложных организационно-технических систем.
50. Этический кодекс.
51. Политика управления информационной безопасностью.
52. Регламенты и процедуры системы комплексной защиты информации на предприятии.
53. Формирование группы эксплуатации системы комплексной защиты информации на предприятии.
54. Генерирование множества альтернатив с применением экспертных методов при разработке Систем Защиты Информации (СЗИ).
55. Пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.
56. Пример исследования эффективности СЗИ с использованием морфологической матрицы.
57. Модель процесса защиты информации предприятия.
58. Оценка альтернативных проектов организации СЗИ с использованием критериального метода.
59. Оценка альтернативных проектов организации СЗИ с использованием метода парных сравнений.
60. Перспективные направления в организации и управлении системой защиты информации на предприятии.

4.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестации по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по дисциплине (модулю) выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля)

5.1.1. Основная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: ***https://www.biblio-online.ru/bcode/434171***

5.1.2. Дополнительная литература

1. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

5.2.1. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Безопасность информационных технологий– наша профессия.- Режим доступа: http://www.cbi-info.ru
2. Комплексное обеспечение информационной безопасности.- Режим доступа: www.npo-echelon.ru
3. Научно-технический центр ЕВРААС.- Режим доступа: http://www.evraas.ru
4. Создание систем инженерно-технической защиты (СИТЗ) объектов.- Режим доступа: http://www.jsc-amulet.ru
5. Технические системы обеспечения безопасности.- Режим доступа: http://www.nelk.ru
6. CMMI® for Development, Version 1.2: http://www.sei.cmu.edu/cmmi/models/models.html.
7. Сайт проекта Eclipse Process Framework: http://www.eclipse.org/epf.
8. Технология MSF: http://www.microsoft.com/rus/msdn/msf/default.mspx

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) «Основы управления информационной безопасностью» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины (модуля) . Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс

предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

5.4. Информационно-технологическое обеспечение образовательного процесса по дисциплине (модулю)

5.4.1. Информационные технологии

1. Персональные компьютеры;
2. Доступ к Интернет
3. Проектор.

При изучении дисциплины (модуля) «Основы управления информационной безопасностью» используются современные информационные технологии такие как:

- онтологии в ИТ;
- таксономические методы работы с информацией, информационными потоками, процессами, системами;
- современные технологии защит информации;
- технологии ITIL\ITSM, IBM Rational; FSM; PJM ORECLE; ICB IPMA;
- процессные технологии;
- технологии управления проектами, программами и портфелями.

В процессе проведения лабораторных работ по дисциплине (модулю) «Основы управления информационной безопасностью» используются ПО из расширенного профессионального пакета MS: MS VISIO, MS Project.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.5. Информационные справочные системы и профессиональные базы данных

Обучающиеся по программе **«Информационная безопасность»** в университете имеют доступ к следующим современным профессиональным базам данных, информационным справочникам:

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная	Библиотека предоставляет доступ более чем	https://grebennikon.ru

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	библиотека «Grebennikon»	к 30 журналам, выпускаемых Издательским домом "Гребенников".	

5.6. Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) **«Основы управления информационной безопасностью»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки **10.03.01 Информационная безопасность** используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

По всем темам проводятся лабораторные занятия в лаборатории, оснащенной специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет), а также специализированным лабораторным оборудованием (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением)

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.7. Образовательные технологии

Освоение дисциплины (модуля) **«Основы управления информационной безопасностью»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме компьютерных симуляций в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

В рамках дисциплины (модуля) **«Основы управления информационной безопасностью»** предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

«УТВЕРЖДАЮ»

Декан факультета информационных технологий

_____ /С.В. Крапивка/

«06»___июня___2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технология защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022

Рабочая программа дисциплины (модуля) **«Сети и системы передачи информации»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки **10.03.01 Информационная безопасность (уровень бакалавриата)**, утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*

– *06.032 Специалист по безопасности компьютерных систем и сетей*

– *06.033 Специалист по защите информации в автоматизированных системах*

06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля) разработана рабочей группой в составе:
д.т.н., профессор Неизестный С.И.., к.т.н. Симонов В.Л.

Руководитель основной профессиональной образовательной программы
к.п.н., доцент — Н.Г. Витковская

(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06_»_июня___2022 года

Декан факультета
К.п.н. доцент — С.В. Крапивка

(подпись)

Рабочая программа дисциплины (модуля) рекомендована к утверждению представителями организаций-работодателей
АО ПВП «Амулет»
зам. ген. директора по науке,
к.т.н., доцент — А.С. Мосолов

(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:
.д.т.н. , доцент, профессор кафедры информационных технологий ,
ГБОУВО Академия ГПС МЧС России*)* — С.Ю. Бутузов

(подпись)

к.ф.-м.н, доцент
кафедра прикладной математики и информатики РГСУ — Н.П. Третьяков

(подпись)

Согласовано
Научная библиотека, директор — И.Г. Маляр

(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) заключается в получении обучающимися теоретических знаний теоретических основ обработки информации с последующим применением навыков на практике, а также применение методов построения статистических моделей и интерпретации результатов в научно-исследовательской и профессиональной деятельности.

Задачи дисциплины (модуля) :

- овладение теоретическими знаниями в области управления информационными ресурсами систем и сетей;
- приобретение прикладных знаний об объектах и методах проектирования защищенных информационных системах;
- овладение навыками самостоятельного использования программных систем для проектирования информационных систем.

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы.

Учебная дисциплина «**Сети и системы передачи информации**» реализуется в базовой **части** основной профессиональной образовательной программой высшего образования «Информационная безопасность» по направлению10.03.01 Информационная безопасность (уровень бакалавриата) очной формы обучения.

Изучение дисциплины (модуля) «Сети и системы передачи информации» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала учебных дисциплин: «Информатика и информационные технологии в правоохранительной деятельности», «Базы данных».

Изучение дисциплины (модуля) «Сети и системы передачи информации» является базовым для последующего освоения программного материала дисциплины «Проектирование и документирование систем информационной безопасности», «Управление службой защиты информации на предприятии», а также написания выпускной квалификационной работы.

1.3. Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основной профессиональной образовательной программы.

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих профессиональных компетенций ОПК-5, ОПК-7, ОПК-11, ПК-2, ПК-9, ПК-14 в соответствии с основной профессиональной образовательной программой высшего образования Информационная безопасность по специальности 10.03.01 Информационная безопасность (уровень бакалавриата).

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	**Код компе**	**Формулировка компетенции**	**Код и наименование индикатора**	**Результаты обучения**

	тенции		**достижения компетенции**	
	ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-5.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-5.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Знать: состав и содержание Российских и международных нормативных правовых актов, нормативных и методических документов, межгосударственных и международных стандартов, регламентирующих деятельность по защите информации
				Уметь: применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации
				Знать: методами поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации

	ОПК-7	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-7.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-7.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	*Знать:* основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий. *Уметь:* применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ.

				Владеть: навыками программирования, отладки и тестирования прототипов программно-технических комплексов задач.
	ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ОПК-11.ИД-2. Планирует и выполняет практические действия в рамках компетенции ОПК-11.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - основы электроники - основные физические законы, явления и процессы, на которых основаны принципы действия объектов профессиональной деятельности
				Уметь: использовать для решения прикладных задач соответствующий аппарат
				Владеть: методами решения типовых задач в рамках профессиональной деятельности
	ПК-2	Способен применять программные средства системного, прикладного и специального	ПК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических	**Знать:** - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ

		назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	действий в рамках компетенции ПК-2.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	- основы администрирования вычислительных сетей - системы управления БД
				Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
				Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации

	ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-9.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-9.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-9.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах.

				Уметь: проводить аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации.

				Владеть: современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации.
	ПК-14	Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	ПК-14.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-14.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-14.ИД-3. Применяет методы анализа практической	**Знать:** - сущность и содержание работы исполнителей - виды управленческих решений в области организации работ по проекту и нормированию труда - особенности процесса организации работы исполнителей **Уметь:** - анализировать содержание работы исполнителей - разрабатывать, анализировать и оценивать необходимость применения различных форм работы - разрабатывать план по реализации управленческих решений в области

			деятельности и ее результатов в рамках компетенции	организации работ по проекту и нормированию труда навыками
				Владеть: - навыками анализа и установления форм и направлений деятельности в работе исполнителей - навыками оценки труда исполнителей - навыками разработки плана реализации управленческих решений в области организации работ по проекту и нормированию труда

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем дисциплины (модуля) , включая контактную работу обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 6 зачетных единиц.

Вид учебной работы	**Всего часов**	**Семестры**				
		5	6			
Контактная работа обучающихся с педагогическими работниками	**108**	**54**	**54**			
Учебные занятия лекционного типа	24	12	12			
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	36	18	18			
из них: в форме практической подготовки						
Иная контактная работа	48	24	24			
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**36**	**18**	**18**			
из них: в форме практической подготовки	*6*	*3*	*3*			
Контроль промежуточной аттестации	**72**	**36**	**36**			
Форма промежуточной аттестации		экзам	экзам			
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**216**	**108**	**108**			

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	Виды учебной работы, академических часов											
	Всего	**Самостоятельная работа**	*из них: в форме практической подготовки*	**Контактная работа обучающихся с педагогическими работниками**								
				Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*
Модуль 1 (семестр 5)													
Раздел 1.1	24	6	*1*	18		4				6		8	
Раздел 1.2	24	6	*1*	18		4				6		8	
Раздел 1.3	24	6	*1*	18		4				6		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**108**	**18**	***3***	**54**		**12**				**18**		**24**	
Форма промежуточной аттестации	**экзамен**												
Модуль 2 (семестр 6)													
Раздел 2.1	24	6	*1*	18		4				6		8	
Раздел 2.2	24	6	*1*	18		4				6		8	
Раздел 2.3	24	6	*1*	18		4				6		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**108**	**18**	***3***	**54**		**12**				**18**		**24**	

Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**216**	**36**	***6***	**108**		**24**				**36**		**48**	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1. Виды самостоятельной работы обучающихся по дисциплине (модулю)

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**
Модуль 1 (семестр 5)							
Раздел 1.1	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**18**	**6**		**6**		**6**	
Модуль 2 (семестр 6)							

Раздел 2.1	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.3	6	2	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	2	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**18**	**6**		**6**		**6**	
Общий объем по дисциплине (модулю), часов	**36**	**12**		**12**		**12**	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю)

Модуль 1

Раздел 1.1 Средства информационных процессов и систем

Раздел 1.2. Логические основы вычислительной техники

Цель: заключается в получении обучающимися теоретических знаний в области теории информационных процессов и систем с последующим применением в профессиональной сфере и практических навыков построении и реализации информационных систем на основе современных методологий и стандартов.

Перечень изучаемых элементов содержания:

Применение булевой алгебры при анализе и синтезе узлов и при организации вычислений. Законы алгебры логики. Алгоритмы анализа и минимизации электрических схем аппаратных средств. Оценка сложности комбинационных схем. Анализ и синтез электронных схем в различных базисах: (И, ИЛИ, НЕ), (И-НЕ), (ИЛИ-НЕ). «Физические основы вычислительной техники»: конструктивные и функциональные модули ЭВМ. Техническая реализация элементарных функций

Вопросы для самоподготовки:

1. Применение булевой алгебры при анализе и синтезе узлов и при организации вычислений.
2. Законы алгебры логики.

3. Алгоритмы анализа и минимизации электрических схем аппаратных средств. Оценка сложности комбинационных схем.
4. Анализ и синтез электронных схем в различных базисах: (И, ИЛИ, НЕ), (И-НЕ), (ИЛИ-НЕ).
5. Конструктивные и функциональные модули.
6. Техническая реализация элементарных функций.
7. Конструктивные и функциональные модули.
8. Техническая реализация элементарных функций.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: расчетное практическое задание

Выполнение расчетного практического задания сводится к выполнению математических расчетов по заранее определенному алгоритму.

При подготовке отчета следует придерживаться следующей структуры:
титульный лист (в соответствии с шаблоном);
условие задачи;
обоснование выбранного алгоритма;
проведение расчетов;
обсуждение результатов.

Задание 1. Вычислить логические выражения. Среди предложенных результатов (Y1 ÷ Y4) указать правильный.

Вариант 1
выражение 1
y = NOT ((&H23 IMP 23) AND &H5) IMP &O13
Y1=1111111111111010 Y2=101 Y3=1111 Y4=1111111111011111
выражение 2
y = (36 EQV &H29 EQV NOT 20) AND &H16
Y1=1111111111100110 Y2=1111111111101011 Y3=110 Y4=1111111111110010

Вариант 2
выражение 1
y = NOT NOT (&O47 EQV &O10 EQV 17) IMP &O0
Y1=111110 Y2=1111111111000001 Y3=111110 Y4=10001
выражение 2
y = 21 OR (&O45 EQV NOT (&O11 AND &H24))
Y1=1111111111111111 Y2=0 Y3=110101 Y4=1001

Вариант 3
выражение 1
y = ((&O53 XOR &H4) OR &H29) AND 17
Y1=101111 Y2=1 Y3=101111 Y4=100
выражение 2
y = (&HD EQV &H8) OR NOT NOT (2 OR &O55)
Y1=1111111111010000 Y2=101111 Y3=101101 Y4=1111111111111111

Вариант 4
выражение 1
y = 15 EQV (&O55 IMP (&O32 IMP 3))
Y1=111 Y2=11 Y3=11010 Y4=101101
выражение 2
y = (&O22 EQV (NOT &O0 IMP &H20)) OR NOT 7
Y1=1111111111111101 Y2=1111111111001101 Y3=100000 Y4=100000

Вариант 5

выражение 1
y = &H18 XOR &H14 EQV &H1A IMP &O14
Y1=11110 Y2=11010 Y3=1100 Y4=10100
выражение 2
y = NOT (&O42 XOR &H1C IMP 30) OR &H17
Y1=100000 Y2=1111111111011111 Y3=110111 Y4=111110

Вариант 6

выражение 1
y = (&H1A OR &H23) AND &O54 AND &O21
Y1=101000 Y2=0 Y3=111011 Y4=100011
выражение 2
y = NOT (18 EQV NOT &H29 AND &H12) XOR &HC
Y1=0 Y2=1100 Y3=10010 Y4=10010

Вариант 7

выражение 1
y = (&HD OR &H15) AND &O7 EQV &O34
Y1=101 Y2=1111111111100110 Y3=11101 Y4=10101
выражение 2
y = (&H8 EQV &HD) AND 25 EQV &O50
Y1=11000 Y2=11001 Y3=1111111111111010 Y4=1111111111001111

Вариант 8

выражение 1
y = &O25 OR &H2A OR &O12 OR 7
Y1=1111 Y2=111 Y3=1010 Y4=111111
выражение 2
y = (&H2 OR &H2C IMP 39) OR 26
Y1=1111111111111111 Y2=100111 Y3=101110 Y4=101100

Вариант 9

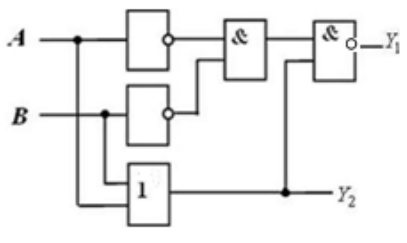
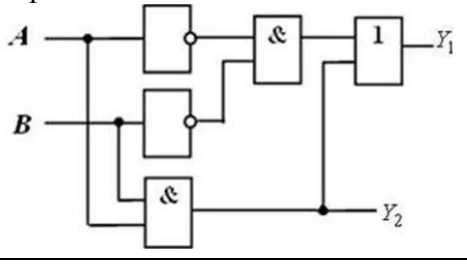
выражение 1
y = (&H4 XOR &H25) AND &O31 OR 6
Y1=1 Y2=11001 Y3=100001 Y4=111
выражение 2
y = (&O45 XOR &H2F) OR &H1D OR &O43
Y1=11111 Y2=111111 Y3=1010 Y4=101111

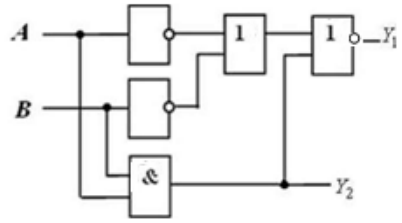
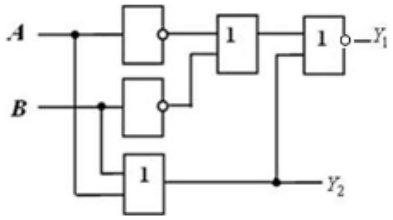
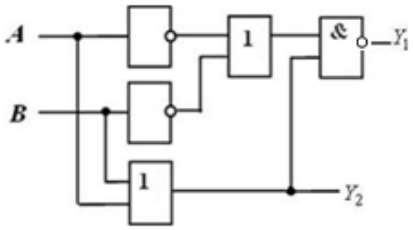
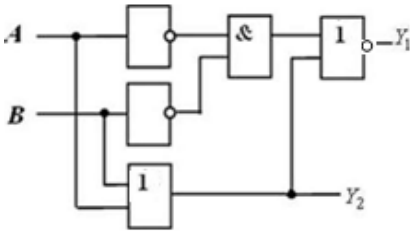
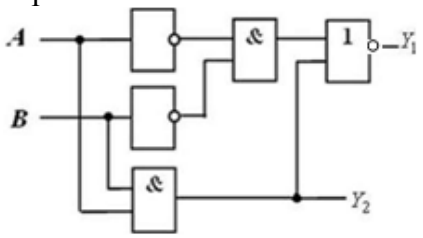
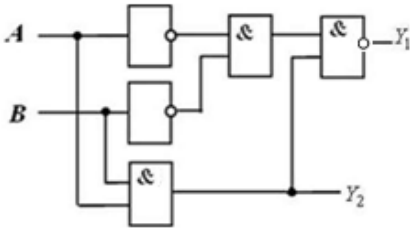
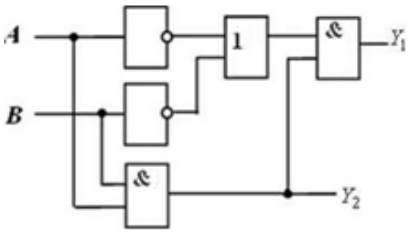
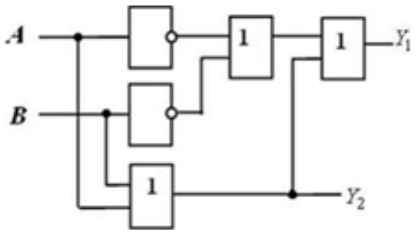
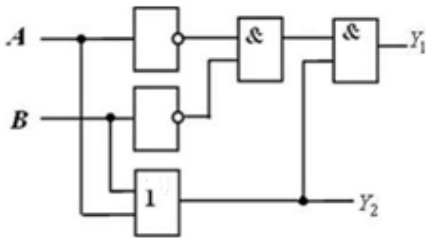
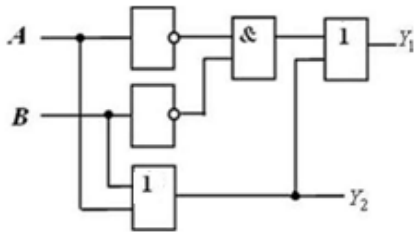
Вариант 10

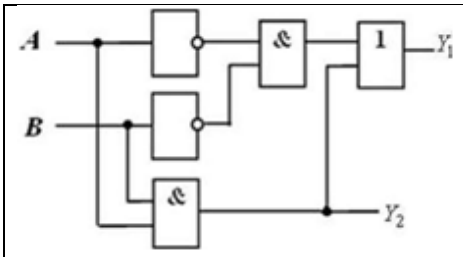
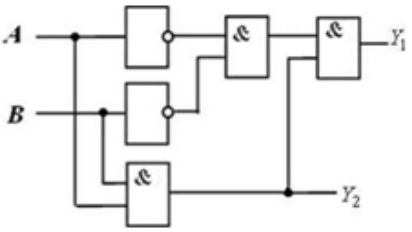
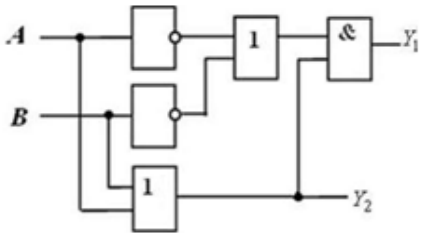
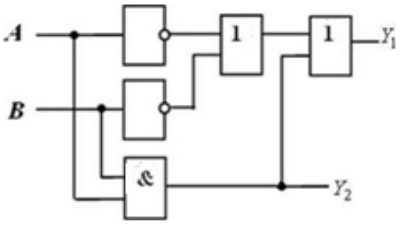
выражение 1
y = &O54 EQV &H0 EQV &H4 IMP &H12
Y1=101000 Y2=100 Y3=1111111111010011 Y4=1111111111010111
выражение 2
y = (&O54 EQV 43) OR &O41 OR &O13
Y1=1111111111111001 Y2=1111111111111011 Y3=111111111111100 Y4=101011

Логические схемы

Задание 1. По логической схеме составить логическую функцию

Вариант 1	Вариант 9
	

Вариант 2 	Вариант 10 
Вариант 3 	Вариант 11 
Вариант 4 	Вариант 12 
Вариант 5 	Вариант 13 
Вариант 6 	Вариант 14 
Вариант 7	Вариант 15

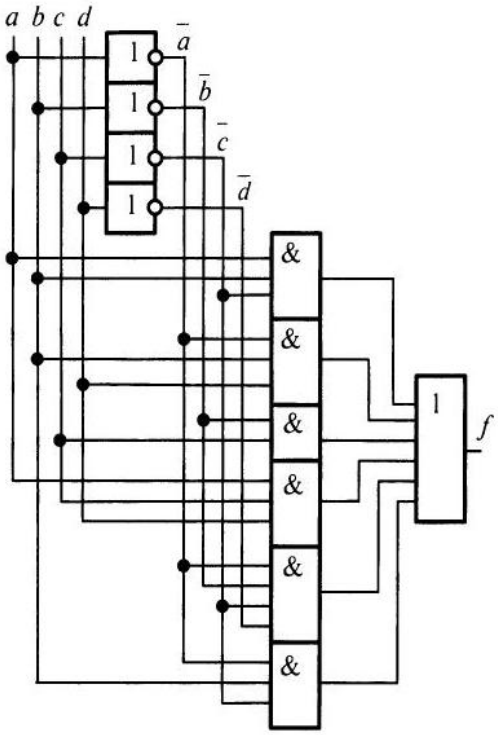
	
Вариант 8 	Вариант 16 

Задание 2. По логической функции составить логическую схему

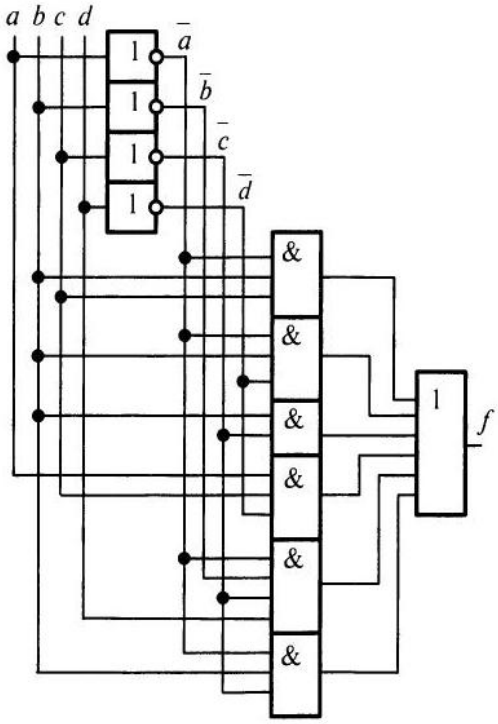
Вариант 1 а) $F = A \& \overline{B}$;	Вариант 9 а) $F = \overline{A \& \overline{B}}$;
Вариант 2 а) $F = \overline{A \& C}$;	Вариант 10 а) $F = \overline{\overline{A} \& \overline{B}}$;
Вариант 3 а) $F = \overline{A} \& \overline{B}$;	Вариант 11 а) $F = \overline{A} \& B$;
Вариант 4 а) $F = \overline{\overline{A} \& B}$;	Вариант 12 а) $F = A + \overline{B}$;
Вариант 5 а) $F = \overline{A + C}$;	Вариант 13 а) $F = \overline{A} + \overline{B}$;
Вариант 6 а) $F = \overline{A + \overline{B}}$;	Вариант 14 а) $F = \overline{\overline{A} + \overline{B}}$;
Вариант 7 а) $F = \overline{\overline{A} + B}$;	Вариант 15 а) $F = \overline{A} + B$;
Вариант 8 а) $F = \overline{A} + A$;	Вариант 16 а) $F = \overline{\overline{A} \& A}$;

Задание 3. Минимизировать заданную логическую схему и написать соответствующую каноническую сумму минтермов.

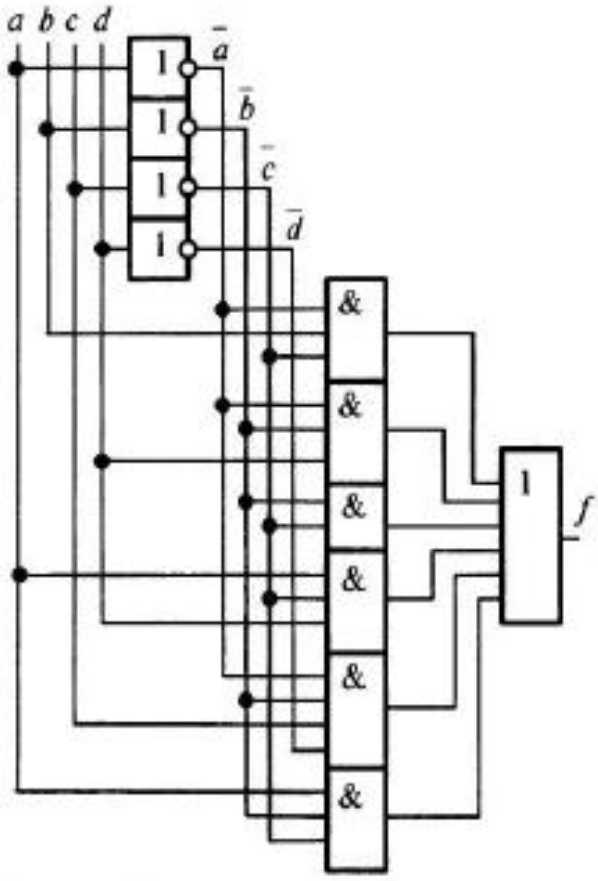
Вариант 1	Вариант 9



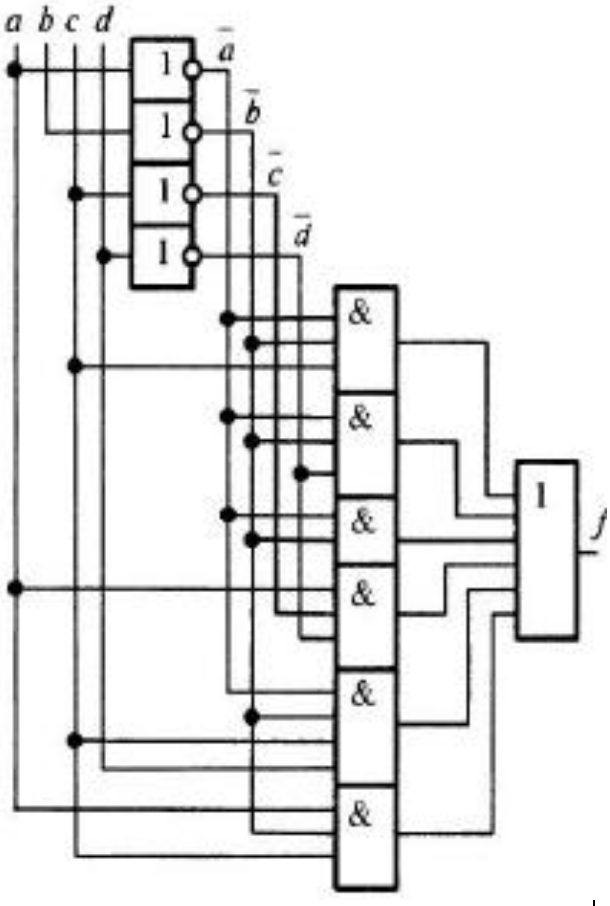
Вариант 2



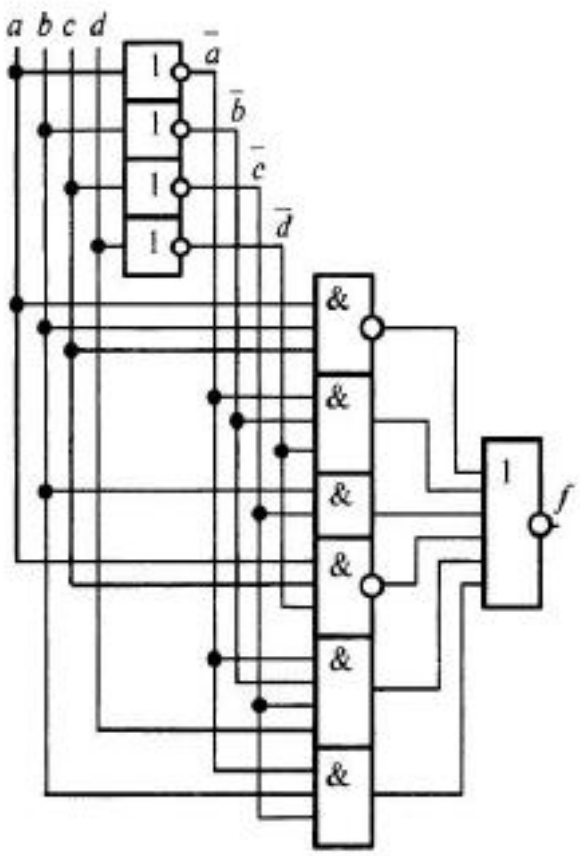
Вариант 10



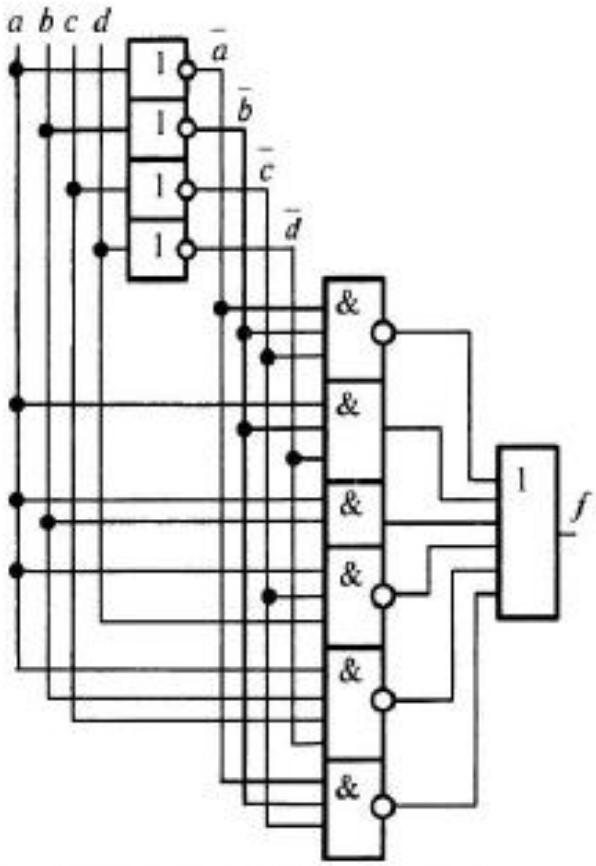
Вариант 3



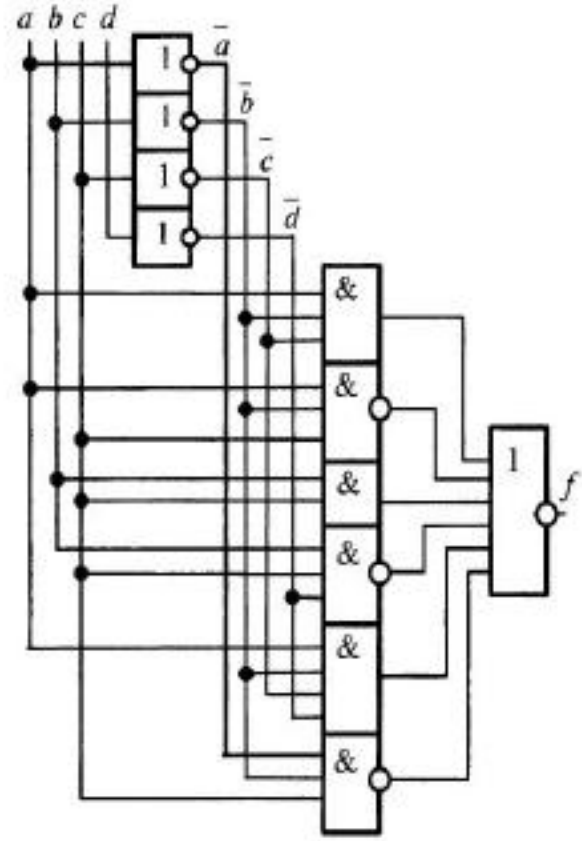
Вариант 11



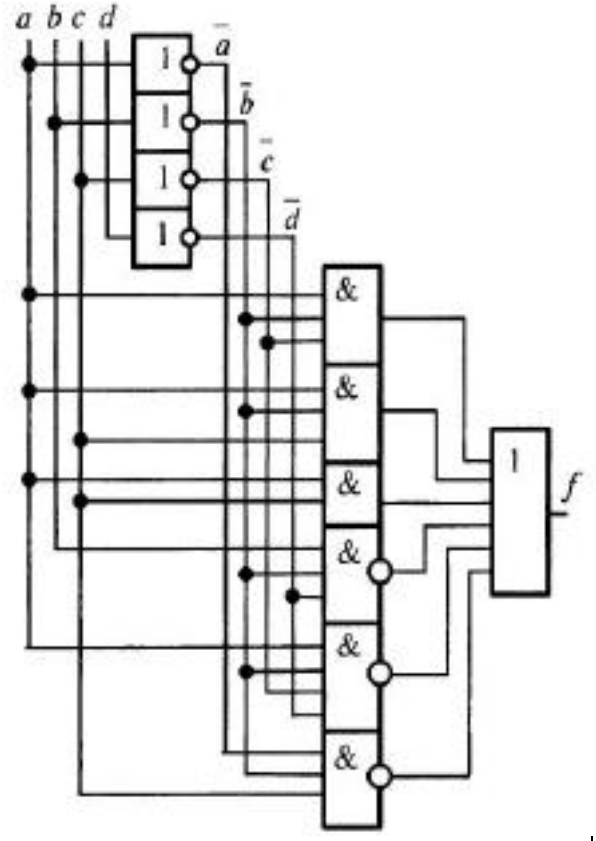
Вариант 4



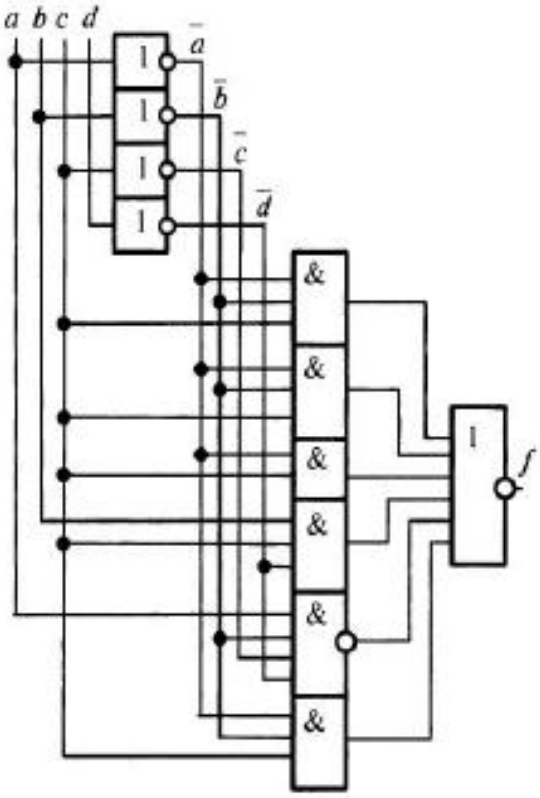
Вариант 12



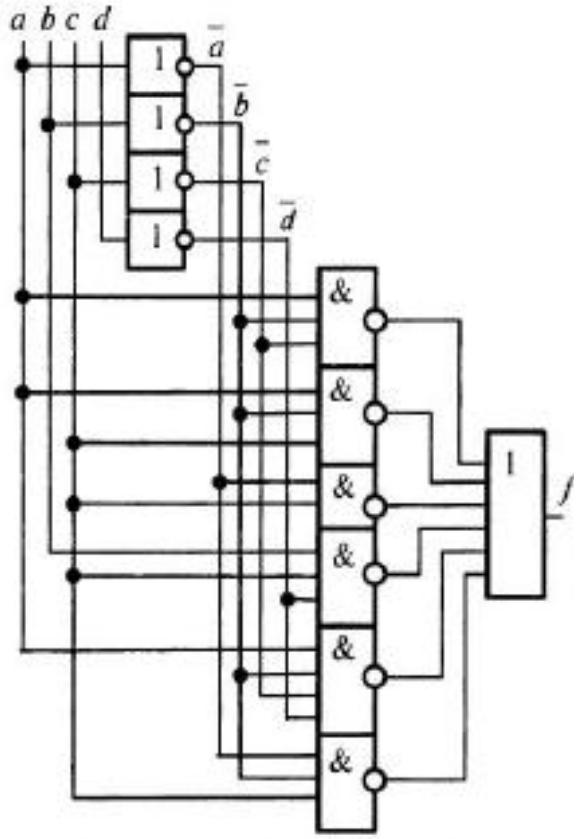
Вариант 5



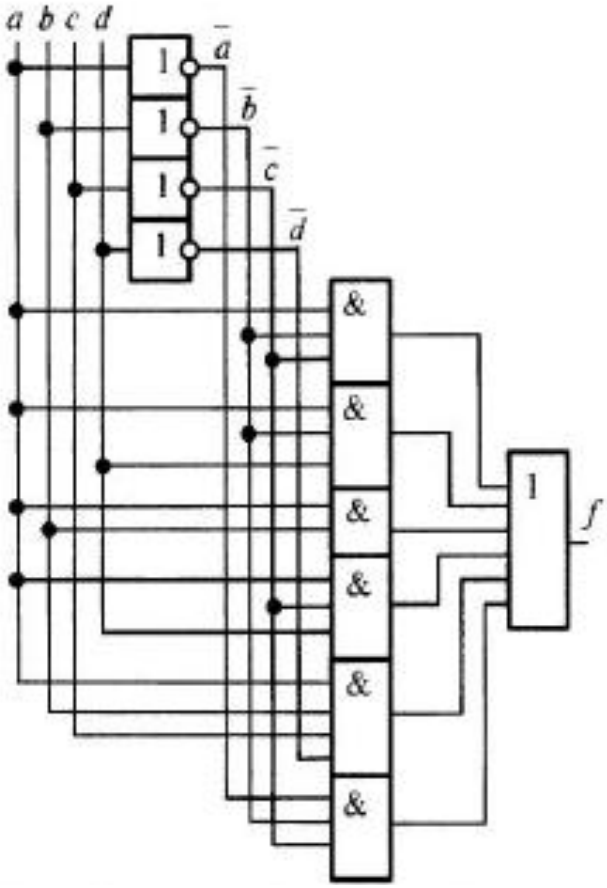
Вариант 13



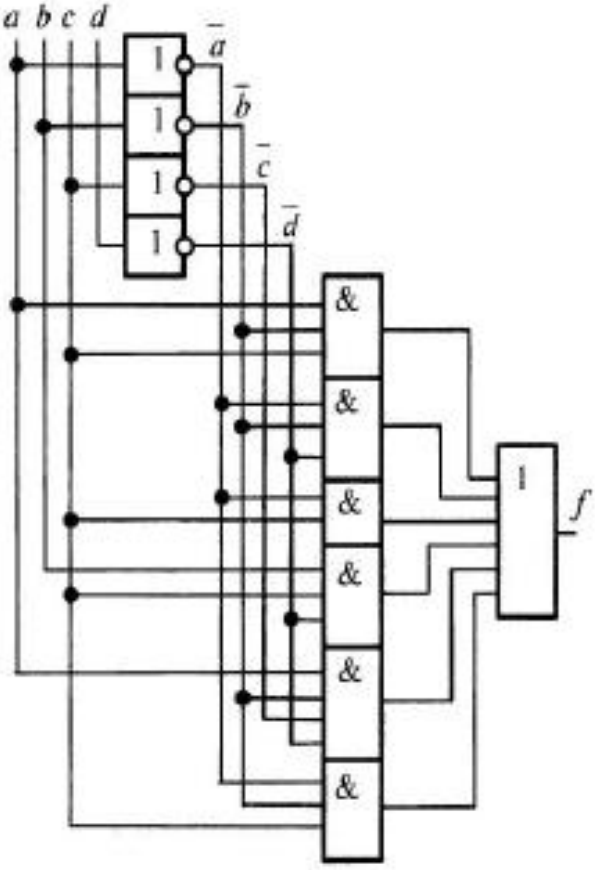
Вариант 6



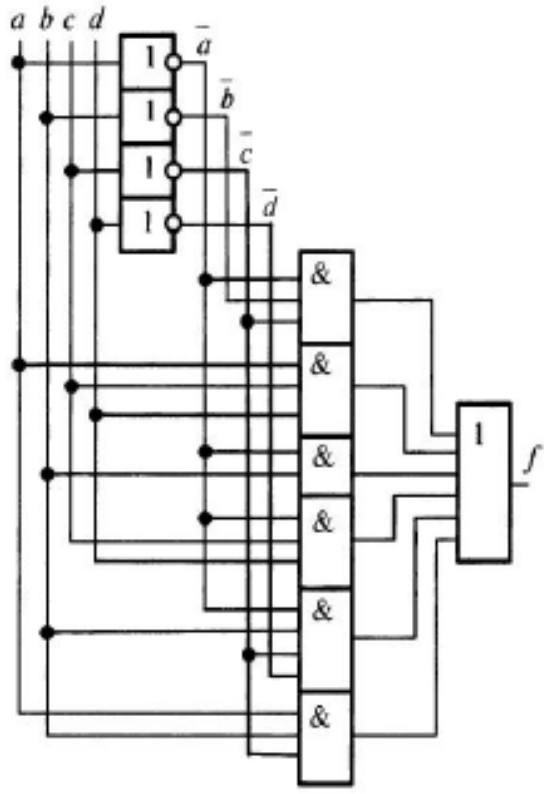
Вариант 14

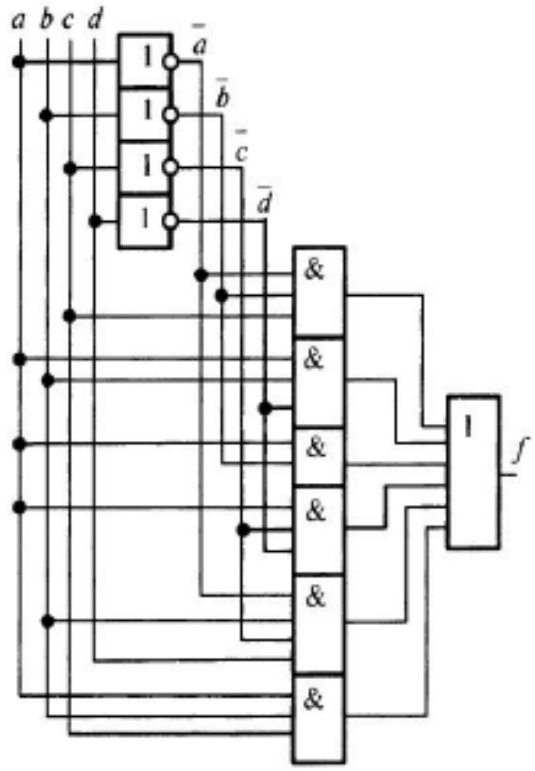


Вариант 7

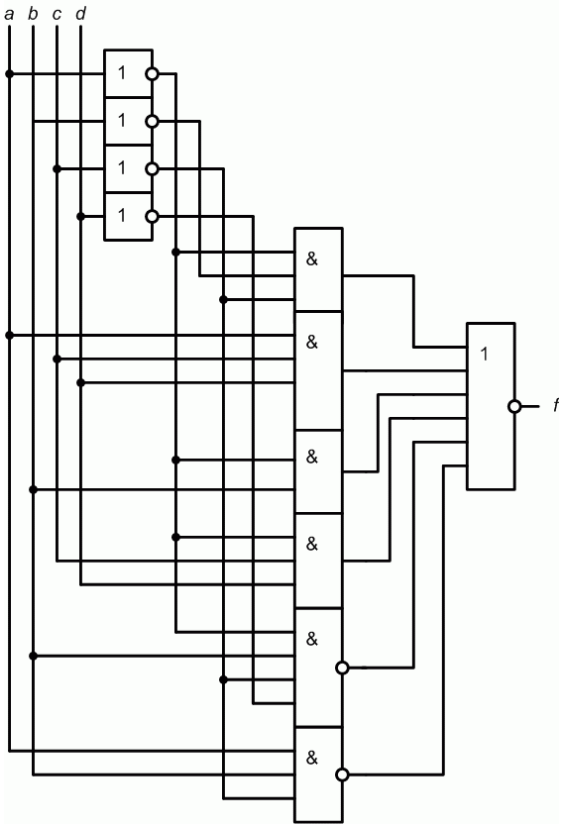


Вариант 15

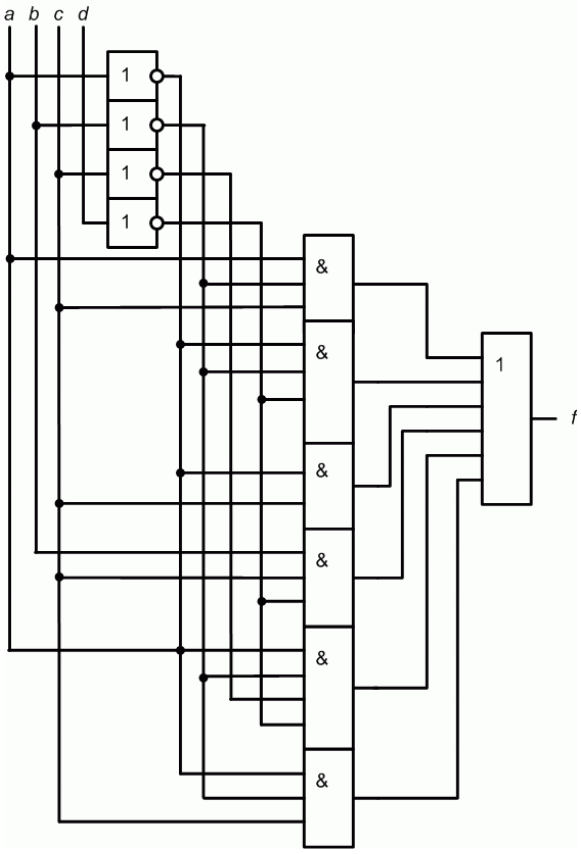




Вариант 8



Вариант 16



Цель: заключается в получении обучающимися теоретических знаний в области теории информационных процессов и систем с последующим применением в профессиональной сфере и практических навыков построении и реализации информационных систем на основе современных методологий и стандартов .

Перечень изучаемых элементов содержания: основные характеристики, сравнение параметров. Классификация элементов ВМ, их реализация в различных технологиях. «Аппаратные средства комбинационного типа»: классификация узлов ЭВМ. Виды и схемная реализация типовых узлов комбинационного и накапливающего типа. Назначение, виды и обозначение шифраторов, дешифраторов, сумматоров, схем сравнения, мультиплексоров. «Основы построения и функционирования устройств с памятью»: особенности анализа и синтеза элементов с памятью. Понятие триггера (RS, JK, T), их содержательное и математическое описание, схемная реализация. Назначение, виды и обозначение счетчиков, регистров.

Вопросы для самоподготовки:

1. Интегральные микросхемы: основные характеристики, сравнение параметров.
2. Классификация элементов ВМ, их реализация в различных технологиях.
3. Классификация узлов ЭВМ. Виды и схемная реализация типовых узлов комбинационного и накапливающего типа. Назначение, виды и обозначение шифраторов, дешифраторов, сумматоров, схем сравнения, мультиплексоров.
4. Основы построения и функционирования устройств с памятью: особенности анализа и синтеза элементов с памятью.
5. Понятие триггера (RS, JK, T), их содержательное и математическое описание, схемная реализация. Назначение, виды и обозначение счетчиков, регистров.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: расчетное практическое задание

Выполнение расчетного практического задания сводится к выполнению математических расчетов по заранее определенному алгоритму.

При подготовке отчета следует придерживаться следующей структуры:
титульный лист (в соответствии с шаблоном);
условие задачи;
обоснование выбранного алгоритма;
проведение расчетов;
обсуждение результатов.

Моделирование простейших логических схем

Таблица истинности для задания определяется датой дня рождения студента. Для этого необходимо дату представить в формате ДД:ММ:Гг.

Десятилетие Г исключается (просто откидывается). В результате получаем ДДММг. Полученное число нужно перевести в двоичный формат представления данных. Результат необходимо дополнить до 16 разрядов дописав перед числом необходимое количество нулей.

Пример:

Дата 03.04.20. Отбрасываем «2» получаем **03040**. Переводим в двоичную систему счисления. Результат – 1011 1110 0000. Дополняем до 16-ти разрядов нулями в старших порядках. В итоге получим

0000 1011 1110 0000 – это и будет результирующая логическая функция.

X_3	X_2	X_1	X_0	f
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	1
0	1	0	1	0
0	1	1	0	1
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Таблица 1. Сформированный вариант задания студента

Задание

1. Реализовать полученную функцию на логических элементах

Задание 1.

В результирующей логической функции количество единиц меньше, чем нулей. Поэтому рационально использовать **совершенную дизъюнктивную нормальную форму** (СДНФ), в противном случае использовать **совершенную конъюнктивную нормальную форму** (СКНФ).

$f(x_3, x_2, x_1, x_0)=\overline{x_3}\cdot x_2\cdot\overline{x_1}\cdot\overline{x_0} + \overline{x_3}\cdot x_2\cdot x_1\cdot\overline{x_0} + \overline{x_3}\cdot x_2\cdot x_1\cdot x_0 + + x_3\cdot\overline{x_2}\cdot\overline{x_1}\cdot\overline{x_0} + x_3\cdot\overline{x_2}\cdot\overline{x_1}\cdot x_0 + x_3\cdot\overline{x_2}\cdot x_1\cdot\overline{x_0}$

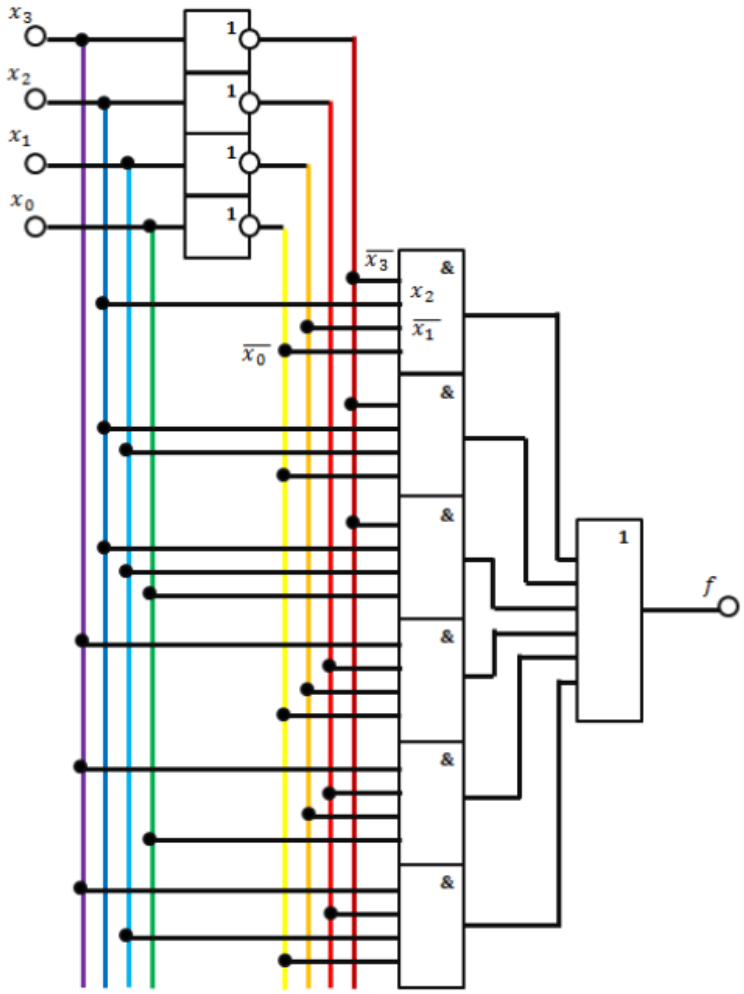


Рис.1. Схема реализации функции на логических элементах

2. Реализовать полученную функцию на дешифраторе

Как упоминалось ранее в значениях заданной логической функции количество единиц меньше, чем нулей. Поэтому разработаем схему по тем же **минтермам.**

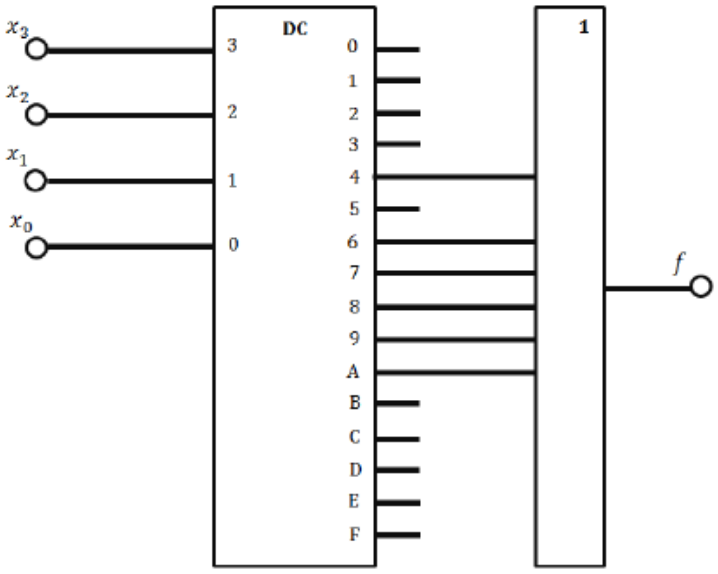


Рис.2. Схема реализации функции на дешифраторе

При подаче на вход дешифратора сигнала **0100,** являющимся первым минтермом в СДНФ, дешифратор выдаст на выходе «4» уровень логической единицы. Затем этот сигнал поступает на лог. элемент «**ИЛИ**». Результатом операции будет лог.1 на выходе схемы. Выходы дешифратора, на которых при подаче других минтермов устанавливается лог.1 на выходе, для согласования результата функции, так же заведены на элемент «ИЛИ». Во всех остальных случаях результатом работы схемы будет лог.0.

3. Выполнить минимизацию по карте Карно, синтезировать схему на базисе, определенного вариантом, привести синтезируемую схему, выполнить проверку на соответствие исходной таблице истинности.

1 - 4 вариант -> И-НЕ

5 - 8 вариант -> ИЛИ-НЕ

9 - 12 вариант -> И-НЕ

13 - 16 вариант -> ИЛИ-НЕ

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – контрольная работа

Раздел 1.4 Основные понятия теории моделирования систем

РАЗДЕЛ 1. ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ МОДЕЛИРОВАНИЯ СИСТЕМ. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА МОДЕЛИРОВАНИЯ СИСТЕМ

Цель: заключается в получении обучающимися теоретических знаний в области моделирования информационных процессов и систем с последующим применением в профессиональной сфере и практических навыков построении и реализации информационных систем на основе современных методологий и стандартов.

Перечень изучаемых элементов содержания дисциплины

Понятие моделирование. Сущность теории моделирования. Методы и средства моделирования систем. Аналитические и имитационные методы. Принципы системного подхода в

моделировании систем. Характеристики моделей систем. Адаптивность модели. Цели моделирования. Классификация видов моделирования систем. Средства моделирования систем. Обеспечение и эффективность имитационного моделирования.

Вопросы для самоподготовки:

1. Теория моделирования. Система и элементы системы. Понятие модели. Цели моделирования.
2. Подходы к исследованию систем. Стадии разработки моделей.
3. Классификация моделей. Физические и математические модели.
4. Математическая модель. Основные этапы построения математической модели. Требования к математической модели. Уравнение <вход-выход>.
5. Уравнение состояния. Общесистемные и конструктивные модели. Этапы построения модели функционирования системы.
6. Дискретно- детерминированные модели. Автоматы Мили и Мура.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: лабораторный практикум

Цель:

получить навыки работы с языком имитационного моделирования GPSS

Контрольные вопросы:

1. Понятие моделирования. Характеристики моделей.
2. Понятия моделирования: система, внешняя среда. Типы атрибутов элементов и системы.
3. Классификация систем.
4. Основные понятия: событие, действие, процесс, очередь, модельное время, системы массового обслуживания, системная величина.
5. Элементы процедуры решения: собятия, категории событий; таймер модельного времени, методы увеличения значения таймера; завершение моделирования; алгоритмизация моделирования.
6. Языки имитационного моделирования систем: SIMULA, SIMSCRIPT, GPSS и др. Имитационное моделирование систем на GPSS.
7. Блочно-ориентированная концепция GPSS.
8. Функциональная структура GPSS. Типы объектов: транзакты, блоки, списки, устройства, памяти, логические ключи, очереди, таблицы, ячейки, функции, переменные.
9. Понятие транзакта. Списки событий (текущих и будущих). Блоки GPSS, связанные с транзактами.
10. Блок GENERATE создания транзакта. Его параметры и стандартные числовые атрибуты (СЧА). Пример использования блока GENERATE.
11. Блок ASSIGN присваивания и изменения значений параметров. Запись текущего модельного времени в заданный параметр транзакта
12. Блок MARK Изменение приоритета транзакта. Блок PRIORITY. Удаление транзактов из модели. Блок TERMINATE.
13. Моделирование обслуживания заявок (задержки транзактов на определенный отрезок модельного времени) с помощью блока ADVANCE.
14. Переменные и функции. Оператор VARIABLE. Определение функций. Пример модели.
15. Блоки GPSS, связанные с аппаратными объектами. Блоки SIZE создания и RELEASE освобождения одноканальных устройств
16. Моделирования захвата и освобождения одноканального устройства с помощь блоков PREEMPT и RETURN.

17. Определение многоканальных устройств (МКУ). Оператор определения STORAGE (память).
18. Блоки ENTER (войти) и LEAVE (покинуть) занятия и освобождения каналов обслуживания МКУ.
19. Создание объектов типа «очередь». Блоки QUEUE (стать в очередь) DEPART (уйти из очереди). Оператор QTABLE создания таблицы.
20. Задержка или изменение маршрутов транзактов с помощью блока GATE.
21. Приемы конструирования GPSS–моделей. Технология работы с пакетом GPSS. Приемы конструирования GPSS–моделей.
22. Загрузка интегрированной среды. Ввод новой модели. Редактирование текста модели. Запись и считывание модели с диска.
23. Прогон модели и наблюдение за моделированием. Получение и интерпретация стандартного отчета. Примеры построения GPSS–моделей.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – контрольная работа

Контрольная работа проводится на практическом занятии.

Теоретические вопросы:

1. Понятие моделирования. Характеристики моделей.
2. Понятия моделирования: система, внешняя среда. Типы атрибутов элементов и системы.
3. Классификация систем.
4. Основные понятия: событие, действие, процесс, очередь, модельное время, системы массового обслуживания, системная величина.
5. Элементы процедуры решения: собятия, категории событий; таймер модельного времени, методы увеличения значения таймера; завершение моделирования; алгоритмизация моделирования.
6. Языки имитационного моделирования систем: SIMULA, SIMSCRIPT, GPSS и др. Имитационное моделирование систем на GPSS.
7. Блочно-ориентированная концепция GPSS.
8. Функциональная структура GPSS. Типы объектов: транзакты, блоки, списки, устройства, памяти, логические ключи, очереди, таблицы, ячейки, функции, переменные.
9. Понятие транзакта. Списки событий (текущих и будущих). Блоки GPSS, связанные с транзактами.
10. Блок GENERATE создания транзакта. Его параметры и стандартные числовые атрибуты (СЧА). Пример использования блока GENERATE.
11. Блок ASSIGN присваивания и изменения значений параметров. Запись текущего модельного времени в заданный параметр транзакта
12. Блок MARK Изменение приоритета транзакта. Блок PRIORITY. Удаление транзактов из модели. Блок TERMINATE.
13. Моделирование обслуживания заявок (задержки транзактов на определенный отрезок модельного времени) с помощью блока ADVANCE.
14. Переменные и функции. Оператор VARIABLE. Определение функций. Пример модели.
15. Блоки GPSS, связанные с аппаратными объектами. Блоки SIZE создания и RELEASE освобождения одноканальных устройств
16. Моделирования захвата и освобождения одноканального устройства с помощь блоков PREEMPT и RETURN.
17. Определение многоканальных устройств (МКУ). Оператор определения STORAGE (память).
18. Блоки ENTER (войти) и LEAVE (покинуть) занятия и освобождения каналов

обслуживания МКУ.

19. Создание объектов типа «очередь». Блоки QUEUE (стать в очередь) DEPART (уйти из очереди). Оператор QTABLE создания таблицы.
20. Задержка или изменение маршрутов транзактов с помощью блока GATE.
21. Приемы конструирования GPSS–моделей. Технология работы с пакетом GPSS. Приемы конструирования GPSS–моделей.
22. Загрузка интегрированной среды. Ввод новой модели. Редактирование текста модели. Запись и считывание модели с диска.

Прогон модели и наблюдение за моделированием. Получение и интерпретация стандартного отчета. Примеры построения GPSS–моделей

Раздел 1.5 Математические схемы моделирования систем

Цель: заключается в получении обучающимися теоретических знаний в области моделирования информационных процессов и систем с последующим применением в профессиональной сфере и практических навыков построении и реализации информационных систем на основе современных методологий и стандартов.

Перечень изучаемых элементов содержания дисциплины

Формальная модель объекта. Типовые математические схемы. Непрерывно-детерминированные модели (D-схемы). Дискретно-детерминированные модели (F-схемы). Дискретно-стохастические модели (P-схемы). Непрерывно-стохастические модели (Q-схемы). Сетевые модели (N-схемы). Комбинированные модели (A-схемы).

Этапы моделирования систем. Построение концептуальных моделей систем и их формализация. Алгоритмизация моделей систем и их машинная реализация. Получение и интерпретация результатов моделирования систем

Вопросы для самоподготовки:

1. Формальная модель объекта.
2. Типовые математические схемы.
3. Непрерывно-детерминированные модели (D-схемы).
4. Дискретно-детерминированные модели (F-схемы).
5. Дискретно-стохастические модели (P-схемы).
6. Непрерывно-стохастические модели (Q-схемы).
7. Сетевые модели (N-схемы).
8. Комбинированные модели (A-схемы).
9. Структура агрегативной системы, особенности функционирования.
10. Формализация и алгоритмизация информационных процессов.
11. Алгоритмизация моделей.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: расчетное практическое задание

1. Пусть задан абстрактный автомат $A=(X,Q,Y,q_1\in Q,F(x\in X/y\in Y))$. В предположении, что автомат является автоматом первого рода, построить:

а) таблицы переходов и выходов;

б) графоид;

в) матрицу соединений.

2. Пусть дан автомат Мура $B=(X,Q,Y,q_1\in Q,F\ \ (x\in X))$. Построить:

а) отмеченную таблицу переходов;

б) графоид;

в) матрицу соединений;

г) автомат Мили, интерпретирующий автомат Мура (таблицы переходов и выходов, алгебраическую форму).

3. Для автомата Мили постройте эквивалентный ему автомат Мура. Для полученного автомата Мура постройте эквивалентный ему автомат Мили.

Варианты заданий

Вариант 1.

1. $X=\{x_1,x_2,x_3,x_4,x_5,x_6\}$, $Q=\{q_1,q_2,q_3,q_4,q_5,q_6\}$, $Y=\{y_1,y_2,y_3,y_4\}$, отображение F множества Q в себя определяется следующим образом:

$$Fq_1 = \{q_1(x_6 / y_2), q_6(x_2 / y_1), q_2(x_3 / y_4), q_5(x_1 / y_1)\},$$
$$Fq_2 = \{q_1(x_3 / y_3), q_3(x_6 / y_1), q_6(x_2 / y_4), q_2(x_1 / y_2), q_5(x_5 / y_4)\},$$
$$Fq_3 = \{q_5(x_4 / y_3), q_1(x_2 / y_2), q_3(x_1 / y_4), q_2(x_5 / y_2)\},$$
$$Fq_4 = \{q_1(x_1 / y_3), q_5(x_3 / y_4), q_4(x_4 / y_2), q_3(x_6 / y_1), q_2(x_5 / y_4)\}.$$
$$Fq_5 = \{q_4(x_1 / y_2), q_6(x_2 / y_2), q_2(x_6 / y_1), q_3(x_3 / y_4)\}.$$
$$Fq_6 = \{q_6(x_6 / y_4), q_3(x_3 / y_1), q_4(x_2 / y_4), q_2(x_5 / y_4), q_5(x_1 / y_4)\}.$$

2. $X = \{x_1, x_2, x_3\}$, $Q = \{q_1, q_2, q_3, q_4, q_5\}$, $Y = \{y_1, y_2, y_3, y_4, y_5\}$, причем

$$Fq_1(y_1) = \{q_3(x_3), q_2(x_1), q_5(x_2)\};$$
$$Fq_2(y_2) = \{q_5(x_1), q_3(x_2), q_4(x_3)\};$$
$$Fq_3(y_5) = \{q_1(x_1), q_5(x_1), q_2(x_3)\};$$
$$Fq_4(y_4) = \{q_5(x_2), q_4(x_3), q_2(x_1)\}.$$
$$Fq_5(y_3) = \{q_2(x_3), q_1(x_2), q_5(x_1)\};$$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_1/y_1	z_3/y_1	z_3/y_1	z_2/y_2	z_5/y_1
x_2	z_3/y_2	z_1/y_1	z_2/y_1	z_3/y_1	z_1/y_2
x_3	z_1/y_2	z_4/y_2	z_4/y_2	z_5/y_2	z_2/y_1

Вариант 2.

1. $X=\{x_1,x_2,x_3\}$, $Q=\{q_1,q_2,q_3,q_4\}$, $Y=\{y_1,y_2,y_3\}$, отображение F множества Q в себя определяется следующим образом:

$$Fq_1 = \{q_3(x_1 / y_3), q_2(x_2 / y_2), q_4(x_3 / y_3)\},$$
$$Fq_2 = \{q_2(x_1 / y_3), q_3(x_3 / y_2), q_1(x_2 / y_1)\},$$
$$Fq_3 = \{q_2(x_2 / y_3), q_3(x_1 / y_2), q_4(x_3 / y_1)\},$$
$$Fq_4 = \{q_4(x_1 / y_1), q_2(x_2 / y_2), q_3(x_3 / y_3)\}.$$

2. $X = \{x_1, x_2, x_3, x_4, x_5\}$, $Q = \{q_1, q_2, q_3, q_4\}$, $Y = \{y_1, y_2, y_3, y_4\}$, причем

$$Fq_1(y_1) = \{q_3(x_2), q_2(x_5), q_4(x_3), q_1(x_4), q_3(x_1)\};$$
$$Fq_2(y_4) = \{q_4(x_1), q_2(x_3), q_1(x_4), q_1(x_5)\};$$
$$Fq_3(y_3) = \{q_1(x_2), q_4(x_5), q_1(x_1), q_4(x_4); q_1(x_3)\};$$
$$Fq_4(y_2) = \{q_1(x_2), q_3(x_3), q_2(x_4), q_4(x_5)\}.$$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_3/y_1	z_1/y_1	z_1/y_1	z_2/y_2	z_5/y_1
x_2	z_1/y_2	z_3/y_1	z_2/y_1	z_1/y_1	z_3/y_2
x_3	z_3/y_2	z_4/y_2	z_4/y_2	z_5/y_2	z_2/y_1

Вариант 3.

1. $X=\{x_1,x_2,x_3,x_4\}$, $Q=\{q_1,q_2,q_3,q_4,q_5\}$, $Y=\{y_1,y_2\}$, отображение F множества Q в себя определяется следующим образом:

$$Fq_1=\{q_5(x_1/y_1),q_4(x_2/y_2),q_1(x_1/y_1),q_4(x_4/y_1)\},$$
$$Fq_2=\{q_3(x_4/y_2),q_2(x_3/y_1),q_1(x_2/y_1),q_5(x_2/y_2)\},$$
$$Fq_3=\{q_1(x_1/y_2),q_5(x_2/y_1),q_4(x_1/y_2),q_3(x_1/y_1)\},$$
$$Fq_4=\{q_2(x_3/y_1),q_3(x_1/y_2),q_4(x_4/y_1),q_1(x_3/y_1)\}.$$
$$Fq_5=\{q_3(x_4/y_1),q_1(x_2/y_2),q_5(x_3/y_2),q_2(x_1/y_1)\}.$$

2. $X=\{x_1,x_2,x_3\}$, $Q=\{q_1,q_2,q_3,q_4\}$, $Y=\{y_1,y_2\}$, причем

$$Fq_1(y_1)=\{q_2(x_1),q_4(x_1)\};$$
$$Fq_2(y_2)=\{q_4(x_2),q_2(x_3)\};$$
$$Fq_3(y_1)=\{q_4(x_1),q_3(x_2),q_1(x_3)\};$$
$$Fq_4(y_2)=0.$$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_1/y_1	z_3/y_1	z_3/y_1	z_2/y_2	z_3/y_1
x_2	z_5/y_2	z_1/y_1	z_2/y_1	z_5/y_1	z_1/y_2
x_3	z_1/y_2	z_4/y_2	z_4/y_2	z_3/y_2	z_2/y_1

Вариант 4.

1. $X=\{x_1,x_2,x_3,x_4\}$, $Q=\{q_1,q_2,q_3,q_4,q_5,q_6\}$, $Y=\{y_1,y_2,y_3,y_4,y_5\}$, отображение F множества Q в себя определяется следующим образом:

$$Fq_1=\{q_1(x_1/y_2),q_3(x_2/y_4),q_2(x_3/y_5),q_6(x_4/y_5)\},$$
$$Fq_2=\{q_5(x_1/y_5),q_1(x_3/y_5),q_3(x_2/y_4),q_6(x_4/y_1)\},$$
$$Fq_3=\{q_2(x_2/y_4),q_1(x_1/y_5),q_6(x_3/y_3),q_5(x_4/y_4)\},$$
$$Fq_4=\{q_5(x_3/y_4),q_2(x_1/y_4),q_1(x_4/y_2),q_3(x_2/y_5)\},$$
$$Fq_5=\{q_3(x_2/y_5),q_2(x_4/y_2),q_1(x_1/y_1),q_4(x_3/y_3)\},$$
$$Fq_6=\{q_6(x_4/y_4),q_5(x_1/y_1),q_4(x_3/y_2),q_1(x_2/y_4)\}.$$

2. $X=\{x_1,x_2,x_3,x_4,x_5\}$, $Q=\{q_1,q_2,q_3,q_4,q_5\}$, $Y=\{y_1,y_2,y_3,y_4,y_5\}$, причем

$$Fq_1(y_1) = \{q_4(x_1), q_2(x_5), q_4(x_3), q_1(x_2), q_3(x_4)\};$$
$$Fq_2(y_2) = \{q_4(x_2), q_2(x_3), q_1(x_1), q_5(x_5)\};$$
$$Fq_3(y_5) = \{q_1(x_2), q_4(x_3), q_3(x_4), q_5(x_1), q_2(x_5)\};$$
$$Fq_4(y_4) = \{q_1(x_1), q_2(x_3), q_2(x_5), q_4(x_2), q_4(x_4)\};$$
$$Fq_5(y_3) = \{q_4(x_3), q_1(x_5), q_3(x_2), q_4(x_4), q_2(x_1)\}.$$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_4/y_2	z_2/y_1	z_5/y_1	z_5/y_1	z_5/y_1
x_2	z_3/y_1	z_1/y_1	z_2/y_1	z_3/y_1	z_1/y_2
x_3	z_1/y_2	z_4/y_2	z_1/y_2	z_5/y_2	z_2/y_1

Вариант 5.

1. $X=\{x_1,x_2,x_3,x_4,x_5\}$, $Q=\{q_1,q_2,q_3,q_4,q_5\}$, $Y=\{y_1,y_2,y_3,y_4,y_5\}$, отображение F множества Q в себя определяется следующим образом:

$$Fq_1 = \{q_2(x_4 / y_2), q_3(x_5 / y_2), q_1(x_3 / y_4), q_5(x_4 / y_5)\},$$
$$Fq_2 = \{q_5(x_5 / y_3), q_2(x_4 / y_1), q_3(x_2 / y_4), q_1(x_1 / y_5)\},$$
$$Fq_3 = \{q_3(x_4 / y_5), q_1(x_1 / y_2), q_4(x_3 / y_2), q_2(x_2 / y_2)\},$$
$$Fq_4 = \{q_2(x_1 / y_3), q_5(x_2 / y_4), q_1(x_4 / y_2), q_3(x_3 / y_5)\},$$
$$Fq_5 = \{q_2(x_2 / y_5), q_5(x_4 / y_2), q_1(x_3 / y_4), q_4(x_5 / y_3)\}.$$

2. $X = \{x_1, x_2, x_3, x_4, x_5\}$, $Q = \{q_1, q_2, q_3, q_4\}$, $Y = \{y_1, y_2, y_3, y_4\}$, причем

$$Fq_1(y_1) = \{q_3(x_1), q_4(x_5), q_2(x_3), q_1(x_4), q_3(x_2)\};$$
$$Fq_2(y_2) = \{q_4(x_2), q_2(x_1), q_1(x_4), q_1(x_3)\};$$
$$Fq_3(y_5) = \{q_1(x_2), q_2(x_1), q_4(x_4), q_1(x_5); q_3(x_3)\};$$
$$Fq_4(y_4) = \{q_1(x_5), q_1(x_3), q_3(x_4), q_4(x_1)\}.$$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_1/y_1	z_3/y_1	z_3/y_1	z_2/y_2	z_5/y_1
x_2	z_3/y_2	z_1/y_1	z_2/y_1	z_3/y_1	z_1/y_2
x_3	z_1/y_2	z_4/y_2	z_4/y_2	z_5/y_2	z_2/y_1

Вариант 6.

1. $X=\{x_1,x_2,x_3\}$, $Q=\{q_1,q_2,q_3,q_4,q_5,q_6\}$, $Y=\{y_1,y_2,y_3,y_4,y_5,y_6\}$, отображение F множества Q в себя определяется следующим образом:

$$Fq_1 = \{q_2(x_1 / y_2), q_3(x_2 / y_1), q_1(x_3 / y_4)\},$$
$$Fq_2 = \{q_1(x_1 / y_6), q_3(x_3 / y_1), q_6(x_2 / y_4)\},$$
$$Fq_3 = \{q_3(x_3 / y_5), q_1(x_1 / y_2), q_2(x_2 / y_5)\},$$
$$Fq_4 = \{q_5(x_3 / y_3), q_2(x_2 / y_4), q_1(x_1 / y_6)\}.$$
$$Fq_5 = \{q_4(x_2 / y_5), q_1(x_1 / y_2), q_4(x_3 / y_1)\},$$
$$Fq_6 = \{q_4(x_3 / y_4), q_5(x_2 / y_1), q_2(x_1 / y_6)\}.$$

2. $X=\{x_1,x_2,x_3,x_4,x_5\}$, $Q=\{q_1,q_2,q_3,q_4,q_6,q_6\}$, $Y=\{y_1,y_2,y_3,y_4,y_5\}$, причем

$Fq_1(y_1)=\{q_4(x_1),q_2(x_5),q_4(x_3),q_1(x_2),q_3(x_4)\};$

$Fq_2(y_2)=\{q_4(x_2),q_5(x_1),q_1(x_4),q_1(x_5)\};$

$Fq_3(y_5)=\{q_4(x_5),q_1(x_3),q_4(x_1),q_1(x_2);q_6(x_4)\};$

$Fq_4(y_4)=\{q_1(x_5),q_6(x_3),q_3(x_1),q_4(x_2)\};$

$Fq_5(y_3)=\{q_1(x_5),q_3(x_4),q_1(x_2),q_4(x_3);q_2(x_1)\};$

$Fq_6(y_5)=\{q_3(x_3),q_6(x_4),q_3(x_5),q_2(x_1);q_4(x_2)\}.$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_1/y_1	z_2/y_2	z_5/y_1	z_1/y_1	z_3/y_1
x_2	z_2/y_1	z_1/y_1	z_3/y_2	z_5/y_2	z_1/y_1
x_3	z_4/y_2	z_5/y_2	z_2/y_1	z_1/y_2	z_3/y_2

Вариант 7.

1. $X=\{x_1,x_2,x_3\}$, $Q=\{q_1,q_2,q_3,q_4,q_5\}$, $Y=\{y_1,y_2\}$, отображение F множества Q в себя определяется следующим образом:

$Fq_1=\{q_3(x_1/y_1),q_5(x_3/y_2),q_4(x_2/y_2)\},$

$Fq_2=\{q_1(x_1/y_1),q_1(x_2/y_1),q_2(x_3/y_2)\},$

$Fq_3=\{q_4(x_3/y_1),q_1(x_1/y_1),q_2(x_2/y_1)\},$

$Fq_4=\{q_5(x_3/y_2),q_3(x_2/y_1),q_2(x_1/y_2)\}.$

$Fq_5=\{q_1(x_2/y_2),q_5(x_1/y_1),q_3(x_3/y_1)\}.$

2. $X=\{x_1,x_2,x_3,x_4,x_5\}$, $Q=\{q_1,q_2,q_3,q_4,q_6,q_6\}$, $Y=\{y_1,y_2,y_3,y_4,y_5\}$, причем

$Fq_1(y_1)=\{q_4(x_1),q_2(x_5),q_4(x_3),q_1(x_2),q_3(x_4)\};$

$Fq_2(y_2)=\{q_5(x_2),q_4(x_1),q_1(x_4),q_1(x_5)\};$

$Fq_3(y_5)=\{q_4(x_5),q_1(x_3),q_4(x_1),q_1(x_2);q_6(x_4)\};$

$Fq_4(y_4)=\{q_1(x_5),q_3(x_3),q_6(x_1),q_4(x_2)\};$

$Fq_5(y_3)=\{q_1(x_5),q_3(x_4),q_4(x_2),q_1(x_3);q_2(x_1)\};$

$Fq_6(y_5)=\{q_6(x_3),q_3(x_4),q_3(x_5),q_2(x_1);q_4(x_2)\}.$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_3/y_1	z_1/y_1	z_1/y_1	z_2/y_2	z_5/y_1
x_2	z_4/y_2	z_1/y_1	z_2/y_1	z_3/y_1	z_1/y_2
x_3	z_3/y_2	z_4/y_2	z_4/y_2	z_5/y_2	z_2/y_1

Вариант 8.

1. $X=\{x_1,x_2,x_3\}$, $Q=\{q_1,q_2,q_3,q_4,q_5\}$, $Y=\{y_1,y_2\}$, отображение F множества Q в себя определяется следующим образом:

$Fq_1 = \{q_1(x_1 / y_1), q_4(x_3 / y_2), q_2(x_2 / y_1)\},$

$Fq_2 = \{q_2(x_1 / y_2), q_3(x_2 / y_1), q_5(x_3 / y_2)\},$

$Fq_3 = \{q_2(x_3 / y_1), q_5(x_1 / y_1), q_1(x_2 / y_2)\},$

$Fq_4 = \{q_5(x_3 / y_2), q_3(x_2 / y_1), q_5(x_1 / y_1)\}.$

$Fq_5 = \{q_1(x_2 / y_2), q_5(x_1 / y_1), q_2(x_3 / y_1)\}.$

2. $X = \{x_1, x_2, x_3, x_4, x_5\}$, $Q = \{q_1, q_2, q_3, q_4\}$, $Y = \{y_1, y_2, y_3, y_4\}$, причем

$Fq_1(y_1) = \{q_4(x_1), q_3(x_5), q_2(x_3), q_3(x_4), q_1(x_2)\};$

$Fq_2(y_2) = \{q_4(x_2), q_1(x_1), q_2(x_4), q_1(x_3)\};$

$Fq_3(y_5) = \{q_2(x_2), q_1(x_1), q_4(x_4), q_1(x_5); q_3(x_3)\};$

$Fq_4(y_4) = \{q_4(x_5), q_1(x_3), q_3(x_4), q_1(x_1)\}.$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_5/y_1	z_5/y_1	z_5/y_1	z_2/y_2	z_3/y_1
x_2	z_2/y_1	z_3/y_1	z_1/y_2	z_5/y_1	z_1/y_2
x_3	z_1/y_2	z_5/y_2	z_2/y_1	z_3/y_2	z_2/y_1

Вариант 9.

1. $X=\{x_1,x_2,x_3\}$, $Q=\{q_1,q_2,q_3,q_4,q_5\}$, $Y=\{y_1,y_2\}$, отображение F множества Q в себя определяется следующим образом:

$Fq_1 = \{q_5(x_1 / y_1), q_1(x_3 / y_2), q_2(x_2 / y_1)\},$

$Fq_2 = \{q_5(x_1 / y_1), q_3(x_2 / y_1), q_5(x_3 / y_2)\},$

$Fq_3 = \{q_5(x_1 / y_1), q_1(x_2 / y_2), q_2(x_3 / y_1)\},$

$Fq_4 = \{q_2(x_1 / y_2), q_5(x_2 / y_1), q_3(x_3 / y_2)\}.$

$Fq_5 = \{q_1(x_2 / y_2), q_3(x_1 / y_1), q_2(x_3 / y_1)\}.$

2. $X = \{x_1, x_2, x_3, x_4, x_5\}$, $Q = \{q_1, q_2, q_3, q_4, q_5\}$, $Y = \{y_1, y_2, y_3, y_4, y_5\}$, причем

$Fq_1(y_1) = \{q_2(x_1), q_2(x_5), q_5(x_3), q_1(x_2), q_3(x_4)\};$

$Fq_2(y_2) = \{q_4(x_2), q_5(x_3), q_1(x_1), q_5(x_5)\};$

$Fq_3(y_5) = \{q_1(x_2), q_3(x_3), q_3(x_4), q_5(x_1), q_2(x_5)\};$

$Fq_4(y_4) = \{q_2(x_1), q_2(x_3), q_2(x_5), q_4(x_2), q_4(x_4)\};$

$Fq_5(y_3) = \{q_1(x_3), q_1(x_5), q_3(x_2), q_4(x_4), q_2(x_1)\}.$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_1/y_1	z_2/y_2	z_5/y_1	z_5/y_1	z_5/y_1
x_2	z_2/y_1	z_3/y_1	z_1/y_2	z_3/y_1	z_1/y_2
x_3	z_4/y_2	z_5/y_2	z_2/y_1	z_5/y_2	z_2/y_1

Вариант 10.

1. $X=\{x_1,x_2,x_3\}$, $Q=\{q_1,q_2,q_3,q_4,q_5\}$, $Y=\{y_1,y_2\}$, отображение F множества Q в себя определяется следующим образом:

$$Fq_1 = \{q_3(x_1 / y_1), q_3(x_3 / y_2), q_4(x_2 / y_2)\},$$
$$Fq_2 = \{q_1(x_1 / y_1), q_1(x_2 / y_1), q_4(x_3 / y_2)\},$$
$$Fq_3 = \{q_1(x_1 / y_1), q_2(x_2 / y_1), q_4(x_3 / y_2)\},$$
$$Fq_4 = \{q_2(x_1 / y_2), q_3(x_2 / y_1), q_5(x_3 / y_2)\}.$$
$$Fq_5 = \{q_1(x_2 / y_2), q_5(x_1 / y_1), q_2(x_3 / y_1)\}.$$

2. $X = \{x_1, x_2, x_3, x_4, x_5\}$, $Q = \{q_1, q_2, q_3, q_4\}$, $Y = \{y_1, y_2, y_3, y_4\}$, причем

$$Fq_1(y_1) = \{q_2(x_2), q_2(x_5), q_1(x_3), q_1(x_4), q_3(x_1)\};$$
$$Fq_2(y_4) = \{q_3(x_1), q_2(x_3), q_1(x_4), q_4(x_5)\};$$
$$Fq_3(y_3) = \{q_2(x_2), q_4(x_5), q_1(x_1), q_4(x_4); q_1(x_3)\};$$
$$Fq_4(y_2) = \{q_4(x_2), q_1(x_3), q_2(x_4), q_3(x_5)\}.$$

3.

	z_1	z_2	z_3	z_4	z_5
x_1	z_3/y_1	z_1/y_1	z_1/y_1	z_2/y_2	z_5/y_1
x_2	z_4/y_2	z_1/y_1	z_2/y_1	z_3/y_1	z_1/y_2
x_3	z_5/y_2	z_2/y_2	z_4/y_1	z_5/y_2	z_3/y_1

4. Решить в соответствии с вариантом дифференциальное уравнение аналитическим и операторным методом. Результаты представить в виде таблицы и графика (Excel).

5. Представить графический результат моделирования неоднородного дифференциального уравнения в VisSim.

6. Решить дифференциальное уравнение методом Эйлера первого порядка. Результат представить в виде рекурсивной формулы, таблицы и графика. (Excel).

7. Преобразовать дифференциальное уравнение в передаточную функцию.

8. Провести моделирование системы в VisSim, представленной передаточной функцией; построить АФХ, АЧХ, ФЧХ.

9. Получить АФХ, АЧХ, ФЧХ в Excel. Результаты представить в виде таблиц и графиков.

Замечание. Для построения ФЧХ в Excel использовать функцию **ATAN2**(*x*;*y*), где *x* – это действительная часть частотной передаточной функции, *y* – мнимая часть частотной передаточной функции.

Варианты заданий

Номер варианта	Дифференциальное уравнение
1	$y'' - 4y' + 3y = 7x - 2$
2	$y'' + 3y' + 2y = 3x + 2$
3	$y'' + 6y' + 5y = 5x - 2$
4	$y'' + 2y' + y = 2x + 2$
5	$y'' - 7y' + 12y = 7x - 2$
6	$y'' - 6y' + 9y = 5x - 2$
7	$y'' - 4y' + 4y = 3x + 3$
8	$y'' + 2y' + 10y = x + 2$

9	$y'' - 2y' - y = x + 3$
10	$y'' - 8y' + 7y = 8x - 2$

Начальные условия:

$y(0) = 0;\ \ y'(0) = 0.$

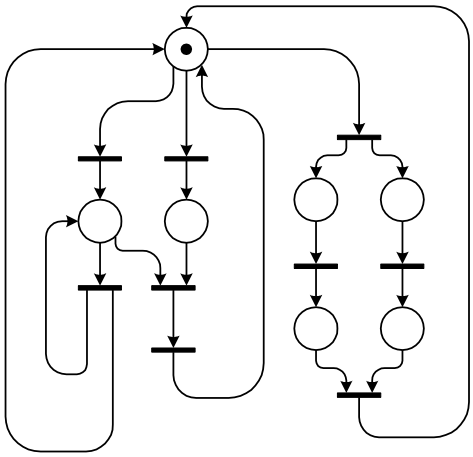
Входное воздействие:

$x(t)=1(t)$ – единичная ступенчатая функция.

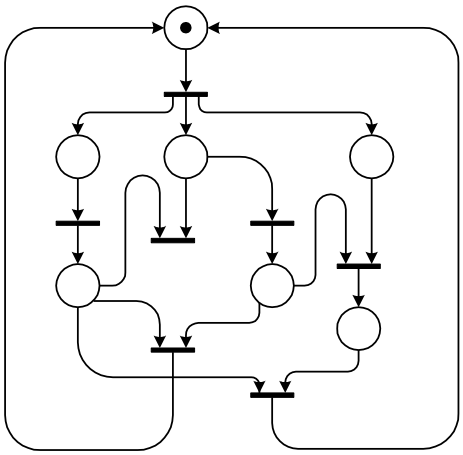
10. Выбрать структуру СП в соответствии с номером варианта из приложения 1. Описать заданную СП-модель с помощью матриц $F,H,\ \mu_0$.
11. Провести исследование СП-модели на основе матричных методов. Сделать заключение о живости и безопасности сети.
12. Провести исследование СП-модели путем построения дерева достижимых разметок (ДДР.
13. На основе проведенных исследований оценить корректность СП-модели и предложить варианты устранения недостатков в случае их обнаружения. Допустимо добавлять новые элементы и ограниченно видоизменять топологию сети. Полученная модель должна отвечать требованиям живости и безопасности.
14. Провести исследование полученной сети с помощью матричных методов и ДДР.
15. Выбрать вычислительную структуру в соответствии с номером варианта
16. Разработать СП-модель в соответствии с ее словесным описанием.
17. Провести анализ полученной СП-модели при помощи матричных методов и дерева достижимых разметок.
18. На основе исследования сделать выводы о корректности модели, предложить варианты устранения недостатков в случае их обнаружения.

Приложение 1.

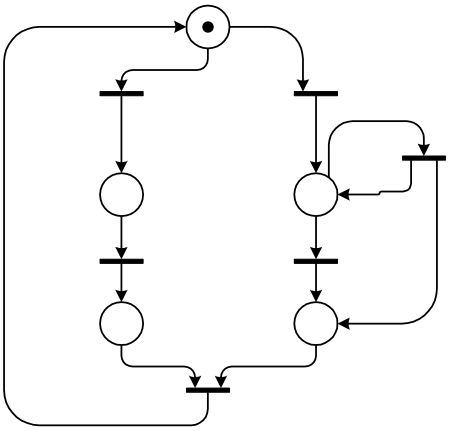
1



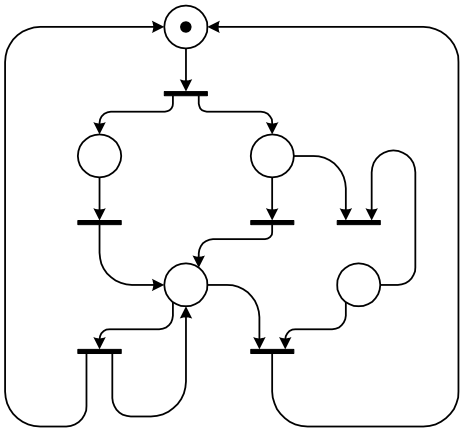
2



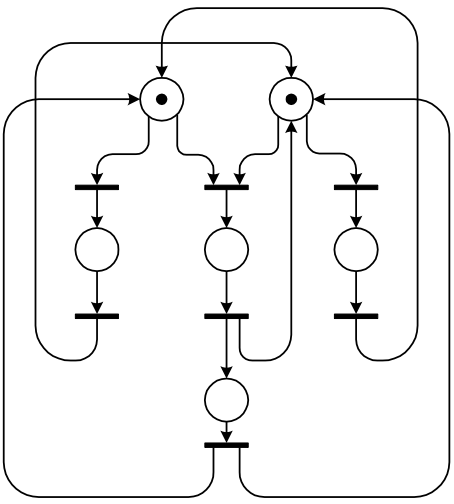
3



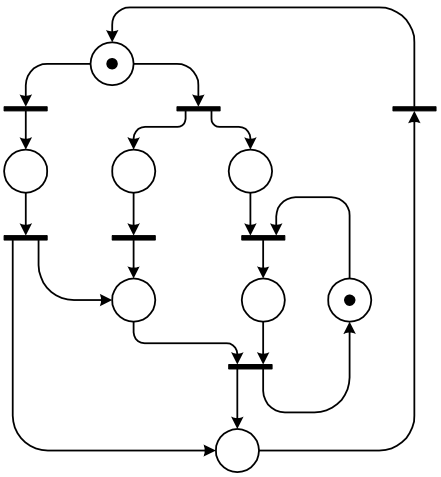
4



5



6



Приложение 2.

1.	Дана вычислительная структура, которая состоит из двух независимых подканалов *ПКВ1*, который вводит данные, и *ПКВ2*, который выводит данные. Обработка данных ведется на конвейерном процессоре, состоящем из трех процессорных элементов. Если работает процессор, то ввод данных запрещен.
2.	Дана вычислительная структура, которая включает канал ввода-вывода, состоящий из подканалов ПКВ1, ПКВ2, ПКВ3, и параллельный процессор, состоящий из трех процессорных элементов ПЭ1, ПЭ2, ПЭ3. Ввод данных выполняют подканалы ПКВ1 и ПКВ2, вывод - подканал ПКВ2. Подканал ПКВ3 управляет передачей данных в процессорные элементы: ПЭ1 занимает подканал ПКВ3 на все время обработки данных, ПЭ2 – только на время ввода и вывода, ПЭ3 – только на время вывода.
3.	Даны вычислительные структуры ВС1 и ВС2. ВС1 имеет параллельный процессор, состоящий из двух процессорных элементов. ВС2 имеет конвейерный процессор, также состоящий из двух процессорных элементов. Канал ввода-вывода включает два подканала ПКВ1 и ПКВ2. Ввод и обработка данных в ВС1 производится под управлением подканала ПКВ1, а в ВС2 – под управлением подканала ПКВ2. Вывод данных из ВС1 и ВС2 требует занятия канала ввода-вывода полностью.
4.	Даны вычислительные структуры ВС1 и ВС2, которые имеют соответственно параллельный (ПЭ1||ПЭ2||ПЭ3) и последовательный (ПЭ1−ПЭ2) процессоры. Обработка данных в процессорах ВС1 и ВС2 начинается одновременно. Канал ввода-вывода имеет один подканал и выполняет ввод и вывод данных в каждой вычислительной структуре.
5.	Даны вычислительные структуры ВС1, ВС2, ВС3 и канал ввода-вывода, состоящий из подканалов ПКВ1, ПКВ2, ПКВ3. ВС1 выполняет ввод данных с использованием подканалов ПКВ1 и ПКВ2. ВС2 выполняет обработку данных на процессоре со следующей структурой ((ПЭ1||ПЭ2)−ПЭ3). ВС3 выполняет вывод данных с использованием подканалов ПКВ2 и ПКВ3.
6.	Даны вычислительные структуры ВС1, ВС2, ВС3 и канал ввода-вывода, который включает два подканала ПКВ1 и ПКВ2. ВС1 вводит данные с использованием подканалов ПКВ1 и ПКВ2. ВС2 выводит данные с использованием подканала ПКВ2. Обработка ведется ВС3 на последовательно-параллельном процессоре со структурой (ПЭ1 (ПЭ2||ПЭ3)).
7.	Дана вычислительная структура и канал ввода-вывода, который может использоваться при вводе и выводе данных одновременно. Обработке данных ведется на параллельном процессоре со структурой (ПЭ1||ПЭ2||ПЭ3).
8.	Дана конвейерная система, которая включает вычислительные структуры ВС1, ВС2, ВС3 и канал ввода-вывода с подканалами ПКВ1 и ПКВ2. ВС1 и подканал ПКВ1 вводят данные, ВС2 и подканал ПКВ2 выводят данные, ВС3 выполняет обработку. Обработка ведется на процессоре со структурой ((ПЭ1||ПЭ2)−ПЭ3−(ПЭ4||ПЭ5)).
9.	Дана параллельная система, которая включает вычислительные структуры ВС1, ВС2, ВС3 и канал ввода-вывода, который вводит и выводит данные во все

	структуры синхронно. Каждая вычислительная структура имеет последовательный процессор, состоящий из двух процессорных элементов ПЭ1 и ПЭ2. Условием начала работы ПЭ2 в ВС2 является окончание обработки данных в ВС3, а условием начала работы ПЭ2 в ВС1 является окончание обработки данных в ВС2.
10.	Даны вычислительные структуры ВС1, ВС2, ВС3 и ВС4. Все вычислительные структуры обмениваются данными с одним и тем же буфером. Передача данных осуществляется каналом ввода-вывода, содержащим подканал ПКВ1. Процессоры вычислительных структур являются последовательными и состоят из двух процессорных элементов. Обработку данных вычислительные структуры ведут в следующем порядке: ВС1, ВС3, ВС4, ВС2.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – контрольная работа

Контрольная работа проводится на практическом занятии.

Теоретические вопросы:

1. Дискретно- детерминированные модели. Автоматы Мили и Мура.
2. Каким образом представляются детерминированные и вероятностные автоматы в виде ориентированных графов?
3. Как на основе графовой модели можно составить формализованное описание конечного детерминированного (вероятностного) автомата?
4. Каким образом можно представить стохастическую дискретную систему (вероятностный автомат) в виде детерминированной дискретной системы (детерминированного автомата) со случайным входом?
5. D-схемы
6. Что такое СП и с помощью каких параметров она задается?
7. Что такое живость, безопасность, ограниченность и достижимость СП?
8. Как интерпретируются для моделируемой ВС живость, ограниченность и достижимость СП?
9. Как выглядит уравнение состояния СП?
10. В чем заключаются матричные методы исследования СП-моделей?
11. Что такое полная *p*-цепь и полная *t*-цепь?
12. Что такое дерево достижимых разметок?
13. Какие приемы использованы в алгоритме построения дерева достижимых разметок для ограничения дерева?
14. Какие свойства СП исследуются в процессе анализа?
15. Какова интерпретация позиций и переходов при описании СП вычислительных структур?
16. Как можно доказать корректность иерархической СП-модели?
17. Как определяется степень детализации иерархической СП-модели ВС?
18. Какие Вы знаете пути практического применения СП при проектировании и анализе ВС?
19. Какие методы проектирования многоуровневых ВС Вам известны? В чем достоинства и недостатки данных методов?
20. Обобщенные модели (А-схемы)

Аналитические задания:

1. Построить направленный граф, записать матрицу состояний для конечного *F*-автомата Мили, который описан таблицами переходов и выходов:

X	*Z*

X	*Z*

	z_0	z_1	z_2	z_3
x_1	z_1	z_2	z_0	z_1
x_2	z_0	z_0	z_3	z_3
x_3	z_1	z_2	z_1	z_0

	z_0	z_1	z_2	z_3
x_1	y_1	y_2	y_1	y_2
x_2	y_2	y_1	y_2	y_1
x_3	y_1	y_1	y_2	y_2

2. Построить направленный граф, записать матрицу состояний и вектор выходов для конечного *F*-автомата Мура, имеющего следующие количественные данные по множествам входного и выходного алфавита и внутренних состояний: $|X|=2;\ |Y|=3;\ |Z|=5$, описываемого таблицей переходов следующего вида:

X	Y				
	y_1	y_1	y_3	y_2	y_3
	z_0	z_1	z_2	z_3	z_4
x_1	z_1	z_4	z_4	z_2	z_2
x_2	z_3	z_1	z_1	z_0	z_0

3. Построить направленный граф работы *F*-автомата Мура, который описан таблицей переходов:

X	Y		
	y_1	y_2	y_3
	z_0	z_1	z_2
x_1	z_1	z_1	z_1
x_2	z_2	z_1	z_2
x_3	z_0	z_0	z_2

4. Постройте графы, найдите расширенную входную и выходную функции следующих сетей Петри:

а) $C=\{P, T, F, H\}$, $P=\{p_1, p_2, p_3, p_4, p_5, p_6\}$, $T=\{t_1, t_2, t_3, t_4, t_5\}$,

$F(t_1)=\{p_1\}$, $H(t_1)=\{p_2, p_3\}$,
$F(t_2)=\{p_3\}$, $H(t_2)=\{p_3, p_5, p_5\}$,
$F(t_3)=\{p_2, p_3\}$, $H(t_3)=\{p_2, p_4\}$,
$F(t_4)=\{p_4, p_5, p_5, p_5,\}$, $H(t_4)=\{p_4\}$,
$F(t_5)=\{p_2\}$, $H(t_5)=\{p_6\}$,

б) $C=\{P, T, F, H\}$, $P=\{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\}$,
$T=\{t_1, t_2, t_3, t_4, t_5, t_6\}$,

$F(t_1)=\{p_1\}$, $H(t_1)=\{p_2, p_3\}$,
$F(t_2)=\{p_8\}$, $H(t_2)=\{p_1, p_7\}$,
$F(t_3)=\{p_2, p_5\}$, $H(t_3)=\{p_6\}$,
$F(t_4)=\{p_3\}$, $H(t_4)=\{p_4\}$,
$F(t_5)=\{p_6, p_7\}$, $H(t_5)=\{p_9\}$,
$F(t_6)=\{p_4, p_9\}$, $H(t_3)=\{p_5, p_8\}$,

5. На графах сетей Петри из задачи 4, укажите маркировку:

а) μ=(1,0,2,0,3,1); б) μ=(1,2,3,4,34,0,0,0,1).

6. Какие переходы разрешены в маркированной сети Петри на рис 1-4?

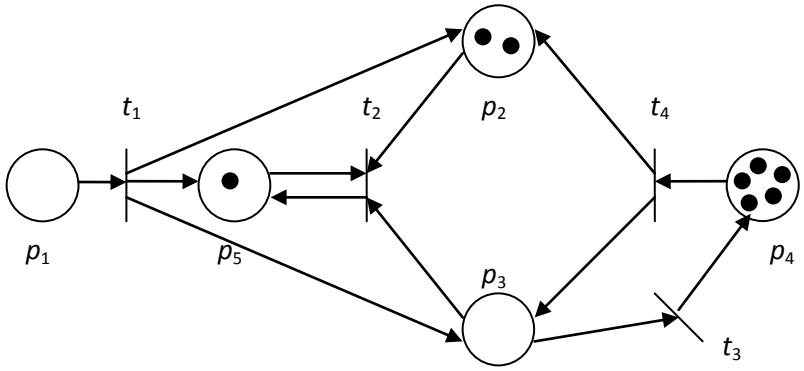


Рис. 1.

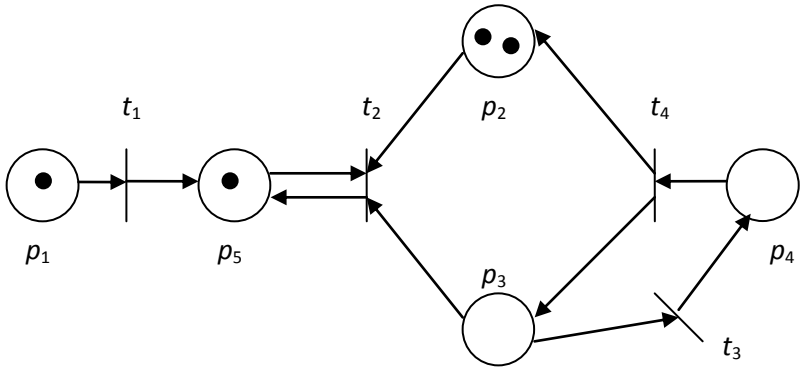


Рис. 2.

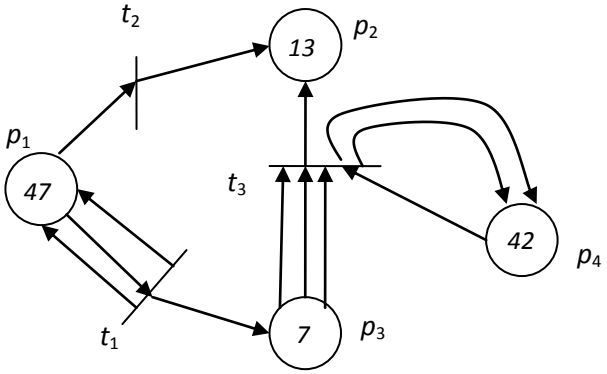


Рис. 3

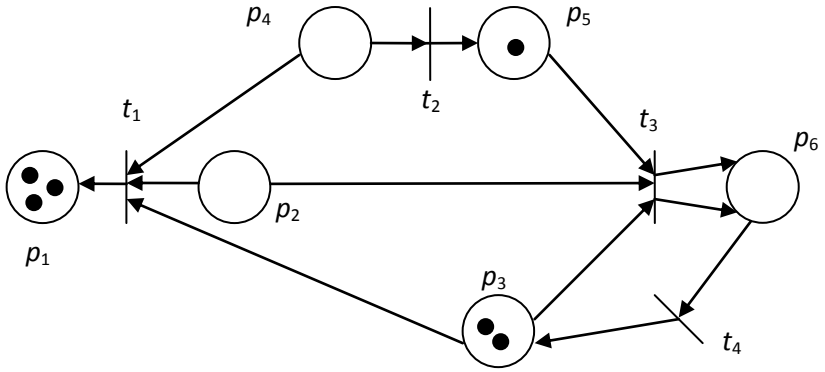


Рис. 4

7. Какая маркировка получится при запуске перехода t_1 (рис.1)? Какая маркировка получится при запуске перехода t_4 (рис.2)? Какая маркировка получится в результате выполнения следующих операций: сначала – запуск t_4, затем – запуск t_2 (рис. 2)?

8. Определите последовательность маркировок для маркированной сети Петри (рис. 5).

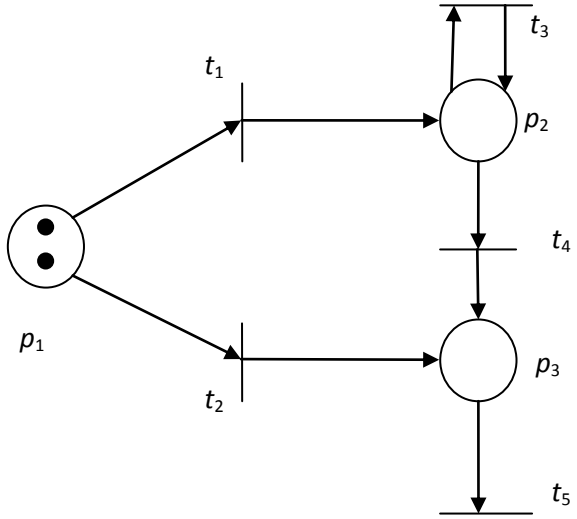
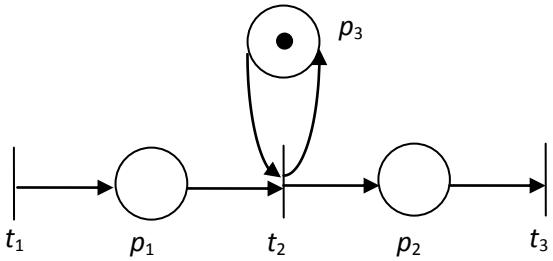


Рис. 5.

9. Постройте деревья достижимости для маркированных сетей, представленных на рис. 6 и рис. 7.



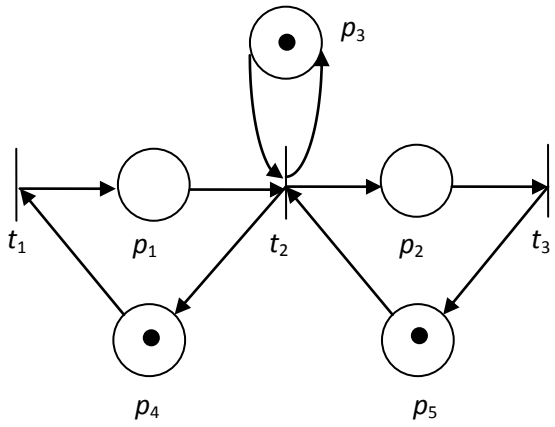


Рис. 6 Рис.7

9. Какая маркировка получится при запуске последовательности переходов $\sigma=t_2,t_5,t_1,t_3$ (рис. 5)? Является ли маркировка (0,2,0), (0,0,6), (0,3,1), (0,0,1) достижимой из маркировки (2,0,0)?

Модуль 2 Т**ехнологии проектирования ИС**

РАЗДЕЛ 1. ОСНОВНЫЕ КОМПОНЕНТЫ ТЕХНОЛОГИИ ПРОЕКТИРОВАНИЯ ИС.

Цель: заключается в получении обучающимися теоретических знаний в области проектирования информационных систем и сетей с последующим применением в профессиональной сфере и практических навыков проектирования информационных систем на основе современных методологий и стандартов.

Перечень изучаемых элементов содержания дисциплины: Методы и средства проектирования ИС. Краткая характеристика применяемых технологий проектирования. Требования, предъявляемые к технологии проектирования ИС. Выбор технологии проектирования ИС.

Вопросы для самоподготовки:

1. Понятие информационной системы в широком и узком смысле. Понятия проектирования ПС и проектирования ПО.
2. Предметная область: понятие, модель, цель моделирования, требования к моделям.
3. Бизнес-логика, бизнес-процесс, виды бизнес-процессов. Подходы к проектированию информационной системы.
4. Методология проектирования ПС: цель, задачи, эффект от внедрения.
5. Области проектирования ПС. Цель проекта по созданию ПС. Процесс и этапы создания ИС

РАЗДЕЛ 2. КАНОНИЧЕСКОЕ ПРОЕКТИРОВАНИЕ ИС.

Цель: заключается в получении обучающимися теоретических знаний в области проектирования информационных систем и сетей с последующим применением в профессиональной сфере и практических навыков проектирования информационных систем на основе современных методологий и стандартов.

Перечень изучаемых элементов содержания дисциплины: Стадии и этапы процесса проектирования ИС. Состав работ на предпроектной стадии, стадии технического и рабочего проектирования, стадии ввода в действие ИС, эксплуатации и сопровождения. Состав проектной документации.

Вопросы для самоподготовки:

1. Каноническое проектирование: понятие, этапы.
2. Наиболее распространенные стандарты на ЖЦ ПО: ГОСТ 34.601-90. CDM. RUP. MSF, XP.
3. Спиральная модель ЖЦ: понятие, риски, которые учитывает модель, прототипы, преимущества, недостатки.
4. Итеративная модель ЖЦ: понятие, преимущества, недостатки, пример.
5. Каскадная модель ЖЦ: понятие, область применимости, преимущества, недостатки, пример.
6. Жизненный цикл ПО: понятие, формальное описание, модель, процессы.
7. Требования пользователей к информационной системе: понятие, разработка, группы требований.
8. Виды требований по уровням. Этапы разработки требований по ГОСТ 34.
9. Обследование: понятие, этапы, использование результатов.
10. Формирование требований: этапы, источники.
11. Характеристики качества требований.
12. Методы выявления требований.
13. Этапы разработки концепции АС.
14. Техническое задание: понятие, решаемые задачи. Состав раздела «Общие сведения».
15. Состав раздела «Назначение и цели создания системы» ТЗ. Показатели объекта.
16. Состав подраздела «Требования к системе в целом» ТЗ. Пример.
17. Состав подраздела «Требования к функциям (по подсистемам)» ТЗ. Пример.

18. Состав подраздела «Требования к видам обеспечения» ТЗ. Примеры.

19. Состав разделов «Состав и содержание работ по созданию системы», «Порядок контроля и приемки системы» ТЗ.

20. Состав разделов «Требования к составу и содержанию работ по подготовке объекта к вводу системы в действие», «Требования к документированию».

21. Эскизный проект: понятие, содержание.

22. Технический проект: понятие, содержание разделов «Пояснительная записка», «Функциональная и организационная структура системы».

23. Содержание разделов. «Постановка задач и алгоритмы решения». «Организация информационной базы», «Система математического обеспечения» ТП.

24. Содержание разделов «Принцип построения комплекса технических средств», «Расчет экономической эффективности системы». «Мероприятия по подготовке объекта к внедрению системы» ТП.

25. Стадии «Создание рабочей документации» и «Испытания».

РАЗДЕЛ 3. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИС

Цель: заключается в получении обучающимися теоретических знаний в области проектирования информационных систем и сетей с последующим применением в профессиональной сфере и практических навыков проектирования информационных систем на основе современных методологий и стандартов.

Перечень изучаемых элементов содержания дисциплины: Состав, содержание и принципы организации информационного обеспечения ИС. Проектирование документальных БД: анализ предметной области, разработка состава и структуры БД, проектирование логико-семантического комплекса.

Вопросы для самоподготовки:

1. Структура ИС. Понятие информационного обеспечения. Унифицированные системы документации.
2. Схемы информационных потоков. Задачи информационного обеспечения. Состав информационного обеспечения. Требования к информационному обеспечению.
3. Понятие внутримашинного информационного обеспечения. Электронная форма документа. Этапы проектирования форм электронных документов.
4. Понятие информационной базы. Требования к организации информации в информационной базе. Способы организации информационной базы.
5. Цель моделирования данных. Этапы проектирования информационной базы.
6. Информационно-логическая модель предметной области. Концептуальная и физическая модели.

РАЗДЕЛ 3. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИС

Цель: заключается в получении обучающимися теоретических знаний в области проектирования информационных систем и сетей с последующим применением в профессиональной сфере и практических навыков проектирования информационных систем на основе современных методологий и стандартов.

Перечень изучаемых элементов содержания дисциплины: Состав, содержание и принципы организации информационного обеспечения ИС. Проектирование документальных БД: анализ предметной области, разработка состава и структуры БД, проектирование логико-семантического комплекса.

Вопросы для самоподготовки:

7. Структура ИС. Понятие информационного обеспечения. Унифицированные системы документации.
8. Схемы информационных потоков. Задачи информационного обеспечения. Состав информационного обеспечения. Требования к информационному обеспечению.
9. Понятие внутримашинного информационного обеспечения. Электронная форма документа. Этапы проектирования форм электронных документов.

10. Понятие информационной базы. Требования к организации информации в информационной базе. Способы организации информационной базы.

11. Цель моделирования данных. Этапы проектирования информационной базы.

12. Информационно-логическая модель предметной области. Концептуальная и физическая модели.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ К РАЗДЕЛАМ 1-4

Форма практического задания: лабораторный практикум.

Примерный перечень тем лабораторных работ к разделу 1

1. Стандарты и методологии создания и эксплуатации информационных систем

Примерный перечень тем лабораторных работ к разделу 2

2. Построение функциональной модели.

3. Построение диаграммы потоков данных. Создание диаграммы IDEF3. Стоимостный анализ

Примерный перечень тем лабораторных работ к разделу 3

4. Разработка технического задания к программному продукту

Модуль 3 Распределенные системы

РАЗДЕЛ 1. Введение в распределенные системы

Цель: Ознакомление с основными понятиями распределенных систем

Перечень изучаемых элементов содержания дисциплины

Понятие распределенной системы. Определение распределенной системы. Программные компоненты. Требования к распределенным системам. Понятие промежуточной среды

Вопросы для самоподготовки:

1. Понятие распределенной системы.
2. Определение распределенной системы.
3. Программные компоненты.
4. Требования к распределенным системам.
5. Понятие промежуточной среды

Форма практического задания: Лабораторная работа «Использование промежуточных сред».

РУБЕЖНЫЙ КОНТРОЛЬ: форма рубежного контроля – отчет к лабораторным работам

РАЗДЕЛ 2. Взаимодействие компонентов распределенной системы

Цель: Ознакомление с основными видами Android-приложений.

Перечень изучаемых элементов содержания дисциплины

Модели взаимодействия компонент распределенной системы. Обмен сообщениями. Дальний вызов процедур. Использование удаленных объектов. Модель единственного вызова. Модель единственного экземпляра. Активация по запросу клиента. Состояние компоненты распределенной системы. Использование свойств удаленных объектов. Распределенные события. Распределенные транзакции. Безопасность в распределенных системах. Промежуточные среды в Microsoft .NET Framework

Вопросы для самоподготовки:

1. Модели взаимодействия компонент распределенной системы
2. Обмен сообщениями
3. Дальний вызов процедур
4. Использование удаленных объектов

5. Модель единственного вызова
6. Модель единственного экземпляра
7. Активация по запросу клиента
8. Состояние компоненты распределенной системы
9. Использование свойств удаленных объектов
10. Распределенные события
11. Распределенные транзакции
12. Безопасность в распределенных системах
13. Промежуточные среды в Microsoft .NET Framework

Форма практического задания: Лабораторная работа «Создание информационной системы распределенной обработки информации в рамках заданного бизнес-процесс».

РУБЕЖНЫЙ КОНТРОЛЬ: форма рубежного контроля – отчет к лабораторным работам

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю) .

Контрольным мероприятием промежуточной аттестации обучающихся по дисциплине (модулю) является экзамен, которые проводятся в письменной форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Код компетенции	Содержание компетенции	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-5	Способен использовать нормативные правовые акты в профессиональной деятельности	**Знать:** основы состав и основные направления организационно-технического и правового обеспечения информационной безопасности, основные нормативные международные и Российские правовые акты в области обеспечения	Этап формирования знаний

		информационной безопасности, ведомственные нормативные и методические документы, ФСБ России, ФСТЭК России, МВД России, Росгвардии и МЧС России, в области обеспечения защиты информации. **Уметь:** применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **Владеть:** профессиональной терминологией в области обеспечения информационной безопасности.	Этап формирования умений Этап формирования навыков и опыта
ОПК-7	Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных	Знать: принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода Уметь: Проводить анализ исходных	Этап формирования знаний

	процессов и особенностей функционирования объекта защиты	данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно-следственных связей. Владеть: • основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту информатизации; • методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования.	Этап формирования умений Этап формирования навыков и опыта
ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов	**Знать:** - основы электроники - основные физические законы, явления и процессы, на которых основаны принципы действия объектов профессиональной деятельности	Этап формирования знаний
		Уметь: использовать для решения прикладных задач соответствующий аппарат	Этап формирования умений
		Владеть: методами решения типовых задач в рамках профессиональной	Этап формирования навыков и опыта

		деятельности	
ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать:** - математический аппарат для решения профессиональных задач (ОПК-2) - инструментальные средства, языки и системы программирования для решения профессиональных задач **Уметь:** применять соответствующий математический аппарат для решения профессиональных задач **Владеть:** способностью применять соответствующий математический аппарат для решения профессиональных задач способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап формирования знаний Этап формирования умений Этап формирования навыков и опыта
ПК-9	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения информационной безопасности, так и работающих в пограничных сферах. **Уметь:** проводить	Этап формирования знаний

	по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	аналитический поиск сведений о появлении новых деструктивных факторах, воздействующих на объекты информатизации, современных организационных, технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации. **Владеть:** современными технологиями информационного поиска и дифференцированного анализа сведений о современных угрозах, методам и средствах защиты объектов информатизации.	Этап формирования умений Этап формирования навыков и опыта
ПК-14	Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать:** - сущность и содержание работы исполнителей - виды управленческих решений в области организации работ по проекту и нормированию труда - особенности процесса организации работы исполнителей **Уметь:** - анализировать содержание работы исполнителей - разрабатывать, анализировать и оценивать необходимость применения различных форм работы - разрабатывать план по реализации управленческих решений в области организации работ по проекту и нормированию труда навыками	Этап формирования знаний Этап формирования умений

		Владеть: - навыками анализа и установления форм и направлений деятельности в работе исполнителей - навыками оценки труда исполнителей - навыками разработки плана реализации управленческих решений в области организации работ по проекту и нормированию труда	Этап формирования навыков и опыта

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Этапы формирования компетенций	Показатель оценивания компетенции	Критерии и шкалы оценивания
ОПК-5; ОПК-7; ОПК-11; ПК-2; ПК-9; ПК-14	Этап формирования знаний	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не

			знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.
ОПК-5; ОПК-7; ОПК-11; ПК-2; ПК-9; ПК-14	Этап формирования навыков и опыта	Аналитическое задание *(задачи,)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части

			программного материала, допускает существенные ошибки -0-4 балла.

4.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Информационные процессы и системы

1. Применение булевой алгебры при анализе и синтезе узлов и при организации вычислений.
2. Законы алгебры логики.
3. Алгоритмы анализа и минимизации электрических схем аппаратных средств. Оценка сложности комбинационных схем.
4. Анализ и синтез электронных схем в различных базисах: (И, ИЛИ, НЕ), (И-НЕ), (ИЛИ-НЕ).
5. Конструктивные и функциональные модули.
6. Техническая реализация элементарных функций.
7. Интегральные микросхемы: основные характеристики, сравнение параметров.
8. Классификация элементов ВМ, их реализация в различных технологиях.
9. Классификация узлов ЭВМ. Виды и схемная реализация типовых узлов комбинационного и накапливающего типа. Назначение, виды и обозначение шифраторов, дешифраторов, сумматоров, схем сравнения, мультиплексоров.
10. Основы построения и функционирования устройств с памятью: особенности анализа и синтеза элементов с памятью.
11. Понятие триггера (RS, JK, T), их содержательное и математическое описание, схемная реализация. Назначение, виды и обозначение счетчиков, регистров.
12. Информационные системы в решении задач бизнеса.
13. Типы предприятий.
14. Концепции построения информационных систем управления.
15. Современные решения в области информационных систем управления.
16. Обзор стандартов и систем класса MRP, MRPII, ERP, ERPII, CSRP.
17. Структура планов, определяемая стандартом MRPII и методы их реализации.
18. Структура планов, определяемая стандартом ERP и методы их реализации.
19. Реферативная модель планирования и управления ресурсами предприятия ERP.
20. Комплекс требований к аппаратным и программно- технологическим средствам для построения и поддержки корпоративных порталов.
21. Анализ портальных решений в составе интегрированных систем управления предприятием
22. Системы управления взаимоотношениями с клиентами.
23. Система электронного документооборота
24. Теория моделирования. Система и элементы системы. Понятие модели. Цели моделирования.
25. Подходы к исследованию систем. Стадии разработки моделей.
26. Классификация моделей. Физические и математические модели.

27. Математическая модель. Основные этапы построения математической модели. Требования к математической модели. Уравнение <вход-выход>.
28. Уравнение состояния. Общесистемные и конструктивные модели. Этапы построения модели функционирования системы.
29. Дискретно- детерминированные модели. Автоматы Мили и Мура.
30. Теория массового обслуживания. Случайный процесс.
31. Математические модели простейших систем массового обслуживания
32. Моделирование систем и языки программирования. Классификация языков моделирования.
33. Измеряемые характеристики моделируемых систем. Математическое ожидание, дисперсия и среднее по времени значение выходной характеристики.
34. Блочные иерархические модели процессов функционирования систем. Особенности реализации процессов с использованием Q-схем.
35. Методы планирования эксперимента на модели. Факторы и реакции.
36. Функция отклика.
37. Стратегическое планирование машинных экспериментов с моделями систем.
38. Тактическое планирование машинных экспериментов с моделями систем

Технологии проектирования информационных систем

1. Понятие информационной системы в широком и узком смысле. Понятия проектирования ПС и проектирования ПО.
2. Предметная область: понятие, модель, цель моделирования, требования к моделям.
3. Бизнес-логика, бизнес-процесс, виды бизнес-процессов. Подходы к проектированию информационной системы.
4. Методология проектирования ПС: цель, задачи, эффект от внедрения.
5. Области проектирования ПС. Цель проекта по созданию ПС. Процесс и этапы создания ИС
6. Каноническое проектирование: понятие, этапы.
7. Наиболее распространенные стандарты на ЖЦ ПО: ГОСТ 34.601-90. CDM. RUP. MSF, XP.
8. Спиральная модель ЖЦ: понятие, риски, которые учитывает модель, прототипы, преимущества, недостатки.
9. Итеративная модель ЖЦ: понятие, преимущества, недостатки, пример.
10. Каскадная модель ЖЦ: понятие, область применимости, преимущества, недостатки, пример.
11. Жизненный цикл ПО: понятие, формальное описание, модель, процессы.
12. Требования пользователей к информационной системе: понятие, разработка, группы требований.
13. Виды требований по уровням. Этапы разработки требований по ГОСТ 34.
14. Обследование: понятие, этапы, использование результатов.
15. Формирование требований: этапы, источники.
16. Характеристики качества требований.
17. Методы выявления требований.
18. Этапы разработки концепции АС.
19. Техническое задание: понятие, решаемые задачи. Состав раздела «Общие сведения».
20. Состав раздела «Назначение и цели создания системы» ТЗ. Показатели объекта.
21. Состав подраздела «Требования к системе в целом» ТЗ. Пример.
22. Состав подраздела «Требования к функциям (по подсистемам)» ТЗ. Пример.
23. Состав подраздела «Требования к видам обеспечения» ТЗ. Примеры.
24. Состав разделов «Состав и содержание работ по созданию системы», «Порядок контроля и приемки системы» ТЗ.

25. Состав разделов «Требования к составу и содержанию работ по подготовке объекта к вводу системы в действие», «Требования к документированию».
26. Эскизный проект: понятие, содержание.
27. Технический проект: понятие, содержание разделов «Пояснительная записка», «Функциональная и организационная структура системы».
28. Содержание разделов. «Постановка задач и алгоритмы решения». «Организация информационной базы», «Система математического обеспечения» ТП.
29. Содержание разделов «Принцип построения комплекса технических средств», «Расчет экономической эффективности системы». «Мероприятия по подготовке объекта к внедрению системы» ТП.
30. Стадии «Создание рабочей документации» и «Испытания».
31. Понятия моделирования ПО и модели ПО. Уровни моделирования.
32. Требования к моделям ПО. Язык и нотация моделирования.
33. Определение, принципы и характеристики структурного анализа. Понятия системного анализа. Структурные модели ПО.
34. Объектные и функциональные модели ПО: понятие, уровни разработки.
35. Моделирование структуры управления: понятие, описание событий, уровни разработки.
36. Организационная структура: понятие, уровни моделирования.
37. Техническая структура: понятие, уровни моделирования.
38. Функциональная методика IDEF0: цель методики, понятия функционального блока, интерфейсной дуги, декомпозиции, глоссария.
39. Контекстная диаграмма IDEFO-модели, цель и точка зрения, выделение подпроцессов, туннели, ограничения сложности.
40. Процесс разработки IDEFO-модели. Достоинства IDEFO-модели.
41. Функциональная методика DFD: цель методики, контекстная диаграмма, поток данных, процесс, хранилище, внешняя сущность.
42. Процесс построения DFD-модели. Достоинства и недостатки DFD-модели
43. Объектно-ориентированная методика: отличия от функционального подхода, цель методики, принципы построения объектной модели.
44. Понятия языка моделирования и процесса моделирования. Сравнения функциональной и объектно-ориентированной методик.
45. Понятие архитектуры системы, моделирования архитектуры при помощи видов. Специфика систем реального времени, систем с архитектурой «клиент-сервер», распределенных систем.
46. Понятие вида, виды с точки зрения прецедентов, проектирования, процессов, реализации, развертывания.
47. Структура ИС. Понятие информационного обеспечения. Унифицированные системы документации.
48. Схемы информационных потоков. Задачи информационного обеспечения. Состав информационного обеспечения. Требования к информационному обеспечению.
49. Понятие внутримашинного информационного обеспечения. Электронная форма документа. Этапы проектирования форм электронных документов.
50. Понятие информационной базы. Требования к организации информации в информационной базе. Способы организации информационной базы.
51. Цель моделирования данных. Этапы проектирования информационной базы.
52. Информационно-логическая модель предметной области. Концептуальная и физическая модели.

Распределенные информационные системы

1. В чем состоит отличие между параллельной и распределенной системами?
2. Какие мотивации привели к созданию распределенных систем?

3. Что характеризует масштабируемое приложение и способы достижения масштабируемости?
4. Что такое прозрачность, формы прозрачности?
5. Что такое открытая система, ее преимущества?
6. Какие концепции аппаратных решений существуют для построения распределенных систем, их особенности?
7. Какие концепции программных решений существуют для построения распределенных систем, их особенности?
8. Какие преимущества и недостатки распределенных систем?
1. Что такое межуровневый интерфейс?
2. Что такое протокол?
3. Модель OSI, ее уровни и их назначение.
4. Что такое удаленный вызов процедур, заглушки? Опишите по шагам процесс удаленного вызова. Какие существуют расширенные модели RPC?
5. Как происходит обращение к удаленному объекту. В чем разница между статическим и динамическим обращение к объекту?
6. Что такое сохранность?
7. В чем отличие явной и неявной привязки ссылок на объект?
1. Какие типы связей существуют в распределенных системах и их примеры?
2. Какие требования предъявляются программистом к современным ОС?
3. Какие стандартные API имеются в современных ОС?
4. Что такое многозадачность и какие имеются разновидности.
5. Что такое многопоточность?
6. Что такое планировщик ОС и какие имеются алгоритмы планирования? Как реализован планировщик в Windows и UNIX-системах?
7. Что такое изоляция приложений и методы ее обеспечения?
8. Что такое взаимная блокировка (dead-lock) и как ее избежать?
9. Что такое инверсия приоритетов и как ее предотвратить,
10. Какие механизмы существуют для обмена данными между процессами?
11. Для чего необходимо управление правами доступа? Какие основные цели и средства описаны в «Критериях определения безопасности компьютерных систем»?
12. В чем стоит принцип мандатного управления доступом?
13. В чем стоит принцип избирательного (дискреционного) управления доступом?
14. Какие средства сетевого взаимодействия существуют в современных ОС?
15. Почему необходимо синхронизировать время в распределенной системе? Приведите пример.
16. Алгоритм Кристиана.
17. Алгоритм Беркли.
18. Децентрализованный алгоритм.
19. Понятие логического времени.
20. Отметки времени Лампорта.
21. Что такое глобальное состояние и алгоритм получения распределенного снимка состояния?
22. Алгоритмы голосования: алгоритм забияки и кольцевой алгоритм.
23. Алгоритмы взаимного исключения: централизованный и распределенный алгоритмы, алгоритм маркерного кольца.
24. Перечислите этапы развития реляционных СУБД и дайте определение основным понятиям теории реляционных БД.
25. В чем заключается целостность базы данных, перечислите операции реляционной алгебры?
26. Опишите модель сервера БД (DBS).

27. Опишите модель сервера приложений (AS).
28. Опишите эволюцию серверов БД.
29. Перечислите состав задач активного сервера.
30. Приведите аспекты сетевого взаимодействия в распределенных системах.
31. Сформулируйте принципы взаимодействия «клиент-сервер».
32. Опишите технологию распределения и тиражирования данных. Приведите пример гетерогенной системы.
33. Сравните технологии обработки данных в распределенной среде.
34. Что такое транзакция и в чем состоит принцип ACID? Какие примитивы транзакций вы знаете? Что такое вложенные транзакции и их особенность?
35. Как реализуются распределенные транзакции? Менеджеры транзакций.
36. Для чего используется журнал транзакций. Опишите механизм отката транзакций.
37. Опишите механизм распределенных транзакций.
38. Как организован одновременный доступ к данным. Опишите механизм блокировок.
39. В чем стоит принцип двухфазной блокировки? В чем отличие реализации централизованной и распределенной двухфазной блокировки?
40. Что такое оптимистичная блокировка?
41. Какие компоненты составляют архитектуру CORBA?
42. Что такое ORB и какие задачи он решает?
43. Как описывается интерфейс к объекту в CORBA?
44. Зачем нужны IDL-стабы (заглушки)?
45. Что такое интерфейс динамических вызовов?
46. Что такое репозиторий интерфейсов?
47. Что такое сервант?
48. Что такое IIOP/GIOP?
49. В чем состоит роль объектного адаптера?
50. Какие модели многопоточности поддерживает POA?
51. Какие изменения внесла новая спецификация CORBA 3.0 в объектный адаптер?
52. Опишите как происходит вызов метода объекта в CORBA.
53. Какие службы определены в CORBA и их задачи.
54. На какой технологии базируется DCOM и какие новшества она привнесла?
55. От какого интерфейса наследуются все интерфейсы в DCOM и какие задачи решает этот базовый интерфейс?
56. Через какой интерфейс происходит динамическое обращение к объекту в DCOM?
57. Какую функцию выполняет библиотека типов в DCOM?
58. В чем похожи и чем отличаются технологии CORBA и DCOM?
59. Опишите, какие модели доступа существуют в распределенной файловой системе?
60. Опишите базовую архитектуру NFS.
61. Какие задачи решает виртуальная файловая система (VFS)?
62. Какова модель файловой системы NFS?
63. Какие изменения произошли в протоколе NFS версии 4 по сравнению с версией 3?
64. Именование в файловой системе NFS.
65. Какие существуют семантики совместного использования файлов?
66. Каким образом реализуется блокировка в NFS?
67. Каким образом осуществляется кэширование и репликация в NFS?
68. Каким образом RPC решает проблему отказов?
69. Какие существуют методы аутентификации в NFS?
70. Каковые основные проблемы теории и практики распределенных систем?
71. Каковы особенности обработка информации в суперсетях (Грид)?
72. Расскажите о основных принципах построения архитектуры Грид.
73. Что такое мобильный компьютинг?
74. Что называют глобальным «умным» пространством?

4.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестации по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20-балльной шкале, а итоговая оценка по дисциплине (модулю) выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля) .

5.1.1. Основная литература

1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249
2. Смирнов, В.И. Защита информации / В.И. Смирнов ; Поволжский государственный технологический университет. – Йошкар-Ола : ПГТУ, 2017. – 67 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=476512 – Библиогр. в кн. – ISBN 978-5-8158-1866-8. – Текст : электронный

5.1.2. Дополнительная литература

1. Программно-аппаратные средства защиты информационных систем / Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков ; Министерство образования и науки Российской Федерации, Федеральное государственное джетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499013 – Библиогр.: с. 190. – ISBN 978-5-8265-1737-6. – Текст : электронный

2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=428820. – Текст : электронный

5.2. Перечень ресурсов информационно-коммуникационной сети «Интернетнеобходимых для освоения дисциплины (модуля)

№№	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и	http://elibrary.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
		патентов	
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) **«Сети и системы передачи информации»** предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины (модуля) . Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

5.4. Информационно-технологическое обеспечение образовательного процесса по дисциплине (модулю)

5.4.1. Информационные технологии

1. Персональные компьютеры;

2. Доступ к Интернет
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.5. Информационные справочные системы и профессиональные базы данных

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.6. Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) **«Сети и системы передачи информации»** используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения: проектором для электронных презентаций и экраном; компьютерное и мультимедийное оборудование для поиска и

изучения справочной информации, нормативных правовых актов, учебной и научной литературы на официальных сайтах органов государственного управления, различных организаций и учреждений; компьютерные справочно-правовые системы для поиска необходимых документов, установленные в компьютерных классах РГСУ (Консультант-Плюс, Гарант, и др.); электронная библиотека университета.

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения: проектором для электронных презентаций и экраном; компьютерное и мультимедийное оборудование для поиска и изучения справочной информации, нормативных правовых актов, учебной и научной литературы на официальных сайтах органов государственного управления, различных организаций и учреждений; компьютерные справочно-правовые системы для поиска необходимых документов, установленные в компьютерных классах РГСУ (Консультант-Плюс, Гарант, и др.); электронная библиотека университета.

5.7. Образовательные технологии

При реализации дисциплины (модуля) **«Сети и системы передачи информации»** применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины (модуля) предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме деловых и ролевых игр, разбора конкретных ситуаций в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. Учебные часы дисциплины предусматривают классическую контактную работу преподавателя с обучающимся в аудитории.

В рамках дисциплины (модуля) **«Сети и системы передачи информации»** предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/
«06» __июня___2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ПРОГРАММИРОВАНИЕ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технология защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022

Рабочая программа дисциплины (модуля) **«Программирование»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.04 "Информационная безопасность" (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
– *06.032 Специалист по безопасности компьютерных систем и сетей*
– *06.033 Специалист по защите информации в автоматизированных системах*
- 06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля) разработана рабочей группой в составе: д-р. техн. наук, профессора Кораблин Ю.П., к.ф.-м.н., доцент Красников А. С.

Руководитель основной профессиональной образовательной программы
к.п.н., доцент _____ Н.Г. Витковская
(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года

Декан факультета
К.п.н. доцент _____ С.В. Крапивка
(подпись)

Рабочая программа дисциплины (модуля) рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет»
зам. ген. директора по науке,
к.т.н., доцент _____ А.С. Мосолов
(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

ФГБОУ ВО «Московский политехнический университет», НОЦ инфокогнитивных технологий, доктор технических наук, профессор _____ Н.И. Гданский
(подпись)

к.т.н., доцент кафедры информационных систем, сетей и безопасности _____ В.Л. Симонов
(подпись)

Согласовано
Научная библиотека, директор _____ И.Г. Маляр
(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) заключается в получении обучающимися знаний о теоретических основах программирования и анализа создаваемых программ с последующим применением в профессиональной сфере и практических навыков решения задач разработки и тестирования программ.

Задачи дисциплины (модуля) :

1. изучение основных понятий, методов, приемов и средств алгоритмизации обработки данных на ЭВМ и технологии структурного программирования на языке высокого уровня;
2. приобретение навыков разработки, тестирования, отладки и документирования программных продуктов с использованием изучаемой в курсе системы программирования;
3. формирование базовых знаний, умений и навыков для успешного (в т. ч. самостоятельного) освоения различных технологий и средств программирования.

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы

Учебная дисциплина «Программирование» реализуется в вариативной части основной профессиональной образовательной программы «Информационная безопасность» по направлению подготовки «10.03.01 Информационная безопасность» очной формы обучения.

Изучение дисциплины (модуля) «Программирование» является базовым для последующего освоения программного материала учебных дисциплин базовой и вариативной части, а также при прохождении учебных и производственных практик

1.3. Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основной профессиональной образовательной программы

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих общепрофессиональных и профессиональных компетенций: ПК-2, ПК-3, ПК-8 в соответствии с основной профессиональной образовательной программой «Информационная безопасность» по направлению подготовки «10.03.01 Информационная безопасность».

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
	ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы	ПК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-2.ИД-2. Планирует и	Знать: - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ - основы администрировани

		программирования для решения профессиональных задач	выполняет практические действия в рамках компетенции ПК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	я вычислительных сетей - системы управления БД
				Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
				Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации
	ПК-3	Способен администрировать подсистемы информационной безопасности объекта защиты	ПК-3.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции	Знать: - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ

			ПК-3.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-3.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	- основы администрирования вычислительных сетей - системы управления БД - эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности - основные направления политик защиты информации на предприятии (организации) - возможные угрозы информационной безопасности, связанные с аспектами деятельности предприятия (организации), особенностями технологических процессов, организационной структуры и др.
				Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействиия

				нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты - выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации
				Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации
	ПК-8	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-8.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-8.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Знать: критерии защищенности объекта информатизации, состав оборудования и методологию контроля, изложенных в нормативно-методических документах, федерального, ведомственного и производственного уровней.

				Уметь: при оформлении отчетных материалов четко формулировать цель проведенных работ, объект и предмет работ, результаты инструментальных исследований, выводы и рекомендации по результатам проведенных работ, в понятной, как техническому специалисту, так и специалисту в сфере управления форме.
				Владеть: навыками написания отчетных материалов, в том числе технически и экономически обоснованных выводов и рекомендаций, в понятной как техническому специалисту, так и специалисту в сфере управления форме.

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем дисциплины (модуля) , включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 19 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		1	2	3	4	
Контактная работа обучающихся с педагогическими работниками	**342**	**54**	**90**	**108**	**90**	
Учебные занятия лекционного типа	66	12	18	18	18	
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						

Лабораторные занятия	124	18	32	42	32	
из них: в форме практической подготовки						
Иная контактная работа	152	24	40	48	40	
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**252**	**45**	**54**	**99**	**54**	
из них: в форме практической подготовки	*27*	*9*	*3*	*12*	*3*	
Контроль промежуточной аттестации	**90**	**9**	**36**	**9**	**36**	
Форма промежуточной аттестации		зачет	экзам	зачет	экзам	
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**684**	**108**	**180**	**216**	**180**	

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	**Виды учебной работы, академических часов**												
	Всего	**Самостоятельная работа**	*из них: в форме практической подготовки*	**Контактная работа обучающихся с педагогическими работниками**									
				Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*
Модуль 1 (семестр 1)													
Раздел 1.1	33	15	*3*	18		4				6		8	
Раздел 1.2	33	15	*3*	18		4				6		8	
Раздел 1.3	33	15	*3*	18		4				6		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**108**	**45**	***9***	**54**		**12**				**18**		**24**	
Форма промежуточной аттестации	**зачет**												

Модуль 2 (семестр 2)													
Раздел 2.1	24	18	*1*	30		6				10		14	
Раздел 2.2	24	18	*1*	30		6				12		14	
Раздел 2.3	24	18	*1*	30		6				10		12	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**180**	**54**	***3***	**90**		**18**				**32**		**40**	
Форма промежуточной аттестации	**экзамен**												
Модуль 3 (семестр 3)													
Раздел 3.1	33	24	*3*	18		4				10		12	
Раздел 3.2	34	24	*3*	18		4				10		12	
Раздел 3.3	34	26	*3*	18		4				10		12	
Раздел 3.4	34	25	*3*	18		6				12		12	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**216**	**99**	***12***	**108**		**18**				**42**		**48**	
Форма промежуточной аттестации	**зачет**												
Модуль 4 (семестр 4)													
Раздел 4.1	48	18	*1*	30		6				10		14	
Раздел 4.2	48	18	*1*	30		6				10		14	
Раздел 4.3	48	18	*1*	30		6				12		12	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**180**	**54**	***3***	**90**		**18**				**32**		**40**	
Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**684**	**252**	***27***	**342**		**66**				**124**		**152**	

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1. Виды самостоятельной работы обучающихся по дисциплине

Раздел, тема	Всего	Виды самостоятельной работы обучающихся					
		Академическая активность, час	Форма академической активности	Выполнение практ. заданий, час	Форма практического задания	Рубежный текущий контроль, час	Форма рубежного текущего контроля
Модуль 1 (семестр 1)							
Раздел 1.1	15	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	15	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	15	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**45**	**18**		**21**		**6**	
Модуль 2 (семестр 2)							
Раздел 2.1	18	8	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	18	8	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 2.3	18	8	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**54**	**24**		**24**		**6**	
Модуль 3 (семестр 3)							
Раздел 3.1	24	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.2	24	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.3	24	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 3.4	27	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**99**	**27**		**28**		**8**	
Модуль 4 (семестр 4)							
Раздел 4.1	18	8	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4.2	18	8	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 4.3	18	8	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**54**	**24**		**24**		**6**	
Общий объем по дисциплине (модулю), часов	**252**	**93**		**97**		**26**	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю»)

МОДУЛЬ 1. «ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ»

РАЗДЕЛ 1. ОСНОВЫ АЛГОРИТМИЗАЦИИ, ЯЗЫКИ И СИСТЕМЫ ПРОГРАММИРОВАНИЯ.

Цель: овладеть основными понятиями алгоритмизации, получить практические навыки построения алгоритмов.

Перечень изучаемых элементов содержания:

Структура ЭВМ и программный принцип управления Дж. фон Неймана. Характеристика основных устройств ЭВМ; процессор, оперативная память, внешние устройства. Программное и аппаратное обеспечение ЭВМ.

Алгоритм. Свойства алгоритма. Формы записи алгоритма. Основные алгоритмы. Понятие о языках программирования, общая характеристика языков. Основные элементы языка: алфавит, ключевые слова, идентификаторы, синтаксические диаграммы и нотации Бэкуса-Наура.Структура программы. Разделы описания и операторов. Операторы как элементы действия алгоритма. Программные блоки: программы, подпрограммы, модули, объекты. Понятие о типе данных. Языки сильной типизации данных. Основные стандартные типы данных: целые и вещественные числа, булевский тип, символьный тип, строки. Константы и переменные. Выражения (арифметические, логические, символьные, строковые). Описание переменных и констант в программе. Оператор присваивания и его использование. Соответствие типов в операторе присваивания. Автоматическое преобразование в выражениях и операторах присваивания. Функции преобразования типов. Композиция условий и операторов и ее использование. Операторы if-then-else и if-then. Использование операторных скобок. Примеры программ с разветвляющейся структурой алгоритмов. Итерационные циклы. Примеры использования итерационных циклов. Проблема завершения циклов. Цикл разработки программы и его этапы. Проект программы и основные его разделы: входные и выходные переменные, аномалии, экранная форма. Разработка алгоритма задачи. Использование блок-схем алгоритмов и псевдокодов. Примеры разработки алгоритмов.

Вопросы для самоподготовки:

1. Какие основные этапы включает в себя решение задач на компьютере?
2. Какие этапы компьютерного решения задач осуществляются без участия компьютера?

3. Из каких последовательных действий состоит процесс разработки программы?
4. Что называется алгоритмом?
5. Какими основными свойствами должен обладать алгоритм?
6. Какие существуют способы описания алгоритмов?
7. Какими графическими символами принято изображать в схемах алгоритма?
8. Использование блок-схем алгоритмов и псевдокодов.
9. Понятие типа данных.
10. Простые операторы языка программирования (ввода-вывода, присваивания, ветвления).
11. Циклические конструкции в языках программирования.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 2 ПРОГРАММИРОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ АЛГОРИТМОВ НА ЯЗЫКЕ ВЫСОКОГО УРОВНЯ (ПАСКАЛЬ JAVA, C).

Цель: овладеть теоретическими знаниями и практическим опытом разработки программ на выбранном языке программирования.

Перечень изучаемых элементов содержания:

Типы данных, конструируемые программистом. Операторы выбора. Использование селектора для альтернативного выбора из нескольких возможностей. Примеры программ с оператором выбора и перечислимыми типами. Описание массивов. Индексы и доступ к элементу массива. Одномерные массивы (векторы) и двумерные массивы (матрицы). Циклы с параметром for-to и for-downto. Примеры использования циклов с параметром для обработки массивов. Вложенные циклы. Ограничение на параметр и границы изменения параметра. Концепция множества. Описание множества. Константы типа множества и конструктор множества. Операции и отношения над множеством. Принадлежность множеству. Присваивание множествам. Примеры программ с использованием множеств. Структурирование неоднородных данных. Описание типа Запись. Поля записи и их идентификация. Доступ к полям записи: составные имена и оператор with-do. Примеры программ обработки записи данных. Концепция файлов, виды файлов и их описание. Стандартные операторы и функции работы с файлами. Текстовые файлы и их особенности. Структура текстового файла. Работа с текстовыми файлами. Примеры программ обработки текстовых файлов

Вопросы для самоподготовки:

1. Совместимость и приведение типов данных.
2. Одномерные массивы (векторы) и двумерные массивы (матрицы). Индексы и доступ к элементу массива.
3. Концепция множества. Описание множества. Константы типа множества и конструктор множества.
4. Операции и отношения над множеством. Принадлежность множеству. Присваивание множествам.
5. Описание типа Запись. Поля записи и их идентификация.
6. Доступ к полям записи: составные имена и оператор with-do.
7. Концепция файлов, виды файлов и их описание. Стандартные операторы и функции работы с файлами.
8. Текстовые файлы и их особенности. Структура текстового файла. Работа с текстовыми файлами.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 3. ПОДПРОГРАММЫ (МЕТОДЫ) И МОДУЛИ В ЯЗЫКАХ ПРОГРАММИРОВАНИЯ И ИХ ИСПОЛЬЗОВАНИЕ.

Цель: познакомиться с основными методами разработки программного обеспечения на основе процедурного и модульного подхода.

Перечень изучаемых элементов содержания:

Основные парадигмы программирования. Понятие структурного программирования. Концепция подпрограммы. Процедуры и функции как подпрограммы. Механизм связи подпрограммы с основной программой. Формальные и фактические параметры . Параметры-значения, параметры-переменные. Структура описания процедуры. Вызов процедуры. Примеры программ с процедурами. Стандартные процедуры. Структуры описания функции. Вызов функции. Примеры программ с функциями. Побочный эффект в функциях и его предотвращение. Типы значений функции. Расширенный синтаксис вызова функций. Использование параметров-массивов и параметров-процедур в подпрограммах. Процедурные типы. Области действия имен. Глобальные и локальные имена в программе. Использование глобальных имен для связи с подпрограммами. Концепция модуля. Структура описания модуля: разделы интерфейса, реализации и инициализации. Раздел завершения модуля. Компиляция модулей. Использование модулей в программах. Особенности методики разработки программ с подпрограммами и модулями. Стандартные модули. Стандартные графические модули.

Вопросы для самоподготовки:

1. Основные парадигмы программирования.
2. Понятие структурного программирования.
3. Процедуры и функции как подпрограммы. Механизм связи подпрограммы с основной программой.
4. Формальные и фактические параметры . Параметры-значения, параметры-переменные.
5. Описания процедур и функций. Вызов процедуры и вызов функции.
6. Стандартные процедуры и функции.
7. Побочный эффект в функциях и его предотвращение.
8. Использование параметров-массивов и параметров-процедур в подпрограммах. Процедурные типы.
9. Области действия имен. Глобальные и локальные имена в программе. Использование глобальных имен для связи с подпрограммами.
10. Концепция модуля. Структура описания модуля: разделы интерфейса, реализации и инициализации. Раздел завершения модуля.
11. Особенности разработки программ с подпрограммами и модулями. Стандартные модули. Стандартные графические модули.

.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – защита лабораторных работ.

Примерный перечень тем лабораторных работ модуля 1 **«ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ»**

1. Лабораторная работа № 1. Циклические алгоритмы. Вывод результатов в теле цикла.
2. Лабораторная работа № 2. Накопление результатов в цикле.
3. Лабораторная работа № 3. Построение циклических алгоритмов с разветвлением в теле цикла.
4. Лабораторная работа № 4. Разработка циклических программ с исследованием природы итерационных циклов.
5. Лабораторная работа № 5. Использование простого цикла for для обработки одномерных массивов.
6. Лабораторная работа № 6. Использование кратного цикла for для обработки двумерных массивов (матриц).
7. Лабораторная работа № 7. Программирование задач с разными структурами данных: 1) исходные данные – простые переменные; 2) исходные данные – массивы.
8. Лабораторная работа № 8. Разработка сложных алгоритмов на матрицах с использованием метода нисходящего проектирования.
9. Лабораторная работа № 9. Разработка процедур и функций Турбо Паскаля для задач, рассмотренных на предыдущих лабораторных занятиях. Формальные и фактические параметры процедур.
10. Лабораторная работа № 10. Разработка программ с процедурами-параметрами.
11. Лабораторная работа № 11. Тип Запись как средство для программирования алгоритмов обработки документов сложной структуры.
12. Лабораторная работа № 12. Модули: разработка и использование.

МОДУЛЬ 2. «АЛГОРИТМЫ И СТРУКТУРЫ ДАНЫХ»

РАЗДЕЛ 1. СОРТИРОВКИ. МЕТОД ДЕКОМПОЗИЦИИ. ОЦЕНКИ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ.

Цель: изучить теоретические основы и получить практические навыки анализа корректности и оценки временных параметров выполнения алгоритмов.

Перечень изучаемых элементов содержания: Сортировка методом вставки (Insertion_Sort). Инварианты цикла и корректность сортировки вставкой. Время работы алгоритма Insertion_Sort. Сортировка методом выбора (Selection_Sort). Инварианты цикла и корректность сортировки вставкой. Время работы алгоритма Selection_Sort. Метод декомпозиции. Алгоритм *сортировки слиянием* (Merge sort) . Корректность сортировки методом слияния. Время работы алгоритма Merge sort. Асимптотические оценки: θ, O, o, Ω, ω. Сравнение асимптотических функций Рекуррентные соотношения. Методы решения рекуррентных уравнений. Алгоритм пирамидальной сортировки и оценка его эффективности. Быстрая сортировка (Quick_Sort). Рандомизированная версия быстрой сортировки. Блуждающая сортировка (Stooge_Sort). Оценка эффективности сортировок

Вопросы для самоподготовки:

1. Понятие инварианта цикла и его применение для доказательства частичной корректности программ.
2. Реализация алгоритмов сортировки вставкой и выборкой на языке высокого уровня (Java, C++, Паскаль).
3. Доказательство корректности сортировки вставкой..
4. Доказательство корректности сортировки выборкой..
5. Исследование временных характеристик работы алгоритмов сортировки вставкой и выборкой.

6. Реализация алгоритма сортировки слиянием на языке высокого уровня (Java, C++, Паскаль).
7. Доказательство корректности сортировки алгоритмом Merge sort.
8. Исследование временных характеристик работы алгоритма сортировки Merge sort.
9. Нахождение асимптотических оценок выполнения алгоритма методом вставки (Insertion_Sort).
10. Нахождение асимптотических оценок выполнения алгоритма методом выборки (Selection_Sort).
11. Нахождение асимптотических оценок выполнения алгоритма методом слияния (Merge _Sort). Понятие пирамиды. Убывающая и возрастающая пирамиды..
12. Анализ эффективности алгоритма пирамидальной сортировки, алгоритма быстрой сортировки, алгоритма блуждающей сортировки

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 2. СТРУКТУРЫ ДАННЫХ. СТЕКИ, ОЧЕРЕДИ, СПИСКИ И ОПЕРАЦИИ НАД НИМИ. КОРНЕВЫЕ ДЕРЕВЬЯ. БИНАРНЫЕ ДЕРЕВЬЯ. ОПЕРАЦИИ С БИНАРНЫМ ДЕРЕВОМ ПОИСКА.

Цель: изучить теоретические основы и получить практические навыки использования различных структур данных для разработки программного обеспечения.

Перечень изучаемых элементов содержания: Определение бинарного дерева. Алгоритм бинарного поиска в таблице с прямым доступом и с упорядоченными именами. Анализ эффективности бинарного поиска. Корневое дерево, лес, бинарное дерево. Машинное представление деревьев. Стратегии прохождения деревьев. Расширенные бинарные деревья, внутренние и внешние узлы. Полностью сбалансированные деревья. Связанные списки, стеки и очереди. Операции включения и исключения для этих структур. Циклический список и дважды связанный список. Реализация списка (с помощью 3-х массивов и с помощью одного массива). Стеки, примеры их использования. Реализация стека: Алгоритмы включения и выдачи элементов стека Очереди, примеры их использования. Реализация очереди. Алгоритмы включения и выдачи элемента очереди. Реализация указателей и объектов**.** Вставка (удаление) элемента (значения *v*) в динамическое множество, представленное бинарным деревом поиска. Понятие об оптимальных деревьях поиска при известных частотах обращений.

Вопросы для самоподготовки:

1. Понятия списка, стека, очереди.
2. Реализация операций на списках, стеках и очередях.
3. Реализация указателей и объектов..
4. Реализация алгоритма сортировки с помощью упорядоченного списка.
5. Анализ эффективности алгоритма сортировки с использованием упорядоченного списка.
6. Построение бинарного дерева поиска..
7. Анализ эффективности операций на бинарном дереве поиска.
8. Полностью сбалансированные деревья. Красно-черные деревья.
9. Алгоритм сортировки с использованием красно-черного дерева.
10. Разработка программы построения красно-черного дерева.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 3. ХЕШИРОВАНИЕ. ХЕШ-ФУНКЦИИ. МЕТОДЫ РАЗРАБОТКИ ХЕШ-ТАБЛИЦ.

Цель: получить практические навыки работы с инструментальными средствами поддержки приложений, предназначенных для хранения больших объемов информации, и повышения быстродействия при работе с этими приложениями.

Перечень изучаемых элементов содержания: Хеширование. Способы построения хеш-функций. Схемы поиска, включения и исключения в идеальной хеш-таблице. Понятие коллизии и простейший метод разрешения коллизий поиска.

Вопросы для самоподготовки:

1. Понятие хеш-функции.
2. Способы создания хеш-таблиц.
3. Выбор размера хеш-таблицы.
4. Выбор хеш-функции.
5. Разработать словарь иностранного языка на 50 слов с использованием хеш-таблицы

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – защита лабораторных работ.

Примерный перечень тем лабораторных работ модуля 2 «АЛГОРИТМЫ И СТРУКТУРЫ ДАНЫХ»

Лабораторная работа № 1 «Простые алгоритмы сортировки и их анализ»
Лабораторная работа № 2 «Алгоритм сортировки слиянием Merge_Sort и его анализ»
Лабораторная работа № 3 «Быстрая сортировка. Рандомизированная быстрая сортировка»
Лабораторная работа № 4 «Пирамидальная сортировка»
Лабораторная работа № 5 Сортировка на упорядоченных списках»
Лабораторная работа № 6 «Сортировка с использованием бинарных деревьев поиска»
Лабораторная работа № 7 «Разработка хеш-таблицы для создания англо-русс кого словаря»

МОДУЛЬ 3. «ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ ПРОГРАММИРОВАНИЕ»

РАЗДЕЛ 1. ОСНОВЫ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ.

Цель: изучить теоретические основы и освоить практические навыки модульного программирования.

Перечень изучаемых элементов содержания: Эволюция методологий программирования. Парадигмы программирования. Основные принципы объектного подхода. Абстрагирование. Инкапсуляция. Модульность. Иерархия. Типизация. Параллелизм. Сохраняемость. Объект с точки зрения ООП. Состояние. Поведение. Идентичность и жизненный цикл объектов. Взаимоотношения между объектами. Природа классов. Метамодель. Инстанцирование. Структура класса. Абстрактные классы и интерфейсы. Отношения между классами. Ассоциация и агрегация. Иерархии классов. Зависимость.

Вопросы для самоподготовки:

1. Эволюция методологий программирования. Парадигмы программирования.
2. Основные принципы объектного подхода. Абстрагирование.
3. Основные принципы объектного подхода. Инкапсуляция.
4. Основные принципы объектного подхода. Модульность.
5. Основные принципы объектного подхода. Иерархия.
6. Основные принципы объектного подхода. Типизация.
7. Основные принципы объектного подхода. Параллелизм. Сохраняемость.
8. Объект с точки зрения ООП. Состояние. Поведение.
9. Объект с точки зрения ООП. Идентичность и жизненный цикл объектов.

10. Объект с точки зрения ООП. Взаимоотношения между объектами.
11. Классы. Природа классов. Метамодель. Инстанцирование.
12. Классы. Структура класса. Абстрактные классы и интерфейсы.
13. Классы. Отношения между классами. Ассоциация и агрегация.
14. Классы. Иерархии классов. Зависимость.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 2. ПРОЕКТИРОВАНИЕ ПРОГРАММ.

Цель: получить практические навыки проектирования программ.

Перечень изучаемых элементов содержания: Архитектура программного обеспечения. Методы проектирования программных продуктов.

Вопросы для самоподготовки:

Архитектура программного обеспечения.

Методы проектирования программных продуктов.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 3. РАЗРАБОТКА ПРОЕКТОВ.

Цель: познакомиться с основными методами разработки программного обеспечения.

Перечень изучаемых элементов содержания: методология разработки программного обеспечения.

Вопросы для самоподготовки:

Методология разработки программного обеспечения.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – защита лабораторных работ.

МОДУЛЬ 4. «ТЕХНОЛОГИИ ПРОГРАММИРОВАНИЯ

РАЗДЕЛ 1. СЛОЖНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ПУТИ ОГРАНИЧЕНИЯ СЛОЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ЭВОЛЮЦИЯ ТЕХНОЛОГИЙ ПРОГРАММИРОВАНИЯ.

Цель: изучить теоретические основы и получить практические навыки оценки сложности программного обеспечения.

Перечень изучаемых элементов содержания: Промышленные программные продукты. Признаки сложности программных продуктов. Пути ограничения сложности программного обеспечения. Алгоритмическая декомпозиция. Объектно-ориентированная декомпозиция. Эволюция технологий программирования. Краткий обзор: процедурный стиль программирования, функциональный стиль программирования, логическое программирование, структурное программирование, объектно-ориентированное программирование.

Вопросы для самоподготовки:

1. Промышленные программные продукты.
2. Признаки сложности программных продуктов.
3. Пути ограничения сложности программного обеспечения.
4. Алгоритмическая декомпозиция.
5. Объектно-ориентированная декомпозиция.
6. Эволюция технологий программирования.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 2. ПОДХОДЫ К РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.

Цель: изучить теоретические основы и получить практические навыки использования различных подходов к разработке программного обеспечения.

Перечень изучаемых элементов содержания: Функциональная декомпозиции: выделение функций, организация иерархических структур, определение обмена информацией. Метод функционального моделирования SADT: принципы построения диаграмм декомпозиции, состав функциональной модели. Моделирование потоков данных: потоки, внешние сущности, процессы, накопители данных. Моделирование данных: создание концептуальной базы данных, сущности, связи, атрибуты.

Вопросы для самоподготовки:

1. Функциональная декомпозиции: выделение функций, организация иерархических структур, определение обмена информацией.
2. Метод функционального моделирования SADT: принципы построения диаграмм декомпозиции, состав функциональной модели.
3. Моделирование потоков данных: потоки, внешние сущности, процессы, накопители данных.
4. Моделирование данных: создание концептуальной базы данных, сущности, связи, атрибуты

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – защита лабораторных работ.

РАЗДЕЛ 3. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ПОДДЕРЖКИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.

Цель: получить практические навыки работы с инструментальными средствами поддержки разработки программного обеспечения.

Перечень изучаемых элементов содержания: CASE- средства для анализа и разработки программ и документирования результатов. Создание программ с использованием All Fusion Process Modeler. Инструментальная среда Bpwin разработки функциональных модулей. Инструментальная среда DFD для создания моделей потоков данных. Создание моделей данных с помощью Erwin Data Modeling.

Вопросы для самоподготовки:

1. CASE- средства для анализа и разработки программ и документирования результатов.
2. Создание программ с использованием All Fusion Process Modeler.
3. Инструментальная среда Bpwin разработки функциональных модулей.
4. Инструментальная среда DFD для создания моделей потоков данных.
5. Создание моделей данных с помощью Erwin Data Modeling.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторная работа

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – защита лабораторных работ.

Оформление работ, выполняемых в рамках самостоятельной работы осуществляется в соответствии с Методическими указаниями по оформлению письменных работ обучающихся в рамках самостоятельной работы, утвержденными Учебно-методическим советом РГСУ, Протокол № 2 от 25 июня 2015 года.

Конкретные практические задания и задания для рубежного контроля определяются в учебно-методических материалах по работе обучающихся в электронной информационно-образовательной среде РГСУ с применением технологий электронного обучения по данной дисциплине, утверждаемых ежегодно.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по дисциплине (модулю) являются зачеты (семестр 1, 3) по итогам выполнения лабораторных работ и экзамен (семестр 2, 4), который проводится в устной форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать: программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования	Этап формирования знаний
		Уметь: применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап формирования умений
		Владеть: программными средствами системного, прикладного и специального назначения, инструментальными средствами, языками и системами программирования для решения	Этап формирования навыков и получения опыта

		профессиональных задач	
ПК-3	Способен администрировать подсистемы информационной безопасности объекта защиты	Знать: - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ - основы администрирования вычислительных сетей - системы управления БД - эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности - основные направления политик защиты информации на предприятии (организации) - возможные угрозы информационной безопасности, связанные с аспектами деятельности предприятия (организации), особенностями технологических процессов, организационной структуры и др.	Этап формирования знаний
		Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействиия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты - выполнять работы по установке, конфигурированию и эксплуатации технических	Этап формирования умений

		и программных средств обеспечения информационной безопасности и защиты информации	
		Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Этап формирования навыков и получения опыта
ПК-8	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать: критерии защищенности объекта информатизации, состав оборудования и методологию контроля, изложенных в нормативно-методических документах, федерального, ведомственного и производственного уровней.	Этап формирования знаний
		Уметь: при оформлении отчетных материалов четко формулировать цель проведенных работ, объект и предмет работ, результаты инструментальных исследований, выводы и рекомендации по результатам проведенных работ, в понятной, как техническому специалисту, так и специалисту в сфере управления форме.	Этап формирования умений
		Владеть: навыками написания отчетных материалов, в том числе технически и экономически обоснованных выводов и рекомендаций, в понятной как техническому специалисту, так и специалисту в сфере управления форме.	Этап формирования навыков и получения опыта

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	**Этапы формирования компетенций**	**Показатель оценивания компетенции**	**Критерии и шкалы оценивания**
ПК-2, ПК-3, ПК-8	Этап формирования знаний	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.

ПК-2, ПК-3, ПК-8	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией - 9-10 баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании -7-8 баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению5-6 баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания - 0-4 баллов.
ПК-2, ПК-3, ПК-8	Этап формирования навыков и получения опыта	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

4.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Теоретический блок вопросов:

1. Какие основные этапы включает в себя решение задач на компьютере?

2. Какие этапы компьютерного решения задач осуществляются без участия компьютера?
3. Что называют математической моделью объекта или явления?
4. Почему невозможно точное исследование поведения объектов или явлений?
5. Какие способы моделирования осуществляются с помощью компьютера?
6. Из каких последовательных действий состоит процесс разработки программы?
7. Что называется алгоритмом?
8. Какими основными свойствами должен обладать алгоритм?
9. Какие существуют способы описания алгоритмов?
10. Какими графическими символами принято изображать в схемах алгоритма?
11. Системное и специальное ПО.
12. Инструментальная среда программирования.
13. Языки программирования и их краткая характеристика.
14. Специальное ПО и этапы его разработки.
15. Технология разработки программ на алгоритмическом языке.
16. Документируемость ПО.
17. Основные парадигмы программирования.
18. Понятие структурного программирования.
19. Понятие объектно-ориентированного программирования.
20. Понятие функционального программирования.
21. Определение алгоритма. Свойства алгоритма. Формы записи алгоритмов. Примеры.
22. Запись алгоритмов блок-схемами. Основные элементы блок-схем.
23. Алгоритмы с ветвлением. Пример алгоритма.
24. Алгоритм цикла с предусловием. Пример алгоритма.
25. Алгоритм цикла с постусловием. Пример алгоритма.
26. Алгоритм цикла с управляющей переменной. Пример алгоритма.
27. Основные типы данных
28. Целый и вещественный типы данных. Операции с переменными этого типа.
29. Логический тип данных. Символьный тип данных. Операции с переменными этого типа.
30. Назовите поколения языков программирования и их характеристики.
31. Дайте определение алфавита и лексики языка программирования. Приведите пример.
32. Дайте определение синтаксиса и семантики программирования. Приведите пример.
33. Из каких частей состоит исходная программа.
34. Что такое система программирования. Назовите классы систем программирования.
35. Объясните суть процессов трансляции и компиляции.
36. Что такое библиотеки подпрограмм и для чего их используют.
37. Файл. Типы файлов.
38. Общие принципы разработки ПО.
39. Частотный принцип разработки ПО и принцип модульности.
40. Принцип функциональной избирательности при разработке ПО и принцип генерируемости.
41. Принцип функциональной избыточности при разработке ПО и принцип «по умолчанию».
42. Общесистемные принципы разработки ПО.
43. В чем отличие циклической структуры с предусловием от циклической структуры с постусловием?
44. Что такое параметр цикла?
45. В чем отличие регулярной циклической структуры от итеративной?
46. Доказывает ли получение правдоподобного результата правильность программы?
47. Какие ошибки могут остаться не выявленными, если не провести проверку (просмотр, прокрутку) программы?
48. Чем тестирование программы отличается от её отладки?
49. Можно ли с помощью тестирования доказать правильность программы?
50. На какой стадии работы над программой вычисляются эталонные результаты тестов?

51. Назовите основные этапы процесса тестирования.
52. В чём заключается отличие синтаксических ошибок от семантических?
53. О чём свидетельствует отсутствие сообщений машины о синтаксических ошибках?
54. Какие разновидности ошибок транслятор не в состоянии обнаружить?
55. Основные этапы развития технологии разработки
56. Эволюция моделей жизненного цикла программного обеспечения
57. Стандарты, регламентирующие процесс разработки программного обеспечения
58. Введение в системный анализ
59. Анализ проблемы и моделирование предметной области с использованием системного подхода
60. Методология ARIS
61. Стандарты IDEF0IDEF3
62. Методы определения требований
63. Формализация требований
64. Планирование архитектуры
65. Проектирование архитектуры
66. Документирование программной архитектуры
67. Методы анализа архитектуры
68. Использование архитектуры, управляемой моделью
69. Язык объектных ограничений OCL
70. Возможности технологии ECO
71. Управление документированием программного обеспечения
72. Требования к содержанию документов на автоматизированные системы
73. Принципы разработки руководства программиста
74. Разработка руководства пользователя
75. Компонентный подход и CASEтехнологии
76. Гибкие технологии разработки программных систем
77. ГОСТ Р ИСО/МЭК 1220799
78. Методы определения системы и ее компонентов
79. Определение проблемы
80. Функциональная модель Модель целей
81. Модель DFD
82. CRCкарточки (Class Responsibility Collaboration, класс обязанность взаимодействие)
83. Конечные автоматы Диаграммы деятельности
84. Программный процесс и архитектурно-экономический цикл
85. Методы проектирования
86. Диаграмма развертывания. Диаграмма компонентов
87. Метод анализа стоимости и эффективности
88. Модели MDA
89. Применение языка OCL при описании архитектуры
90. Архитектура ECO
91. Планирование документирования
92. Перечень необходимой документации, включаемой в состав поставки ПО
93. Описание структуры ПО в руководстве программиста
94. Принципы написания руководства пользователя
95. Качество ПО. Характеристики. Подхарактеристики. Метрики.
96. Сложность ПО. Причины. Признаки сложной системы. Пути ограничения сложности ПО.
97. Эволюция технологий программирования.
98. Структурное программирование.

99. Объектно-ориентированное проектирование.
100. Каскадная (водопадная) модель жизненного цикла.
101. Итеративная и инкрементальная модель ЖЦ.
102. Спиральная модель Боэма.
103. Методологии разработки сложных программных систем (RUP).
104. Методологии разработки сложных программных систем (Экстремальное программирование).
105. Назначение языка UML.
106. Варианты использования (прецеденты). Диаграммы ВИ.
107. Диаграммы классов.
108. Ассоциации. Обобщения. Атрибуты.
109. Операции. Агрегирование и композиция.
110. Классы ассоциаций. Интерфейсы и абстрактные классы.
111. Диаграммы пакетов. Диаграммы взаимодействия.
112. Диаграммы состояний. Диаграммы деятельностей.
113. Диаграммы компонентов. Диаграммы развертывания.
114. Тестирование. Методы тестирования (обзор).
115. Тестирование по методу «черного» ящика.
116. Тестирование по методу «белого» ящика.
117. Структурное программирование.
118. Структурирование программ.
119. Теорема о структурировании программ.
120. Операторы, реализующие структурное программирование, их классификация: составные (блоки), с меткой, выражения (пустой, с побочными эффектами), выбора, итерации, перехода, asm-операторы и др.
121. Агрегаты данных.
122. Структуры, их объявление, инициализация.
123. Доступ к компонентам структур.
124. Размещение в памяти, выравнивание по границе слова.
125. Пространство имен структур.
126. Теги структур.
127. Битовые поля и доступ к ним.
128. Модуль, его свойства, достоинства, недостатки.
129. Функции, реализующие модульное программирование.
130. Заголовок, тело функции, прототип функции.
131. Функции пользователя.
132. Эволюция методологий программирования. Парадигмы программирования.
133. Основные принципы объектного подхода. Абстрагирование.
134. Основные принципы объектного подхода. Инкапсуляция.
135. Основные принципы объектного подхода. Модульность.
136. Основные принципы объектного подхода. Иерархия.
137. Основные принципы объектного подхода. Типизация.
138. Основные принципы объектного подхода. Параллелизм. Сохраняемость.
139. Объект с точки зрения ООП. Состояние. Поведение.
140. Объект с точки зрения ООП. Идентичность и жизненный цикл объектов.
141. Объект с точки зрения ООП. Взаимоотношения между объектами.
142. Классы. Природа классов. Метамодель. Инстанцирование.
143. Классы. Структура класса. Абстрактные классы и интерфейсы.
144. Классы. Отношения между классами. Ассоциация и агрегация.
145. Классы. Иерархии классов. Зависимость.

Аналитическое задание:

1. **Система информации об авиарейсах и билетах**
   Система управления информацией о рейсах, наличии билетов и ценах на них, а также продажи билетов
   Поддерживаемые данные
   - Авиарейсы
     - Компания, номер
     - Аэропорты вылета и прилета
     - Время и даты вылета и прилета
     - Стоимость билетов
     - Количество мест и наличие свободных мест
   - Клиенты
     - ФИО
     - Контактная информация: адрес, телефон, e-mail
     - Заказанные билеты, оплаченные билеты
     - Наличие бонусных карт авиакомпаний
     - Налетанные километры по каждой авиакомпании, их использование для оплаты других билетов

   Поддерживаемые операции

   - Получение списка авиарейсов по датам и направлениям, информации о ценах билетов и наличии свободных мест
   - Получение списка клиентов, в т.ч. летавших определенным рейсом, любыми рейсами авиакомпании, заказавших и оплативших билеты
   - Получение истории заказов клиента, информации о его бонусах и их использовании
   - Заказ и оплата билетов на выбранный рейс
   - Добавление и удаление рейса, чтение и редактирование данных о нем
   - Добавление и удаление клиента, чтение и редактирование данных о нем

2. **Система информации об автобусных рейсах и билетах**
   Система управления информацией об автобусных рейсах, наличии билетов и ценах на них, а также продажи билетов. Поддерживаемые данные
   - Рейсы
     - Компания, номер
     - Пункты убытия и прибытия, промежуточные остановки
     - Время и даты всех остановок
     - Стоимость билетов для всех пар остановок
     - Количество мест и наличие свободных мест с учетом промежуточных остановок
   - Клиенты
     - ФИО
     - Контактная информация: адрес, телефон, e-mail
     - Заказанные билеты

   Поддерживаемые операции

   - Получение списка рейсов по датам, направлениям и промежуточным остановкам, информации о ценах билетов и наличии свободных мест
   - Получение списка клиентов, в т.ч. ехавших определенным рейсом, любыми рейсами компании, заказавших билеты
   - Получение истории заказов клиента
   - Заказ билетов на выбранный рейс между выбранными пунктами
   - Добавление и удаление рейса, чтение и редактирование данных о нем
   - Добавление и удаление клиента, чтение и редактирование данных о нем

3. **Театральная касса**
   Система учета данных о представлениях и продажи билетов на них.
   Поддерживаемые данные
   - Театры
     - Режиссеры, актеры
     - Адрес
     - Количество мест в зале разных видов: партер, балконы, бельэтаж
     - Представления
   - Представления
     - Театр, режиссер, участвующие актеры
     - Даты и время проведения (может быть несколько)
     - Продолжительность
     - Информация о свободных местах разных видов
     - Стоимость билетов разных видов

   Поддерживаемые операции

   - Получение списка театров и представлений по театру, режиссеру, занятым актерам, датам проведения
   - Получение данных о наличии свободных мест и стоимости билетов разных видов на представление
   - Покупка билетов
   - Добавление и удаление театра, чтение и редактирование данных о нем
   - Добавление и удаление спектакля, чтение и редактирование данных о нем

4. **Система информации о спортивных соревнованиях**
   Система учета данных о спортивных соревнованиях и продажи билетов на них.
   Поддерживаемые данные
   - Соревнования
     - Вид спорта (футбол, синхронное плавание, фигурное катание, гимнастика и пр.)
     - Название, турнир, частью которого оно является
     - Место и время проведения
     - Участвующие (в зависимости от вида спорта): команды и отдельные спортсмены
     - Количество мест в зале разных видов: передние ряды, средние ряды, задние ряды
     - Заказанные и свободные места (для еще не состоявшихся)
     - Результаты (для уже состоявшихся): счет или очки, распределение мест
   - Спортсмены
     - ФИО, возраст
     - История участия в командах и соревнованиях
   - Команды
     - Название
     - Тренеры
     - Состав
     - История участия в соревнованиях

   Поддерживаемые операции

   - Получение списка соревнований по видам спорта, участникам, местам и времени проведения
   - Получение данных о наличии свободных мест и стоимости билетов разных видов на представление
   - Покупка билетов
   - Добавление и удаление соревнования, чтение и редактирование данных о нем
   - Добавление и удаление команд и спортсменов, чтение и редактирование данных о них

5. **Интернет-магазин бытовой техники**
   Система учета данных о товарах и заказах.
   Поддерживаемые данные
   - Товары
     - Вид (телевизоры, DVD-проигрыватели, холодильники, стиральные машины и пр.)
     - Цена
     - Компания-производитель, место сборки
     - Характеристики, в зависимости от вида (телевизор — габариты, диагональ, разрешение, формат экрана, количество каналов, и пр.; холодильник — габариты, цвет, одно/двухкамерный, расположение камер, мин. температура в морозильнике, объем камер, энергопотребление и пр.; стиральная машина — габариты, макс. загрузка, обороты, энергопотребление и пр.)
     - Наличие, количество
   - Клиенты
     - ФИО
     - Контактная информация: адрес, телефон, e-mail
     - Сделанные заказы
   - Заказы
     - Дата и время
     - Клиент
     - Товары и их количество, общая стоимость
     - Условия доставки (адрес, время — определяются клиентом)
     - Текущий статус: в обработке, собран, поставлен

   Поддерживаемые операции

   - Получение списка товаров по типам, производителям и характеристикам
   - Получение данных о характеристиках, наличии и цене товара
   - Оформление заказа
   - Проверка статуса заказа
   - Добавление и удаление клиента, чтение и редактирование данных о нем
   - Добавление и удаление товара, чтение и редактирование данных о нем

6. **Книжный Интернет-магазин**
   Система учета данных о клиентах, книгах и заказах на них.
   Поддерживаемые данные
   - Книги
     - Название
     - Авторы
     - Жанр
     - Издательство, год издания, количество страниц, вид обложки
     - Цена
     - Наличие, количество
   - Клиенты
     - ФИО
     - Контактная информация: адрес, телефон, e-mail
     - Сделанные заказы
   - Заказы
     - Дата и время
     - Клиент
     - Товары и их количество, общая стоимость
     - Условия доставки (адрес, время — определяются клиентом)
     - Текущий статус: в обработке, собран, поставлен

   Поддерживаемые операции

   - Получение списка книг по жанрам, авторам и др. характеристикам
   - Получение данных о наличии и цене книг
   - Оформление заказа, проверка и изменение статуса заказа
   - Добавление и удаление клиента, чтение и редактирование данных о нем
   - Добавление и удаление книги, чтение и редактирование данных о ней

7. **Информационная система автосалона**
   Система учета данных о клиентах, автомобилях и заказах.
   Поддерживаемые данные
   - Автомобили
     - Марка
     - Производитель
     - Регистрационный номер
     - Технические характеристики (объем и мощность двигателя, расход топлива, количество дверей, мест, вместимость багажника, автоматическая коробка передач, круиз-контроль, требуемое топливо и т.п.)
     - Встроенные устройства (кондиционер, радио, видео, GPS-навигатор и пр.)
     - Потребительские характеристики (обивка салона, цвет и пр.)
     - Изменяемые характеристики (пробег, последнее ТО и др.)
     - Цена
     - Клиенты, проводившие тест-драйв
   - Клиенты
     - ФИО
     - Контактная информация: адрес, телефон, e-mail
     - Сделанные заказы
   - Заказы
     - Дата и время
     - Клиент
     - Характеристики автомобиля
     - Нужен ли предварительный тест-драйв
     - Текущий статус: в обработке, ожидание поставки, есть в салоне, в тест-драйве, выполнен

   Поддерживаемые операции

   - Получение списка автомобилей по разным характеристикам
   - Получение списка клиентов по характеристикам их заказов
   - Оформление заказа, проверка и изменение статуса заказа
   - Добавление и удаление клиента, чтение и редактирование данных о нем
   - Добавление и удаление марки автомобилей или конкретного автомобиля, чтение и редактирование данных о них

8. **Складской учет**
   Система учета данных о товарах на складе, поставщиках и потребителях.
   Поддерживаемые данные
   - Товары
     - Наименование
     - Вид (продукты, бытовая химия, одежда-обувь, бытовая электроника)
     - Характеристики, в зависимости от вида: габариты, срок хранения
     - Поставщики и потребители
     - Наличие, количество и единицы его измерения
     - Время хранения и статус (для портящихся)
     - Место хранения (номера помещения и полки)
   - Поставщики и потребители
     - Наименование
     - Контактная информация: адрес(а), телефон(ы), e-mail(ы)
     - Сделанные поставки и заказы
   - Поставки и выдачи
     - Дата и время
     - Поставщик (для поставок) или потребитель (для выдач)
     - Товары и их количество

   Поддерживаемые операции

   - Получение списка имеющихся товаров по видам, сроку хранения, поставщику и пр.
   - Получение данных о поставках и выдачах за заданный период времени
   - Оформление поставки или выдачи
   - Проверка наличия свободного места для поставки
   - Добавление и удаление товара, чтение и редактирование данных о нем
   - Добавление и удаление поставщиков и потребителей, чтение и редактирование данных о них

9. **Учебное расписание**

Система составления расписаний и ведения данных об учебных курсах в ВУЗе.

Поддерживаемые данные

- Студенты
  - ФИО
  - Год обучения, поток, группа
  - Какие курсы и когда посещал
- Преподаватели
  - ФИО
  - Проводимые курсы (ранее и теперь)
- Аудитории
  - Номер
  - Вместимость
- Курсы
  - Название
  - Охват: поток, группа, спец. курс
  - Интенсивность (сколько пар в неделю)
  - Год обучения (для обязательных)
- Занятия
  - Курс, преподаватель
  - Аудитория
  - Время
  - Студенты

Поддерживаемые операции

- Получение списков студентов по потокам и группам
- Получение списков преподавателей, в т.ч. по проводимым курсам
- Получение списков аудиторий, свободных в определенном интервале
- Получение расписания на заданный интервал времени для студента, преподавателя или аудитории
- Составление расписания занятий для курса на семестр
- Добавление и удаление студентов и преподавателей, чтение и редактирование данных о них, занесение студента в список слушателей спец. курса
- Добавление и удаление курса, чтение и редактирование данных о нем

10. **Учебный центр**

Система составления расписаний и ведения данных об учебных курсах в тренинговом центре.

Поддерживаемые данные

- Обучающиеся
  - ФИО
  - Посещаемые курсы
- Компании
  - Название, адрес
  - Проводимые курсы
  - Преподаватели
- Преподаватели
  - ФИО
  - Компания
  - Проводимые курсы
- Курсы
  - Время — день, несколько дней, две недели, месяц
  - Интенсивность (сколько часов в день)
- Занятия
  - Курс, преподаватель
  - Время
  - Обучающиеся

Поддерживаемые операции

- Получение списков обучающихся по курсам, истории обучения для данного человека
- Получение списков преподавателей, в т.ч. по проводимым курсам
- Получение расписания на заданный интервал времени для обучающегося, преподавателя
- Составление расписания занятий для курса
- Добавление и удаление обучающихся и преподавателей, чтение и редактирование данных о них, занесение обучающегося в список слушателей курса
- Добавление и удаление курса, чтение и редактирование данных о нем

11. **Система информации о персонале компании**

Система управления информацией о персонале.

Поддерживаемые данные

- Служащие
  - ФИО
  - Домашний адрес
  - Образование
  - Срок работы в компании
  - История занимаемых должностей
- Должности
  - Название
  - Обязанности
- Подразделения
  - Название
  - Руководитель
  - Должности (с количеством позиций) и занимающие их люди
  - Внутренние подразделения
  - Головное подразделение

Поддерживаемые операции

- Получение списка подразделений, структуры подразделений
- Получение списка служащих, в т.ч. по подразделениям, по сроку работы, по должностям
- Получение истории для данного служащего
- Назначение служащего на новую должность в заданном подразделении
- Добавление и удаление служащего, чтение и редактирование данных о нем
- Добавление и удаление подразделения или должности, чтение и редактирование данных о них

12. **Кадровое агентство**

Система управления информацией о вакансиях и резюме.

Поддерживаемые данные

- Люди
  - ФИО
  - Домашний адрес
  - Образование
  - История работы: компании, должности, зарплаты
  - Статус: ищет работу или нет, если ищет, какие условия (должность, зарплата)
- Компании
  - Название
  - Вакансии: должность + предлагаемая зарплата + требования к образованию и послужному списку

Поддерживаемые операции

- Получение списка резюме по образованию, компаниям, в которых люди работали, по занимавшимся должностям, зарплатам
- Получение списка вакансий по компаниям, должностям, зарплатам
- Получение истории работы для данного человека
- Поиск подходящих вакансий на резюме и подходящих резюме на вакансию
- Добавление и удаление данных о человеке, чтение и редактирование данных о нем, добавление данных о новом трудоустройстве
- Добавление и удаление компании, чтение и редактирование данных о них, добавление, удаление и редактирование вакансий

13. **Зарплатная ведомость**

Система управления информацией о зарплатах служащих компании.

Поддерживаемые данные

- Служащие
  - ФИО
  - Домашний адрес
  - Дата рождения
  - Образование
  - Стаж работы в компании
  - Текущая должность
  - Участие в проектах и выполняемые роли
  - История занимаемых должностей и участия в проектах проектов
  - Общая история всех выплат
  - Премии и даты их выписки
- Проекты
  - Название, даты начал и окончания
  - Роли в проекте (руководитель, аналитик, секретарь, эксперт)
- Политики выплат
  - По должностям
  - По проектам и ролям
  - За стаж
  - Премиальные на Новый год, дни рождения, круглые даты в истории компании

Поддерживаемые операции

- Получение списка служащих, в т.ч. по должностям, проектам, стажу, премированных и пр.
- Получение истории участия в проектах и карьерной истории для служащего
- Получение истории выплат для служащего
- Назначение служащего на новую должность, добавление в/удаление из проекта
- Добавление и удаление служащего, чтение и редактирование данных о нем
- Добавление и удаление проекта, чтение и редактирование данных о нем
- Добавление и удаление политик выплат, чтение и редактирование данных о них

14. **Клиентская база юридической фирмы**

Система управления информацией о клиентах и оказываемых им услугах.

Поддерживаемые данные

- Клиенты – организации и физические лица
  - Наименование или ФИО
  - Контакты: контактные лица, адрес(а), телефон(ы), e-mail(ы)
  - История услуг: услуги, в какое время оказывались, кто из служащих был задействован
- Служащие
  - ФИО
  - Домашний адрес, телефон(ы), e-mail(ы)
  - Образование, должность
  - История работы: участие в оказании услуг
- Услуги
  - Наименование (создание, восстановление и сопровождение документов, банкротство, эмиссия акций, сопровождение сделок, судебное представительство, консультации)
  - Стоимость

Поддерживаемые операции

- Получение списка клиентов, в т.ч. по оказываемым услугам в заданном интервале времени, задействованным служащим и пр.
- Получение списка служащих по их участию в оказании услуг заданным клиентам и в заданное время
- Регистрация договора об оказании услуги
- Добавление и удаление данных о клиенте, чтение и редактирование данных о нем
- Добавление и удаление служащего, чтение и редактирование данных о нем

15. **Биллинговая база оператора связи**

Система управления информацией о клиентах, оказываемых им услугах и об оплате услуг.

Поддерживаемые данные

- Клиенты – физические лица и организации
  - Наименование или ФИО
  - Контакты: контактные лица, адрес(а), телефон(ы), e-mail(ы)
  - История услуг: услуги, в какое время оказывались
- Услуги
  - Наименование
  - Характеристики: номер, группа номеров, Интернет, SMS, спец. предложения
  - Тарифный план (какая часть услуги в какое время сколько будет стоить)
- Счета клиентов
  - Баланс
  - Поступления на счет
  - Списания за оказание услуг связи
  - Ограничения: размер максимального кредита и сроки его погашения

Поддерживаемые операции

- Получение списка клиентов, в т.ч. по оказываемым услугам в заданном интервале времени, по характеристикам их счетов
- Получение росписи операций по счету клиента за заданный интервал времени
- Регистрация договора об оказании услуги
- Регистрация поступлений на счет и списаний
- Добавление и удаление данных о клиенте, чтение и редактирование данных о нем
- Добавление и удаление услуги, чтение и редактирование данных о ней

16. **Система информации о счетах клиентов банка**

Система управления информацией о клиентах и их счетах.

Поддерживаемые данные

- Отделения
  - Название
  - Адрес
  - Клиенты и счета
- Клиенты – физ. лица и организации
  - Наименование или ФИО
  - Контакты: контактные лица, адрес(а), телефон(ы), e-mail(ы)
  - Счета
- Счета
  - Номер
  - Клиент
  - Текущий баланс
  - Вид счета
  - Отделение
  - Начисления/списания
- Виды счетов
  - Наименование
  - Максимальный кредит и ограничения на его погашение
  - Доходность, интервал и метод выплаты процентов (на этот же счет, на другой)
  - Возможности списания/начисления и ограничения на списываемые/начисляемые суммы

Поддерживаемые операции

- Получение списка клиентов, в т.ч. по типам, видам счетов в заданном интервале времени и пр.
- Получение списка счетов по их видам, списаниям/начислениям за заданный период
- Получение списка отделений, в. т.ч. по клиентам, счетам и пр.
- Оформление списания/начисления, включая автоматический учет процентов
- Заведение счета и его закрытие, чтение данных о нем
- Добавление и удаление данных о клиенте, чтение и редактирование данных о нем
- Добавление и удаление отделения, чтение и редактирование данных о нем

17. **Библиотека**

Система библиотечного учета для управления данными о читателях и книгах, о выдаче книг читателям.

Поддерживаемые данные

- Читатели
  - ФИО
  - Номер читательского билета
  - Контактная информация: адрес, телефон
  - Какие книги и когда ему выдавались, когда он их возвращал
- Книги
  - Название
  - Авторы
  - Издательство, год издания, ISBN
  - Количество экземпляров в библиотеке и свободных экземпляров
  - Для каждого экземпляра: кому и когда его выдавали, когда он возвращался

Поддерживаемые операции

- Получение списка читателей и книг, книг - по авторам, названиям и издательствам
- Получение истории выдачи и приема книг у читателя, списка находящихся у него книг
- Получение истории выдачи и приема экземпляров книги, сводных сведений о наличии, выдаче и приеме книг за заданный интервал времени
- Внесение информации о выдаче книг читателю и получении от него
- Добавление и удаление читателя, чтение и редактирование данных о нем
- Добавление и удаление книги и отдельных экземпляров, чтение и редактирование данных о книгах и их экземплярах

18. **Web-форум**

Система управления информацией об обсуждениях на форуме.

Поддерживаемые данные

- Пользователь
  - Login/пароль
  - Дата регистрации
  - Права — пользователь или модератор
- Тема
  - Раздел форума
  - Сообщения по теме
    - Пользователь, приславший сообщение
    - Заголовок сообщения
    - Дата и время поступления
    - Прикрепленные файлы

Поддерживаемые операции

- Получение списка пользователей, в т.ч. по участию в различных разделах и по активности (количеству сообщений в заданном интервале времени)
- Получение списка разделов, тем в разделе, сообщений в теме
- Для модераторов: создание/удаление раздела, удаление тем, сообщений, создание и блокирование пользователей
- Для обычных пользователей: создание тем, создание сообщений в теме

19. **Видеопрокат**

Система управления данными о видеокассетах и дисках, об их выдаче клиентам.

Поддерживаемые данные

- Клиенты
  - ФИО
  - Контактная информация: адрес, телефон
  - Какие носители с фильмами, когда и по какой цене ему выдавались, когда он их возвращал
- Фильмы
  - Название
  - Компания, режиссер, год выхода
  - Носители (кассеты, диски) и стоимость проката каждого типа носителя
  - Количество экземпляров на каждом типе носителя и свободных экземпляров
  - Для каждого экземпляра: кому и когда его выдавали, когда он возвращался

Поддерживаемые операции

- Получение списка клиентов и фильмов
- Получение истории выдачи и приема фильмов у клиента, списка находящихся у него фильмов
- Получение истории выдачи и приема экземпляров фильма, сводных сведений о наличии, выдаче и приеме фильмов за заданный интервал времени
- Внесение информации о выдаче фильма клиенту, получении от него и оплате
- Добавление и удаление клиента, чтение и редактирование данных о нем
- Добавление и удаление фильма и отдельных экземпляров, чтение и редактирование данных о фильмах и их экземплярах

20. **Система генеалогической информации**

Система управления информацией о родственных связях людей.

Поддерживаемые данные

- Человек
  - Полное имя
  - Даты рождения и смерти
  - Краткая характеристика — кто это такой, чем занимался(ется)
  - Места проживания
  - Родители
  - Супруги и даты брака и развода (если был развод)
  - Дети от разных браков и внебрачные

Поддерживаемые операции

- Получение списка людей по фамилиям, разнообразным родственным связям с определенным человеком (родители, дети, супруги, братья-сестры, родственники во втором колене, по супругам и пр).
- Получение генеалогического дерева человека — все предки
- Получение дерева потомков человека
- Получение всех видов родственных связей между двумя людьми
- Добавление данных о человеке, их чтение и редактирование

21. **Система информации о структуре собственности**

Система управления информацией о структуре собственности для некоторой группы компаний.

Поддерживаемые данные

- Физические лица
  - ФИО
  - Краткая биография
  - Собственность — в каких компаниях каким процентом акций владеет
- Компании
  - Название
  - Действует/потеряла статус отдельного юр. лица
  - Год основания
  - История смены названий
  - История сделок по покупке/поглощению других компаний
  - Владельцы — кто или какая компания какой частью акций владеет
  - Владения — в каких компаниях какой частью владеет

Поддерживаемые операции

- Получение списка людей по прямо или непрямо контролируемым ими компаниям
- Получение полной информации о собственности для человека или компании — каким процентом где владеют, с транзитивным замыканием
- Получение полной структуры владения для компании — кто и какой частью владеет, с транзитивным замыканием
- Получение цепочки связи между двумя компаниями (как направленной, как и со сменой направления владения)
- Добавление данных о человеке или компании, их чтение и редактирование

22. **Астрономический каталог**

Система управления информацией об астрономических объектах и явлениях.

Поддерживаемые данные

- Объекты
  - Класса: звезда (в т.ч. кратная), туманность, галактика, планета, малая планета, спутник, астероид, комета, метеорный поток
  - Тип в классе: для звезд — цвет и пр., для галактик — форма, и т.д.
  - Имена и идентификаторы по разным каталогам
  - Дата открытия
  - Первооткрыватель
  - Характеристики для неподвижных (относительно звезд) объектов: координаты, созвездие, светимость, масса, расстояние от Солнца
  - Характеристики для подвижных: параметры орбиты, вариации скорости движения, масса, изменения светимости
  - Связанные явления
- Явления
  - Вид: прохождение, покрытие, затмение, соединение, противостояние, прохождение апоцентра и перицентра, вспышка, столкновение и пр.
  - Связанные объекты и их роли
  - Время начала и конца

Поддерживаемые операции

- Получение списка объектов по типам и др. характеристикам, по связанным явлениям в заданном интервале времени, в заданной области неба
- Получение списка явлений по объектам, в заданном интервале времени, в заданной области неба
- Добавление данных об объекте или явлении, их чтение и редактирование

23. **Коллекция минералов**

Система управления данными о минералогической коллекции.

Поддерживаемые данные

- Минералы
  - Название
  - Классификация (раздел, класс, подкласс) (см. Wikipedia)
  - Состояние (жидкое, газообразное, аморфное, кристаллическое)
  - Для твердых - тип кристаллической решетки, твердость, хрупкость
  - Блеск, цвет, магнитные свойства
  - Химическая формула
  - Происхождение (осадочное, вулканическое, метаморфическое)
  - Имеющиеся образцы
- Образцы
  - Входящие минералы и способ их включения (кристаллы, вкрапления, примерная % часть образца)
  - Возможное происхождение (метеорит, извержение, осадочные слои и пр.)
  - Место обнаружения (координаты и описание, например, обрыв на правом берегу реки Камы)
  - Источник (экспедиция, дар, обмен с другими коллекциями, пр.)
- Экспедиции
  - Даты начала и конца
  - Участники
  - Собранные образцы и места сбора

Поддерживаемые операции

- Получение списка образцов по минералам, источникам и др. характеристикам
- Добавление данных о минерале, их чтение и редактирование
- Добавление данных об экспедициях и образцах, их чтение и редактирование

24. **Информационная система заповедника**

Система управления данными о животных в заповеднике.

Поддерживаемые данные

- Животные
  - Классификация: тип, класс, семейство, вид, латинское название
  - Персональный идентификатор или имя
  - Устанавливавшиеся метки (кольца, RFID и пр.), их идентификаторы, время установки и снятия, кто устанавливал
  - Особенности внешнего вида
  - Особенности поведения
  - Статус: мигрирующее, постоянно в заповеднике; живое или уже нет
  - Связи с другими животными: родители, потомки, текущее положение в группе/стае, текущий партнер
  - История болезней: болезнь, время фиксации болезни, время фиксации выздоровления, кто и какую помощь оказывал, последствия
- Работник заповедника
  - ФИО
  - Образование
  - Стаж работы
  - С животными каких видов работал

Поддерживаемые операции

- Получение списка животных по видам, имеющимся или прошлым меткам, перенесенным болезням
- Получение списка сотрудников по обарзования и опыту работу, с какими животными имел дело
- Получение деталей по животному, истории его меток, истории его болезней, связей с другими
- Добавление данных о животном или работнике, их чтение и редактирование

25. **Агентство недвижимости**

Система управления информацией о предложениях и заказах в агентстве недвижимости.

Поддерживаемые данные

- Заказы
  - Контактная информация клиента
  - Вид сделки: аренда, покупка, обмен
  - Требования (с ограничениями, точными значениями или без органичений)
    - объект: комната/квартира/дом
    - тип дома: деревянный/панельный/кирпичный/монолит
    - площадь: общая/жилая, комнат, кухни, прихожей
    - наличие и площадь лоджии/балкона
    - наличие удобств: раздельный/совмещенный санузел, внешние удобства, электричество, газ, канализация, водопровод, телефон, телевидение, Интернет
    - этаж
    - состояние: новостройка/нет, время после последнего ремонта
    - расстояние до метро, МКАД, ближайшей ж/д станции, остановки автобуса/троллейбуса/трамвая
    - расположение: округ/район Москвы, район/город Московской обл.
    - максимальная цена
  - Предложения
    - Контактная информация
    - Вид сделки
    - Характеристики (те же, что в заказах, с точными значениями, кроме адреса и цены)
    - Адрес
    - Начальная цена

Поддерживаемые операции

- Получение списка заказов/предложений по различным характеристикам
- Поиск подходящих предложений на заказ и заказов на предложение
- Добавление и удаление данных о заказе или предложении, чтение и редактирование данных о них

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Промежуточная аттестации по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по дисциплине (модулю) выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам

бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля)

5.1.1. Основная литература

1. *Трофимов, В. В.* Алгоритмизация и программирование : учебник для вузов / В. В. Трофимов, Т. А. Павловская ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2022. — 137 с. — (Высшее образование). — ISBN 978-5-534-07834-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491215
2. *Зыков, С. В.* Программирование. Объектно-ориентированный подход : учебник и практикум для вузов / С. В. Зыков. — Москва : Издательство Юрайт, 2022. — 155 с. — (Высшее образование). — ISBN 978-5-534-00850-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490423
3. *Зыков, С. В.* Программирование : учебник и практикум для вузов / С. В. Зыков. — Москва : Издательство Юрайт, 2022. — 320 с. — (Высшее образование). — ISBN 978-5-534-02444-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489754

5.1.2. Дополнительная литература

1. *Зыков, С. В.* Программирование. Функциональный подход : учебник и практикум для вузов / С. В. Зыков. — Москва : Издательство Юрайт, 2022. — 164 с. — (Высшее образование). — ISBN 978-5-534-00844-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490870
2. *Огнева, М. В.* Программирование на языке C++: практический курс : учебное пособие для вузов / М. В. Огнева, Е. В. Кудрина. — Москва : Издательство Юрайт, 2022. — 335 с. — (Высшее образование). — ISBN 978-5-534-05123-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/492984
3. *Нагаева, И. А.* Программирование: Delphi : учебное пособие для вузов / И. А. Нагаева, И. А. Кузнецов ; под редакцией И. А. Нагаевой. — Москва : Издательство Юрайт, 2022. — 302 с. — (Высшее образование). — ISBN 978-5-534-07098-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493669
4. *Подбельский, В. В.* Программирование. Базовый курс C# : учебник для вузов / В. В. Подбельский. — Москва : Издательство Юрайт, 2022. — 369 с. — (Высшее образование). — ISBN 978-5-534-10616-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469616.

5.2. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. programmer.com – сборник интерактивных задач по программированию.
2. codeacademy.com – сборник материалов по программированию

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская	Электронная библиотека, обеспечивающая доступ высших и средних учебных	http://biblioclub.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	библиотека онлайн»	заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) «Программирование» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины (модуля) . Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

5.4.Информационно-технологическое обеспечение образовательного процесса по дисциплине (модулю)

5.4.1. Информационные технологии

1. Персональные компьютеры;
2. Доступ к Интернет
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.4.3. Информационные справочные системы и профессиональные базы данных

Обучающиеся по программе **«Информационная безопасность»** в университете имеют доступ к следующим современным профессиональным базам данных, информационным справочникам:

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.5. Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) **«Программирование»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки **«10.03.01 Информационная безопасность»** используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет.

Лабораторные занятия проводятся лабораторный занятий в лаборатории**,** оснащенной специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет персональные компьютеры с установленным программным обеспечением согласно пункту 9.2).

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.6. Образовательные технологии

При реализации дисциплины (модуля) **«Программирование»** применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины (модуля) **«Программирование»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме компьютерных симуляций, деловых и ролевых игр, метода проектов в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

При освоении дисциплины (модуля) «Программирование» предусмотрено применением электронного обучения.

Учебные часы дисциплины «Программирование» предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках дисциплины (модуля) **«Программирование»** предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Российский государственный социальный университет»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/
«06» __июня___2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ПРОЕКТИРОВАНИЕ БАЗ ДАННЫХ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технология защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ – УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022 г.

Рабочая программа дисциплины (модуля) «**Проектирование баз данных**» разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки **10.03.01 "Информационная безопасность" (уровень бакалавриата),** утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 г № 1427, учебного плана по основной профессиональной образовательной программе высшего образования – программе *бакалавриата* по *направлению подготовки 10.03.01 Информационная безопасность,* а также с учетом профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

– *06.030 Специалист по защите информации в телекоммуникационных системах и сетях*
– *06.032 Специалист по безопасности компьютерных систем и сетей*
– *06.033 Специалист по защите информации в автоматизированных системах*
- 06.034 Специалист по технической защите информации.

Рабочая программа дисциплины (модуля) разработана рабочей группой в составе: д-р техн. наук, профессор Кораблин Ю.П., канд. физ.-мат. наук, доцент Григорьева С.В., ст. пр. Елисеева Д.Ю.

Руководитель основной профессиональной образовательной программы — Н.Г. Витковская

(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года.

Декан факультета
К.п.н. доцент — С.В. Крапивка

(подпись)

Рабочая программа дисциплины (модуля) рекомендована к утверждению представителями организаций-работодателей:

АО ПВП «Амулет»
зам. ген. директора по науке, к.т.н., доцент — А.С. Мосолов

(подпись)

Рабочая программа дисциплины (модуля) рецензирована и рекомендована к утверждению:

ФГБОУ ВО «Московский политехнический университет», НОЦ инфокогнитивных технологий, доктор технических наук, профессор — Н.И. Гданский

(подпись)

к.т.н., доцент кафедры информационных систем, сетей и безопасности — В.Л. Симонов

(подпись)

Согласовано
Научная библиотека, директор — И.Г. Маляр

(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля) .

Цель дисциплины (модуля) заключается в получении обучающимися теоретических знаний о принципах организации баз и банков данных с последующим применением в профессиональной сфере и практических навыков (формирование) по проектированию баз данных, построению моделей данных (иерархической, сетевой и реляционной), нормализации отношений.

Задачи дисциплины (модуля) :

- овладение теоретическими знаниями в области проектирования базы данных;
- приобретение прикладных знаний о современных инструментальных средствах создания базы данных;
- овладение навыками программирования и отладки интерфейса по управлению базой данных.
- овладение навыками создания и управления сетевыми и распределенными приложениями.

1.2. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы.

Учебная дисциплина «**Проектирование баз данных**» реализуется в вариативной части основной профессиональной образовательной программы "Информационная безопасность" по направлению подготовки 10.03.01 "Информационная безопасность" очной формы обучения.

Изучение дисциплины (модуля) «Проектирование баз данных» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Информатика и информационные технологии», «Программирование», ряда модулей дисциплины «Проектирование и администрирование информационных систем».

Изучение дисциплины (модуля) «Проектирование баз данных» является базовым для последующего освоения программного материала учебных дисциплин: «Управление данными и знаниями»

1.3. Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основной профессиональной образовательной программы.

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих профессиональных компетенций: ПК-2, ПК-3, ПК-7 в соответствии с основной профессиональной образовательной программой " Информационная безопасность " по направлению подготовки 10.03.01 " Информационная безопасность "

В результате освоения дисциплины (модуля) обучающийся должен демонстрировать следующие результаты:

Категория компетенций	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
	ПК-2	Способен применять программные средства системного, прикладного и	ПК-2.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения	Знать: - аппаратные средства вычислительной техники - операционные

		специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	практических действий в рамках компетенции ПК-2.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-2.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	системы персональных ЭВМ - основы администрирования вычислительных сетей - системы управления БД
				Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
				Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации
	ПК-3	Способен администрировать подсистемы информационной безопасности объекта защиты	ПК-3.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции	Знать: - аппаратные средства вычислительной техники - операционные системы персональных ЭВМ

				- основы администрирования вычислительных сетей - системы управления БД - эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности - основные направления политик защиты информации на предприятии (организации) - возможные угрозы информационной безопасности, связанные с аспектами деятельности предприятия (организации), особенностями технологических процессов, организационной структуры и др.
			ПК-3.ИД-2. Планирует и выполняет практические действия в рамках компетенции	Уметь: - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе - осуществлять меры противодействиия

				нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты - выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации
			ПК-3.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Владеть: методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации
	ПК-7	Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции ПК-7.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-7.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** - принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода; - номенклатуру и основные параметры сертифицированны

				х средств обеспечения информационной безопасности.
				Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно-следственных связей.
				Владеть : - основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту информатизации; - методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования. - основными технологиями селективного информационного поиска и анализа результатов работы с информационными ресурсами по номенклатуре сертифицированных средств защиты объектов информатизации.

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем дисциплины (модуля) , включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 8 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		3	4			
Контактная работа обучающихся с педагогическими работниками	**144**	**72**	**72**			
Учебные занятия лекционного типа	32	16	16			
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	48	24	24			
из них: в форме практической подготовки						
Иная контактная работа	64	32	32			
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**99**	**63**	**36**			
из них: в форме практической подготовки	*21*	*14*	*7*			
Контроль промежуточной аттестации	**45**	**9**	**36**			
Форма промежуточной аттестации		диф. зач	экзам			
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**288**	**144**	**144**			

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	**Виды учебной работы, академических часов**											
	Всего	**Самостоятельная работа**	*из них: в форме практической подготовки*	**Контактная работа обучающихся с педагогическими работниками**								
				Всего	*из них: в форме практической подготовки*	**Лекционные занятия**	*из них: в форме практической подготовки*	**Семинарские/практические занятия**	*из них: в форме практической подготовки*	**Лабораторные занятия**	*из них: в форме практической подготовки*	**Иная контактная работа**	*из них: в форме практической подготовки*

Модуль 1 (семестр 3)													
Раздел 1.1	33	15	*4*	18		4				6		8	
Раздел 1.2	34	16	*4*	18		4				6		8	
Раздел 1.3	34	16	*3*	18		4				6		8	
Раздел 1.4	34	16	*3*	18		4				6		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**144**	**63**	***14***	**72**		**16**				**24**		**32**	
Форма промежуточной аттестации	**дифференцированный зачет**												
Модуль 2 (семестр 4)													
Раздел 2.1	27	9	*2*	18		4				6		8	
Раздел 2.2	27	9	*2*	18		4				6		8	
Раздел 2.3	27	9	*2*	18		4				6		8	
Раздел 2.4	27	9	*1*	18		4				6		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**144**	**36**	***7***	**72**		**16**				**24**		**32**	
Форма промежуточной аттестации	**экзамен**												

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

3.1. Виды самостоятельной работы обучающихся по дисциплине

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**
Модуль 1 (семестр 3)							

Раздел 1.1	15	6	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.4	16	7	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	7	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**63**	**27**		**28**		**8**	
Модуль 2 (семестр 4)							
Раздел 2.1	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.3	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.4	9	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	4	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Общий объем по модулю/семестру, часов	**36**	**12**		**16**		**8**	
Общий объем по дисциплине (модулю), часов	**99**	**39**		**44**		**16**	

3.2. Методические указания к самостоятельной работе по дисциплине (модулю»)

МОДУЛЬ «Основы баз данных»

РАЗДЕЛ 1. Введение в теорию баз данных

Цель: заключается в получении обучающимися теоретических знаний построения концептуальной, логической и физической моделей базы данных с последующим применением в профессиональной сфере и практических навыков проектирования интерфейса по управлению базой данных по обеспечению надежной работы методов обработки и управления данными на основе современных методологий и стандартов (ПК-2, ПК-3).

Перечень изучаемых элементов содержания

Назначение баз данных. Основные понятия теории баз данных: сущность, предметная область. Система управления базами данных (СУБД). Классификация баз данных по форме хранимой информации, по способу организации, по модели данных, по степени распределённости хранения и передачи данных, по содержимому. Классификация СУБД по используемой модели данных, по степени распределённости, по способу доступа к БД, по языкам общения, по числу уровней в архитектуре, по степени универсальности. Основные функции СУБД. Критерии качества баз данных.

Вопросы для самоподготовки:

1. Назначение БД
2. Виды связей между таблицами
3. Технология ввода и редактирования данных.
4. Сортировка данных
5 Поиск и замена данных.
6. Технология применения Автофильтра
7. Технология применения Расширенного фильтра.
8. Технология создания запроса на выборку
9.Групповые операции в запросах
10. Технология создания перекрестного запроса

РАЗДЕЛ 2. Общие принципы построения (архитектура) баз данных

Цель: заключается в получении обучающимися теоретических знаний построения концептуальной, логической и физической моделей базы данных с последующим применением в профессиональной сфере и практических навыков проектирования интерфейса по управлению базой данных по обеспечению надежной работы методов обработки и управления данными на основе современных методологий и стандартов (ПК-2, ПК-3).

Перечень изучаемых элементов содержания

Трехуровневая модель системы управления базой данных ANSI. Схемы баз данных. Внешний уровень представления информации в БД. Внутренний уровень представления информации в БД. Концептуальный уровень представления информации в БД. Независимость данных в БД. Процесс прохождения пользовательского запроса. Пользователи банков данных. Основные типы архитектуры баз данных с сетевым доступом.

Вопросы для самоподготовки:

1. Типы данных в БД
2. Понятие ключевого поля.
3. Создание схемы данных
4. Средства контроля ввода данных
5. Средства автоматизации ввода данных.
6. Создание списков.
7. Виды стандартных автоформ.
8. Создание подчиненных форм.
9. Технология создания запроса на добавление.
10. Технология создания запроса на удаление данных.

РАЗДЕЛ 3. Модели данных

Цель: заключается в получении обучающимися теоретических знаний построения концептуальной, логической и физической моделей базы данных с последующим применением в профессиональной сфере и практических навыков проектирования интерфейса по управлению базой данных по обеспечению надежной работы методов обработки и управления данными на основе современных методологий и стандартов (ПК-2, ПК-3).

Перечень изучаемых элементов содержания

Понятие модели данных. Объектные модели данных. Общая классификация моделей данных. Уровни моделирования баз данных. Общие и специальные критерии оценки качества логической и физической моделей данных. Основные принципы построения БД - 12 правил Кодда. Отношения в РБД. Их основные понятия. Соотношение основных понятий реляционного подхода. Ключи переменной отношения. Целостность реляционных данных. Функциональные зависимости между атрибутами в отношениях РБД. Связи в реляционных БД. Универсальное отношение. Избыточность данных. Аномалии.

Вопросы для самоподготовки:

1. Технология построения запроса на создание таблиц.
2. Технология создания запроса на обновление данных.
3. Виды соединения таблиц в запросах
4. Свойства запроса.
5. Запросы с параметром.
6. Построитель выражений..
7. Страницы доступа данных
8. Виды стандартных отчетов
9. Группировка в отчетах
10. Макросы

МОДУЛЬ: Организация распределенных и удаленных баз данных

РАЗДЕЛ 4. Базисные операции с реляционными данными

Цель: заключается в получении обучающимися теоретических знаний построения концептуальной, логической и физической моделей базы данных с последующим применением в профессиональной сфере и практических навыков проектирования интерфейса по управлению базой данных по обеспечению надежной работы методов обработки и управления данными на основе современных методологий и стандартов (ПК-2, ПК-3).

Перечень изучаемых элементов содержания

Специальные подходы к выполнению операций над множествами. Реляционная алгебра. Операции над отношениями. Теоретико-множественные операции над отношениями. Специальные реляционные операции. Реляционное исчисление.

Вопросы для самоподготовки:

1. Формат команды на выборку SELECT.

2. Основные опции команды SELECT.
3. Формат команды редактирования данных INSERT
4. Форматы команды редактирования данных UPDATE.
5. Форматы команды редактирования данных DELETE
6. Формат команды создания таблиц SELECT INTO.
7. Формат команды создания таблиц CREATE TABLE.
8. Опции соединения таблиц в запросах.
9. Формат команды объединения данных UNION
10. Формат команды перекрестного запроса TRANSFORM

РАЗДЕЛ 5. Нормальные формы в реляционных базах данных

Цель: заключается в получении обучающимися теоретических знаний построения концептуальной, логической и физической моделей базы данных с последующим применением в профессиональной сфере и практических навыков проектирования интерфейса по управлению базой данных по обеспечению надежной работы методов обработки и управления данными на основе современных методологий и стандартов (ПК-2, ПК-3).

Перечень изучаемых элементов содержания

Нормальные формы в РБД. Нормализация. Функциональные зависимости атрибутов в отношениях. Первая нормальная форма (1НФ). Вторая нормальная форма (2НФ). Третья нормальная форма (3НФ). Алгоритм нормализации (приведение к 3НФ). Корректность процедуры нормализации. Теорема Хеза. Нормальная форма Бойса-Кодда, четвертая и пятая нормальные формы. Пример логического моделирования БД при помощи нормальных форм. Области применения и проблемы логического моделирования БД при помощи нормальных форм.

Вопросы для самоподготовки:

1. Формат команды на выборку SELECT.
2. Основные опции команды SELECT.
3. Формат команды редактирования данных INSERT
4. Форматы команды редактирования данных UPDATE.
5. Форматы команды редактирования данных DELETE
6. Формат команды создания таблиц SELECT INTO.
7. Формат команды создания таблиц CREATE TABLE.
8. Опции соединения таблиц в запросах.
9. Формат команды объединения данных UNION
10. Формат команды перекрестного запроса TRANSFORM

ПРАКТИЧЕСКИЕ ЗАДАНИЯ К РАЗДЕЛАМ

Форма практического задания: лабораторный практикум.

МОДУЛЬ «Базы данных и системы управления базами данных»

Примерный перечень тем лабораторных работ к разделу 1

Знакомство с Access

Лабораторная работа № 1.1 «Основные понятия БД. Объекты Access»
Лабораторная работа № 1.2 «Ввод и редактирование данных»
Лабораторная работа № 1.3 «Сортировка, Поиск и Замена»
Лабораторная работа № 1.4 «Фильтрация»
Лабораторная работа № 1.5 «Фильтр по выделенному»
Лабораторная работа № 1.6 «Автофильтр»
Лабораторная работа № 1.7 «Расширенный фильтр»

Лабораторная работа № 1.8 «Запросы»
Лабораторная работа № 1.9 «Групповые операции»
Лабораторная работа № 1.10 «Перекрестные запросы»

Примерный перечень тем лабораторных работ к разделу 2
Проектирование БД

Лабораторная работа № 2.1 «Разработка инфологической модели и создание БД»
Лабораторная работа № 2.2 «Проектирование БД. Создание таблиц»
Лабораторная работа № 2.3 «Проектирование БД. Создание связей между таблицами»
Лабораторная работа № 2.4 «Средства контроля и автоматизации ввода данных»
Лабораторная работа № 2.5 «Создание экранных форм»
Лабораторная работа № 2.6 «Запросы на добавление данных»
Лабораторная работа № 2.7 «Запросы на удаление данных»

Примерный перечень тем лабораторных работ к разделу 3
Обработка данных

Лабораторная работа № 3.1 «Запросы на создание таблиц»
Лабораторная работа № 3.2 «Виды соединения таблиц в запросах»
Лабораторная работа № 3.3 «Запросы на обновление данных»
Лабораторная работа № 3.4 «Создание отчетов»
Лабораторная работа № 3.5 «Создание страниц доступа к данным»
Лабораторная работа № 3.6 «Макросы»
Лабораторная работа № 3.7 «Кнопочная форма»

Примерный перечень тем лабораторных работ к разделу 4
Конструкции языка SQL

Лабораторная работа № 4.1 «Команда запроса на выборку SELECT»
Лабораторная работа № 4.2 «Команды редактирования данных INSERT, UPDATE, DELETE»
Лабораторная работа № 4.3 «Команды создания таблиц»
Лабораторная работа № 4.4 «Соединение таблиц в запросах»

Примерный перечень тем лабораторных работ к разделу 5
Конструкции языка SQL

Лабораторная работа № 5.1 «Команда запроса объединения данных UNION»
Лабораторная работа № 5.2 «Групповые операции в запросах»
Лабораторная работа № 5.3 «Команда перекрестного запроса TRANSFORM»

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛАМ: форма рубежного контроля – отчет к лабораторным работам

Оформление работ, выполняемых в рамках самостоятельной работы осуществляется в соответствии с Методическими указаниями по оформлению письменных работ обучающихся в рамках самостоятельной работы, утвержденными Учебно-методическим советом РГСУ, Протокол № 2 от 25 июня 2015 года.

Конкретные практические задания и задания для рубежного контроля определяются в учебно-методических материалах по работе обучающихся в электронной информационно-образовательной среде РГСУ с применением технологий электронного обучения по данной дисциплине, утверждаемых ежегодно кафедрой.

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Форма промежуточной аттестации обучающегося по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по дисциплине (модулю) являются дифференцированный зачет, **экзамен,** которые проводятся в **устной** форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ПК-2		Знать: компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	Этап формирования знаний
		Уметь: разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	Этап формирования умений
		Владеть: способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	Этап формирования навыков и получения опыта
ПК-3		Знать: методы принятия проектных решений, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	Этап формирования знаний

		Уметь: обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	Этап формирования умений
		Владеть: способностью обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	Этап формирования навыков и получения опыта
ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений	**Знать:** - принципы построения подсистем и средств обеспечения информационной безопасности, критерии и методы объективной оценки угроз объекту информатизации, с учетом дифференцированного и системного подхода; - номенклатуру и основные параметры сертифицированных средств обеспечения информационной безопасности.	Этап формирования знаний
		Уметь: Проводить анализ исходных данных и выделять наиболее важные составляющие, на основе дифференцированного подхода, с учетом иерархических и причинно- следственных связей.	Этап формирования умений
		Владеть : - основными навыками работы с программными продуктами, реализующих анализ рисков и оценку угроз объекту	Этап формирования навыков и получения опыта

		информатизации; - методами анализа результатов проектирования слаботочных систем, в том числе основными принципами графического представления результатов проектирования. - основными технологиями селективного информационного поиска и анализа результатов работы с информационными ресурсами по номенклатуре сертифицированных средств защиты объектов информатизации.	

4.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	**Этапы формирования компетенций**	**Показатель оценивания компетенции**	**Критерии и шкалы оценивания**
ПК-2, ПК-3, ПК-7	Этап формирования знаний	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно обобщать и излагать материал, не допуская ошибок – 9-10 баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно

			применять теоретические положения -7-8 баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала - 5-6 баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки -0-4 балла.
ПК-2, ПК-3, ПК-7	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией - 9-10 баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании -7-8 баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению5-6 баллов; 4) практические задания, задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и
ПК-2, ПК-3, ПК-7	Этап формирования навыков и получения опыта	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	

			заключений по решению задания, сделаны неверные выводы по решению задания - 0-4 баллов.

4.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Теоретический блок вопросов:

МОДУЛЬ «Основы баз данных»
МОДУЛЬ «Организация распределенных и удаленных баз данных»

1. Информация и данные, база данных, система управления базами данных (СУБД).
2. Эволюция концепции обработки данных, СУБД.
3. Требования к СУБД, основные особенности СУБД, составные части СУБД.
4. Системы быстрой разработки приложений. Модели данных.
5. Реляционная БД, история появления, принципы организации данных, достоинства и недостатки.
6. Базовые понятия реляционных БД: тип данных, домен, атрибут, кортеж, отношение, схема отношений.
7. Проектирование баз данных.
8. Нормализация БД, цели нормализации, 1НФ.
9. Нормализация БД, определение 1НФ, 2НФ, 3НФ.
10. Разработка приложений в среде MS Windows
11. Архитектура Microsoft Access.
12. Назначение объектов MS Access
13. Построение таблиц в MS Access.
14. Формы ввода-вывода данных.
15. Основные операции реляционной алгебры.
16. Дополнительные операции реляционной алгебры.
17. Запросы в MS Access.
18. Параметры запросов на выборку данных.
19. Перекрестные запросы.
20. Многотабличные запросы и схема данных.
21. Понятие технологии "клиент-сервер".
22. Общие сведения о языке запросов SQL.
23. Сетевые БД, архитектура «файл-сервер», «клиент-сервер».
24. Язык SQL: общие сведения о языке, роль и место в современных СУБД, стандарт ANSI.
25. Запрос выборки данных в SQL, простейшая выборка из одной таблицы.
26. Специальные операторы SQL IN, BETWEEN, LIKE, IS NULL.
27. Соединение таблиц с использованием операции JOIN.
28. SQL: запрос выборки данных, функции агрегирования AVG, SUM, MAX, MIN.
29. Форматирование выходных данных запроса, секции GROUP BY и HAVING.
30. Соединение таблиц.
31. Вложенные подзапросы.

32.Связанные подзапросы. Оператор EXISTS.

33.Вложенные и связанные подзапросы. Операторы ANY, SOME, ALL.

34.Объединение запросов.

35.SQL: запрос выборки данных по нескольким таблицам, оператор JOIN, левое, правое и внутреннее соединение.

36.Запросы обновления таблиц INSERT, UPDATE, DELETE..

37.Создание, модификация и уничтожение таблиц. Ограничения на множество допустимых значений данных. Значение по умолчанию.

38.Создание и уничтожение индексов. Поддержка ссылочной целостности

39.Создание представлений.

40.Определение прав доступа к данным.

41.Определение синонимов объектов. Понятие транзакций. Управление параллелизмом

42.Сервер баз данных, базовые понятия.

43.СУБД DB2. Иерархия объектов базы данных.

44.Объекты DB2, их назначение.

45.SQL: хранимые процедуры, область применения.

4.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестации по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам в Российском государственном социальном университете и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по дисциплине (модулю) выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам – программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры в Российском государственном социальном университете.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины (модуля)

5.1.1. Основная литература

1. *Гутгарц, Р. Д.* Проектирование автоматизированных систем обработки информации и управления : учебное пособие для вузов / Р. Д. Гутгарц. — Москва : Издательство Юрайт, 2022. — 304 с. — (Высшее образование). — ISBN 978-5-534-07961-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494408

2. *Грекул, В. И.* Проектирование информационных систем : учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — Москва : Издательство Юрайт, 2022. — 385 с. — (Высшее образование). — ISBN 978-5-9916-8764-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489918

5.1.2. Дополнительная литература

1. *Астапчук, В. А.* Корпоративные информационные системы: требования при проектировании : учебное пособие для вузов / В. А. Астапчук, П. В. Терещенко. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 113 с. — (Высшее образование). — ISBN 978-5-534-08546-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/492141
2. Рыбальченко, М. В. Архитектура информационных систем : учеб. пособие для вузов / М. В. Рыбальченко. — Москва : Издательство Юрайт, 2019. — 91 с. — (Серия : Университеты России). — ISBN 978-5-534-01159-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/book/arhitektura-informacionnyh-sistem-437686

5.2. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) «**Базы данных**» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины (модуля) и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы дисциплины (модуля) . Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе http://biblioclub.ru, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания;

систематизирует учебный материал;

ориентирует в учебном процессе.

С этой целью:

внимательно прочитайте материал предыдущей лекции;

ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

постарайтесь уяснить место изучаемой темы в своей подготовке;

узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от

степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету**.**

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

5.4.Информационно-технологическое обеспечение образовательного процесса по дисциплине (модулю)

5.4.1. Информационные технологии

1. Персональные компьютеры;
2. Доступ к Интернет
3. Проектор.

5.4.2. Программное обеспечение

1. Операционная система: Windows 7 или Astra Linux SE
2. Microsoft Office Professional Plus 2007 Russisn Academic или LibreOffice
3. Справочная система Консультант+
4. Acrobat Reader DC или Okular
5. 7-zip или Ark
6. SKY DNS
7.TrueConf (client)

5.4.3. Информационные справочные системы и профессиональные базы данных

Обучающиеся по программе **«Информационная безопасность»** в университете имеют доступ к следующим современным профессиональным базам данных, информационным справочникам:

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных «EastView»	Полнотекстовая база данных периодических изданий	http://ebiblioteka.ru/
5.	Электронная библиотека «Grebennikon»	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru

5.5. Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) **«Проектирование баз данных»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки 10.03.01 "Информационная безопасность" используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду университета, программным обеспечением).

5.6. Образовательные технологии

При реализации дисциплины (модуля) **«Проектирование баз данных»** применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины (модуля) **«Проектирование баз данных»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных

занятий в форме компьютерных симуляций, в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Учебные часы дисциплины «**Проектирование баз данных»** предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках дисциплины (модуля) **«Проектирование баз данных»** предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с направленностью (профилем) реализуемой основной профессиональной образовательной программы.

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			