ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

Подписано цифровой подписью: Шимановская Янина Васильевна
Дата: 2023.07.14 14:40:20 +03'00'

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ /С.В. Крапивка/

«06» __июня___2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
КОНТРОЛЬ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

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) **«Контроль безопасности в компьютерных сетях»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 1**0.03.01 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: доцент Малиничев Д.М.

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 обеспечении знаний теоретических и практических основ в организации и функционировании компьютерных сетей, формирование у студентов целостного представления о современных технологиях обеспечения информационной безопасности в компьютерных сетях, получение теоретических знаний о принципах и методах защиты информации в компьютерных сетях, обучение навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

Задачи дисциплины (модуля):

В результате изучения курса выпускник должен решать следующие *профессиональные задачи* (в сфере эксплуатационной, проектно-технологической, экспериментально-исследовательской, организационно-управленческой видов профессиональной деятельности):

1. знакомство с методами и инструментами защиты информации в операционных системах и компьютерных сетей, их практическое применение;
2. установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
3. администрирование подсистем информационной безопасности объекта;
4. участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;
5. сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
6. сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
7. участие в совершенствовании системы управления информационной безопасностью.

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

Учебная дисциплина «**Контроль безопасности в компьютерных сетях**» реализуется в **вариативной** части основной профессиональной образовательной программы **«Информационная безопасность»** по направлению подготовки **«10.03.01 Информационная безопасность» очной обучения.**

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

Изучение дисциплины (модуля) «**Контроль безопасности в компьютерных сетях**» является базовым для последующей подготовки 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 и профессионально-специальных** компетенций: ПК-1, ПК-6, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14 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-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-6	Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6.ИД-1. Сформирован понятийный аппарат и теоретическая 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	**Знать:** - основные принципы оценки работоспособности и тестирования 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 коммуникационного оборудования и аппаратуры обработки данных, криптографических систем
	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 р еализации 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-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 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	**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,

			компетенции	технических и технологических направлениях, связанных с проблемой обеспечения безопасности объектов информатизации.
	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 практические действия в рамках компетенции ПК-12.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** функциональное назначение, технические и конструктивные особенности применения, общие принципы построения и работы исследуемой системы защиты информации.
				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.

				Владеть: теоретическими знаниями и навыками по практическому применению соответствующего специализированного оборудования и измерительных приборов для проведении экспериментальных исследований системы защиты информации мероприятий
	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 выполняет практические действия в рамках компетенции ПК-14.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**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
				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 работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет 11 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		6	7	8		
Контактная работа обучающихся с педагогическими работниками	**198**	**54**	**72**	**72**		
Учебные занятия лекционного типа	44	12	16	16		
из них: в форме практической подготовки						
Практические занятия	16		8	8		
из них: в форме практической подготовки						
Лабораторные занятия	50	18	16	16		
из них: в форме практической подготовки						
Иная контактная работа	88	24	32	32		
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**171**	**45**	**63**	**63**		
из них: в форме практической подготовки	*37*	*9*	*14*	*14*		
Контроль промежуточной аттестации	**27**	**9**	**9**	**9**		
Форма промежуточной аттестации		зачет	диф. зач	диф. зач		
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**396**	**108**	**144**	**144**		

2.1. Учебно-тематический план по очной форме обучения

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 6)													
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 7)													
Раздел 2.1	33	15	*4*	18		4		2		4		8	
Раздел 2.2	34	16	*4*	18		4		2		4		8	
Раздел 2.3	34	16	*3*	18		4		2		4		8	
Раздел 2.4	34	16	*3*	18		4		2		4		8	
Контроль промежуточной аттестации (час)	**9**												

Общий объем, часов	**144**	**63**	***14***	**72**		**16**		**8**		**16**		**32**	
Форма промежуточной аттестации	**дифференцированный зачет**												
Модуль 3 (семестр 8)													
Раздел 3.1	33	15	*4*	18		4		2		4		8	
Раздел 3.2	34	16	*4*	18		4		2		4		8	
Раздел 3.3	34	16	*3*	18		4		2		4		8	
Раздел 3.4	34	16	*3*	18		4		2		4		8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**144**	**63**	***14***	**72**		**16**		**8**		**16**		**32**	
Форма промежуточной аттестации	**дифференцированный зачет**												
Общий объем, часов	**396**	**171**	***37***	**198**		**44**		**16**		**50**		**88**	

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 6)							
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 7)							
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 8)							
Раздел 3.1	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 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
Общий объем по модулю/семестру, часов	**63**	**27**		**28**		**8**	
Общий объем по дисциплине (модулю), часов	**171**	**72**		**77**		**22**	

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

МОДУЛЬ «КОМПЬЮТЕРНЫЕ СЕТИ»

РАЗДЕЛ 1. ЭВОЛЮЦИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Цель: Рассмотреть эволюцию сетей передачи данных.

Перечень изучаемых элементов содержания:

Коммутация каналов, коммутация пакетов, коммутатор пакетов, маршрутизация, датаграмма, сеть, не ориентированная на соединения, сеть, ориентированная на соединение, ITU, эталонная модель OSI, IETF, RFC.

Вопросы для самоподготовки:

1. Принципы коммутации пакетов
2. История создания компьютерных сетей
3. Модель взаимосвязи открытых систем
4. Стандартизация в сетях Интернет

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторный практикум.
Цель: Изучить основные понятия сетей передачи данных.

Контрольные вопросы:

1. В чем основное различие принципов коммутации каналов и коммутации пакетов?

2. Поясните понятия «сеть, ориентированная на соединения» и «сеть, не ориентированная на соединения».
3. Какой была цель введения эталонной модели OSI?
4. В чем разница между протоколом и процессом?
5. Дайте характеристику уровней эталонной модели OSI.
6. Поясните роль Комитета IETF.
7. Что такое RFC?

1. Число уровней эталонной модели ВОС было выбрано равным семи. Докажите правомерность этого решения или попробуйте его опровергнуть.
2. В 2001 году глобальная сеть Интернет обеспечивала обработку всего трафика при суммарной пропускной способности магистральной сети, равной 1 Тбит/с. Рассчитайте пропускную способность сети Интернет, которая потребуется в 2010 году, учитывая, что трафик данных растет в год примерно на 50%.

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

РАЗДЕЛ 2. СЕТИ НА БАЗЕ ВИРТУАЛЬНЫХ СОЕДИНЕНИЙ

Цель: Рассмотреть сети на базе виртуальных соединений.

Перечень изучаемых элементов содержания:

Сеть с коммутацией пакетов, протокол X.25, виртуальный канал, коммутируемое виртуальное соединение, постоянное виртуальное соединение, оконечное оборудование данных ООД, аппаратура канала данных АКД, сборщик/разборщик пакетов, протокол Frame Relay, гарантированная скорость передачи, технология ATM, гарантированное качество обслуживания, ячейка ATM, классы обслуживания уровня AAL, классы обслуживания ATM.

Вопросы для самоподготовки:

1. Сети на базе протокола X.25
2. Сети на базе протокола Frame Relay
3. Сети ATM (Структура ячейки ATM. Эталонная модель протоколов ATM. Классы обслуживания на уровне AAL. Классы обслуживания в сети ATM и показатели качества обслуживания).

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторный практикум.
Цель: Изучить организацию виртуальных соединений.

Контрольные вопросы:

1. Объясните принцип организации виртуальных соединений.
2. В чем разница между коммутируемыми и постоянными виртуальными каналами?
3. Назовите основные достоинства и недостатки протокола X.25.
4. Почему появилась возможность перехода от протокола X.25 к протоколу Frame Relay
5. В чем основные недостатки протокола X.25 по сравнению с протоколом Frame Relay?
6. Для какого нового вида сетей. была разработана технология ATM?
7. Определите функции уровней эталонной модели ATM
8. Объясните разделение на классы обслуживания в соответствии с рекомендациями ITU-T.
9. Объясните разделение на классы обслуживания в соответствии с рекомендациями Форума ATM.

10. Определите избыточность кадра и пакета для переноса информации в протоколе X.25
11. Каким образом в протоколе X.25 общее число возможных виртуальных каналов достигает величины 4096?
12. Определите, сколько пар «источник-получатель» может быть задано в одной ячейке ATM?

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

РАЗДЕЛ 3. СЕТИ НА БАЗЕ ПРОТОКОЛОВ TCP/IP

Цель: Рассмотреть протоколы TCP/IP**.**

Перечень изучаемых элементов содержания:

Стек протоколов Интернет TCP/IP, протокол IP, протокол TCP, протокол UDP, датаграмма, фрагмент, IP-маршрутизатор, маршрутизация, заголовок протокола IPv4, заголовок протокола IPv6, принцип «наилучшей попытки».

Вопросы для самоподготовки:

1. Сети Интернет
2. Эталонная модель протоколов сети Интернет
3. Протоколы стека TCP/IP
4. Принципы организации сети Интернет
5. **Структура заголовков IPv4 и IPv6**
6. **Структура заголовков TCP и UDP**

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторный практикум.
Цель: Изучить основные элементы протоколов..

Контрольные вопросы:

1. Поясните основные свойства сетей Интернет.
2. В чем различие эталонных моделей OSI и IETF?
3. Объясните принцип «наилучшей попытки».
4. В чем главное отличие протокола IP от протокола TCP?
5. Что означает поле «Время жизни» в заголовке датаграммы?
6. Перечислите основные свойства протокола IPv6.
7. Поясните назначение поля «Тип обслуживания».
8. Чем характеризуется качество обслуживания в сетях Интернет?
9. В чем отличие протокола TCP от протокола UDP?
10. Определите общее число адресов, доступных при использовании протокола IPv4.
11. Сколько уровней приоритета датаграммы можно определить в протоколе IPv4?

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

РАЗДЕЛ 4. **СИСТЕМЫ СИГНАЛИЗАЦИИ VoIP**

Цель: Рассмотреть системы сигнализации VoIP.

Перечень изучаемых элементов содержания:

Протокол инициирования сеансов SIP, стек TCP/IP, персональная мобильность, описание сеансов, протокол SDP, протокол управления шлюзами, протокол H.248, сигнализация H.323, привратник, устройство управления конференциями, протокол RAS, рекомендация H.225, рекомендация H.245, рабочая группа Sigtran, протокол SCTP, протоколы адаптации M2UA, M2PA и M3UA, протоколы SUA и IUA, PINT, SPIRITS, протокол TRIP.

Вопросы для самоподготовки:

1. Создание архитектуры SIP
2. Протокол SDP
3. Управление медиашлюзами
4. Протокол H.323
5. Сигнализация ОКС7 поверх IP (Протокол управления потоками SCTP. Протоколы адаптации M2UA, M2PA и M3UA. Протоколы SUA и IUA).

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: лабораторный практикум.

Цель: Изучить основные протоколы.

Контрольные вопросы:

1. Какие свойства протоколов SIP/1.0 и SCIP перешли в SIP?
2. На каких протоколах стека TCP/IP базируется SIP?
3. Объясните двойное наименование протокола MEGACO/H.248.
4. В чем заключается принцип декомпозиции шлюзов?
5. Назовите четыре основных сетевых элемента H.323.
6. Нарисуйте и объясните стек протоколов H.323.
7. Почему используются протоколы ОКС поверх IP в стеке протоколов Sigtran?
8. Нарисуйте и объясните стек протоколов Sigtran.

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

РАЗДЕЛ 5. СИСТЕМЫ АДРЕСАЦИИ И МАРШРУТИЗАЦИИ В СПД

Цель: Рассмотреть системы адресации и маршрутизации в СПД.

Перечень изучаемых элементов содержания:

Адресация в сетях Интернет, адрес сети, адрес хоста, классы адресов, маршрутизация, маска, бесклассовая междоменная маршрутизация, статическая маршрутизация, динамическая маршрутизация, маршрутизатор, таблица маршрутизации, оптимальный маршрут, система доменных имен, концепция ENUM.

Вопросы для самоподготовки:

1. Нумерация и адресация
2. Принципы назначения адресов в сетях IP
3. Протоколы поддержки системы адресации
4. Принципы маршрутизации датаграмм в сетях IP
5. Протоколы маршрутизации
6. Концепция ENUM

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5

Форма практического задания: лабораторный практикум.
Цель: Изучить системы адресации и маршрутизации в СПД**.**

Контрольные вопросы:

1. Какую роль играют классы в системах адресации?
2. Что такое «фиксированная граница» в адресном пространстве?
3. С какой целью была введена маска сети?
4. Какие критерии используются для определения маршрутов при динамической маршрутизации?
5. Для каких целей используется кэш-таблица в протоколах маршрутизации?
6. Чем различаются протоколы RIP и OSPF?
7. С какой частотой передается информация о маршрутах в протоколах RIP и OSPF?
8. Как сеть узнает, что хост вышел из группы многоадресной передачи?
9. Для каких целей была разработана концепция ENUM?
10. Задан 1P-адрес 234.32.115.10. Запишите этот адрес в двоичной системе. Определите класс адреса адрес сети и адрес хоста. Посчитайте, сколько сетей может быть задано в классе С. Определите число сетей, выделенных для автономных систем.

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

РАЗДЕЛ 6. ТЕХНОЛОГИИ ПОДДЕРЖКИ НОВЫХ УСЛУГ В СЕТЯХ ИНТЕРНЕТ

Цель: Рассмотреть технологии поддержки новых услуг в сетях Интернет.

Перечень изучаемых элементов содержания:
IP-телефония, IP-коммуникации, VoIP, кодек, управление обслуживанием вызова, шлюз, привратник, контроллер шлюза, сервер обработки вызовов, протокол RTP, протокол RTCP, технология IPTV, интерактивное ТВ, VoD, источник контента, узел услуг, широкополосные сети, оборудование пользователя, ТВ-приставка, стандарты сжатия, стандарты цифрового вещания, транспортные протоколы, протоколы маршрутизации.

Вопросы для самоподготовки:

1. Услуги IP-коммуникаций
2. Технология VoIP
3. Основные функции, реализуемые в сети VoIP
4. Архитектура сети VoIP
5. Сервер обработки вызовов
6. Шлюз
7. Особенности использования сети IP для передачи речи
8. Протокол RTP
9. Определение и основные свойства IPTV
10. Архитектура IPTV

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 6

Форма практического задания: лабораторный практикум.
Цель: Изучить технологии поддержки новых услуг в сетях Интернет**.**

Контрольные вопросы:

1. По каким признакам различаются кодеки ITU-T?

2. Назовите основные функции сервера обработки вызовов VoIP.
3. Назовите основные функции шлюза VoIP.
4. Назовите основные функции магистрального шлюза и шлюза доступа.
5. Можно ли использовать протокол RTP для контроля качества обслуживания?
6. В чем разница между поддержкой интерактивного ТВ и персонализацией?
7. Опишите функции основных компонентов системы IPTV.
8. Длительность пакета IP в системе VoIP составляет 20 мс. Рассчитайте:
   - Количество пакетов в течение 1 с?
   - Сколько битов на один пакет требуется при использовании кодеков: G.711; G.729?
   - Сколько байтов на один пакет нужно для тех же кодеков?

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

РАЗДЕЛ 7. Традиционные услуги в сетях Интернет

Цель: Рассмотреть традиционные услуги в сетях Интернет.

Перечень изучаемых элементов содержания:

Протокол пересылки файлов, единый локатор ресурсов, URL, Всемирная Паутина, World Wide Web (VWWV), HyperText Transfer Protocol (HTTP), Hypertext Markup Language (HTML), Web-сервер, Web-браузер, Web-страница, Web-сайт, гипертекстовая ссылка, электронная почта, протокол SMTP, протокол MIME.

Вопросы для самоподготовки:

1. Протокол пересылки файлов FTP
2. Протокол пересылки гипертекстовых сообщений HTTP и Всемирная Паутина
3. Протокол электронной почты SMTP

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 7

Форма практического задания: лабораторный практикум.
Цель: Изучить традиционные услуги в сетях Интернет**.**

Контрольные вопросы:

1. Какая разница между HTTP и HTML?
2. Чем различаются Web-браузер и Web-сереер?
3. Для чего нужны гиперссылки?
4. Чем различаются версии протокола HTTP 1.0 и 1.1? Почему использование HTTP 1.0 является неэффективным?
5. Для чего предназначен протокол MIME?
6. Информация каких видов может передаваться по электронной почте?
7. Нарисуйте диаграммы сеансов для протокола HTTP версий 1.0 и 1.1.

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

МОДУЛЬ «ТЕХНОЛОГИИ КОМЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

РАЗДЕЛ 1. Основные понятия и принципы безопасности

Цель: Рассмотреть основные понятия и принципы безопасности.

Перечень изучаемых элементов содержания

Идентификация. Аутентификация. Авторизация. Модели информационной безопасности. Уязвимость, угроза, атака, ущерб..

Вопросы для самоподготовки

1. Термины и определения.
2. ИС как система контролируемого доступа к ресурсам.
3. Концепция совместного использования ресурсов.
4. Идентификация.
5. Аутентификация.
6. Авторизация.
7. Модели информационной безопасности.
8. Триада «Конфиденциальность, доступность, целостность».
9. Гексада Паркера и модель STRIDE.
10. Уязвимость, угроза, атака, ущерб.
11. Типы и примеры атак.
12. Пассивные и активные атаки.
13. Отказ в обслуживании.
14. Внедрение вредоносных программ.
15. Кража личности, фишинг.
16. Сетевая разведка.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторный практикум.

Цель:

Изучить идентификацию и аутентификацию пользователей.

Контрольные вопросы

1. Как соотносятся понятия «безопасность компьютерных сетей» и «безопасность информационных систем»?
2. Что может быть отнесено к субъектам системы контроля доступа к ресурсам ИС?
3. Что может быть отнесено к объектам системы контроля доступа к ресурсам ИС?
5. Какие свойства образуют триаду безопасности CIA?
6. Какие свойства образуют гексаду Паркера?
8. Какие атаки являются активными?
10. Если система контроля доступа не разрешила пользователю распечатать документ на принтере, то как такую ситуацию можно назвать?
11. Для каких из ИС доступность может быть важнее конфиденциальности?
12. Приведите примеры ситуаций, при которых обеспечивается конфиденциальность, но не гарантируется целостность данных.
13. Приведите примеры действий воображаемого злоумышленника, направленных на нарушение доступности данных.

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

РАЗДЕЛ 2. Управление рисками

Цель: Рассмотреть вопросы управления рисками.

Перечень изучаемых элементов содержания

Идентификация. Аутентификация. Авторизация. Модели информационной безопасности. Уязвимость, угроза, атака, ущерб..

Вопросы для самоподготовки

1. Анализ уязвимостей и угроз
2. Ущерб как мера риска
3. Управление рисками
4. Стандартные методики оценки рисков
5. Рекомендации NIST
6. Методика оценки рисков RiskWatch
7. Методика CRAMM
8. Методика OCTAVE
9. Определение профилей угрозы для ключевых активов
10. Идентификация уязвимостей инфраструктуры
11. Разработка стратегии безопасности и планов снижения рисков

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторный практикум.

Цель:

Изучить идентификацию и аутентификацию пользователей.

Контрольные вопросы

1. Что является конечной целью управления рисками?
2. Возможные источники рисков предприятия.
4. Возможные факторы риска, связанного с несанкционированным доступом к кодам разрабатываемого на софтверном предприятии программного комплекса.
5. Какой процедурой пользовался администратор при исследовании системы, если известно, что ему удалось обнаружить совершенно новый тип уязвимости?
7. Какие меры могут быть предприняты по отношению к каждому риску при управлении рисками?
8. Что используется для оценки вероятности возникновения угроз?
9. На каком этапе завершается процесс управления рисками.
10. Когда можно не предпринимать никаких действий по отношению к выявленному риску.
12. Для чего создается типовой профиль угрозы в методике OCTAVE?
13. Предложите собственный вариант качественных шкал оценки вероятностей, ущерба и риска, а также правило соответствия пар (вероятность, ущерб) уровням риска. Для каждой градации шкалы составьте описание.

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

РАЗДЕЛ 3. Технологии защищенного канала

Цель: Рассмотреть технологии защищенного канала.

Перечень изучаемых элементов содержания

Защищенный канал. Протоколы.

Вопросы для самоподготовки

1. Способы образования защищенного канала
2. Иерархия технологий защищенного канала
3. Туннелирование
4. Протокол IPSec

5. Распределение функций между протоколами IPSec
6. Безопасная ассоциация
7. Транспортный и туннельный режимы
8. Протокол AH
9. Протокол ESP
10. Базы данных SAD И SPD

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторный практикум.

Цель:

Защищенный канал. Протоколы.

Контрольные вопросы

1. Какие основные функции выполняет защищенный канал?
2. Какие цели преследует туннелирование?
3. Какой адрес назначения указывается в заголовке несущего протокола при туннелировании?
4. Какие протоколы включает IPsec?
6. Какие из функций являются обязательными для протокола AH?
7. Какие задачи решает протокол ESP?
8. Что определяет база данных политики безопасности (SPD)?
9. С какой целью в семействе протоколов IPSec функции обеспечения целостности и аутентичности данных дублируются в двух протоколах - AH и ESP?

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

РАЗДЕЛ 4. Технологии анализа трафика и состояния сети

Цель: Рассмотреть технологии анализа трафика и состояния сети **.**

Перечень изучаемых элементов содержания

Аудит. Трафик. Файервол.

Вопросы для самоподготовки

1. Аудит
2. Подотчетность
3. Задачи аудита
4. Файерволы
5. Сегментация сети
6. Фильтрация трафика
7. Определение файервола
8. Типы файерволов
9. Системы обнаружения вторжений
10. Типы систем обнаружения вторжений
11. Функциональная схема IDS
12. Правила обнаружения атак

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: лабораторный практикум.

Цель:

Рассмотреть технологии анализа трафика и состояния сети

Контрольные вопросы
1. Какие функции системы безопасности направлены на обеспечение подотчетности?
2. К какому типу средств вы бы отнесли аудит?
3. Что дает сегментация сети?
6. Как называют комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой путем анализа и фильтрации проходящего между ними трафика?
7. Какими признаками будет обладать корпоративный файервол?
8. Какие действия выполняют файерволы сеансового уровня?
9. Что входит в число основных функций IDS?
10. Какие из атак могут быть обнаружены файерволом?

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

РАЗДЕЛ 5. Транспортная инфраструктура и ее уязвимости

Цель: Рассмотреть уязвимости транспортной инфраструктуры.

Перечень изучаемых элементов содержания

Уязвимость. Протоколы. Атаки.

Вопросы для самоподготовки

1. Протоколы и их уязвимости
2. Атаки на траспортную инфраструктуру
3. TCP-атаки
4. Затопление SYN-пакетами
5. Подделка TCP-сегмента
6. Повторение TCP-сегментов
7. Сброс TCP-соединения
8. ICMP-атаки
9. Перенаправление трафика
10. ICMP Smurf-атака
11. Ping смерти и ping-затопление
12. UDP-атаки
13. UDP-затопление
14. ICMP/UDP-затопление
15. UDP/echo/chargen-затопление
16. IP-атаки
17. Атака IP-опции
18. Атака IP-фрагментация
19. DNS-атаки
20. Организация DNS
21. Атаки на DNS
22. Методы защиты службы DNS
23. Сетевая разведка

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5

Форма практического задания: лабораторный практикум.

Цель:

Рассмотреть уязвимости трансопртной инфраструктуры.

Контрольные вопросы

1. Что является элементом транспортной инфраструктуры сети?
2. Почему транспортная инфраструктура сети является заманчивой целью дли злоумышленников?
4. В чем состоит главная уязвимость протокола IP?
5. Что входит в функции протокола TCP?
6. Что может злоумышленник с помощью протокола ICMP?
8. Как работает атака SYN Flood?
9. Что является признаком атаки SYN Flood?
10. С какой целью злоумышленник должен подавить отправку АСК-сегментов на атакуемый сервер в ходе атаки SYN Flood?
11. Для чего применяется техника «Проверка обратного пути»?
12. В чем заключается идея механизма SYN cookie?
13. Соединения какого типа проще использовать для атаки «Подделка TCP сегмента»?
14. Какими средствами можно предотвратить атаки «Повторение сегментов» и «Сброс соединения»?
15. Каким образом можно направить трафик по ложному маршруту?
16. Каким образом можно предотвратить атаку ICMP Smurf?
17. К чему приводит атака Ping of Death?
18. Почему с атаками, использующими протокол UDP, сложнее бороться, чем с атаками, использующими протокол TCP?
20. Чем атака «DNS-спуфинг» отличается от атаки «Отравление DNS-кэшах ?
21. Можно ли использовать систему DNS для атаки затопления?

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

РАЗДЕЛ 6. Фильтрация и мониторинг трафика

Цель: Рассмотреть понятия фильтрации и мониторинга траффика.

Перечень изучаемых элементов содержания

Трафик. Мониторинг. Файервол.

Вопросы для самоподготовки

1. Фильтрация трафика и файерволы
2. Типы фильтрации трафика
3. Файерволы на основе маршрутизаторов
4. Файерволы с функцией NAT.
5. Мониторинг сети
6. Сетевые снифферы
7. Система мониторинга NetFlow
8. Типовые архитектуры сетей, защищаемых файерволами
9. Демилитаризованная зона
10. Обобщенная архитектура сети с защитой периметра и разделением внутренних зон

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 6

Форма практического задания: лабораторный практикум.

Цель:

Изучить фильтрацию и мониторинг траффика.

Контрольные вопросы

1. Какие функции выполняют списки доступа маршрутизаторов?
2. Какие признаки в пакете сможет учитывать файервол на основе маршрутизатора?

3. Какое условие подразумевается неявным образом в конце каждого списка доступа маршрутизатора Cisco:
4. Можно ли фильтровать трафик по адресу назначения в стандартных списках доступа маршрутизаторов Cisco?
6. Какую фильтрацию выполняет список доступа **ip as-path access-list 1 permit ^117?**
9. Для чего используется технология NAT?
10. Можно ли использовать традиционную технологию NAT для доступа из Интернета к внутреннему серверу, имеющему частный IP-адрес?
11. Какой параметр пакета использует технология NAPT для различения внутренних хостов при использовании только одного публичного IP-адреса?
12. Возможности сетевого анализатора.
14. Для чего используется протокол NetFlow?
15. Какими параметрами характеризуется поток трафика в версии NetFlow v5?
16. На чем основан метод распознавания атак «Top N Sessions»?
17. Какие компьютеры вы бы включили в демилитаризованную зону корпоративной сети?
18. По каким признакам компьютеры должны объединяться в зоны, корпоративной сети, защищаемой файерволом:

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

РАЗДЕЛ 7. Безопасность маршрутизации на основе BGP

Цель: Рассмотреть понятие безопасности маршрутизации на основе BGP.

Перечень изучаемых элементов содержания

Протокол. Уязвимости. Инциденты.

Вопросы для самоподготовки

1. Принципы работы протокола маршрутизации BGP
2. Уязвимости и инциденты BGP
3. Защита BGP сессии между соседними маршрутизаторами
4. Защита маршрутизации BGP на основе данных региональных информационных центров Интернет
5. Сертификаты ресурсов и их использование для защиты BGI
6. Защита полного маршрута

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 7

Форма практического задания: лабораторный практикум.

Цель:

Изучить безопасность маршрутизации на основе BGP.

Контрольные вопросы

3. Будет ли принято или отвергнуто маршрутное объявление «AS 13999, AS 688, AS 376, AS 10388, AS 542, 195.47.108.0/24», полученное BGP-маршрутизатором AS 376 от соседнего BGP-маршрутизатора AS 13999?
4. Что было причиной инцидента AS7007, когда из таблиц маршрутизации многих провайдеров исчезли записи, ведущие к крупным сетям Интернета?
5. Каким образом можно «подделать» маршрутное объявление BGP, которое вы передаете вашему соседу, если ваша AS является транзитной для этого маршрута, а вы хотите, чтобы сосед не использовал этот маршрут для передачи трафика?
6. Какие меры предпринимают провайдеры при фильтрации маршрутных объявлений BGP от своих соседей?

7. Какие типы объектов содержит база данных маршрутов Интернета IRR?
8. По каким причинам провайдеры используют базу данных маршрутов Интернета IRR не эффективно?
9. Для чего используются сертификаты ресурсов RPKI?
10. Что удостоверяет объект ROA?
11. На чем основан протокол BGPSEC?

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

МОДУЛЬ «ЗАЩИТА ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ СЕТИ»

РАЗДЕЛ 1. Виртуальные частные сети

Цель: Рассмотреть понятия виртуальных частных сетей.

Перечень изучаемых элементов содержания

Виртуальная частная сеть.

Вопросы для самоподготовки

1. Определение виртуальной частной сети
2. Свойства частной сети, имитируемые VPN
3. Типы VPN
4. MPLS VPN
5. VPN на основе шифрования

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторный практикум.

Цель:

Изучить понятие виртуальной частной сети.

Контрольные вопросы

1. Какие свойства частной сети имитирует виртуальная частная сеть?
2. Может ли некоторая VPN быть одновременно классифицирована как VPN на основе виртуальных каналов, VPN, поддерживаемая провайдером, и VPN с топологией «звезда»?
3. Может ли MPLS VPN быть классифицирована как VPN, поддерживаемая клиентом?
4. Каким способом MPLS VPN обеспечивают безопасность передачи данных?
5. Технология MPLS VPN поддерживает следующие топологии соединений пользователей:
6. Технология L3 MPLS VPN называется технологией третьего уровня, потому что:
7. С какой целью VPN на основе шифрования используют туннелирование?
8. Что из перечисленного ниже не характеризует VPN на основе каналов SSL:

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

РАЗДЕЛ 2. Безопасность локальных беспроводных сетей

Цель: Рассмотреть понятия безопасности локальных беспроводных сетей.

Перечень изучаемых элементов содержания

Уязвимости. Методы. Протоколы.

Вопросы для самоподготовки

1. Уязвимости локальных беспроводных сетей
2. Две схемы организации беспроводной сети
3. Методы защиты локальных беспроводных сетей
4. Протокол WEP
5. Стандарт WPA2
6. Беспроводные системы обнаружения вторжений

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторный практикум.

Цель:

Изучить безопасность локальных беспроводных сетей.

Контрольные вопросы

1. Беспроводные локальные сети стандартов 802.11b/g/n более уязвимы, чем проводные локальные сети Ethernet, потому что:
2. Вы защитили свою домашнюю беспроводную сеть, активировав строгую аутентификацию и шифрование данных по протоколу WPA2 на точке доступа. Какую уязвимость может использовать злоумышленник для проникновения в вашу сеть?
3. Верно ли утверждение «Запрет широковещательной рассылки SSID точкой доступа существенно повышает безопасность беспроводной локальной сети»?
4. Верно ли утверждение «Точка доступа, работающая по протоколу WEP, всегда получает пароль пользователя в открытом виде»?
5. Что из перечисленного характеризует спецификацию 802.1x:
6. Для обнаружения компьютера злоумышленника система WIDS использует следующий прием:

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

РАЗДЕЛ 3. Безопасность облачных сервисов

Цель: Рассмотреть понятия безопасности облачных сервисов.

Перечень изучаемых элементов содержания

Облачный сервис.

Вопросы для самоподготовки

1. Что такое «облачные сервисы»
2. Определение облачных вычислений
3. Свойства облачных вычислений
4. Технологии облачных вычислений
5. Модели сервисов облачных вычислений
6. Преимущества облачных сервисов
7. Проблемы безопасности облачных сервисов
8. Значимость облачных сервисов

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторный практикум.

Цель:

Изучить безопасность облачного сервиса.

Контрольные вопросы
1. Модель публичных облачных вычислений характеризуется тем, что:
2. Что из перечисленного является свойствами модели публичных облачных вычислений:
3. Основной технологией, на которой основаны облачные вычисления, является:
4. Какие из приведенных ниже утверждений корректно описывают свойства модели "Приложения как сервис" (SaaS):
5. В какой модели облачных вычислений клиент имеет полный контроль над приложениями?
6. Какие факторы позволяют модели облачных вычислений обеспечивать более высокую безопасность информационной системы по сравнению с традиционной моделью вычислений:

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

РАЗДЕЛ 4. Безопасность электронной почты

Цель: Рассмотреть понятия безопасности электронной почты.

Перечень изучаемых элементов содержания

Почтовый сервис. Шифрование. Спам.

Вопросы для самоподготовки

1. Организация почтового сервиса
2. Электронные сообщения
3. Протокол SMTP
4. Непосредственное взаимодействие клиента и сервера
5. Схема с выделенным почтовым сервером
6. Схема с двумя почтовыми серверами посредниками
7. Протоколы POP3 и IMAP
8. Угрозы и механизмы защиты почты
9. Угрозы почтовому сервису
10. Аутентификация отправителя
11. Шифрование содержимого письма
12. Защита метаданных пользователя
13. Атаки на компьютер с помощью почты
14. Спам
15. Атаки почтовых приложений

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: лабораторный практикум.

Цель:

Изучить безопасность электронной почты.

Контрольные вопросы
1. Каким элементом почтовой системы Интернета обрабатываются данные служебных полей конверта сообщения?
2. С какой целью в почтовой службе Интернета используется алгоритм base64?
3. Иногда вы получаете цифровую фотографию в виде приложения к электронному письму, а иногда она встроена в текст сообщения. От чего зависит режим передачи фотографии?
4. Что из перечисленного является разрешенным типом части тела электронного письма в стандарте MIME?
5. Какие типы части тела электронного сообщения определяет стандарт S/MIME?
6. Какие из перечисленных ниже протоколов почтовый клиент может использовать для приема электронного письма:

7. Является ли следующее утверждение верным: «Почтовый сервер обязан послать отрицательное уведомление почтовому клиенту отправителя»?
8. Какие из перечисленных ниже протоколов почтовый клиент может использовать для отправки электронного письма:
9. Вы работаете со своей электронной почтой, используя несколько компьютеров. Какой протокол вы должны использовать в почтовых клиентах этих компьютеров, чтобы содержимое локальных почтовых ящиков ваших компьютеров было идентичным, независимо от того, на каком компьютере вы прочитали то или иное письмо?
10. На отражение каких угроз направлен механизм аутентификации отправителя электронного письма на основе его цифровой подписи?
11. Охватывает ли цифровая подпись и шифрование по стандарту S/MIMI приложения к электронному письму?
12. Каким образом проверяется подлинность публичного ключа отправителя в стандарте PGP?
13. Что из перечисленного относится к метаданным электронной почты:
14. Записи какого типа составляют список DNSBL:

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

МОДУЛЬ «КОНТРОЛЬ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ»

РАЗДЕЛ 1. СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК.

Цель: Рассмотреть системы обнаружения атак.

Перечень изучаемых элементов содержания
Уязвимости. Атаки.

Вопросы для самоподготовки

1. Уязвимости традиционных средств защиты
2. Уязвимости стека протоколов TCP/IP
3. Слабости МЭ, и способы его обхода
4. Уязвимости системы аутентификации и авторизации
5. Анатомия атаки, этапы осуществления атаки
6. Классификация уязвимостей
7. Модель атаки
8. Этапы реализации атаки
9. Классификация атак
10. Задача обнаружения атак
11. Понятие системы обнаружения атак
12. Реальные возможности систем обнаружени атак и пределы их возможностей
13. Схема работы системы обнаружения атак
14. Основные принципы обнаружения атак
15. Признаки атак
16. Источники информации об атаках
17. Технологии и подходы к обнаружению атак

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: лабораторный практикум.

Цель:
Изучить системы обнаружения атак.

Контрольные вопросы

1. Обнаружение следов атак
2. Контроль изменений файлов
3. Анализ журналов регистрации
4. Анализ сетевого трафика
5. Классификация систем обнаружения атак
6. Системы анализа защищенности
7. Анализаторы журналов регистрации
8. Обманные системы
9. Системы контроля целостности
10. Выбор системы обнаружения атак
11. Предварительный анализ
12. Критерии оценки
13. Тестирование
14. Размещение системы обнаружения атак
15. Размещение сенсоров
16. Использование сетевых сенсоров коммутируемых сетях
17. Размещение системы анализа защищенности
18. Размещение системы контроля целостности
19. Системы виртуальных ловушек (Honey Pot и Padded Cell)
20. Методы развертывания и эксплуатации СОА
21. Общие проблемы
22. Сетевые системы
23. Узловые системы

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

РАЗДЕЛ 2. ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ АТАК

Цель: Рассмотреть технологии обнаружения атак.

Перечень изучаемых элементов содержания
Атака. Технологии обнаружения атак.

Вопросы для самоподготовки

1. Необходимость технологии обнаружения атак.
2. Терминология.
3. Источники данных для систем обнаружения атак.
4. Признаки атак.
5. Методы обнаружения атак.
6. Механизмы реагирования.
7. Специализированные системы обнаружения атак
8. Взаимодействие с другими средствами защиты.
9. Анализ результатов работы систем обнаружения атак.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: лабораторный практикум.

Цель:

Изучить технологии обнаружения атак.

Контрольные вопросы

1. Обнаружение атак как механизм защиты.
2. События безопасности и уязвимости. Атаки. Модель традиционной и распределенной атаки. Этапы и средства реализации атак. Классификация атак. Базы данных атак и уязвимостей. Инциденты. Архитектура системы обнаружения атак
3. Принципы работы и варианты подключения сетевых систем обнаружения атак. Скрытый режим работы сетевой системы обнаружения атак. Обнаружение атак на уровне отдельного узла. Network Flow Data как дополнительный источник данных.
4. Повтор определенных событий. Неправильные команды. Использование уязвимостей. Несоответствующие параметры сетевого трафика. Несоответствие стандартам. Непредвиденные атрибуты.
5. Обнаружение аномалий и злоупотребелений. Анализ протоколов. Построение профиля поведения.
6. Варианты оповещений. Регистрация. Блокировка. Особенности использования систем противодействия атакам.
7. Особенности защиты беспроводных сетей. Защита от атак на СУБД и Web-приложения.
8. Обнаружение атак и другие защитные механизмы. Корреляция.
9. Управление инцидентами.

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

РАЗДЕЛ 3. ТИПОВЫЕ УДАЛЕННЫЕ АТАКИ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Цель: Рассмотреть понятия типовых удаленных атак.

Перечень изучаемых элементов содержания

Типовая удаленная атака..

Вопросы для самоподготовки

1. Понятие типовой удаленной атаки
2. Классификация удаленных атак.
3. Типовые удаленные атаки и механизмы их реализации.
4. Анализ сетевого трафика.
5. Подмена доверенного объекта или субъекта системы
6. Внедрение ложного объекта в систему
7. Внедрение ложного объекта путем навязывания ложного маршрута
8. Внедрение ложного объекта путем использования недостатков алгоритмов удаленного поиска
9. Использование ложного объекта для организации удаленной атаки на систему
10. Селекция потока информации и сохранение его на ложном объекте системы
11. Модификация информации.
12. Подмена информации.
13. Отказ в обслуживании

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторный практикум.

Цель:

Изучить типовые удаленные атаки.

Контрольные вопросы

1. Анализ типовых уязвимостей позволяющих реализовать успешные удаленные атаки.
2. Отсутствие выделенного канала связи между объектами системы
3. Недостаточная, очно-заочная идентификация и аутентификация объектов и субъектов системы
4. Взаимодействие объектов без установления виртуального канала
5. Использование нестойких алгоритмов идентификации объектов при создании виртуального канала
6. Отсутствие контроля за виртуальными каналами связи между объектами системы
7. Отсутствие возможности контроля за маршрутом сообщений
8. Отсутствие в системе полной информации о ее объектах
9. Отсутствие криптозащиты сообщений.

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

РАЗДЕЛ 4. ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ.

Цель: Рассмотреть понятия безопасного взаимодействия в глобальных компьютерных сетях.

Перечень изучаемых элементов содержания

Аутентификация. Сертификат. Угрозы.

Вопросы для самоподготовки

1. Аутентификация и управление сертификатами
2. Цифровые подписи .
3. Управление ключами и сертификация ключей .
4. Концепция доверия в информационной системе.
5. Иерархическая модель доверия .
6. Сетевая модель доверия .
7. Аутентификация с использованием протоколов открытого ключа.
8. Протокол конфиденциального обмена данными SSL.
9. Обеспечение безопасности беспроводных сетей .
10. Угрозы безопасности беспроводных соединений.
11. Обнаружение беспроводных сетей.
12. Прослушивание .
13. Активные атаки .
14. Протокол WEP .
15. Протокол 802.1X - контроль доступа в сеть по портам.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: лабораторный практикум.

Цель:

Изучить понятия безопасного взаимодействия в глобальных компьютерных сетях.

Контрольные вопросы

1. Обеспечение безопасности электронной почты.
2. Риски, связанные с использованием электронной почты.
3. Средства обеспечения безопасности электронной почты .
4. Политика использования электронной почты.
5. Системы контроля содержимого электронной почты .
6. Требования к системам контроля содержимого электронной почты .
7. Принципы функционирования систем контроля содержимого электронной почты
8. Категоризация писем и фильтрация спама .
9. Реализация политики использования .
10. Долговременное хранение и архивирование .
11. Контекстный контроль содержимого .

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: 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 кафедрой.

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

4.1. Форма промежуточной аттестации по дисциплине (модулю)

Контрольным мероприятием промежуточной аттестации обучающихся по дисциплине (модулю) является **зачет и дифференцированный зачет,** 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-1	Способен выполнять работы	**Знать:** методы установки,	Этап формирования знаний

	по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	настройки и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
		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 – 6	Способен 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	Этап формирования навыков и получения опыта

		навыками по проведению мероприятий по контролю средств защиты информации на основе критериев и методологии, изложенных в нормативно- методических документах, федерального, ведомственного и производственного уровней.	
ПК-10	Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**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	Этап формирования знаний
		Уметь: - оценивать экономическую эффективность и целесообразность реализации защитных мероприятий - внедрять системы управления информационной безопасностью и/или готовится к сертификации по современным международным стандартам	Этап формирования умений
		Владеть: - методикой оценки и управления рисками в организации - методикой контроля рисков информационной безопасности во всех сферах деятельности	Этап формирования навыков и получения опыта
ПК – 11	Способен проводить эксперименты по заданной методике,	**Знать:** основных субъектов информационного пространства, специализирующихся как на вопросах обеспечения	Этап формирования знаний

	обработку, оценку погрешности и достоверности их результатов	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.	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 – 12	Способен 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-13	Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять	**Знать:** политики, стратегии и технологии информационной безопасности и защиты информации, способы организации и оптимизации и управления системы комплексного обеспечения информационной безопасности.	Этап формирования знаний
		Уметь:	Этап формирования

	процессом их реализации	- реализовывать на практике принципы криптографической, технической и физической защиты информации и информационных систем, заложенных в соответствующие разделы политики безопасности предприятия, как концептуального (стратегического), так и локального (тактического) уровня.	умений
		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 и информационных систем.	Этап формирования навыков и получения опыта
ПК-14	Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать:** политики, стратегии и технологии информационной безопасности и защиты информации, способы организации и оптимизации и управления системы комплексного обеспечения информационной безопасности.	Этап формирования знаний
		- основные критерии защищенности информации и информационных систем от внешних и внутренних угроз;	Этап формирования умений
		- методологию проведения инструментальных исследований, применения соответствующее	Этап формирования навыков и получения опыта

		оборудование для проведения объективных экспериментальных исследований системы защиты информации и информационных систем, в том числе от угроз, связанных с применением методов социального инжиниринга.	

5.3. 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-1, ПК-6, ПК-10, ПК-11, ПК-12, ПК-13, 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.

ПК-1, ПК-6, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14	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-1, ПК-6, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14	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:

Модуль «Компьютерные сети»

1. Принципы коммутации пакетов
2. История создания компьютерных сетей
3. Модель взаимосвязи открытых систем
4. Стандартизация в сетях Интернет
5. Сети на базе протокола X.25
6. Сети на базе протокола Frame Relay

7. Сети АТМ (Структура ячейки АТМ. Эталонная модель протоколов АТМ. Классы обслуживания на уровне AAL. Классы обслуживания в сети АТМ и показатели качества обслуживания).
8. Сети Интернет
9. Эталонная модель протоколов сети Интернет
10. Протоколы стека TCP/IP
11. Принципы организации сети Интернет
12. Структура заголовков IPv4 и IPv6
13. Структура заголовков TCP и UDP
14. Создание архитектуры SIP
15. Протокол SDP
16. Управление медиашлюзами
17. Протокол H.323
18. Сигнализация ОКС7 поверх IP (Протокол управления потоками SCTP. Протоколы адаптации M2UA, M2PA и M3UA. Протоколы SUA и IUA).
19. Нумерация и адресация
20. Принципы назначения адресов в сетях IP
21. Протоколы поддержки системы адресации
22. Принципы маршрутизации датаграмм в сетях IP
23. Протоколы маршрутизации
24. Концепция ENUM
25. Услуги IP-коммуникаций
26. Технология VoIP
27. Основные функции, реализуемые в сети VoIP
28. Архитектура сети VoIP
29. Сервер обработки вызовов
30. Шлюз
31. Особенности использования сети IP для передачи речи
32. Протокол RTP
33. Определение и основные свойства IPTV
34. Архитектура IPTV
35. Протокол пересылки файлов FTP
36. Протокол пересылки гипертекстовых сообщений HTTP и Всемирная Паутина
37. Протокол электронной почты SMTP

Модуль "Технологии компьютерной безопасности ".

1. Термины и определения. ИС как система контролируемого доступа к ресурсам. Концепция совместного использования ресурсов.
2. Идентификация. Аутентификация. Авторизация. Модели информационной безопасности. Триада «Конфиденциальность, доступность, целостность».
3. Гексада Паркера и модель STRIDE. Уязвимость, угроза, атака, ущерб.
4. Типы и примеры атак. Пассивные и активные атаки. Отказ в обслуживании.
5. Внедрение вредоносных программ. Кража личности, фишинг. Сетевая разведка.
6. Управление рисками. Анализ уязвимостей и угроз.
7. Ущерб как мера риска.
8. Управление рисками.
9. Стандартные методики оценки рисков. Рекомендации NIST.
10. Методика оценки рисков RiskWatch. Методика CRAMM.
11. Методика OCTAVE. Определение профилей угрозы для ключевых активов.
12. Идентификация уязвимостей инфраструктуры. Разработка стратегии безопасности и планов снижения рисков.

13. Технология защищенного канала. Способы образования защищенного канала. Иерархия технологий защищенного канала.
14. Туннелирование. Протокол IPSec. Распределение функций между протоколами IPSec. Безопасная ассоциация.
15. Транспортный и туннельный режимы. Протокол AH.
16. Протокол ESP. Базы данных SAD И SPD.
17. Аудит. Подотчетность. Задачи аудита.
18. Файерволы. Сегментация сети. Фильтрация трафика.
19. Определение файервола.
20. Типы файерволов.
21. Системы обнаружения вторжений. Типы систем обнаружения вторжений. Функциональная схема IDS. Правила обнаружения атак.
22. Протоколы и их уязвимости.
23. Атаки на траспортную инфраструктуру. TCP-атаки. Затопление SYN-пакетами. Подделка TCP-сегмента.
24. Повторение TCP-сегментов. Сброс TCP-соединения. ICMP-атаки. Перенаправление трафика. ICMP Smurf-атака. Ping смерти и ping-затопление.
25. UDP-атаки. UDP-затопление. ICMP/UDP-затопление. UDP/echo/chargen-зэтопление. IP-атаки. Атака IP-опции. Атака IP-фрагментация.
26. Организация DNS.
27. Атаки на DNS. Методы защиты службы DNS.
28. Сетевая разведка.
29. Фильтрация трафика и файерволы. Типы фильтрации трафика. Файерволы на основе маршрутизаторов.
30. Файерволы с функцией NAT.
31. Мониторинг сети. Сетевые снифферы.
32. Система мониторинга NetFlow.
33. Типовые архитектуры сетей, защищаемых файерволами. Демилитаризованная зона. Обобщенная архитектура сети с защитой периметра и разделением внутренних зон.
34. Принципы работы протокола маршрутизации BGP. Уязвимости и инциденты BGP.
35. Защита BGP сессии между соседними маршрутизаторами. Защита маршрутизации BGP на основе данных региональных информационных центров Интернет. Сертификаты ресурсов и их использование для защиты BGI. Защита полного маршрута BGP с помощью сертификатов RPKI.

Модуль " Защита транспортной инфраструктуры сети "

1. Определение виртуальной частной сети
2. Свойства частной сети, имитируемые VPN
3. Типы VPN
4. MPLS VPN
5. VPN на основе шифрования

1. Какие свойства частной сети имитирует виртуальная частная сеть?
2. Может ли некоторая VPN быть одновременно классифицирована как VPN на основе виртуальных каналов, VPN, поддерживаемая провайдером, и VPN с топологией «звезда»?
3. Может ли MPLS VPN быть классифицирована как VPN, поддерживаемая клиентом?
4. Каким способом MPLS VPN обеспечивают безопасность передачи данных?
5. Технология MPLS VPN поддерживает следующие топологии соединений пользователей:
6. Технология L3 MPLS VPN называется технологией третьего уровня, потому что:
7. С какой целью VPN на основе шифрования используют туннелирование?
8. Что из перечисленного ниже не характеризует VPN на основе каналов SSL:

6. Уязвимости локальных беспроводных сетей

7. Две схемы организации беспроводной сети
8. Методы защиты локальных беспроводных сетей
9. Протокол WEP
10. Стандарт WPA2
11. Беспроводные системы обнаружения вторжений
12. Что такое «облачные сервисы»
13. Определение облачных вычислений
14. Свойства облачных вычислений
15. Технологии облачных вычислений
16. Модели сервисов облачных вычислений
17. Преимущества облачных сервисов
18. Проблемы безопасности облачных сервисов
19. Значимость облачных сервисов
20. Организация почтового сервиса
21. Электронные сообщения
22. Протокол SMTP
23. Непосредственное взаимодействие клиента и сервера
24. Схема с выделенным почтовым сервером
25. Схема с двумя почтовыми серверами посредниками
26. Протоколы POP3 и IMAP
27. Угрозы и механизмы защиты почты
28. Угрозы почтовому сервису
29. Аутентификация отправителя
30. Шифрование содержимого письма
31. Защита метаданных пользователя
32. Атаки на компьютер с помощью почты
33. Спам
34. Атаки почтовых приложений

Модуль "Контроль безопасности в компьютерных сетях "

18. Уязвимости традиционных средств защиты
19. Уязвимости стека протоколов TCP/IP
20. Слабости МЭ, и способы его обхода
21. Уязвимости системы аутентификации и авторизации
22. Анатомия атаки, этапы осуществления атаки
23. Классификация уязвимостей
24. Модель атаки
25. Этапы реализации атаки
26. Классификация атак
27. Задача обнаружения атак
28. Понятие системы обнаружения атак
29. Реальные возможности систем обнаружения атак и пределы их возможностей
30. Схема работы системы обнаружения атак
31. Основные принципы обнаружения атак
32. Признаки атак
33. Источники информации об атаках
34. Технологии и подходы к обнаружению атак
35. Необходимость технологии обнаружения атак.
36. Терминология.
37. Источники данных для систем обнаружения атак.
38. Признаки атак.

39. Методы обнаружения атак.
40. Механизмы реагирования.
41. Специализированные системы обнаружения атак
42. Взаимодействие с другими средствами защиты.
43. Анализ результатов работы систем обнаружения атак.
44. Понятие типовой удаленной атаки
45. Классификация удаленных атак.
46. Типовые удаленные атаки и механизмы их реализации.
47. Анализ сетевого трафика.
48. Подмена доверенного объекта или субъекта системы
49. Внедрение ложного объекта в систему
50. Внедрение ложного объекта путем навязывания ложного маршрута
51. Внедрение ложного объекта путем использования недостатков алгоритмов удаленного поиска
52. Использование ложного объекта для организации удаленной атаки на систему
53. Селекция потока информации и сохранение его на ложном объекте системы
54. Модификация информации.
55. Подмена информации.
56. Отказ в обслуживании
57. Аутентификация и управление сертификатами
58. Цифровые подписи .
59. Управление ключами и сертификация ключей .
60. Концепция доверия в информационной системе.
61. Иерархическая модель доверия .
62. Сетевая модель доверия .
63. Аутентификация с использованием протоколов открытого ключа.
64. Протокол конфиденциального обмена данными SSL.
65. Обеспечение безопасности беспроводных сетей .
66. Угрозы безопасности беспроводных соединений.
67. Обнаружение беспроводных сетей.
68. Прослушивание .
69. Активные атаки .
70. Протокол WEP .
71. Протокол 802.1X - контроль доступа в сеть по портам.

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.

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. 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. *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. *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	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским	https://grebennikon.ru

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	«Grebennikon»	домом "Гребенников".	

5.3. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся дисциплины (модуля) «Разработка Корпоративной информационной системы» 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, очно-заочной 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

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 дисциплине (модулю)

Для изучения дисциплины (модуля) **«Контроль безопасности в компьютерных сетях»** 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 **компьютерной 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

Указываются образовательные технологии, которые рекомендуется использовать при реализации различных видов учебной работы.

Освоение дисциплины (модуля) **«Контроль безопасности в компьютерных сетях»** 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) **«Контроль безопасности в компьютерных сетях»** 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)
КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технологии защиты информации
Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022

Рабочая программа дисциплины (модуля) **«Комплексная защита объектов информатизации»** 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:
к.т.н. Сиротский А.А., ст. 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  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  Н.П. Третьяков
информатики РГСУ

(подпись)

Согласовано  И.Г. Маляр
Научная библиотека, директор

(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) состоит в приобретении студентами знаний теоретических основ по применению специализированных технических средств и общепромышленных измерительных приборов для проведения инструментальной и экспертной оценки наличия технических каналов утечки конфиденциальной информации и степени их влияния на уязвимость объекта информатизации.

Задачи дисциплины (модуля):

- овладение практическими навыками разработки систем защиты и обеспечения безопасности;
- развитие знаний об основных технических средствах анализа информационной защищенности.
- усвоение основных понятий о технических каналах утечки информации и физических принципах их возникновения;
- формирование знаний о стадиях и этапах создания системы защиты от утечки по техническим каналам, типовых средствах защиты.

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

Учебная дисциплина «Комплексная защита объектов информатизации» реализуется в вариативной части основной профессиональной образовательной программы «Информационная безопасность» по направлению «10.03.01 Информационная безопасность» очной формы обучения.

Изучение дисциплины (модуля) «Комплексная защита объектов информатизации» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Криптографическая защита информации», «Программно-аппаратная защита информации», «Техническая защита информации».

Изучение дисциплины (модуля) «Комплексная защита объектов информатизации» является базовым для последующего освоения программного материала учебных дисциплин: «Контроль безопасности в компьютерных сетях», «Управление информационной безопасностью».

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-4 и ПК-14 в соответствии с основной профессиональной образовательной программой **«Информационная безопасность»** по направлению специальности **«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-4	Способен участвовать в работах по реализации	ПК-4.ИД-1. Сформирован понятийный аппарат и теоретическая	Знать: - эксплуатационные и технико-экономические

		политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	основа для выполнения практических действий в рамках компетенции ПК-4.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-4.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	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: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты 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 выполняет	Знать: - сущность и содержание работы исполнителей - виды управленческих решений в области организации работ по проекту и нормированию труда - особенности

			практические действия в рамках компетенции ПК-14.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	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
				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 работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля) составляет __12__ зачетных единиц.

Вид учебной работы	Всего	Семестры

	часов	7	8			
Контактная работа обучающихся с педагогическими работниками	**216**	**108**	**108**			
Учебные занятия лекционного типа	48	24	24			
из них: в форме практической подготовки						
Практические занятия	56	28	28			
из них: в форме практической подготовки						
Лабораторные занятия	16	8	8			
из них: в форме практической подготовки						
Иная контактная работа	96	48	48			
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**171**	**99**	**72**			
из них: в форме практической подготовки	*26*	*12*	*14*			
Контроль промежуточной аттестации	**45**	**9**	**36**			
Форма промежуточной аттестации		зачет	экзам			
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**432**	**216**	**216**			

2.2. Учебно-тематический план по очной форме обучения

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 7)													
Раздел 1.1	33	15	*3*	28		6		8		2		12	
Раздел 1.2	34	16	*3*	28		6		6		2		12	
Раздел 1.3	34	16	*3*	26		6		8		2		12	
Раздел 1.4	34	16	*3*	26		6		6		2		12	

Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**216**	**99**	***12***	**108**		**24**		**28**		**8**		**48**	
Форма промежуточной аттестации	**зачет**												
Модуль 2 (семестр 8)													
Раздел 2.1	28	12	*3*	16		4		4				8	
Раздел 2.2	28	12	*3*	16		4		4				8	
Раздел 2.3	30	12	*2*	18		4		4		2		8	
Раздел 2.4	30	12	*2*	18		4		4		2		8	
Раздел 2.5	32	12	*2*	20		4		6		2		8	
Раздел 2.6	32	12	*2*	20		4		6		2		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**216**	**72**	***14***	**108**		**24**		**28**		**8**		**48**	
Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**432**	**171**	***26***	**216**		**48**		**56**		**16**		**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 7)							

Раздел 1.1	15	12	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	12	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.2	16	12	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	12	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.3	16	12	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	12	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 1.4	16	9	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	10	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**99**	**45**		**46**		**8**	
Модуль 2 (семестр 8)							
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	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 2.3	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 2.4	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 2.5	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 2.6	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	**171**	**75**		**76**		**20**	

3.2. Методические указания к самостоятельной работе по дисциплине.

РАЗДЕЛ 1. ОСНОВНЫЕ СВОЙСТВА ИНФОРМАЦИИ КАК ПРЕДМЕТА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ

Цель: Ввести понятия информации, данных, знаний, защиты информации.

Перечень изучаемых элементов содержания

Изучение основных характеристик приборов виброакустической защиты применяемых для виброакустического зашумления строительных конструкций помещения при защите речевой информации от утечки по вибрационному и акустическому каналам.

Вопросы для самоподготовки:

1. Определение данных и информации.
2. Понятие защиты информации.
3. Основные свойства информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №1 К РАЗДЕЛУ 1

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «Исследование приборов виброакустической защиты».

Контрольные вопросы:

1. При установке электромагнитных излучателей на стену рекомендуется устанавливать их на расстоянии не менее … от пола, потолка, угла стены. Почему?
2. Излучатели какого типа нельзя использовать в режиме 2 прибора SI-3001?
3. Какие типы излучателей должны быть использованы для защиты от утечки информации по вибрационному каналу через стены и перекрытия?
4. Какие типы излучателей должны быть использованы для защиты от утечки информации по вибрационному каналу через стекла, зеркала и другие тонкие отражающие поверхности?

5. Какие типы излучателей должны быть использованы для защиты от утечки информации по вибрационному каналу через инженерные коммуникации, трубы и батареи отопления, водопроводные трубы, деревянные или металлические двери?
6. Какие типы излучателей должны быть использованы для защиты от утечки информации по акустическому каналу через воздуховоды, открытые окна, двери?
7. Для чего в приборе SI-3001 установлено гнездо «микрофон»?
8. Для чего в приборе SI-3001 установлено гнездо «диктофон»?
9. Для чего в каждом канале, на лицевой панели прибора SI-3030 используется по 2-а светодиода?
10. Для чего в каждом канале прибора SI-3030 используется регуляторы «АЧХ»?
11. Как зафиксировать один из режимов работы в приборе SI-3100?
12. Как пользоваться прибором SI-8001?
13. Как подключить прибор "ГРОМ-ЗИ-4"?
14. Что представляет собой система «Шторм-2»?
15. Состав и функции системы «Шторм-5»?

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

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №2 К РАЗДЕЛУ 1

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Пассивные методы защиты
2. Активные методы защиты
3. Виды экранирования технических средств
4. Фильтрация опасных сигналов

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – реферат.

РАЗДЕЛ 2. ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ ОБЪЕКТОВ ЗАЩИТЫ

Цель: изучение понятия демаскирующих признаков объектов защиты информации.

Перечень изучаемых элементов содержания

Изучение основных характеристик видеокамер применяемых в системах видеоохраны и видеонаблюдения.

Вопросы для самоподготовки:

1. Определение демаскирующих признаков.
2. Защита от обнаружения и снятия перехватов.
3. Системы видеоохраны и видеонаблюдения.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №1 К РАЗДЕЛУ 2

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «Видеокамеры».

Контрольные вопросы:

1. Для чего используются высокоскоростные купольные видеокамеры серии ET8010 и ET8020?
2. Как по маркировке купольной видеокамеры серии ET8010 определить место ее установки?
3. Интерфейс и протоколы управления высокоскоростными купольными видеокамерами серии ET8010 и ET8020.
4. Как крепятся высокоскоростные купольные видеокамеры серии ET8010 и ET8020 на стену?
5. Как можно задать адрес и скорость передачи управляющего сигнала
6. купольной видеокамеры серии ET8010 и ET8020?
7. Для чего на пульте управления ET8260 используется жидкокристаллический дисплей?
8. Какое разрешение в ТВЛ имеют видеокамеры серии ET8010 и ET8020?
9. Как по маркировке среднескоростной купольной видеокамеры серии JQ1707 определить место ее установки?
10. Интерфейс и протоколы управления среднескоростными купольными видеокамерами серии JQ1707.
11. Как крепятся среднескоростные купольные видеокамеры серии JQ1707?

РУБЕЖНЫЙ КОНТРОЛЬ К ЗАДАНИЮ №1 К РАЗДЕЛУ 2: форма рубежного контроля – отчет по лабораторной работе.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №2 К РАЗДЕЛУ 2

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Виды демаскирующих признаков по характеристикам объекта
2. Косвенные демаскирующие признаки
3. Прямые демаскирующие признаки
4. Именные демаскирующие признаки

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – реферат.

РАЗДЕЛ 3. ИСТОЧНИКИ ОПАСНЫХ СИГНАЛОВ

Цель: изучение видов источников опасных сигналов.

Перечень изучаемых элементов содержания

Теоретическое изучение способов измерения параметров электрических сигналов. Измерения параметров сигнала с использованием осциллографа.

Вопросы для самоподготовки:

1. Виды опасных сигналов.
2. Источники опасных сигналов.
3. Основные характеристики опасных сигналов.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №1 К РАЗДЕЛУ 3

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. Исследование параметров опасных сигналов

Контрольные вопросы:

1. В чем состоят особенности временного и спектрального способов представления сигналов?
2. Каково назначение электронно-лучевых осциллографов и в чем состоят их достоинства?
3. Назовите основные характеристики осциллографа, определяющие его выбор для проведения измерений?
4. Опишите принцип действия осциллографа с электростатическим управлением луча.
5. Какие виды разверток используются в электронно-лучевых осциллографах и чем определяется вид развертки?
6. Назовите условие, необходимое для получения неподвижной кривой напряжения исследуемого сигнала.
7. От чего зависит величина искажения формы кривой исследуемого сигнала?
8. В каких случаях применяется ждущая развертка и как она формируется?
9. Чем определяется выбор вида синхронизации при исследовании процессов с помощью осциллографа7
10. Как влияет напряжение входного сигнала на искажение его формы при отображении на экране осциллографа?
11. Каковы особенности наблюдения импульсных процессов?

РУБЕЖНЫЙ КОНТРОЛЬ К ЗАДАНИЮ №1 РАЗДЕЛУ 3: форма рубежного контроля – отчет по лабораторной работе.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №2 К РАЗДЕЛУ 3

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Виды сигналов
2. Каналы утечки информации
3. Средства, требующие физического проникновения в защищаемые помещения
4. Средства, не требующие физического проникновения в защищаемые помещения

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – реферат.

РАЗДЕЛ 4. СТРУКТУРЫ, ДОБЫВАЮЩИЕ ИНФОРМАЦИЮ

Цель: изучение понятия съема информации и ее защиты.

Перечень изучаемых элементов содержания

Изучение основных характеристик оптико-электронных, вибрационных, емкостных, проводных средств обнаружения несанкционированных проникновений на охраняемые объекты.

Вопросы для самоподготовки:

1. Понятие съема информации.
2. Необходимость защиты информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №1 К РАЗДЕЛУ 4

Форма практического задания: лабораторный практикум.

Лабораторная работа 4. «Извещатели».

Контрольные вопросы:

1. Для чего предназначено устройство охранной сигнализации периметра «GM»?
2. Для охраны каких объектов может быть использовано устройство охранной сигнализации периметра «GM»?
3. Что входит в комплект устройства охранной сигнализации периметра «GM»?
4. Как должны быть установлены элементы устройства охранной сигнализации периметра «GM» для правильной его работы?
5. Для чего предназначено устройство контроллера мультисенсора 1MS018?
6. Интерфейс управления контроллера мультисенсора 1MS018.
7. Сколько шлейфов имеет контроллера мультисенсора 1MS018?
8. Какова максимальная длина сенсорного кабеля, который может быть подключен к контроллеру мультисенсора 1MS018?
9. Что включает устройство ИК активного датчика SASO-PB10P?
10. Пояснить принцип работы ИК активного датчика SASO-PB10P.

РУБЕЖНЫЙ КОНТРОЛЬ К ЗАДАНИЮ №1 РАЗДЕЛУ 4: форма рубежного контроля – отчет по лабораторной работе.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №2 К РАЗДЕЛУ 4

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Потребители информации
2. Система разведки
3. Органы разведки
4. Виды тайн и их классификация

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4: форма рубежного контроля – реферат.

РАЗДЕЛ 5. ОСНОВНЫЕ СПОСОБЫ И ПРИНЦИПЫ РАБОТЫ СРЕДСТВ НАБЛЮДЕНИЯ ОБЪЕКТОВ ПОДСЛУШИВАНИЯ И ПЕРЕХВАТА СИГНАЛОВ

Цель: изучение работы средств подслушивания и перехвата сигналов.

Перечень изучаемых элементов содержания

Теоретическое изучение вопросов, связанных с использованием в радиоизмерениях измерительных генераторов. Исследование возможностей применения генератора высокочастотных сигналов Г4-76А в радиотехнических измерениях.

Вопросы для самоподготовки:

1. Принципы работы средств наблюдения объектов.
2. Принципы работы средств перехвата сигналов.
3. Задачи, решаемые с помощью перехвата сигналов.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №1 К РАЗДЕЛУ 5

Форма практического задания: лабораторный практикум.

Лабораторная работа 5. «Использование измерительных генераторов для измерения опасных сигналов».

Контрольные вопросы:

1. Определите назначение измерительных генераторов при исследовании процессов.
2. С помощью каких характеристик оцениваются измерительные генераторы?
3. Как подразделяются измерительные генераторы по диапазону частот генерируемых колебаний?
4. Почему необходимо согласовывать выходное сопротивление генератора со входным сопротивлением объекта измерения?
5. Назовите особенности применения измерительных генераторов, работающих в ВЧ СВЧ диапазонах.
6. При каких исследованиях в области технической защиты информации может быть использован генератор Г4-76А?
7. Какие виды работ обеспечивает генератор Г4-76А?
8. В каком частотном диапазоне работает генератор Г4-76А? Какова погрешность установки его частоты по шкале прибора и в каких случаях она увеличивается?
9. Назовите основные параметры выходной мощности в режиме НГ и амплитудной модуляции генератора Г4-76А.
10. Какие виды модуляции выходного сигнала предусмотрены в генераторе Г4-76А?

РУБЕЖНЫЙ КОНТРОЛЬ К ЗАДАНИЮ №1 РАЗДЕЛУ 5: форма рубежного контроля – отчет по лабораторной работе.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №2 К РАЗДЕЛУ 5

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Технические характеристики микрофонов
2. Принципы действия микрофонов
3. Технические характеристики акселерометров

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 5: форма рубежного контроля – реферат.

РАЗДЕЛ 6. КОНЦЕПЦИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Цель: изучение концепции инженерно-технической защиты информации и нормативно-правовых актов.

Перечень изучаемых элементов содержания

Теоретическое изучение методики поиска устройств несанкционированного съема информации путем визуального осмотра исследуемого объекта. Визуальное исследование конкретного объекта на предмет наличия предметов несанкционированного съема информации.

Вопросы для самоподготовки:

1. Основные параметры концепции ИТЗИ.
2. Категорирование объектов защиты.
3. Структура системы инженерно-технической защиты информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К ЗАДАНИЮ №1 К РАЗДЕЛУ 6

Форма практического задания: лабораторный практикум.

Лабораторная работа 6. «Поиск устройств несанкционированного съема информации».

Контрольные вопросы:

1. Чем объясняется актуальность и важность проблемы выявления средств негласного съема информации?
2. Объясните необходимость поэтапного проведения работ по выявлению средств НСИ?
3. В чем состоят особенности каждого этапа проведения обследования объекта?
4. С использованием каких технических средств рекомендуется проводить визуальное обследование объекта?
5. Какая техническая документация на объект понадобится для проведения качественного визуального осмотра?
6. Цель проведения внешнего визуального осмотра? На какие объекты необходимо обращать главное внимание?
7. По каким внешним признакам можно определить примерное назначение обнаруженных в зоне, примыкающей к объекту, радиоантенн?
8. Назовите характерные визуальные признаки установки средств НСИ в строительных конструкциях, мебели и предметах интерьера.
9. Назовите перечень предметов, коммуникаций и технических устройств, подлежащих проверке внутри помещения.
10. Назовите внешние признаки возможной установки средств НСИ в электронные приборы.
11. Какие операции и данные фиксируются в ходе проведения визуального обследования?

РУБЕЖНЫЙ КОНТРОЛЬ К ЗАДАНИЮ №1 К РАЗДЕЛУ 6: форма рубежного контроля – отчет по лабораторной работе.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ №2 К РАЗДЕЛУ 6

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Принципы инженерно-технической защиты информации.
2. Принципы построения системы инженерно-технической защиты информации.
3. Роль и место технических средств в организации режима охраны, современная концепция защиты объектов.
4. Основные элементы системы защиты информации

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 дисциплине (модулю) является **зачет / экзамен,** 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-4	Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	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: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	Этап формирования знаний Этап формирования умений Этап формирования навыков и получения опыта
ПК-14	Способен организовывать работу малого коллектива	Знать: - сущность и содержание работы исполнителей - виды управленческих	Этап формирования знаний

	исполнителей в профессиональной деятельности	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 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 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-4 ПК-14	Этап формирования знаний.	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и	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

		излагать материал	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-4 ПК-14	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-4 ПК-14	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. Основные свойства информации как предмета инженерно-технической защиты
2. Понятие о защищаемой информации.
3. Виды информации, защищаемой техническими средствами.
4. Свойства информации, влияющие на возможности ее защиты.
5. Демаскирующие признаки объектов защиты.
6. Классификация демаскирующих признаков объектов защиты.
7. Видовые демаскирующие признаки.
8. Источники опасных сигналов
9. Побочные электромагнитные излучения и наводки.
10. Побочные преобразования акустических сигналов в электрические сигналы.
11. Виды угроз безопасности информации, защищаемой техническими средствами.
12. Органы добывания информации.
13. Принципы добывания и обработки информации техническими средствами. Классификация технической разведки.
14. Основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов.
15. Способы и средства наблюдения.
16. Средства наблюдения в оптическом диапазоне. Оптические системы. Визуально-оптические приборы.
17. Способы и средства перехвата сигналов.
18. Средства перехвата радиосигналов. Антенны.
19. Способы и средства подслушивания акустических сигналов.
20. Акустические приемники.
21. Концепция инженерно-технической защиты информации
22. Принципы инженерно-технической защиты информации.
23. Принципы построения системы инженерно-технической защиты информации.
24. Способы и средства инженерной защиты и технической охраны.
25. Концепция охраны объектов. Категорирование объектов защиты. Характеристика методов физической защиты информации.
26. Структура системы инженерно-технической защиты информации.
27. Способы и средства обнаружения злоумышленников и пожара.
28. Извещатели.
29. Средства контроля и управления средствами охраны.
30. Способы и средства видеоконтроля.

31. Средства телевизионной охраны. Средства освещения.
32. Способы и средства нейтрализации угроз.
33. Средства управления системой охраны.
34. Классификация средств инженерно-технической защиты информации.
35. Способы и средства защиты информации от наблюдения.
36. Способы и средства противодействия наблюдению в оптическом диапазоне волн.
37. Способы и средства противодействия радиолокационному и гидроакустическому наблюдению.
38. Способы и средства защиты информации от подслушивания.
39. Способы и средства информационного скрытия акустических сигналов и речевой информации.
40. Структурное скрытие речевой информации в каналах связи.
41. Способы и средства предотвращения утечки информации с помощью закладных устройств.
42. Демаскирующие признаки закладных устройств.
43. Методы обнаружения закладных подслушивающих устройств.
44. Методы подавления подслушивающих закладных устройств.
45. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки
46. Экранирование электромагнитных полей.
47. Экранирование электрических проводов. Компенсация полей.
48. Способы предотвращения утечки информации по материально-вещественному каналу
49. Методы защиты информации в отходах производства.
50. Методы защиты демаскирующих веществ в отходах химического производства.
51. Контроль эффективности инженерно-технической защиты информации. Организация инженерно-технической защиты информации на предприятиях
52. Системный подход к инженерно-технической защите информации.
53. Основные положения системного подхода к инженерно-технической защите информации.
54. Принципы моделирования объектов защиты и технических каналов утечки информации.

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.В*нуков, 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. Защита персональных данных в информационных системах / авт.-сост. В.И. Петренко, И.В. Мандрица ; Министерство образования и науки Российской Федерации, Северо-Кавказский федеральный университет. – Ставрополь : СКФУ, 2018. – 118 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=494823. – Текст : электронный.
2. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=429070. – Библиогр. в кн. – Текст : электронный
3. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» —Режим доступа: http://gostexpert.ru/gost/gost-51275-2006 (ГОСЭКСПЕРТ ЕДИНАЯ БАЗА ГОСТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ)

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/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
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) «Комплексная защита объектов информатизации» 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. Дополнительные электронно-библиотечные системы и полнотекстовые базы данных:

Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
Университетская информационная система РОССИЯ (УИС РОССИЯ)	Университетская информационная система РОССИЯ (УИС РОССИЯ) – электронная библиотека и база для исследований и учебных курсов в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений и других гуманитарных наук. УИС РОССИЯ поддерживается на базе Научно-исследовательского вычислительного центра МГУ имени М.В. Ломоносова	https://uisrussia.msu.ru/ 100% доступ
Научное наследие	Библиотека содержит научные труды известных российских и зарубежных	http://e-heritage.ru/index.html

России	ученых и исследователей, работавших на территории России. Программа Президиума РАН.	100% доступ
Электронная библиотека учебников	На сайте представлены учебники, лекции, доклады, монографии по естественным и гуманитарным наукам.	http://studentam.net 100% доступ
Cyberleninka	Содержит каталог научной периодики по большому количеству научных дисциплин, который содержит полную информацию о научных журналах в электронном виде, включающую их описания и все вышедшие выпуски с содержанием, темами научных статей и их полными текстами.	http://cyberleninka.ru/journal 100% доступ
Единое окно доступа к образовательным ресурсам	Информационная система предоставляет свободный доступ к каталогу образовательных интернет-ресурсов и полнотекстовой электронной учебно-методической библиотеке для общего и профессионального образования	http://window.edu.ru/library 100% доступ
Электронные библиотеки. Электронные библиотеки, словари, энциклопедии	Интернет-ресурсы образовательного и научно-образовательного назначения, оформленные в виде электронных библиотек, словарей и энциклопедий, предоставляют открытый доступ к полнотекстовым информационным ресурсам, представленным в электронном формате — учебникам и учебным пособиям, хрестоматиям и художественным произведениям, историческим источникам и научно-популярным статьям, справочным изданиям и др.	http://gigabaza.ru/doc/131454.html 100% доступ

5.7. Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) **«Комплексная защита объектов информатизации»** 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).

5.8. Образовательные технологии

Освоение дисциплины (модуля) **«Комплексная защита объектов информатизации»** 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) **«Комплексная защита объектов информатизации»** 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) ВВЕДЕНИЕ В ПРОФЕССИЮ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технологии защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Форма обучения
Очная

Москва 2022

Рабочая программа дисциплины (модуля) «Введение в профессию» 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 кандидатом педагогических наук, доцентом Витковской Н.Г.

Руководитель основной образовательной программы к.п.н., доцент

_____ Н.Г. Витковская
(подпись)

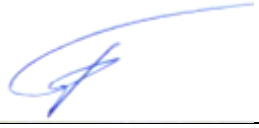
Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании Ученого совета факультета информационных технологий
Протокол № 10 от «06» июня 2022 года

Декан факультета
к.п.н., доцент

_____ С.В. Крапивка
(подпись)

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

ГБОУ ВО Академия ГПС МЧС России, д.т.н., доцент



_____ С.Ю. Бутузов
(подпись)

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

_____ А.С. Мосолов
(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): ознакомление студентов с профессиональной деятельностью в сфере разработки, исследования и эксплуатации систем обеспечения информационной безопасности.

Задачи дисциплины (модуля):

- ознакомление с основными понятиями информационной безопасности, основными принципами построения систем защиты информации, а также основными категориями мер защиты информации;
- развитие умений оценки угрозы безопасности компьютерным сетям;
- формирование готовности к разработке предложений по обеспечению информационной безопасности организации.

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

Дисциплина (модуль) «Введение в профессию» реализуется в вариативной части основной профессиональной образовательной программы по направлению подготовки 10.03.01 *Информационная безопасность очной* формы обучения**.**

Изучение дисциплины (модуля) «Введение в профессию» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда дисциплин (модулей): «Информатика и основы ИКТ» и др.

Изучение дисциплины (модуля) «Введение в профессию» является базовым для последующего освоения программного материала дисциплин (модулей): «Основы информационной безопасности», «Проектирование баз данных» и др.

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: УК-1 в соответствии с основной профессиональной образовательной программой бакалавриата 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**
Системное и критическое мышление	УК-1	Способен осуществлять поиск, критический анализ исинтез информации, применять системный подход для решения поставленных задач	УК-1.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции УК-1.ИД-2. Планирует и выполняет практические действия в рамках компетенции УК-1.ИД-3. Применяет методы анализа прак-	*Знать:* принципы сбора, отбора и обобщения информации
				Уметь: соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.

			тической деятельности и ее результатов в рамках компетенции	
				Владеть: практическим опытом работы с информационными источниками, опыт научного поиска, создания научных текстов

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 2 зачетные единицы.

Вид учебной работы	**Всего часов**	**Семестры**				
		1				
Контактная работа обучающихся с педагогическими работниками	**36**	**36**				
Учебные занятия лекционного типа	10	10				
из них: в форме практической подготовки						
Практические занятия	10	10				
из них: в форме практической подготовки						
Лабораторные занятия						
из них: в форме практической подготовки						
Иная контактная работа	16	16				
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**27**	**27**				
из них: в форме практической подготовки						
Контроль промежуточной аттестации	**9**	**9**				
Форма промежуточной аттестации		зачет				
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**72**	**72**				

2.2. Учебно-тематический план дисциплины (модуля)

Раздел, тема	**Виды учебной работы, академических часов**			
	Всего	**тельная**	*тиче-*	**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	31	13		18		6		4				8	
Раздел 1.2	32	14		18		4		6				8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**72**	**27**		**36**		**10**		**10**				**16**	
Форма промежуточной аттестации	**зачет**												
Общий объем, часов	**72**	**27**		**36**		**10**		**10**				**16**	

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	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	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**	
Общий объем по дисциплине (модулю), часов	**27**	**11**		**12**		**4**	

3.2. Методические указания к самостоятельной работе по дисциплине

РАЗДЕЛ 1. «*Комплексный подход к обеспечению информационной безопасности*»

Цель: заключается в получении обучающимися теоретических знаний о комплексном подходе к обеспечению информационной безопасности

Перечень изучаемых элементов содержания

Тема 1.1. **Понятие и составляющие информационной безопасности**

Основные понятия информационной безопасности. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический.

Тема 1.2. **Угрозы информационной безопасности в компьютерных системах**

Компьютерная система как объект защиты информации. Понятие угрозы информационной безопасности в компьютерных системах. Классификация и общий анализ угроз информационной безопасности в компьютерных системах. Случайные и преднамеренные угрозы информационной безопасности

Тема 1.3. **Законодательный уровень информационной безопасности**

Законодательная и нормативно-правовая база РФ в области информатизации и защиты информации. Ответственность за нарушение законодательства в информационной сфере.

Тема 1.4. **Административный уровень информационной безопасности**

Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем.

.

Вопросы для самоподготовки:

1. Понятие и составляющие информационной безопасности;
2. Виды угроз информации и методы защиты от них;
3. Законы, стандарты и спецификации информационной безопасности;
4. Меры процедурного уровня информационной безопасности;
5. Меры программно-технического уровня информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

1. Проанализировать профессионально значимые источники информации с точки зрения основных аспектов: конфиденциальности, целостности и доступности.
2. Для выбранного объекта защиты информации (например, почтовый сервер, одиночно стоящий компьютер в бухгалтерии, телефонная база ограниченного пользования на электронных носителях и др.) провести анализ защищенности объекта по следующим пунктам: вид угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз, причины нарушения целостности информации, потенциально возможные злоумышленные действия; определить класс защиты информации.
3. Составить перечень основный понятий и определений, используемых в нормативно-правовых документах.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – контрольные вопросы.

Контрольные вопросы

1. Методы аутентификации, использующие пароли.
2. Изучение политики безопасности операционной системы Windows XP.
3. Управление шаблонами безопасности в Windows XP.
4. Разграничение полномочий и доступа к объектам операционной системы Unix.
5. Построение системы разграничения доступа в базе данных на основе ролевой модели.
6. Настройка безопасности почтового клиента.
7. Настройка параметров аутентификации Windows XP.
8. Назначение прав пользователей при произвольном управлении доступом в Windows XP
9. Настройка параметров регистрации и аудита в Windows XP.

РАЗДЕЛ 2. «*Методы и средства обеспечения безопасности информации*»

Цель: заключается в получении обучающимися теоретических знаний о современных методах и средствах обеспечения информационной безопасности

Перечень изучаемых элементов содержания

Тема 2.1. **Защита информации от несанкционированного доступа**

Способы несанкционированного доступа к информации в компьютерных системах.

Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа. Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация. Управление доступом: основные понятия, виды разграничения доступа, особенности дискреционного, мандатного и ролевого управления доступом

Тема 2.2. **Криптографические методы защиты информации информационной безопасности**

Основные понятия криптологии. Классификация криптографических средств. Симметричные и Ассиметричные криптосистемы. Методы шифрования: замены, перестановки, аналитические, аддитивные, комбинированные. Электронная цифровая подпись и ее применение для контроля целостности программ и данных.

Тема 2.3. **Вирусы как угроза ИБ. Средства антивирусной защиты**

Общие сведения и классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов. Методы и средства обнаружения и защиты от компьютерных вирусов. Антивирусные программные комплексы.

Тема 2.4. **Стандарты и спецификации в области информационной безопасности**

Характеристика систем стандартизации в области защиты информации. Оценочные стандарты и технические спецификации: «Оранжевая книга». Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Европейские критерии безопасности информационных технологий. Документы Гостехкомиссии России по защите информации.

Вопросы для самоподготовки:

1. Меры программно-технического уровня информационной безопасности;
2. Методы защита информации от несанкционированного доступа;
3. Способы разграничения полномочий и доступа к объектам;
4. Осуществление регистрации и аудита в компьютерной системе;
5. Проведение оценки рисков компьютерной системы;
6. Применение средств антивирусной защиты.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

1. Рассмотреть неотъемлемые характеристики человека и особенности поведения, используемые при биометрической аутентификации пользователей.
2. Рассмотреть особенности и принципы работы стандартных и специализированных программных средств шифрования и компьютерной стеганографии.
3. Разработать контролирующий, диагностический или демонстрационный материал по теме (кроссворд, тест, ребусы, презентация и др.).

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2:
Форма рубежного контроля – контрольные вопросы

1. Использование функций криптографического интерфейса (CryptoAPI) операционной системы Windows для защиты информации.
2. Шифрующая файловая система EFS и управление сертификатами в Windows XP.
3. Методы криптографического преобразования данных
4. Антивирусные программные комплексы.
5. Восстановление зараженных файлов. Профилактика проникновения «троянских программ».

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,** 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
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	*Знать:* принципы сбора, отбора и обобщения информации	Этап формирования знаний
		Уметь: соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.	Этап формирования умений

		Владеть: практическим опытом работы с информационными источниками, опыт научного поиска, создания научных текстов	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-1	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.

УК-1	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-1	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. Понятие и составляющие информационной безопасности;
2. Виды угроз информации и методы защиты от них;
3. Законы, стандарты и спецификации информационной безопасности;
4. Меры процедурного уровня информационной безопасности;

5. Меры программно-технического уровня информационной безопасности;
6. Методы защита информации от несанкционированного доступа;
7. Способы разграничения полномочий и доступа к объектам;
8. Осуществление регистрации и аудита в компьютерной системе;
9. Проведение оценки рисков компьютерной системы;
10. Применение средств антивирусной защиты.
11. На чем строится политика безопасности организации?
12. Что делать, чтобы риски стали приемлемыми?
13. Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией о методах использования уязвимостей?
14. Что входит в число принципов физической защиты?
15. Что входит в число основных принципов архитектурной безопасности?
16. На что направлены меры информационной безопасности?
17. Что следует учитывать при анализе стоимости мер безопасности?

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Промежуточная аттестация по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам высшего образования – программ 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 для экзамена.

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.

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. *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, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

2. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

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) **«Введение в профессию»** 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	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

5.6. Материально-техническое обеспечение образовательного процесса по дисциплине (модулю)

Для изучения дисциплины (модуля) **«Введение в профессию»** в рамках реализации основной профессиональной образовательной программы по направлению 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

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

Освоение дисциплины (модуля) **«Введение в профессию»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме компьютерных симуляций, разбора конкретных ситуаций, в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При освоении дисциплины (модуля) **«Введение в профессию»** предусмотрено применение электронного обучения.

Учебные часы дисциплины «**Введение в профессию**» 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.).

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)
СТАНДАРТЫ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технологии защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Форма обучения
Очная

Москва 2022

Рабочая программа дисциплины (модуля) «Стандарты в профессиональной деятельности» 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 кандидатом педагогических наук, доцентом Витковской Н.Г.

Руководитель основной 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) рецензирована и рекомендована к утверждению:

ГБОУ ВО Академия ГПС МЧС России, д.т.н., доцент _____ С.Ю. Бутузов
(подпись)

АО ПВП «Амулет»
зам. ген. директора по науке, к.т.н., доцент _____ А.С. Мосолов
(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 современных методах разработки и стандартизации в области информационной безопасности.

Задачи дисциплины (модуля):

- ознакомление с основными понятиями информационной безопасности, основными принципами построения систем защиты информации, а также основными категориями мер защиты информации, их возможностями с точки зрения защиты информации, сильными и слабыми сторонами;
- формирование умений выбора решений из различных категорий методов и средств защиты информаций, соответствующих требованиям защиты информации в конкретных информационных системах;
- развитие умений оценки соответствия существующих решений требованиям защиты информации,
- формирование готовности к разработке предложений по совершенствованию системы обеспечения информационной безопасности организации.

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

Дисциплина (модуль) «Стандарты в профессиональной деятельности» реализуется в вариативной части основной профессиональной образовательной программы по направлению подготовки 10.03.01 *Информационная безопасность очной* формы обучения**.**

Изучение дисциплины (модуля) «Стандарты в профессиональной деятельности» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда дисциплин (модулей): «Информатика и основы ИКТ» и др.

Изучение дисциплины (модуля) «Стандарты в профессиональной деятельности» является базовым для последующего освоения программного материала дисциплин (модулей): «Основы информационной безопасности», «Проектирование баз данных» и др.

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: УК-1 в соответствии с основной профессиональной образовательной программой бакалавриата 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**
Системное и критическое мышление	УК-1	Способен осуществлять поиск, критический анализ исинтез информации, применять системный под-	УК-1.ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических дей-	*Знать:* принципы сбора, отбора и обобщения информации

		ход для решения поставленных задач	ствий в рамках компетенции УК-1.ИД-2. Планирует и выполняет практические действия в рамках компетенции УК-1.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	*Уметь:* соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.
				Владеть: практическим опытом работы с информационными источниками, опыт научного поиска, создания научных текстов

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 2 зачетные единицы.

Вид учебной работы	Всего часов	Семестры				
		1				
Контактная работа обучающихся с педагогическими работниками	**36**	**36**				
Учебные занятия лекционного типа	10	10				
из них: в форме практической подготовки						
Практические занятия	10	10				
из них: в форме практической подготовки						
Лабораторные занятия						
из них: в форме практической подготовки						
Иная контактная работа	16	16				
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**27**	**27**				
из них: в форме практической подготовки						
Контроль промежуточной аттестации	**9**	**9**				
Форма промежуточной аттестации		зачет				
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**72**	**72**				

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	31	13		18		6		4				8	
Раздел 1.2	32	14		18		4		6				8	
Контроль промежуточной аттестации (час)	**9**												
Общий объем, часов	**72**	**27**		**36**		**10**		**10**				**16**	
Форма промежуточной аттестации	**зачет**												
Общий объем, часов	**72**	**27**		**36**		**10**		**10**				**16**	

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	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	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**	
Общий объем по дисциплине (модулю), часов	**27**	**11**		**12**		**4**	

3.2. Методические указания к самостоятельной работе по дисциплине

РАЗДЕЛ 1. «Организационные и правовые основы информационной безопасности»

Цель: заключается в получении обучающимися теоретических знаний о современных методах разработки и стандартизации в области информационной безопасности

Перечень изучаемых элементов содержания

Тема 1.1. Значение информационной безопасности и её место в системе национальной безопасности. Классификация видов национальной безопасности

Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности. Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности,

Тема 1.2. Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности

Обзор законодательства России как основы для обеспечения интересов личности, общества и государства в информационной сфере. Характеристика стандартов в области информационной безопасности.

Тема 1.3. Классификация информации подлежащей защите.

Государственные органы в области защиты информации Свойства информации как предмета защиты. Источник конфиденциальной информации. Сведения, которые могут быть отнесены к государственной тайне. Политический и экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну. Основные виды конфиденциальной информации, нуждающейся в защите. Коммерческая тайна. Банковская тайна. Основные объекты профессиональной тайны.

Тема 1.4. Государственные органы в области защиты информации.

Система безопасности РФ. Характеристика деятельности федеральных служб – основных государственных регуляторов в области информационной безопасности.

.

Вопросы для самоподготовки:

1. Понятие цифровой экономики и компетенции цифровой эпохи
2. Значение информационной безопасности и её место в системе национальной безопасности.
3. Классификация видов национальной безопасности
4. Базовое законодательство в области информационных технологий и защиты информации.
5. Стандарты в области информационной безопасности
6. Классификация информации подлежащей защите.
7. Государственные органы в области защиты информации.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

При изучении дисциплины «Стандарты в профессиональной деятельности» предусмотрено выполнение практического задания, которое выполняется в форме лабораторной работы.

Рубежное тестирование к Разделу 1.

1. Что такое защита информации?
1) защита от несанкционированного доступа к информации;
2) выпуск бронированных коробочек для дискет;
3) комплекс мероприятий, направленных на обеспечение информационной безопасности.
2. К какой группе мер по защите информации относится шифрование информации?
1) организационным;
2) техническим;
3) аппаратным;
4) программным.
3. Укажите принципы создания комплексной системы защиты информации:
1) неизменности;
2) прозрачности;
3) модульности;
4) рациональности;
5) доступности.
4. Внешние техногенные угрозы информационной безопасности обусловлены:
1) средствами связи и помехами от них;
2) близко расположенными опасными производствами;
3) некачественными программными средствами;
4) взаимодействием технических средств.

Общее количество вопросов – 25.
Время прохождения теста – 45 минут.
Максимальное количество баллов за тест – 100.

Критерии оценивания

Количество баллов	<65%	65 %>
Зачет	не зачтено	зачтено

РАЗДЕЛ 2. «Способы и методы защиты информации»

Цель: Ознакомиться с технологиями защиты информации.

Перечень изучаемых элементов содержания

Тема 2.1. Виды атак на информационную систему

Основные способы несанкционированного доступа к конфиденциальной информации. Методы, используемые злоумышленниками для получения доступа к конфиденциальной информации либо вывода из строя информационной системы.

Тема 2.2. Модели информационной безопасности

Способы предупреждения возможных угроз. Способы обнаружения угроз. Способы пресечения или локализации угроз. Основные способы ликвидации последствий. Основные защитные действия при реализации способов защиты информации. Защита от разглашения. Защитные действия от утечки и от несанкционированных действий (НСД) к конфиденциальной информации. Мероприятия по технической защите информации.

Тема 2.3. Классификация автоматизированных систем

Понятие автоматизированной системы. Цели классификации автоматизированных систем. Подходы к классификации автоматизированных систем. Классификация автоматизированных систем и требования к обеспечению безопасности различных классов.

Тема 2.4. Подходы к реализации и этапы построения систем защиты информации

Реализация системы защиты информации на основе встраиваемых и встроенных средств защиты. Организация безопасной среды для работы обработки конфиденциальной информации. Этапы проектирования и реализации систем защиты конфиденциальной информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. Основные меры и архитектурные принципы обеспечения обслуживаемости информационных систем.

Вопросы для самоподготовки:

1. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина пароля специалисту обслуживающей организации).
2. Оценить действия сотрудника предприятия, приведшие к инциденту, связанному с угрозой информационной безопасности (в предлагаемой ситуации).
3. Установка, настройка антивируса, проверка его работоспособности путем создания тестового вирусного файла.
4. Проектирование модели угроз путем сопоставления угроз и методов их парирования.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

При изучении дисциплины «Стандарты в профессиональной деятельности» предусмотрено выполнение практического задания, которое выполняется в форме лабораторной работы.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2:

форма рубежного контроля – тестирование

1. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?

1) организационное;

2) организационно-техническое;

3) техническо-организационное;
4) техническое.
2 .Какие пункты относятся к активным методам защиты речевой информации?
1) создание маскирующих акустических и вибрационных помех;
2) выявление факта несанкционированного подключения к линии;
3) создание прицельных электромагнитных помех акустическим закладным устройствам;
4) выявление излучений акустических закладных устройств;
5) уничтожение средств несанкционированного подключения к телефонной линии.
3 .В число основных принципов построения системы безопасности, с точки зрения её архитектуры, входят:
1) следование признанным стандартам;
2) применение нестандартных решений, не известных злоумышленникам;
3) разнообразие защитных средств.
4.Оценка рисков позволяет ответить на следующие вопросы:
1) Как спроектировать надежную защиту?
2) Какую политику безопасности предпочесть?
3) Какие защитные средства экономически целесообразно использовать?
5 .Окно опасности появляется, когда:
1) становится известно о средствах использования уязвимости;
2) появляется возможность использовать уязвимость;
3) устанавливается новое программное обеспечение.

Общее количество вопросов – 25.
Время прохождения теста – 45 минут.
Максимальное количество баллов за тест – 100.

Критерии оценивания

Количество баллов	<65%	65%>
Зачет	не зачтено	зачтено

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,** 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**
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять	*Знать:* принципы сбора, отбора и обобщения информации	Этап формирования знаний
		Уметь: соотносить разнородные	Этап формирования умений

	системный подход для решения поставленных задач	явления и систематизировать их в рамках избранных видов профессиональной деятельности.	
		Владеть: практическим опытом работы с информационными источниками, опыт научного поиска, создания научных текстов	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-1	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.

УК-1	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания)* 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.
УК-1	Этап формирования навыков и получения опыта	Аналитическое задание *(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. Что такое защита информации?
2. К какой группе мер по защите информации относится шифрование информации?
3. К какой группе угроз информационной безопасности относятся ошибки программного обеспечения?
4. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств?
5. Что относятся к активным методам защиты речевой информации?
6. На чем строится политика безопасности организации?
7. Что делать, чтобы риски стали приемлемыми?
8. Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией о методах использования уязвимостей?

9. Что входит в число принципов физической защиты?
10. Что входит в число основных принципов архитектурной безопасности?
11. На что направлены меры информационной безопасности?
12. Что следует учитывать при анализе стоимости мер безопасности?

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Промежуточная аттестация по дисциплине (модулю) проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам высшего образования – программ 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 для экзамена.

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.

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. *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. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации).
2. Федеральный закон «О безопасности» от 28.12.2010 г. № 390-ФЗ.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ (в ред. от 21.07.2011 г. № 252-ФЗ).
4. Федеральный закон «О государственной тайне» от 21.07.1993 г. № 5485-I (в ред. от 08.11.2011 г. № 309-ФЗ).
5. Федеральный закон «О коммерческой тайне» от 18.12.2006 г. № 231- ФЗ.
6. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 г. № 99-ФЗ (в ред. от 28.07.2012 г. № 133-ФЗ).
7. Федеральный закон «О персональных данных» от 27.07.2006 г. № 149- ФЗ.
8. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 г.).

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) **«Стандарты в профессиональной деятельности»** 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/
7.	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) **«Стандарты в профессиональной деятельности»** в рамках реализации основной профессиональной образовательной программы по направлению 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

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

Освоение дисциплины (модуля) **«Стандарты в профессиональной деятельности»** предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме компьютерных симуляций, разбора конкретных ситуаций, в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При освоении дисциплины (модуля) **«Стандарты в профессиональной деятельности»** предусмотрено применение электронного обучения.

Учебные часы дисциплины «**Стандарты в профессиональной деятельности**» 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.).

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

_____/С.В.Крапивка/
«06» июня__ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ТЕХНОЛОГИИ ВОЗМОЖНОСТЕЙ И БЕЗБАРЬЕРНОЙ СРЕДЫ

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) *«Технологии возможностей и безбарьерной среды»* 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 разработана рабочей группой в составе: канд. пед наук, Афанасьевой О.О.

Руководитель основной 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 практики рецензирована и рекомендована к утверждению:

Заведующий кафедрой медико-социальной реабилитологии
ГАУ «Институт дополнительного профессионального образования работников социальной сферы Департамента труда и социальной защиты населения города Москвы» — М.В.Фирсов

(подпись)

Ученый секретарь Учебно-методического объединения, канд.ист.наук, доцент — О.А.Аникеева

Согласовано
Научная библиотека, директор — И.Г. Маляр

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1 Цель и задачи дисциплины

Цель дисциплины является формирование у обучающихся профессиональных компетенций, предусмотренных современными требованиями ФГОС в области организации безбарьерной среды для лиц с ограниченными возможностями здоровья.

Задачи дисциплины:

1. Ознакомление с законодательными основами организации безбарьерной среды.
2. Формирование системы знаний об особенностях проектирования инклюзивной среды
3. Ознакомление с основными нозологическими особенностями, требующими применения технологий возможностей.
4. Формирование системы знаний о технических средства реабилитации, необходимых для обеспечения доступности среды.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина *«Технологии возможностей и безбарьерной среды»* реализуется в части, формируемой участниками образовательных отношений основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность *очной* форме обучения**.**

Перечень последующих дисциплин, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной: *Проектная деятельность, Основы информационной безопасности, Организационное и правовое обеспечение информационной безопасности.*

1.3 *Планируемые результаты обучения по дисциплине (модулю) в рамках планируемых результатов освоения основной профессиональной образовательной программы высшего образования – программы бакалавриата, соотнесенные с установленными индикаторами достижения компетенций*

Процесс освоения дисциплины направлен на формирование у обучающихся следующих универсальных компетенций: УК-1 в соответствии с основной профессиональной образовательной программой по направлению подготовки 10.03.01 Информационная безопасность.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты:

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Объем дисциплины, включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость дисциплины (модуля), изучаемой в _1_ семестре, составляет _2_ зачетные единицы. По дисциплине (модулю) предусмотрен *зачет*

Вид учебной работы	Всего часов	Семестры			
		1			
Контактная работа обучающихся с педагогическими работниками (по видам учебных занятий) (всего):	**36**	36			
Учебные занятия лекционного типа	10	10			
Практические занятия	10	10			
Лабораторные занятия					
Иная контактная работа	16	16			
Самостоятельная работа обучающихся, всего	**27**	27			
Контроль промежуточной аттестации (час)	**9**	**9**			
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**72**	**72**			

2.2. Учебно-тематический план дисциплины

аздел, тема	Виды учебной работы, академических часов						
	Всего	Самостоятельная работа	Контактная работа обучающихся с педагогическими работниками				
			Всего	Лекционные занятия	Семинарские/ практические занятия	Лабораторные занятия	Иная контактная работа
Семестр 1							
Раздел 1. Человек с инвалидностью как объект технологий возможностей	**32**	**14**	**18**	**5**	**5**	**0**	**8**
Тема 1.1. Дефициты и ресурсы лиц с различными заболеваниями	14	7	9	2	3	0	4
Тема 1.2. Технические средства обеспечения доступности для людей с инвалидностью различных объектов социальной инфраструктуры и услуг	14	7	9	3	2	0	4
Раздел 2. Нормативно-правовое регулирование проектирования безбарьерной среды	**31**	**13**	**18**	**5**	**5**	**0**	**8**
Тема 2.1. Нормативно-правовые основания организации доступной среды	16	7	9	2	3	0	4

аздел, тема	Виды учебной работы, академических часов						
	Всего	Самостоятельная работа	Контактная работа обучающихся с педагогическими работниками				
			Всего	Лекционные занятия	Семинарские/ практические занятия	Лабораторные занятия	Иная контактная работа
Тема 2.2. Принципы проектирования и основные элементы градостроительной и архитектурной среды	15	6	9	3	2	0	4
Контроль промежуточной аттестации (час)	**9**						
Общий объем, часов	**72**	**27**	**36**	**10**	**10**	**0**	**16**
Форма промежуточной аттестации	**Зачет 9**						
Общий объем часов по дисциплине	**72**	**27**	**36**	**10**	**10**	**0**	**16**

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

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
Семестр 1							
Раздел 1. Человек с инвалидностью как объект технологий возможностей	14	4	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	Презентация	2	Компьютерное тестирование

Раздел 2. Нормативно-правовое регулирование проектирования безбарьерной среды	13	3	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	8	Доклад	2	Компьютерное тестирование
Общий объем по модулю/семестру, часов,	**27**	**7**		**16**		**4**	
Общий объем по дисциплине, часов	**27**	**7**		**16**		**4**	

3.2 Методические указания к самостоятельной работе по дисциплине

РАЗДЕЛ 1. ЧЕЛОВЕК С ИНВАЛИДНОСТЬЮ КАК ОБЪЕКТ ТЕХНОЛОГИЙ ВОЗМОЖНОСТЕЙ

Цель: изучить понятие инвалидности и ее отражения на возможностях человека и доступности объектов социальной инфраструктуры и услуг.

Перечень изучаемых элементов содержания

Классификации и типологические особенности лиц с нарушениями зрения. Классификации и типологические особенности лиц с нарушениями слуха. Классификация и типологические особенности лиц с нарушениями функций опорно-двигательного аппарата. Классификации и типологические особенности лиц с соматическими заболеваниями. Классификации и типологические особенности лиц с психическими заболеваниями. Классификации и типологические особенности лиц с нарушениями речи. Содержание категорий жизнедеятельности.

Технические средства, используемые на территории, прилегающей к зданию (участке). Технические средства, используемые на входе (входах) в здание. Технические средства, используемые на пути (путях) движения внутри здания (в т.ч. путях эвакуации). Технические средства, используемые в зоне целевого назначения здания (целевого посещения объекта). Технические средства, используемые в санитарно-гигиенических помещениях. Технические средства, используемые для создания системы информации на объекте (устройства и средства информации и связи и их системы.

Тема 1.1. Дефициты и ресурсы лиц с различными заболеваниями

Вопросы для самоподготовки:

1. Назовите пространственно-средовые барьеры в окружающей среде.
2. Кто относится к категории маломобильных групп населения (МГН)? Каковы характеристики МГН, не относящихся к людям с инвалидностью?
3. Определите соотношение понятий «универсальный дизайн» и «разумное приспособление»

Тема 1.2. Технические средства обеспечения доступности для людей с инвалидностью различных объектов социальной инфраструктуры и услуг

Вопросы для самоподготовки:

1. Раскройте такие параметры доступности как досягаемость, безопасность,

информативность, комфортность.

2. Назовите основные знаки, пиктограммы, которые используются в рамках организации доступной среды для создания системы информации.
3. Соотнесите понятия «технические средства реабилитации» и «технические средства обеспечения доступности». Можно ли их употреблять как синонимичные?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Форма практического задания: презентация.

1. Сделайте презентацию с фото технических средств обеспечения доступности в разрезе нозологий.
2. Презентуйте одно техническое средство обеспечения доступности с подробным описанием его устройства и представлением ассортиментного ряда подобных устройств.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1. форма рубежного контроля – компьютерное тестирование.

РАЗДЕЛ 2. НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОЕКТИРОВАНИЯ БЕЗБАРЬЕРНОЙ СРЕДЫ

Цель: раскрыть сущность и содержание нормативно-правового обеспечения безбарьерной среды

Перечень изучаемых элементов содержания

Конвенция о правах инвалидов (ООН). Федеральный закон от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в РФ». Федеральный закон от 1.12.2014 № 419-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам социальной защиты инвалидов в связи с ратификацией Конвенции о правах инвалидов». Постановление от 29.03.2019 года № 363 «Об утверждении государственной программы Российской Федерации "Доступная среда" (до 2025 года).

Стандарты формирования безбарьерной среды для инвалидов. Нормативное регулирование параметров установки элементов безбарьерной среды. Требования Федерального закона от 30.12.2009 № 384-ФЗ «Технический регламент о безопасности зданий и сооружений».

Применение строительных норм и правил (СНиП) и сводов правил (СП). СНиП 35-01-2001 "Доступность зданий и сооружений для маломобильных групп населения"; РДС 35-201-99 «Порядок реализации требований доступности для инвалидов к объектам социальной инфраструктуры»; СП 35-101-2001 «Проектирование зданий и сооружений с учетом доступности для маломобильных групп населения»; СП 35-102-2001 "Жилая среда с планировочными элементами, доступными инвалидам"; СП 35-103-2001 "Общественные здания и сооружения, доступные маломобильным посетителям"; СП 35-104-2001 "Здания и помещения с местами труда для инвалидов"; СНиП 31-06-2009 "Общественные здания и сооружения"; ГОСТ Р 51631-2008 «Лифты пассажирские. Технические требования доступности, включая доступность для инвалидов и других маломобильных групп населения»; ГОСТ Р 51630-2000 «Платформы подъемные с вертикальным и наклонным перемещением для инвалидов. Технические требования доступности»; ГОСТ Р 52131-

2003 «Средства отображения информации знаковые для инвалидов»; ГОСТ Р 51671-2000 «Средства связи и информации технические общего пользования, доступные для инвалидов. Классификация. Требования доступности и безопасности»; ГОСТ Р 52875-2007 «Указатели тактильные наземные для инвалидов по зрению. Технические требования»; ГОСТ 51261-99 «Устройства опорные стационарные реабилитационные. Типы и технические требования».

Тема 2.1. Нормативно-правовые основания организации доступной среды

Вопросы для самоподготовки:

1. Основные законодательные акты Российской Федерации, содержащие основные права людей с инвалидностью.
2. Отследите динамику изменений госпрограммы «Доступная среда» с 2011 по настоящее время. Какие показатели, блоки изменились? Чем это объяснить?

Тема 2.2. Принципы проектирования и основные элементы градостроительной и архитектурной среды

Вопросы для самоподготовки:

1. Назовите основные нормативно-правовые акты, предусматривающие регулирование параметров установки элементов безбарьерной среды.
2. Назовите основные структурно-функциональные зоны и элементы зданий и сооружений, подлежащие адаптации для инвалидов и других МГН
3. Приведите примеры нарушений данных принципов в современном городе (фото, видео личных наблюдений)

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.

Форма практического задания: доклад.

Примерный перечень тем докладов к разделу 1:

1. Влияние природной среды на состояние человека.
2. Виляние социально-экономической среды на состояние человека.
3. Расскажите о пространственных барьерах для людей с нарушениями опорно-двигательного аппарата.
4. Характеристика «жилой среды»
5. Особенности градостроительной среды
6. Безопасность при проектировании поселений в сельской местности.
7. Безопасность при проектировании малых городов.
8. Особенности проектирования городов при больших индустриальных комбинатах.
9. Принцип удобства в градостроительной и архитектурной политике.
10. Гибкость в градостроительной и архитектурной политике.
11. Простота использования в градостроительной и архитектурной политике
12. Понятность информации в градостроительной и архитектурной политике.
13. Допустимость ошибок в градостроительной и архитектурной политике.
14. Минимальные физические усилия в градостроительной и архитектурной политике.
15. Соответствие размеров и габаритов пространства в градостроительной и архитектурной политике.
16. Опыт США в социальной архитектуре.

17. Опыт Канады в социальной архитектуре.
18. Опыт Англии в социальной архитектуре.
19. Опыт Германии в социальной архитектуре.
20. Опыт Франции в социальной архитектуре.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1. форма рубежного контроля – компьютерное тестирование.

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 дисциплине является **зачет,** 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
УК -1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Знать: основы системного подхода для решения профессиональных задач в социальной работе	Этап формирования знаний
		Уметь: осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Этап формирования умений
		Владеть: методикой поиска, критического анализа и синтеза информации, применения системного подхода для решения 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
УК-1	Этап формирования знаний.	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать	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

		и излагать материал	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-1	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
УК-1	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.	конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания: [0-6] 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

Теоретический блок вопросов:

1. Перечислите основополагающие международные юридические документы, в которых закреплены права детей-инвалидов.
2. Какие этические принципы и нормы отношения к проблемам инвалидов провозглашаются в международных документах, разработанных ООН?
3. Законодательство Российской Федерации, региональное, регулирующее развитие инклюзивного образования в общеобразовательных учреждениях
4. Охарактеризуйте федеральные программные документы РФ, ориентированные на помощь детям-инвалидам.
5. Назовите особенности социальной политики в отношении детей с ОВЗ.
6. Охарактеризуйте роль общественной и государственной инициативы в решении проблем граждан с ограниченными возможностями.
7. Чем отличается отношение к людям с ограниченными возможностями в контексте медицинской, социальной моделей инвалидности?
8. Создание универсальной безбарьерной среды.
9. Экологическая целесообразность среды.
10. Что изучает функциональная антропометрия
11. Сколько уровней отражения воздействий архитектуры психикой человека.
12. Что такое визуальная комфортность.
13. Какие вы знаете виды освещенности?
14. Наименьшие размеры зоны свободного маневрирования для поворота коляски на 90,180,360 градусов
15. Что должны обеспечивать проектные решения объектов доступных для МГН?
16. Назовите четыре разновидности требований к среде, предъявляемых лицами с ограниченными возможностями.
17. Какие архитектурные задачи позволяет решить цветовое кодирование.
18. Применения тактильного кодирования для организации доступной среды.
19. Использование звуковых ориентиров для создания безбарьерной среды.
20. Как решается на государственном уровне создание безбарьерной среды в Российской Федерации?
21. Дайте понятие инвалидности, в чем смысл ограничения жизнедеятельности?
22. В чем заключаются проблемы доступности жилья?
23. В чем заключаются проблемы доступности городской среды?
24. В чем заключаются проблемы доступности транспортной инфраструктуры?
25. В чем заключаются проблемы доступности социальных объектов?
26. Дайте определение понятия «Маломобильные группы населения (МГН)»

27. Каким образом должны быть оборудованы входы в здания и помещения для инвалидов-колясочников?
28. Назовите способы адаптации среды жизнедеятельности к потребностям инвалидов и маломобильных групп населения.
29. Размеры входных площадок и тамбуров
30. Как оборудуются пандусы в местах примыкания к проезжей части для слепых и слабовидящих людей
31. Размеры лифтовой кабины, предназначенной для инвалидов колясочников
32. Как организована городская среда для инвалидов в развитых странах?
33. Назовите основные принципы универсального дизайна.
34. Приведите пример применения принципов универсального дизайна.
35. Что необходимо учитывать при проектировании жилых домов и помещений для обеспечения потребностей инвалидов
36. В чем заключается роль генерального плана города в процессе формирования безбарьерной среды?
37. Назовите особенности отдельных категорий инвалидов.
38. Габариты инвалидной коляски и размеры, необходимые для ее размещения.
39. Что необходимо учитывать при проектировании зон обслуживания инвалидов в общественных зданиях?
40. Какие вы знаете визуальные устройства и средства информации?
41. Мобильность в интерьере с учетом требований инвалидов: перегородки, мебель освещение и т.д.
42. Организация рабочих мест в офисах для инвалидов: габариты, оборудование, материалы рабочих поверхностей ит.д.
43. Организация санитарно- гигиенических зон для МГН: ванные комнаты, туалеты, постирочные.
44. Проходы, коридоры, инженерные коммуникации (габариты, возможность обслуживания).
45. Какой используется шрифт для передачи письменной информации для слепых?

4.5 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

5.1. Перечень основной и дополнительной учебной литературы для освоения дисциплины

5.1.1. Основная литература

1. *Аксенова, Л. И.* Абилитационная педагогика : учебное пособие для вузов / Л. И. Аксенова. — Москва : Издательство Юрайт, 2022. — 377 с. — (Высшее образование). — ISBN 978-5-534-05409-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493354
2. Фуряева, Т. В. *Социализация и социальная адаптация лиц с инвалидностью : учебное пособие для вузов / Т. В. Фуряева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 189 с. — (Высшее образование). — ISBN 978-5-534-08278-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493336*

3. *Фуряева, Т. В.* Социальная инклюзия : учебное пособие для вузов / Т. В. Фуряева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 189 с. — (Высшее образование). — ISBN 978-5-534-07465-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494383

5.1.2. Дополнительная литература

1. *Вишнякова, Ю. А.* Инклюзивное искусство : учебное пособие для вузов / Ю. А. Вишнякова. — Москва : Издательство Юрайт, 2022. — 138 с. — (Высшее образование). — ISBN 978-5-534-13762-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496726
2. Педагогика дополнительного образования. Работа с детьми с особыми образовательными потребностями : учебное пособие для вузов / Л. В. Байбородова [и др.] ; под редакцией Л. В. Байбородовой. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 241 с. — (Высшее образование). — ISBN 978-5-534-06162-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491196

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	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

Освоение обучающимся дисциплины *«Технологии возможностей и безбарьерной среды»* предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций и семинаров. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения дисциплины 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 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 занятия.

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;
- самостоятельное выполнение заданий согласно обозначенной учебной программой тематики;

Главным результатом служит получение положительной оценки по каждому практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к 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 (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.

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

5.4.1. Средства информационных технологий

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

5.4.3. 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)

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/

5.5 Материально-техническое обеспечение образовательного процесса по дисциплине

Для изучения дисциплины *«Технологии возможностей и безбарьерной среды»* в рамках реализации основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность.

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 *«Технологии возможностей и безбарьерной среды»* применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины *«Технологии возможностей и безбарьерной среды»* предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме деловых игр и разбора конкретных ситуаций, в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

При освоении дисциплины *«Технологии возможностей и безбарьерной среды»* предусмотрено применение электронного обучения.

Учебные часы дисциплины *«Технологии возможностей и безбарьерной среды»* 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 *«Технологии возможностей и безбарьерной среды»* 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.			

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 2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

АДАПТИВНЫЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Направление подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

Организация и технологии защиты информации

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ - ПРОГРАММА БАКАЛАВРИАТА

Форма обучения

Очная форма обучения

Москва 2022

Рабочая программа учебной дисциплины «*Адаптивные информационно-коммуникационные технологии*» разработана на основании федерального государственного образовательного 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 учебной дисциплины разработана доцентом, кандидатом физико-математических наук, доцентом факультета информационных технологий О.А. Мудраковой.

Руководитель основной профессиональной образовательной программы кандидат педагогических наук, доцент _____ Н.Г. Витковская

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

Рабочая программа дисциплины рецензирована и рекомендована к утверждению:

ФГБОУ ВО «Московский политехнический университет», НОЦ инфокогнитивных технологий, доктор технических наук, профессор _____ Н.И. Гданский

к.т.н., доцент кафедры информационных систем, сетей и безопасности _____ В.Л. Симонов

Согласовано
Научная библиотека, директор _____ И.Г. Маляр

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Цель и задачи дисциплины

Цель учебной дисциплины заключается в формировании у студентов профессиональных компетенций, связанных с использованием теоретических и практических знаний в области современных информационных процессов и технологий, освоение общих принципов работы и получение практических навыков использования современных информационных технологий для решения прикладных задач.

Задачи учебной дисциплины:

1. формирование у студента знаний принципов сбора, отбора и обобщения информации;
2. обеспечение устойчивых навыков систематизации в условиях локальных и глобальных сетей и систем телекоммуникаций, новых информационных технологий;
3. обучение студентов работе с информационными источниками, приобретение опыта научного поиска, создания научных текстов

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

Дисциплина (модуль) Б1.В.ДВ.01.03 *«Адаптивные информационно-коммуникационные технологии»* реализуется в части, формируемой участниками образовательных отношений основной образовательной программы в разделе дисциплин по выбору по направлению подготовки 10.03.01 Информационная безопасность очной формам обучения**.**

Изучение учебной дисциплины *«Адаптивные информационно-коммуникационные технологии»* базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: *«Информатика и основы информационно-коммуникационных технологий», «Программирование».*

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: *Основы информационной безопасности, Вычислительные системы, сети и телекоммуникации, Средства обработки и передачи информации.*

1.3 Планируемые результаты обучения по учебной дисциплине в рамках планируемых результатов освоения основной профессиональной образовательной программы высшего образования – программы бакалавриата соотнесенные с установленными индикаторами достижения компетенций.

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих профессиональных компетенций: УК-1 в соответствии с основной профессиональной образовательной программой высшего образования – программа бакалавриата 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**

Информационно-коммуникационные технологии для профессиональной деятельности Теоретические и практические основы профессиональной деятельности Системное и критическое мышление	УК-1	Способность осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	**УК-1. ИД-1.** Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции **УК-1. ИД-2.** Планирует и выполняет практические действия в рамках компетенции **УК-1. ИД-3.** Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** основные принципы сбора, отбора и обобщения информации **Уметь:** соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности **Владеть:** практическим опытом работы с информационными источниками, опытом научного поиска, создания научных текстов.

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 семестре, составляет 2 зачетных единицы. По дисциплине предусмотрен *зачет*.

Очная форма обучения

Вид учебной работы	Всего часов	Семестры			
		1			
Контактная работа обучающихся с педагогическими работниками		**36**			
Учебные занятия лекционного типа		10			
из них: в форме практической подготовки					
Практические занятия		10			
из них: в форме практической подготовки					
Лабораторные занятия					
из них: в форме практической подготовки					
Иная контактная работа		16			
из них: в форме практической подготовки					
Самостоятельная работа обучающихся		**27**			

Контроль промежуточной аттестации		**9**			
Форма промежуточной аттестации		**зачет**			
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**72**	**72**			

2.2. Учебно-тематический план дисциплины

Раздел, тема	**Виды учебной работы, академических часов**										
	Всего	**Самостоятельная работа**	**Контактная работа обучающихся с педагогическими работниками**								
			Всего	**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 Основы современных адаптивных информационных технологий	**34**	**16**	**16**	**6**		**4**				**8**	
Тема 1.1.1 Особенности современных адаптивных информационных технологий	14	6	8	2		2				4	
Тема 1.1.2 Использование адаптированной компьютерной техники	20	10	10	4		2				4	
Раздел 1.2 Информационные и коммуникационные технологии как средства коммуникации	**29**	**11**	**18**	**4**		**6**				**8**	
Тема 1.2.1. Дистанционные образовательные технологии	14	6	8	2		2				4	

Раздел, тема	Виды учебной работы, академических часов										
	Всего	**Самостоятельная работа**	**Контактная работа обучающихся с педагогическими работниками**								
			Всего	**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*
Тема 1.2.2 Технические и программные средства телекоммуникационных технологий	15	5	10	2		4				4	
Контроль промежуточной аттестации (час)	**9**										
Общий объем, часов	**72**	**27**	**36**	**10**		**10**				**16**	

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

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 (семестр 1)							

Раздел 1.1 Основы современных адаптивных информационных технологий	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 1.2 Информационные и коммуникационные технологии как средства коммуникации	13	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	6	реферат	2	Создать мультимедийную презентацию на тему « Структура и технология работы электронных библиотек в образовательном учреждении»
Общий объем по модулю/семестру, часов	**27**	**11**		**12**		**4**	
Общий объем по дисциплине, часов	**27**	**11**		**12**		**4**	

3.2 Методические указания к самостоятельной работе по дисциплине (модулю)

МОДУЛЬ 1 (1 семестр)

РАЗДЕЛ 1.1. Основы современных адаптивных информационных технологий

Цель: заключается в формировании у студентов компетенций, связанных с использованием теоретических и практических знаний в области современных адаптивных информационных технологий, освоение общих принципов работы и получение практических навыков использования современных информационных технологий для решения прикладных задач.

Перечень изучаемых элементов содержания

Особенности информационных технологий для людей с ограниченными возможностями здоровья. Организация индивидуального информационного пространства. Адаптивные информационные и коммуникационные технологии поддержки принятия решений.

Тема 1.1.1 Особенности современных адаптивных информационных технологий

Цель: Сформировать знания и умения в области современных адаптивных информационных технологий для решения прикладных задач.

Перечень изучаемых элементов содержания

Новые задачи педагогических коллективов в работе с обучающимся, относящимся к разным категориям лиц с ограниченными возможностями здоровья: создание атмосферы заинтересованности каждого обучающегося в работе группы; использование в ходе учебы дидактического материала и специальных устройств, наиболее доступных и значимых видов и форм учебного содержания.

Вопросы для самоподготовки:

1. Понятие «доступные ИКТ» как весь спектр ассистивных и основных технологий и

форматов

2. Состав «доступных ИКТ»:
    a) базовые технологии (компьютеры и мобильные телефоны, содержащие встроенные специальные возможности);
    b) ассистивные технологии (слуховые аппараты, программы чтения с экрана, адаптивные клавиатуры и т.д.);
    c) форматы доступа (HTML-доступ, книги DAISY (информационная система цифрового доступа) и т.д.)

Тема 1.1.2 Использование адаптированной компьютерной техники

Цель: Сформировать знания и умения в области современных адаптивных информационных технологий: программное обеспечение наиболее распространенных вариантов доступа к инклюзивному образованию.

Перечень изучаемых элементов содержания

Осуществление вызова на мобильный телефон через образовательную сеть «мобильное образование» или «m-обучение». Требование совместимости конкретной ассистивной технологии, например, слухового аппарата или других средств с мобильным телефоном. Специальные компьютерные учебные программы.

Вопросы для самоподготовки:

1. Прикладное программное обеспечение ассистивных технологий.
2. Совместимость слухового аппарата или других средств с мобильным телефоном.
3. Просмотр веб-сайта с помощью «программы чтения с экрана».
4. Использование альтернативных средств коммуникации

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: реферат

Перечень тем рефератов к разделу 1:

1. Интеграция ИКТ в инклюзивное образование.
2. Многоязычие: ключ к инклюзивному образованию в условиях информатизации общества.
3. Компьютеры и мобильные телефоны, содержащие встроенные специальные возможности.
4. Слуховые аппараты, программы чтения с экрана, адаптивные клавиатуры.
5. HTML-доступ, книги DAISY (информационная система цифрового доступа).
6. Информационный рынок: определение, становление, современное состояние.
7. Современные экономические и социальные условия информатизации российского общества.
8. Современные культурные условия информатизации российского общества.
9. Роль библиотек в построении образования информационного общества.
10. Программные и аппаратные технологии Интернет-телефонии.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.1:

форма рубежного контроля – компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

РАЗДЕЛ 1.2 Информационные и коммуникационные технологии как средства коммуникации

Цель: заключается в формировании у студентов компетенций, связанных с получением представления о современном состоянии и структуре рынка информационных ресурсов и технологий для осуществления коммуникаций.

Перечень изучаемых элементов содержания

Дистанционные технологии в образовании: проблемы, возможности, перспективы развития. Электронное обучение. Перспективы развития адаптивных информационных технологий. Глобальные, базовые и прикладные информационные технологии. Современные адаптивные технические и программные средства телекоммуникации. Информационная технология как система.

Тема 1.2.1 Дистанционные образовательные технологии

Цель: заключается в формировании у студентов компетенций, связанных с получением представления о современном состоянии и структуре рынка адаптивных информационных ресурсов и технологий для осуществления коммуникаций при использовании дистанционных технологий.

Перечень изучаемых элементов содержания

Дистанционные образовательные технологии: проблемы, возможности, перспективы развития. Электронное обучение. Интернет курсы. Интернет тестирование. Интернет олимпиады. Использование адаптивных технологий в учебном процессе.

Вопросы для самоподготовки:

1. Дистанционные образовательные технологии: проблемы, возможности, перспективы развития. Понятие электронного обучения.
2. Зарегистрироваться в Российской Научной электронной библиотеке. Изучить «Руководство пользователя» Российской Научной электронной библиотеки (http://elibrary.ru/manual_elibrary_for_user.pdf). Настроить свой персональный профиль. Изучить работу поисковой системы.
3. Роль сетевых технологий в формировании современной информационной среды.
4. Создание безбарьерной среды с использованием ИКТ в условиях образования учащихся с особыми образовательными потребностями.
5. Интернет курсы.
6. Интернет тестирование.
7. Интернет олимпиады.
8. Использование адаптивных технологий в учебном процессе

Тема 1.2.2 Технические и программные средства телекоммуникационных технологий

Цель: заключается в формировании у студентов компетенций, связанных с получением представления об использовании современных технических и программных средств телекоммуникации.

Перечень изучаемых элементов содержания

Понятие о современных технических и программных средствах телекоммуникации. Технические средства создания электронных документов. Технологии распознавания текста и обработки файлов.

Вопросы для самоподготовки:

1. Информационный рынок: определение, становление, современное состояние. Рынок адаптивной образовательной информации.
2. Телекоммуникационные технологии: этапы эволюции.
3. Определение понятий «электронная библиотека», «цифровая библиотека», «виртуальная библиотека», «медиатека».
4. Объективные предпосылки создания и этапы развития электронных библиотек.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.2

Форма практического задания: реферат

Перечень тем рефератов к разделу 1:

1. Перспективы развития адаптивных информационных технологий.
2. Информационная безопасность и защита информации: определения и генезис.
3. Технологии виртуальной реальности.
4. Адаптивные возможности программных и технических средств презентационных технологий.
5. Технологии распознавания текста и обработки файлов.
6. Современные технологии передачи электронной информации в Интернет.
7. Назначение и сущность технологии телеконференций. Вебинар.
8. Состав технологических операций при проведении телеконференции в режимах on-line и off-line.
9. Использование систем искусственного интеллекта для развития адаптивных информационных технологий.
10. Законодательная охрана и правоприменительная практика.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.2:

форма рубежного контроля – создать мультимедийную презентацию на тему « Структура и технология работы электронных библиотек в образовательном учреждении»

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 **зачет,** который проводится в **устной / 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
УК-1	Способность осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1. ИД-1. Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции УК-1. ИД-2. Планирует и выполняет практические действия в рамках компетенции УК-1. ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	Этап формирования знаний Этап формирования умений

			Этап формирования навыков и получения опыта
			Этап формирования умений

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-1	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.
УК-1	Этап формирования умений	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-1	Этап формирования навыков и получения опыта.	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 учебной дисциплине

МОДУЛЬ 1 (1 семестр)

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

1. Новые задачи педагогических коллективов в работе с обучающимся, относящимся к разным категориям лиц с ограниченными возможностями здоровья.
2. Понятие «доступные ИКТ».
3. Состав «доступных ИКТ», общая характеристика.
4. Базовые адаптивные информационные технологии в образовании.
5. Ассистивные технологии образования.
6. Форматы доступа к информации, используемые в инклюзивном образовании.
7. Дистанционные технологии в системе образования.
8. Адаптивное программное обеспечение наиболее распространенных вариантов доступа к образованию, общая характеристика.
9. «Мобильное образование» или «m-обучение» в системе инклюзивного образования.
10. Совместимость слухового аппарата или других средств с мобильным телефоном.
11. Просмотр веб-сайта с помощью «программы чтения с экрана».
12. Использование альтернативных средств коммуникации
13. Инклюзивные веб-технологии.
14. Специальные адаптивные компьютерные учебные программы для образования.
15. Облачные вычисления в инклюзивном образовании.
16. Прикладное программное обеспечение ассистивных технологий, доступное с любого компьютера через интернет.
17. Использование адаптированной компьютерной техники. Использование адаптивных устройств ввода и вывода информации.
18. Использование специального программного обеспечения для студентов с нарушениями опорно-двигательного аппарата.
19. Организация индивидуального информационного пространства. Использование альтернативных средств коммуникации.
20. Всемирная паутина. Поисковые системы.
21. Возможности робототехники и сенсорики в адаптации людей с ограниченными возможностями здоровья.
22. Интеграция адаптивных ИКТ в образование.
23. Многоязычие: ключ к инклюзивному образованию в условиях информатизации общества.
24. Компьютеры и мобильные телефоны, содержащие встроенные специальные возможности.
25. Слуховые аппараты - общая характеристика.
26. Программы чтения с экрана, адаптивные клавиатуры.
27. HTML-доступ, книги DAISY (информационная система цифрового доступа).
28. Информационный рынок: определение, становление, современное состояние.
29. Современные экономические и социальные условия информатизации российского общества.
30. Современные культурные условия информатизации российского общества.
31. Роль библиотек в построении информационного общества.
32. Программные и аппаратные технологии Интернет-телефонии.

33. Дистанционные образовательные технологии: проблемы, возможности, перспективы развития.
34. Понятие электронного обучения.
35. Роль сетевых технологий в формировании современной информационной среды.
36. Создание безбарьерной среды с использованием ИКТ в условиях образования учащихся с особыми образовательными потребностями.
37. Интернет курсы.
38. Интернет тестирование.
39. Интернет олимпиады.
40. Использование адаптивных технологий в учебном процессе
41. Определение понятий «электронная библиотека», «цифровая библиотека», «виртуальная библиотека», «медиатека».
42. Объективные предпосылки создания и этапы развития электронных библиотек
43. Информационная безопасность и защита информации: определения и генезис.
44. Технологии виртуальной реальности.
45. Адаптивные возможности программных и технических средств презентационных технологий.
46. Технологии распознавания текста и обработки файлов.
47. Современные технологии передачи электронной информации в Интернет.
48. Назначение и сущность технологии телеконференций. Вебинар.
49. Состав технологических операций при проведении телеконференции в режимах on-line и off-line.
50. Использование систем искусственного интеллекта для развития адаптивных информационных технологий.
51. Построение системы с использованием информационных технологий.
52. Интеллектуализация информационных технологий.
53. Приоритетные технологии информационного общества.
54. Проблема формирования единого информационного пространства.
55. Информационная среда как новая среда обитания человека.

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 бакалаврита 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 для экзамена.

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 учебной дисциплины

5.1.1. Основная литература

1. *Советов, Б. Я.* Информационные технологии : учебник для вузов / Б. Я. Советов, В. В. Цехановский. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 327 с. — (Высшее образование). — ISBN 978-5-534-00048-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488865
2. *Трофимов, В. В.* Информационные технологии в 2 т. Том 1 : учебник для вузов / В. В. Трофимов. — Москва : Издательство Юрайт, 2022. — 238 с. — (Высшее образование). — ISBN 978-5-534-01935-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490721
3. *Трофимов, В. В.* Информационные технологии в 2 т. Том 2 : учебник для вузов / В. В. Трофимов. — Москва : Издательство Юрайт, 2022. — 390 с. — (Высшее образование). — ISBN 978-5-534-01937-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490722

5.1.2. Дополнительная литература

1. *Кожевникова, Г. П.* Информационные системы и технологии в маркетинге : учебное пособие для вузов / Г. П. Кожевникова, Б. Е. Одинцов. — Москва : Издательство Юрайт, 2022. — 444 с. — (Высшее образование). — ISBN 978-5-534-07447-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489534
2. *Демин, А. Ю.* Информатика. Лабораторный практикум : учебное пособие для вузов / А. Ю. Демин, В. А. Дорофеев. — Москва : Издательство Юрайт, 2022. — 131 с. — (Высшее образование). — ISBN 978-5-534-08366-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490335

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	Электронно-библиотечная система для	https://urait.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	платформа Юрайт	ВУЗов, ССУЗов, обеспечивающая доступ к 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

5.3 Методические указания для обучающихся по освоению учебной дисциплины

Освоение обучающимся учебной дисциплины «*Адаптивные информационно-коммуникационные технологии*» 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 учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с рабочей программы учебной 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 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:

− 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»).

5.4 Информационно-технологическое обеспечение образовательного процесса по учебной дисциплине

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	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и	http://biblioclub.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	онлайн»	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

5.5 Материально-техническое обеспечение образовательного процесса по учебной дисциплине

Для изучения учебной дисциплины *«Адаптивные информационно-коммуникационные технологии»* 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), а также (при наличии) демонстрационными печатными пособиями (указать какими, например, таблицы «Основная грамматика английского языка»), экранно-звуковыми средствами обучения (указать какими, например, CD «Разговорный английский»), демонстрационными материалами (указать какими, например, комплект демонстрационных материалов (фолий) «Страноведение. США»), видеофильмами DVD (указать какими).

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).

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 учебной дисциплины *«Адаптивные информационно-коммуникационные технологии»* применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение учебной дисциплины *«Адаптивные информационно-коммуникационные технологии»* предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме деловых и ролевых игр, разбор конкретных ситуаций, психологические тренинги в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

При освоении учебной дисциплины *«Адаптивные информационно-коммуникационные технологии»* предусмотрено применением электронного обучения.

Учебные часы дисциплины *«Адаптивные информационно-коммуникационные технологии»* 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.

В рамках учебной дисциплины *«Адаптивные информационно-коммуникационные технологии»* 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.			
3.			
4.			

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 (МОДУЛЯ)

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ, СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Направление подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

Организация и технологии защиты информации

Уровень образования

ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации

БАКАЛАВР

Очная форма обучения

Москва 2022

Рабочая программа дисциплины (модуля) «Вычислительные системы, сети и телекоммуникации» разработана на основании федерального государственного образовательного разработана 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: к. пед.н., доцент О.Л. Мнацаканян, ст.преподаватель Д.Ю, Елисеева.

Руководитель основной профессиональной образовательной программы кандидат педагогических 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 практики 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

к.т.н., доцент кафедры информационных систем, сетей и безопасности — В.Л. Симонов

Согласовано
Научная библиотека, директор — И.Г. Маляр

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1 Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) заключается в изучение теоретических основ построения и организации вычислительных систем, сетей и телекоммуникаций для построения программного обеспечения средств вычислительной техники и автоматизированных систем, формирование профессиональных компетенций в части использования и выбора аппаратно-программной платформы, формирование профессиональной информационной культуры.

Задачи дисциплины (модуля):

1. Выработка навыков к способности инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем.
2. Формирование навыков в освоении методики использования программных средств для решения практических задач.
3. Анализ методов проектирования, внедрения и организации эксплуатации информационных систем и информационно-коммуникационных технологий.
4. Выработка умений в решении стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
5. Выработка навыков оценки технико-эксплуатационных возможностей средств вычислительной техники, эффективности различных режимов работы ЭВМ.
6. Приобретение теоретических знаний и практических навыков выбора и использования вычислительной техники для обработки информации на пользовательском уровне.

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

Учебная дисциплина *«Вычислительные системы, сети и телекоммуникации»* реализуется в обязательной части основной образовательной программы по направлению подготовки 10.03.01 *«Информационная безопасность» очной* формы обучения**.**

Изучение дисциплины (модуля) *«Вычислительные системы, сети и телекоммуникации»* базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: *«Комплексная защита объектов информатизации», «Программирование».*

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: *Системы контроля и управления доступом, Методы защиты системного программного обеспечения, Методы обнаружения сетевых атак.*

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

Процесс освоения дисциплины (модуля) направлен на формирование у обучающихся следующих общепрофессиональных компетенций: ПК-1; ПК-2; ПК-12 в соответствии с основной профессиональной образовательной программой высшего образования –

программа бакалавритата 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-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-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	**Знать:** функциональное назначение, технические и конструктивные особенности применения, общие принципы построения и работы исследуемой системы защиты информации.

			компетенции ПК-12.ИД-2. Планирует и выполняет практические действия в рамках компетенции ПК-12.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**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.
				Владеть: теоретическими знаниями и навыками по практическому применению соответствующего специализированного оборудования и измерительных приборов для проведении экспериментальных исследований системы защиты информации мероприятий

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, изучаемой в 3 и 4 семестрах, составляет 9 зачетных единиц. По дисциплине предусмотрен *экзамен*.

Вид учебной работы	**Всего часов**	**Семестры**				
		3	4			
Контактная работа обучающихся с педагогическими работниками	**162**	**90**	**72**			
Учебные занятия лекционного типа	34	18	16			

из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	56	32	24			
из них: в форме практической подготовки						
Иная контактная работа	72	40	32			
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**90**	**54**	**36**			
из них: в форме практической подготовки	*17*	*10*	*7*			
Контроль промежуточной аттестации	**72**	**36**	**36**			
Форма промежуточной аттестации		экзам	экзам			
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**324**	**180**	**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	28	10	*2*	18		4				6		8	
Раздел 1.2	29	11	*2*	18		4				6		8	
Раздел 1.3	29	11	*2*	18		4				6		8	
Раздел 1.4	29	11	*2*	18		4				6		8	
Раздел 1.5	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**												
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**												
Общий объем, часов	**324**	**90**	***17***	**162**		**34**				**56**		**72**	

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 3)							
Раздел 1.1	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 1.2	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 1.3	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 1.4	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 1.5	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**	
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	**90**	**32**		**40**		**18**	

3.2 Методические указания к самостоятельной работе по дисциплине (модулю)

МОДУЛЬ 1. БЕСПРОВОДНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ. ТЕЛЕКОММУНИКАЦИЯ (СЕМЕСТР 1)

РАЗДЕЛ 1.1. СТРУКТУРА БЕСПРОВОДНОЙ СИСТЕМЫ

Цель: приобретение теоретических знаний и практических навыков по типовым элементам, структуре беспроводных компьютерных сетей, принципам построения на их основе и функционирования распределенных систем обработки данных.

Перечень изучаемых элементов содержания

Классификация беспроводных сетей. Компоненты беспроводных сетей. Платы интерфейса сети. Инфраструктуры беспроводных сетей. Контроллеры доступа. Распределительная система. Управляющие системы. Структура сети. Информационные сигналы. Цифровые сигналы. Аналоговые сигналы. Передача информации через беспроводную сеть. Передача беспроводных сигналов. Подключение к инфраструктуре проводной сети.

Беспроводные приемопередатчики. Параметры радиосигналов. Преимущества и недостатки радиочастотных сигналов. Искажение радиочастотного сигнала. Параметры светового сигнала. Преимущества и недостатки световых сигналов. Искажение световых сигналов. Модуляция: подготовка сигналов к передаче. Частотная манипуляция. Фазовая манипуляция. Квадратурная амплитудная модуляция. Расширение спектра. Мультиплексирование с разделением по ортогональным частотам. Сверхширокополосная модуляция.

Вопросы для самоподготовки:

1. Каково главное отличие беспроводной сети от обычной беспроводной системы связи?
2. Передачу информации каких типов обеспечивает беспроводная сеть?
3. Назовите основные четыре разновидности беспроводных сетей.
4. Что делает беспроводную глобальную сеть неэффективной для применения пользователями, находящимися в помещениях?
5. Платы интерфейса беспроводной сети с каким форм-фактором наилучшим образом подходят для миниатюрных беспроводных компьютерных устройств?
6. Приведите примеры факторов, отрицательно влияющих на передачу коммуникационных сигналов через воздушную среду.
7. Каково основное назначение базовой станции?
8. Каковы основные особенности промежуточного программного обеспечения беспроводной сети?
9. На каких уровнях эталонной модели OSI работает беспроводная сеть?
10. В чем состоит отличие между пропускной способностью и скоростью передачи данных?
11. Компьютерное устройство хранит данные в аналоговой форме. Справедливо ли это утверждение?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.1

Форма практического задания: лабораторный практикум.

1. **Лабораторная работа № 1.1.1.** «Беспроводные Ad-Hoc сети». Инфраструктура "точка доступа".
2. **Лабораторная работа № 1.1.2.** «Основные инфраструктуры беспроводных сетей IEEE 802.11».
3. **Лабораторная работа № 1.1.3.** «Определение радиуса действия беспроводной сети и применение способов, увеличивающих данный показатель».
4. **Лабораторная работа № 1.1.4.** «Измерение скорости передачи данных сетей Wi-Fi».

Контрольные вопросы:

1. В какую форму должна преобразовывать сигналы плата интерфейса беспроводной сети, прежде чем передать их через воздушную среду?
2. Какой протокол доступа к среде является общепринятым для беспроводных сетей?
3. Объясните, как работает механизм контроля ошибок ARQ.
4. Приведите примеры применения беспроводных глобальных сетей.
5. Действительно ли радиочастотные сигналы обеспечивают меньший радиус действия, чем световые?
6. Какие метеоусловия существенно влияют на распространение радиочастотных сигналов?
7. Каким образом помехи вызывают появление ошибок в беспроводных сетях?
8. Каковы источники радиочастотных помех?
9. Правда ли, что многолучевое распространение влияет на системы с высокой скоростью передачи данных в системах диапазона 2,4 ГГц сильнее, чем на низкоскоростные?
10. Что понимается под ЯК-системами, использующими рассеянный свет?
11. На каких максимальных дальностях передачи можно использовать направленные ИК-системы?
12. Как модуляция влияет на передачу информации через воздушную среду?
13. Какие параметры сигнала изменяются для представления информация при квадратурной амплитудной модуляции?
14. Нужна ли пользователю лицензия для использования систем с расширением спектра?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.1:

форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 1.2. БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ: СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

Цель: приобретение теоретических знаний и практических навыков по типовым элементам, структуре беспроводных компьютерных сетей, принципам построения на их основе и функционирования распределенных систем обработки данных.

Перечень изучаемых элементов содержания

Компоненты беспроводных персональных сетей. Пользовательские устройства. Радиоплаты интерфейса сети. USB-адаптеры. Маршрутизаторы. Системы на основе беспроводных персональных сетей. Технологии беспроводных персональных сетей. Стандарт 802.15. Bluetooth. Компоненты беспроводных локальных сетей.

Системы беспроводных локальных сетей. Беспроводные локальные сети для домашнего применения. Беспроводные локальные сети предприятий. Технологии беспроводных локальных сетей. Стандарт 802.11. Wi-Fi.

Компоненты беспроводных региональных сетей. Мосты. Системы беспроводных региональных сетей. Системы пакетной радиосвязи. Технологии беспроводных региональных сетей. Стандарт 802.16. Компоненты беспроводных глобальных сетей. Пользовательские устройства беспроводных глобальных сетей. Базовые станции. Системы беспроводных глобальных сетей. Беспроводные глобальные сети с сотовой структурой. Технологии беспроводных глобальных сетей.

Угрозы безопасности. Мониторинг трафика. Неавторизованный доступ. Отказ в обслуживании. Шифрование. WEP. Виртуальные частные сети. Аутентификация. Уязвимость механизма аутентификации стандарта 802.11. MAC-фильтры. Аутентификация с использованием открытого ключа шифрования. Стандарт 802.1x. Политика безопасности. Стадии оценки.

Вопросы для самоподготовки:

5. Какие форм-факторы наиболее употребительны для радиоплат беспроводных персональных сетей?
6. Какие приложения получают особенно большой выигрыш от использования беспроводного USB-адаптера (или "беспроводной заглушки")?
7. Когда имеет смысл использовать маршрутизатор в беспроводной персональной сети?
8. Какова зона действия беспроводной персональной сети?
9. Какая группа IEEE использовала Bluetooth в качестве основы при разработке своего стандарта?
10. В чем разница между точкой доступа и маршрутизатором беспроводной локальной сети?
11. Когда имеет смысл применять повторитель в беспроводной локальной сети?
12. Как радиоплата беспроводной локальной сети определяет, к какой точке доступа нужно привязываться?
13. В чем преимущество использования систем типа "точка-несколько точек" по отношению к системам "точка-точка" в случае, когда необходимо обеспечить соединения для нескольких площадок?
14. В чем преимущество использования пакетной радиосвязи в беспроводных региональных сетях?
15. Какие стандарты используются при создании беспроводных региональных сетей?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.2

Форма практического задания: лабораторный практикум.

1. **Лабораторная работа № 1.2.1.** «Использование беспроводных маршрутизаторов».
2. **Лабораторная работа № 1.2.2.** «Изучение механизмов безопасности сетей Wi-Fi с использованием Windows XP».
3. **Лабораторная работа № 1.2.3.** «Аудит безопасности сетей, шифруемых с использованием WEP, с использованием ОС Linux».
4. **Лабораторная работа № 1.2.4.** «Обнаружение атак диссоциации с использованием ОС Linux».

Контрольные вопросы:

1. Пользовательские устройства каких типов чаще других применяются в беспроводных глобальных сетях?
2. Каковы преимущества спутниковой системы?
3. Системы беспроводных глобальных сетей какого типа наиболее распространены?

4. Какая из двух сотовых систем обеспечивает более высокие скорости передачи данных — GPRS или UMTS?
5. В чем состоит основная проблема метеорной связи?
6. Верно ли, что при использовании технологии доступа с частотным уплотнением пользователи должны поочередно передавать сигналы?
7. За счет чего при использовании технологии CDMA обеспечивается отсутствие взаимных помех?
8. Каковы три основные угрозы безопасности беспроводной сети?
9. Каково основное средство противодействия мониторингу трафика?
10. Как можно воспрепятствовать хакерам в получении доступа к ресурсам компании через беспроводную сеть?
11. Какой метод поможет уменьшить урон от успешно проведенной DoS-атаки?
12. Почему WEP не пригоден для защиты секретной информации?
13. Чем TKIP отличается от WEP?
14. Верно ли, что WPA использует TKIP и является поднабором требований стандарта 802. Hi?
15. Почему использование фильтрации MAC-адресов неэффективно?
16. Что такое подставная точка доступа, и почему при ее использовании возникают проблемы?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.2:

форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 1.3. ТИПЫ СЕТЕЙ СВЯЗИ И ТЕНДЕНЦИИ ИХ РАЗВИТИЯ

Цель: приобретение теоретических знаний и практических навыков по типовым элементам, структуре телекоммуникационных сетей, принципам построения на их основе и функционирования распределенных систем обработки данных.

Перечень изучаемых элементов содержания

Сеть связи общего пользования. Ведомственные сети связи. Выделенные сети связи. Корпоративные сети связи. Линии связи и их характеристики. Проводные линии связи. Кабельные линии. Характеристики линий связи. Амплитудно-частотная характеристика. Полоса пропускания линии связи. Помехоустойчивость линии связи. Достоверность передачи данных. Аппаратура линий связи. Коммутируемые и выделенные каналы связи.

Передача дискретных данных на физическом уровне. Аналоговая модуляция. Цифровое кодирование. Самосинхронизирующие коды. Дискретная модуляция аналоговых сигналов. Асинхронная и синхронная передачи. Передача дискретных данных на канальном уровне. Типы синхронных протоколов канального уровня. Обеспечение достоверности передачи информации. Системы передачи с обратной связью.

Вопросы для самоподготовки:

1. Характерные особенности ТСС.
2. Основные направления интеграционных процессов.
3. Основные преимущества кабельных линий связи.
4. Недостатки волоконно-оптических линий связи.
5. Пропускная способность линии связи.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.3

Форма практического задания: лабораторный практикум.

1. **Лабораторная работа №1.3.1** «Введение в среду построения виртуальных вычислительных сетей».
2. **Лабораторная работа №1.3.2** «Объединение удаленных узлов на основе концентраторов локальных вычислительных сетей».
3. **Лабораторная работа №1.3.3** «Структуризация локальных вычислительных сетей с помощью коммутаторов».
4. **Лабораторная работа №1.3.4** «Маршрутизаторы и применение статической маршрутизации в локальных вычислительных сетях».

Контрольные вопросы:

1. Способы преобразования цифровых данных в аналоговую форму.
2. Основные характеристики и сравнительная оценка самосинхронизирующего кода.
3. Свойства протоколов, работающих на канальном уровне.
4. Способы связи без установления логического соединения.
5. Способ связи, ориентированный на логическое соединение.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.3:

форма рубежного контроля – Отчет по лабораторной работе.

РАЗДЕЛ 1.4. МАРШРУТИЗАЦИЯ ПАКЕТОВ В ТКС. СЕТИ И ТЕХНОЛОГИИ

Цель: приобретение теоретических знаний и практических навыков по типовым элементам, структуре телекоммуникационных сетей, принципам построения на их основе и функционирования распределенных систем обработки данных.

Перечень изучаемых элементов содержания

Алгоритм маршрутизации. Способы маршрутизации. Эффективность алгоритмов маршрутизации. Сравнение способов передачи данных. Виды маршрутизации. Простая маршрутизация. Фиксированная (статическая) маршрутизация. Адаптивная (динамическая маршрутизация). Распределенная адаптивная маршрутизация. Иерархическая маршрутизация. Способы коммутации в ТКС. Коммутация каналов. Преимущества метода коммутации каналов. Коммутация с промежуточным хранением.

Понятие сети X.25. Достоинства сетевой технологии X.25. Понятие протокола ретрансляции фреймов. Эффективность технологии FR. Общие сведения **о** сети ISDN. Проблемы безопасности сети ISDN. Связь удаленного пользователя с локальной сетью корпоративного сетевого центра. Адресация в сетях ISDN. Сети и технологии SDH. Топология сетей SDN. Сети и технологии ATM. Основные особенности ATM-технологии. Спутниковые сети связи.

Вопросы для самоподготовки:

1. Основные факторы, снижающие эффективность алгоритмов маршрутизации.
2. Локальная адаптивная маршрутизация.
3. Централизованная адаптивная маршрутизация.
4. Недостатки метода коммутации каналов.
5. Символьная коммутация.
6. Ограничения сетевой технологии X.25.
7. Преимущества цифровой технологии ISDN.
8. Модули, использующиеся при построении сетей SDN.

9. Отличие АТМ-технологии от других телекоммуникационных технологий.
10. Основные преимущества спутниковых сетей связи.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.4

Форма практического задания: лабораторный практикум.

1. **Лабораторная работа №1.4.1** Разрешение адресов по протоколу ARP. APR-спуфинг».
2. **Лабораторная работа №1.4.2** «Динамическая маршрутизация по протоколу RIP».
3. **Лабораторная работа №1.4.3** «Получение сетевых настроек по DHCP».
4. **Лабораторная работа №1.4.4** «Организация беспроводного доступа к локальной вычислительной сети».

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.4:

форма рубежного контроля – отчет по лабораторной работе.

МОДУЛЬ 2. ГЛОБАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ. ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ (СЕМЕСТР 2)

РАЗДЕЛ 2.1. ПРОЕКТИРОВАНИЕ, МОДЕЛИРОВАНИЕ И ОЦЕНКА ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК ВЫЧИСЛИТЕЛЬНОЙ СЕТИ В САПР NETCRACKER PROFESSIONAL 3.1

Цель: ознакомление с графическим интерфейсом пользователя GUI, с элементами основного прикладного экрана NetCracker и с обращением к инструментальным средствам и режимам.

Перечень изучаемых элементов содержания

Разновидности (типы, категории) мостов и маршрутизаторов, адаптеров. Типы протоколов. Типы линей связи и их технические характеристики.

Вопросы для самоподготовки:

1. Охарактеризуйте назначение и возможности САПР NetnCracker Professional 3.1.
2. Каково назначение мостов?
3. Каково назначение маршрутизаторов?
4. Сколько разновидностей (типов, категорий) мостов и маршрутизаторов содержится в списке Устройств Routers and bridges?
5. Сколько разновидностей базовых маршрутизаторов содержится в списке Backbone routers?
6. Сколько разновидностей базовых маршрутизаторов, изготовленных фирмой Cisco Systems, содержит список Backbone routers?
7. Сколько разновидностей адаптеров локальной сети содержит список LAN adapters?
8. Сколько разновидностей плат адаптеров LAN adapters Ethernet, изготовленных корпорацией 3Com Corp, содержит папка 3Com Corp.?
9. Как создается конфигурация Устройства?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.1

Форма практического задания: лабораторный практикум.

Лабораторная работа №2.1.1 «Проектирование, моделирование и оценка технических характеристик вычислительной сети в САПР NetCracker Professional 3.1»

Контрольные вопросы:

1. Как узнать, какие типы протоколов обмена допускаются для выбранного сменного блока процессора связи системы передачи данных?

2. Сколько предприятий - изготовителей и поставщиков содержится в базе данных Устройств Vendors? Приведите наименования некоторых из них.
3.Перечислите типы линий связи, применяемых при создании ИВС. Какими техническими характеристиками они отличаются друг от друга?
4. Назовите, в каких случаях при создании ЛВС применяются те или иные типы линий связи и сравните их характеристики.
5. Как получить общую информацию об объектах в окне сайта?
6. Как вывести информацию относительно полной сети, какие сведения она содержит?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.5:

форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 2.2. ИСПОЛЬЗОВАНИЕ ОСОБЕННОСТЕЙ АНИМАЦИИ ПРИ СОЗДАНИИ СЕТЕВЫХ ПРОЕКТОВ И ОЦЕНКА ИХ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК В САПР NETCRACKER PROFESSIONAL 3.1

Цель: Изучение методов запуска проектной анимации для предлагаемой двухуровневой кампусной сети, корректировки параметров анимации (размера, интенсивности и быстродействия информационного пакета, увеличение трафика, изменение маршрутизации трафиков).

Перечень изучаемых элементов содержания

Прерывание и востановление сетевых линий связи, создание изгиба связи. Проверка протоколов маршрутизации, получение информации о пакете, добавление, удаление и замена сменных блоков Устройства сетевого оборудования, переименование Окна, вывод нужной информации.

Вопросы для самоподготовки:
1. Каковы функциональные возможности анимационного моделирования сети?
2. Что позволяет выявить процесс анимации?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.2

Форма практического задания: лабораторный практикум.
Примерный перечень тем лабораторных работ к разделу 2.2

Лабораторная работа № 2.2.1 Использование особенностей анимации при создани сетевых проектов и оценка технических характеристик в САПР NetCracker Professional 3.1

Контрольные вопросы:
1. Какие параметры сети можно корректировать и выбирать в процессе анимации?
2. Какие сведения о параметрах информационных пакетов могут быть выведены?
3. Сколько и каких типов протоколов содержится в базе данных NetCracker?
4. Каким образом можно добавить, заменить и удалить устройства сетевого оборудования?
5. Как в проекте сети переименовать здания?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.2:

форма рубежного контроля – отчет к лабораторным работам

РАЗДЕЛ 2.3. СОЗДАНИЕ И МОДЕЛИРОВАНИЕ НОВОГО СЕТЕВОГО ПРОЕКТА В САПР NETCRACKER PROFESSIONAL 3.1 И РАЗМЕЩЕНИЕ ЕГО НА МЕСТНОСТИ

Цель: Изучение методов создания и моделирования нового сетевого проекта.

Перечень изучаемых элементов содержания

Методы создания и моделирования нового сетевого проекта: заполнение проекта аппаратурой Устройств сетевого оборудования: выбор и помещение в рабочее пространство коммутатора (**Switch)** и рабочих станций (**Workgroup)**, помещение плат ЛВС адаптеров (**LAN adapter**) в рабочие станции. Определение совместимости Устройств, установление связи (**Link)** между рабочими станциями и коммутатором, добавление и удаление наращиваемых устройств (например, концентраторов - **Hubs**). Задание и изменение параметров конфигурации трафика. Установка связи после установки выключателей и установка индикации в проектируемой сети. Размещение сети на местности.

Вопросы для самоподготовки:
1. Каково назначение коммутатора?
2. Каково назначение и состав рабочих станций?
3. Каково назначение концентратора?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.3

Форма практического задания: лабораторный практикум.

Примерный перечень тем лабораторных работ к разделу 2.3

Лабораторная работа № 2.3.1 Создание и моделирование нового сетевого проекта в САПР NetCracker Professional 3.1 и размещение его на местности

Контрольные вопросы:
1. Что означают понятия «совместимость» и «несовместимость» Устройств сети?
2. Что означает понятие «наращиваемые»Устройства сети?
3. Сколько типов трафиков насчитывается в базе данных САПР NetCracker Professional. Приведите наименования некоторых из них.
4. Что такое “наращиваемые” устройства? Приведите пример
5. Какие типы носителей используются при построении ЛВС?
6. Какие параметры информационного пакета могут быть изменены в САПР NetCracker Professional?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.3:

форма рубежного контроля – отчет к лабораторным работам

РАЗДЕЛ 2.4 СОЗДАНИЕ И МОДЕЛИРОВАНИЕ МНОГОУРОВНЕВЫХ СЕТЕВЫХ ПРОЕКТОВ В САПР NETCRACKER PROFESSIONAL 3.1

Цель: Изучение методов создания многоуровневых сетевых проектов и работа с созданным многоуровневым проектом сети.

Перечень изучаемых элементов содержания

Методы создания многоуровневых сетевых проектов и работа с созданным многоуровневым проектом сети; перемещение из одного уровня в другой; создание архитектуры клиент/сервер. Отображение итогов моделирования и статистики.

Вопросы для самоподготовки:

1. Какие изменения можно вносить в проект сети?
2. Какие надписи можно наносить на схему проекта?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.4

Форма практического задания: лабораторный практикум.
Лабораторная работа № 2.4.1 Создание и моделирование многоуровневых сетевых проектов в САПР NetCracker Professional 3.1

Контрольные вопросы:

1. Дайте определение сети типа «клиент/сервер».
2. Каково назначение универсального коммутатора?
3. Какие функции выполняют устройства CSU/DSU?
4. Назовите типы и параметры трафиков, установленных в созданной двухуровневой сети «клиент/сервер».
5. Какие сведения о работе сети отражаются в Отчете о статистике ее функционирования?
6. Что показывают временные диаграммы использования связи в процессе работы сети?

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.4:

форма рубежного контроля – отчет по лабораторной работе.

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) являются **зачет с оценкой и экзамен,** который проводится в **устной / 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

ПК-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знать: основы и особенности установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности информации	Этап формирования знаний
		Уметь: осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Этап формирования умений
		Владеть: методами установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности 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 профессиональных задач	Знать: средства защиты информации в правоохранительной сфере	Этап формирования знаний
		Уметь: проектировать, внедрять и использовать системы мониторинга средств защиты информации в правоохранительной сфере	Этап формирования умений
		Владеть: навыками проектирования, внедрения и применения системы мониторинга средств защиты информации	Этап формирования навыков и получения опыта
ПК-12	Способен принимать участие в проведении экспериментальных исследований системы защиты	**Знать:** функциональное назначение, технические и конструктивные особенности применения, общие принципы построения и работы	Этап формирования знаний

	информации	исследуемой системы защиты информации.	
		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

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-1, ПК-2, ПК-12	Этап формирования	Теоретический блок вопросов.	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически

	знаний.	Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал	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-1, ПК-2, ПК-12	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
ПК-1, ПК-2, ПК-12	Этап формирования навыков и	Аналитическое задание *(задачи, ситуационные задания, кейсы,*	

	получения опыта.	*проблемные ситуации и т.д.)* Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	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.

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)

Модуль 1 Беспроводные компьютерные сети. Телекоммуникация . (3 семестр)

Теоретический блок вопросов:

1. Классификация беспроводных сетей. Компоненты беспроводных сетей.
2. Платы интерфейса сети. Инфраструктуры беспроводных сетей.
3. Контроллеры доступа. Распределительная система.
4. Управляющие системы. Структура сети.
5. Информационные сигналы. Цифровые сигналы. Аналоговые сигналы.
6. Передача информации через беспроводную сеть. Передача беспроводных сигналов.
7. Беспроводные приемопередатчики. Параметры радиосигналов.
8. Искажение радиочастотного сигнала. Параметры светового сигнала.
9. Преимущества и недостатки световых сигналов. Искажение световых сигналов.
10. Модуляция: подготовка сигналов к передаче. Частотная манипуляция.
11. Фазовая манипуляция. Квадратурная амплитудная модуляция. Расширение спектра.
12. Мультиплексирование с разделением по ортогональным частотам.
13. Сверхширокополосная модуляция.
14. Компоненты беспроводных персональных сетей. Пользовательские устройства.
15. Радиоплаты интерфейса сети. USB-адаптеры. Маршрутизаторы.
16. Системы на основе беспроводных персональных сетей.
17. Технологии беспроводных персональных сетей. Стандарт 802.15.
18. Bluetooth. Компоненты беспроводных локальных сетей.
19. Системы беспроводных локальных сетей. Беспроводные локальные сети предприятий.
20. Технологии беспроводных локальных сетей. Стандарт 802.11. Wi-Fi.
21. Компоненты беспроводных региональных сетей. Мосты.
22. Системы беспроводных региональных сетей. Системы пакетной радиосвязи.
23. Технологии беспроводных региональных сетей. Стандарт 802.16.
24. Компоненты беспроводных глобальных сетей. Пользовательские устройства беспроводных глобальных сетей. Базовые станции.

25. Системы беспроводных глобальных сетей. Беспроводные глобальные сети с сотовой структурой.
26. Технологии беспроводных глобальных сетей.
27. Угрозы безопасности. Мониторинг трафика.
28. Неавторизованный доступ. Отказ в обслуживании.
29. Шифрование. WEP. Виртуальные частные сети.
30. Аутентификация. Уязвимость механизма аутентификации стандарта 802.11. MAC-фильтры.
31. Аутентификация с использованием открытого ключа шифрования.
32. Стандарт 802.1x. Политика безопасности. Стадии оценки.
33. Сеть связи общего пользования. Ведомственные сети связи.
34. Выделенные сети связи. Корпоративные сети связи.
35. Линии связи и их характеристики.
36. Проводные линии связи. Кабельные линии.
37. Характеристики линий связи. Амплитудно-частотная характеристика. Полоса пропускания линии связи. Помехоустойчивость линии связи.
38. Достоверность передачи данных. Аппаратура линий связи.
39. Коммутируемые и выделенные каналы связи.
40. Передача дискретных данных на физическом уровне.
41. Аналоговая модуляция. Цифровое кодирование.
42. Самосинхронизирующие коды. Дискретная модуляция аналоговых сигналов.
43. Асинхронная и синхронная передачи.
44. Передача дискретных данных на канальном уровне.
45. Типы синхронных протоколов канального уровня.
46. Обеспечение достоверности передачи информации.
47. Системы передачи с обратной связью.
48. Алгоритм маршрутизации.
49. Способы маршрутизации.
50. Эффективность алгоритмов маршрутизации. Сравнение способов передачи данных.
51. Виды маршрутизации. Простая маршрутизация. Фиксированная (статическая) маршрутизация.
52. Адаптивная (динамическая маршрутизация). Распределенная адаптивная маршрутизация. Иерархическая маршрутизация.
53. Способы коммутации в ТКС. Коммутация каналов.
54. Преимущества метода коммутации каналов. Коммутация с промежуточным хранением.
55. Понятие сети X.25. Достоинства сетевой технологии X.25.
56. Понятие протокола ретрансляции фреймов.
57. Эффективность технологии FR.
58. Общие сведения о сети ISDN. Проблемы безопасности сети ISDN.
59. Связь удаленного пользователя с локальной сетью корпоративного сетевого центра. Адресация в сетях ISDN. Сети и технологии SDH.
60. Топология сетей SDN.
61. Сети и технологии ATM. Основные особенности ATM-технологии.
62. Спутниковые сети связи.

Модуль 2 Глобальные компьютерные сети. Вычислительные системы. (4 семестр)

Теоретический блок вопросов:

1. Охарактеризуйте назначение и возможности САПР NetnCracker Professional 3.1.
2. Каково назначение мостов?
3. Каково назначение маршрутизаторов?

4. Сколько разновидностей (типов, категорий) мостов и маршрутизаторов содержится в списке Устройств Routers and bridges?
5. Сколько разновидностей базовых маршрутизаторов содержится в списке Backbone routers?
6. Сколько разновидностей базовых маршрутизаторов, изготовленных фирмой Cisco Systems, содержит список Backbone routers?
7.Сколько разновидностей адаптеров локальной сети содержит список LAN adapters?
8.Сколько разновидностей плат адаптеров LAN adapters Ethernet, изготовленных корпорацией 3Com Corp, содержит папка 3Com Corp.?
9. Как создается конфигурация Устройства?
10. Как узнать, какие типы протоколов обмена допускаются для выбранного сменного блока процессора связи системы передачи данных?
11. Сколько предприятий - изготовителей и поставщиков содержится в базе данных Устройств Vendors? Приведите наименования некоторых из них.
12.Перечислите типы линий связи, применяемых при создании ИВС. Какими техническими характеристиками они отличаются друг от друга?
13. Назовите, в каких случаях при создании ЛВС применяются те или иные типы линий связи и сравните их характеристики.
14. Как получить общую информацию об объектах в окне сайта?
15. Как вывести информацию относительно полной сети, какие сведения она содержит?
16. Каковы функциональные возможности анимационного моделирования сети?
17. Что позволяет выявить процесс анимации?
18. Какие параметры сети можно корректировать и выбирать в процессе анимации?
10. Какие сведения о параметрах информационных пакетов могут быть выведены?
20. Сколько и каких типов протоколов содержится в базе данных NetCracker?
21. Каким образом можно добавить, заменить и удалить устройства сетевого оборудования?
22. Как в проекте сети переименовать здания?
23. Каково назначение коммутатора?
24. Каково назначение и состав рабочих станций?
25. Каково назначение концентратора?
26. Что означают понятия «совместимость» и «несовместимость» Устройств сети?
27. Что означает понятие «наращиваемые»Устройства сети?
28. Сколько типов трафиков насчитывается в базе данных САПР NetCracker Professional. Приведите наименования некоторых из них.
29. Что такое “наращиваемые” устройства? Приведите пример
30. Какие типы носителей используются при построении ЛВС?
31. Какие параметры информационного пакета могут быть изменены в САПР NetCracker Professional?
32. Какие изменения можно вносить в проект сети?
33. Какие надписи можно наносить на схему проекта?
34. Дайте определение сети типа «клиент/сервер».
35. Каково назначение универсального коммутатора?
36. Какие функции выполняют устройства CSU/DSU?
37. Назовите типы и параметры трафиков, установленных в созданной двухуровневой сети «клиент/сервер».
38. Какие сведения о работе сети отражаются в Отчете о статистике ее функционирования?
39. Что показывают временные диаграммы использования связи в процессе работы сети?
40. Перечислите типы сетевого оборудования, содержащегося в списках базы данных (БД) САПР NetCracker Professional 3.1
41. Сколько типов сетевых устройств содержится в БД?
42. Сколько типов слотов для сетевых устройств содержится в БД? Какие типы выбраны вами?
43. Сколько стандартных типов связи с портами содержится в БД? Какие типы в вашем проекте?

44. Поясните, на каких участках сети применяются шины типов ESA, PCI, ISA и расшифруйте их названия
45. Что означает понятие «ATM совместимое оборудование»?
46. Каким образом можно ввести вновь разработанное устройство в базу данных пользователя NetCracker Professional 3.1?

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 бакалаврита/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 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 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 (модуля)

5.1.1. Основная литература

1. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491319

2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491949

5.1.2. Дополнительная литература

1. *Новожилов, О. П.* Архитектура ЭВМ и систем в 2 ч. Часть 1 : учебное пособие для вузов / О. П. Новожилов. — Москва : Издательство Юрайт, 2022. — 276 с. — (Высшее образование). — ISBN 978-5-534-07717-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494314
2. *Новожилов, О. П.* Архитектура ЭВМ и систем в 2 ч. Часть 2 : учебное пособие для вузов / О. П. Новожилов. — Москва : Издательство Юрайт, 2022. — 246 с. —

(Высшее образование). — ISBN 978-5-534-07718-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494315
3. *Замятина, О. М.* Вычислительные системы, сети и телекоммуникации. Моделирование сетей : учебное пособие для вузов / О. М. Замятина. — Москва : Издательство Юрайт, 2022. — 159 с. — (Высшее образование). — ISBN 978-5-534-00335-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490257

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) «*Вычислительные системы, сети и телекоммуникации*» 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 рабочей программы дисциплины (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 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:

- 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»).

5.4 Информационно-технологическое обеспечение образовательного процесса по дисциплине (модулю)

5.4.1. Средства информационных технологий

1. Персональные компьютеры;
2. Средства доступа к Интернет;
3. Проектор.
4.

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 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	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским	https://grebennikon.ru

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	«Grebennikon»	домом "Гребенников".	

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

Для изучения дисциплины (модуля) *«Вычислительные системы, сети и телекоммуникации»* в рамках реализации основной профессиональной образовательной программы высшего образования – программы бакалаврита 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, компьютер).

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) *«Вычислительные системы, сети и телекоммуникации»* применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины (модуля) *«Вычислительные системы, сети и телекоммуникации»* предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме деловых и ролевых игр, разбор конкретных ситуаций, психологические тренинги в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

При освоении дисциплины (модуля) *«Вычислительные системы, сети и телекоммуникации»* предусмотрено применением электронного обучения.

Учебные часы дисциплины *«Вычислительные системы, сети и телекоммуникации»* 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.

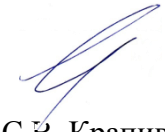
В рамках дисциплины (модуля) *«Вычислительные системы, сети и телекоммуникации»* предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с *направленностью* реализуемой основной профессиональной образовательной программы высшего образования – программы бакалавриата.

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»

Декан факультета
информационных технологий



/ С.В. Крапивка /
«06» июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
СРЕДСТВА ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технологии защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022

Рабочая программа дисциплины (модуля) **«Средства обработки и передачи информации»** 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:
к.т.н. Малиничев Д.М., к.п.н. Мнацаканян О.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) 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) состоит в приобретении студентами знаний теоретических основ по применению специализированных технических средств и общепромышленных измерительных приборов для проведения инструментальной и экспертной оценки наличия технических каналов утечки конфиденциальной информации и степени их влияния на уязвимость объекта информатизации.

Задачи дисциплины (модуля):

- усвоение основных понятий о технических каналах утечки информации и физических принципах их возникновения;
- формирование знаний о стадиях и этапах создания системы защиты от утечки по техническим каналам, типовых средствах защиты;
- овладение практическими навыками разработки систем защиты и обеспечения безопасности;
- развитие знаний об основных технических средствах анализа информационной защищенности.

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

Учебная дисциплина «Средства обработки и передачи информации» реализуется в базовой части основной профессиональной образовательной программы **«Информационная безопасность»** по направлению10.03.01Информационная безопасность (уровень бакалавриата) очной формы обучения.

Изучение дисциплины (модуля) «**Средства обработки и передачи информации**» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Математика», «Физика», «Информатика и информационные технологии в правоохранительной деятельности», «Техническая защита информации».

Изучение дисциплины (модуля) «**Средства обработки и передачи информации**» является базовым для последующего освоения программного материала учебных дисциплин: *Системы контроля и управления доступом, Методы защиты системного программного обеспечения, Методы обнаружения сетевых атак.*

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 компетенций: ПК-1, ПК-2, ПК-12, в соответствии с основной профессиональной образовательной программой **«Информационная безопасность»** по направлению10.03.01Информационна безопасность (уровень бакалавриата) очной формы обучения**.**

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-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-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 практические действия в рамках компетенции ПК-12.ИД-3. Применяет методы анализа практической деятельности и ее результатов в рамках компетенции	**Знать:** функциональное назначение, технические и конструктивные особенности применения, общие принципы построения и работы исследуемой системы защиты информации.
				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.

				Владеть: теоретическими знаниями и навыками по практическому применению соответствующего специализированного оборудования и измерительных приборов для проведении экспериментальных исследований системы защиты информации мероприятий

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 __9__ зачетных единиц.

Вид учебной работы	**Всего часов**	**Семестры**				
		3	4			
Контактная работа обучающихся с педагогическими работниками	**162**	**90**	**72**			
Учебные занятия лекционного типа	34	18	16			
из них: в форме практической подготовки						
Практические занятия						
из них: в форме практической подготовки						
Лабораторные занятия	56	32	24			
из них: в форме практической подготовки						
Иная контактная работа	72	40	32			
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**90**	**54**	**36**			
из них: в форме практической подготовки	*17*	*10*	*7*			
Контроль промежуточной аттестации	**72**	**36**	**36**			
Форма промежуточной аттестации		экзам	экзам			
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**324**	**180**	**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	28	10	*2*	18		4				6		8	
Раздел 1.2	29	11	*2*	18		4				6		8	
Раздел 1.3	29	11	*2*	18		4				6		8	
Раздел 1.4	29	11	*2*	18		4				6		8	
Раздел 1.5	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**												
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**												
Общий объем, часов	**324**	**90**	***17***	**162**		**34**				**56**		**72**	

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 3)							
Раздел 1.1	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 1.2	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 1.3	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 1.4	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 1.5	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**	
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	**90**	**32**		**40**		**18**	

3.2. Методические указания к самостоятельной работе по дисциплине.

РАЗДЕЛ 1. ОСНОВЫ ПОСТРОЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Цель: изучение основ построения телекоммуникационных сетей, их различных видов.

Перечень изучаемых элементов содержания

Теоретическое изучение вопросов, связанных с состоянием современных телекоммуникационных сетей в России и за рубежом.

Вопросы для самоподготовки:

1. **Сети связи общего назначения.**
2. **Транкинговые сети связи.**
3. **Сотовые сети связи.**

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Подвижные сети передачи данных.
2. Стационарные сети передачи данных.
3. Каналы связи.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1: форма рубежного контроля – реферат.

РАЗДЕЛ 2. СЕТИ ПОДВИЖНОЙ СВЯЗИ

Цель: изучение различных видов сетей подвижной связи.

Перечень изучаемых элементов содержания

Теоретическое изучение вопросов, связанных с использованием подвижных сетей передачи данных.

Вопросы для самоподготовки:

1. **Принципы работы базовых станций.**
2. **Принципы работы средств приема/передачи сигналов.**
3. **Задачи, решаемые с помощью перехвата сигналов.**

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Транкинговые системы подвижной радиосвязи.
2. Сотовые системы подвижной радиосвязи.
3. Сети связи 2G, 3G и 4G.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2: форма рубежного контроля – реферат.

РАЗДЕЛ 3. ТЕНДЕНЦИИ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Цель: анализ современных телекоммуникационных сетей и тенденций их развития.

Перечень изучаемых элементов содержания

Теоретическое изучение вопросов, связанных с состоянием современных телекоммуникационных сетей и перспективой их развития.

Вопросы для самоподготовки:

1. Возможности увеличения скорости передачи данных.
2. Сравнение телефонных и интернет сетей.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: реферат.

Примерный перечень тем рефератов:

1. Сети 5G.
2. Сети NGN
3. Сети Wi-Max, Wi-Fi, McWill, GSM.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: 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 дисциплине (модулю) является экзамен**,** 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-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знать: основы и особенности установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности информации	Этап формирования знаний
		Уметь: осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного	Этап формирования умений

		состояния	
		Владеть: методами установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности 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 профессиональных задач	Знать: средства защиты информации в правоохранительной сфере	Этап формирования знаний
		Уметь: проектировать, внедрять и использовать системы мониторинга средств защиты информации в правоохранительной сфере	Этап формирования умений
		Владеть: навыками проектирования, внедрения и применения системы мониторинга средств защиты информации	Этап формирования навыков и получения опыта
ПК-12	Способен 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

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-1, ПК-2, ПК-12	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-1, ПК-2, ПК-12	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-1, ПК-2, ПК-12	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. Первичная сеть связи. Организация и структурная схема первичной сети связи.
2. Основные термины и определения теории коммуникационных сетей.
3. Понятие вторичных сетей. Виды вторичных сетей связи.

4. Понятие первичных сетей. Виды первичных сетей связи.
5. Понятие сетей общего и ограниченного пользования. Виды сетей ограниченного пользования.
6. Понятие абонентских устройств. Виды и типы абонентских устройств.
7. Структурная схема Федеральной сети связи РФ.
8. Взаимосвязанная сеть связи, транспортная сеть, сеть доступа.
9. Первичные преобразователи сигналов в системах связи.
10. Взаимодействие уровней в эталонной модели взаимодействия открытых систем. Изменение структуры передаваемых данных от уровня к уровню.
11. Метод коммутации пакетов, достоинства и недостатки метода. Схема коммутации, состав пакета, фазы установления соединения.
12. Классификация методов коммутации в сетях связи.
13. Метод коммутации каналов, достоинства и недостатки метода. Схема коммутации, достоинства и недостатки метода, фазы установления соединения.
14. Основные способы построения сетей связи.
15. Метод коммутации сообщений с запоминанием: схема коммутации, достоинства и недостатки метода, фазы установления соединения.
16. Уровни эталонной модели взаимодействия открытых систем.
17. Сущность сеансового уровня в эталонной модели взаимодействия открытых систем. Принцип организации диалога в сети.
18. Органы стандартизации и сертификации в сфере связи и телекоммуникаций. Цели и задачи стандартизации и сертификации систем связи.
19. Этапы и стратегии перевода телефонных сетей связи с аналоговых на цифровые. Преимущества и недостатки сетей обоих типов.
20. Нерайонированные городские телефонные сети: структурная схема, свойства, применение, ёмкость.
21. Городские телефонные сети с узлами исходящих и входящих сообщений: структурная схема, особенности, ёмкость.
22. Городские телефонные сети с узлами входящих сообщений: структурная схема, особенности, ёмкость.
23. Принципы построения и структурная схема внутризоновых телефонных сетей.
24. Районированные городские телефонные сети: структурная схема, организация, свойства, применение, ёмкость.
25. Принципы и структурная схема построения сельских телефонных сетей.
26. Сравнительный анализ цифровых и аналоговых сетей связи. Структурная организация цифровых городских телефонных сетей.
27. Структура общегосударственной системы автоматической телефонной связи.
28. Устройство и принцип работы электронного телефонного аппарата. Принцип тонального набора номера.
29. Классификация и параметры коммутационных приборов.
30. Состав и базовая структурная схема типовой сети абонентского доступа.
31. Обобщённая структурная схема коммутационной системы: состав и оборудование.
32. Организация и структурная схема междугородных телефонных сетей.
33. Элементная база систем коммутации, коммутационные приборы и коммутационные поля. Циклы (фазы) работы коммутационных приборов.
34. Физические и энергетические характеристики звуковых сигналов. Звуковое поле.
35. Устройство телефонного аппарата с импульсным набором номера. Принцип импульсного набора номера.
36. Устройство и принцип действия коммутационных приборов типа «реле», «искатель», «соединитель».
37. Коммутационные поля. Структура коммутационного поля. Однозвенная и двухзвенная ступени искания.

38. Способы управления установлением соединения в телефонных сетях.
39. Ступени искания в коммутационных полях: схемы концентрации, расширения, смешивания.
40. Интерфейсы цифровых систем коммутации.
41. Управляющие устройства в телефонных сетях. Цели и задачи управления в сетях связи.
42. Функциональная архитектура цифровых систем коммутации: состав абонентского и группового оборудования.
43. Ступени искания: свободное искание, абонентское искание, групповое искание.
44. Последовательность установления внутристанционного соединения.
45. Характеристики речевых сигналов. Слуховые ощущения человека. Параметры речи.
46. По каким признакам можно классифицировать системы коммутации?
47. Какова функциональная архитектура современной ЦСК?
48. Что такое интерфейс?
49. На какие типы подразделяются интерфейсы ЦСК?
50. Какие виды оборудования входят в состав ЦСК?
51. Какое оборудование используется для доступа к ЦСК?
52. Дать характеристику функций BORSCHT
53. На какие типы подразделяются системы управления ЦСК по способу управления установлением соединения?
54. В чем заключаются достоинства и недостатки различных типов систем управления?
55. На какие типы подразделяются системы управления ЦСК по способу взаимодействия УУ?
56. На какие основные фазы делится цикл работы УУ? Какие действия выполняются на каждой фазе работы?
57. В чем сущность пространственной коммутации?
58. В чем сущность временной коммутации?
59. Каковы особенности ЦКП?
60. По каким признакам классифицируются ЦКП?
61. Что такое алгоритмическое и программное обеспечение?
62. На какие виды делится ПО ЦСК?
63. Каковы основные принципы построения ПО ЦСК?
64. Какова последовательность этапов проектирования ПО ЦСК? Какие виды работ осуществляются на каждом этапе?
65. Что такое постоянные данные?
66. Что такое оперативные данные?
67. Какими возможностями обладают современные ЦСК?
68. Каким модулем аппаратно реализованы узел коммутации в ЦСК Si 2000.V5?
69. Какими модулями аппаратно реализованы узлы доступа в ЦСК Si 2000.V5?
70. Какие типы аппаратных средств входят в состав оборудования ЦСК EWSD?
71. Какие функции выполняет координационный процессор ЦСК EWSD?
72. На какие основные части разделено оборудование AXE-10?
73. Из каких подсистем состоит оборудование ЦСК AXE-10?
74. На какие группы разделены терминальные модули оборудования ЦСК S-12?
75. Пояснить структуру терминального модуля ЦСК S-12.
76. Что такое сигнализация протокол сигнализации?
77. Какие области применения сигнализации включает в себя обслуживание вызова?
78. На какие группы подразделяются сигналы, передаваемые по телефонным каналам?
79. Какие коды используются в существующих системах сигнализации?
80. Пояснить организацию взаимодействия оконечного устройства системой с коммутации.
81. Какие способы набора номера используются на телефонной сети?
82. На какие классы делятся системы межстанционной сигнализации?
83. В чем сущность метода реализации систем сигнализации «из конца в конец»?
84. В чем сущность метода реализации систем сигнализации «от звена к звену»?

85. Пояснить цикловая структура цифрового потока в стандарте ИКМ-30?
86. Пояснить, каким образом, организуется передача сигнальной информации системе сигнализации 2ВСК?
87. По каким признакам классифицируются протоколы сигнализации токами тональных частот?
88. Назначение сети ОКС№7?
89. Из каких основных элементов состоит сеть ОКС№7?
90. В каких режимах может работать сеть ОКС№7?
91. называются пакеты данных, передаваемых по сети ОКС№7?
92. Как называется СЕ, которая используется для передачи сигнальной информации, формируемой подсистемами пользователей и управлением соединением сигнализации?
93. Как называется СЕ, которая передается в звено сигнализации при отсутствии значащей сигнальной единицы и состояния звена сигнализации?
94. Как называется СЕ, которая передается в звено сигнализации при отсутствии значащей сигнальной единицы и состояния звена сигнализации?
95. Как называется СЕ, которая используется для контроля состояния звена сигнализации?
96. Пояснить процесс передачи сигнальных единиц.
97. Что такое система распределения информации?
98. Что является объектом изучения теории телетрафика?
99. Что является предметом изучения теории телетрафика7
100. Какие основные задачи решает теория телетрафика?
101. Что такое поток вызовов?
102. Какие потоки вызовов называются случайными?
103. Какие потоки вызовов называются детерминированными?
104. Что такое параметр потока?
105. Что такое интенсивность потока?
106. В чем заключается свойство стационарности случайного потока?
107. В чем заключается свойство ординарности случайного потока?
108. Каким законом описывается длительность обслуживания вызова?
109. Что такое дисциплина обслуживания потоков вызовов?
110. Какие системы относятся к системам с явными потерями?
111. Какие системы относятся к системам с условными потерями?
112. Каким способами могут обслуживаться задержанные вызовы?
113. Что такое телефонная нагрузка?
114. На какие виды подразделяется телефонная нагрузка?
115. Что такое интенсивность нагрузки?
116. В чем измеряется интенсивность нагрузки?
117. Каковы достоинства беспроводных сетей?
118. На какие виды делятся системы подвижной связи?
119. На какие виды делятся ССПС по форме представления сигнала в разговорном канале?
120. На какие виды делятся ССПС по диапазону частот?
121. На какие виды делятся ССПС по виду множественного доступа?
122. Из каких подсистем состоит ССПС?
123. Какие функции выполняют подсистемы ССПС?
124. Какие базы данных используются при обслуживании вызова в ССПС?
125. Что такое аутентификация?
126. Что такое идентификация?
127. Перечислить основные этапы процесса установления соединения в ССПС.
128. Что такое множественный доступ?
129. В чем сущность множественного доступа с частотным разделением каналов FDMA?
130. В чем сущность множественного доступа с временным разделением каналов TDMA?
131. В чем сущность множественного доступа с кодовым разделением каналов CDMA?

132. В чем сущность принципа повторного использования частот?
133. Чем вызвана необходимость применения повторного использования частот?
134. Что такое кластер?
135. Что такое защитный интервал?
136. Как определяется величина защитного интервала?
137. Какие виды служб относятся к службам документальной электросвязи?
138. Какие службы относятся к телематическим?
139. На какие виды делятся телеграфные сети?
140. Пояснить принцип факсимильной передачи сообщений.
141. В чем отличие абонентских и клиентских служб?
142. Какие услуги предоставляет клиентская служба Бюрофакс?
143. К каким службам относится служба Видеотекст?
144. Какие услуги предоставляет служба Видеотекст?
145. По каким основным признакам можно классифицировать компьютерные сети?
146. Какие компьютерные сети называются локальными?
147. Какие компьютерные сети называются глобальными?
148. Что такое топология сети?
149. Какие основные топологии применяются при построении локальных сетей?
150. Что такое LAN-телефониия?
151. Что такое шлюз?
152. Чем вызвана необходимость создания ЕСДЭС?
153. Пояснить структуру ЕСДЭС.
154. Какие функции выполняют многофункциональные терминалы?
155. Какие виды устройств могут подключаться к многофункциональному терминалу?
156. Назначение цифровой сети с интеграцией обслуживания?
157. В чем заключаются особенности ЦСИО?
158. Какие виды каналов используются для организации доступа абонентов ЦСИО к ЦСК?
159. На какой скорости осуществляется базовый доступ абонентов ЦСИО к ЦСК?
160. На какой скорости осуществляется первичный доступ абонентов ЦСИО к ЦСК?
161. Какие услуги ЦСИО относятся к интерактивным?
162. Какие услуги ЦСИО относятся к широковещательным?
163. Назначение интеллектуальной сети?
164. Пояснить базовую архитектуру интеллектуальной сети?
165. Какой статус может иметь интеллектуальная сеть?
166. Какие коды в планах нумерации выделены для интеллектуальной сети?
167. Пояснить структуру номера для федеральной интеллектуальной сети.
168. Какие аспекты конвергенции рассматриваются в телекоммуникациях?
169. Что предполагает конвергенция услуг телефонии и передачи данных?
170. Что предполагает конвергенция фиксированных и подвижных сетей?
171. Что такое инфокоммуникационная услуга?
172. Какие требования предъявляются к перспективным сетям?

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

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

5.1.1. Основная литература

1. *Дибров, М. В.* Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491319
2. *Дибров, М. В.* Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491949

5.1.2. Дополнительная литература

1. *Новожилов, О. П.* Архитектура ЭВМ и систем в 2 ч. Часть 1 : учебное пособие для вузов / О. П. Новожилов. — Москва : Издательство Юрайт, 2022. — 276 с. — (Высшее образование). — ISBN 978-5-534-07717-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494314
2. *Новожилов, О. П.* Архитектура ЭВМ и систем в 2 ч. Часть 2 : учебное пособие для вузов / О. П. Новожилов. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-07718-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494315

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) «Средства обработки и 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 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) **«Средства обработки и передачи информации»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки **«10.03.01Информационна 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) **«Средства обработки и передачи информации»** 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) **«Средства обработки и 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)
МЕТОДЫ ЗАЩИТЫ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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) **«Методы защиты системного программного обеспечения»** 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:
к.т.н. Сиротский А.А., ст. преподаватель Мальцев Н.В.

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

(подпись)

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 Н.П. Третьяков
информатики РГСУ

(подпись)

Согласовано И.Г. Маляр
Научная библиотека, директор

(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 и практических навыков в области организации и ведении средств антивирусной защиты информационных ресурсов программного обеспечения предприятий, оценки информационных рисков; планирования мер по антивирусной защите; реализации и внедрения комплексной системы антивирусной защиты.

Задачи дисциплины (модуля) «Методы защиты системного программного обеспечения» являются:

1. Подготовка к решению задач, связанных с разработкой и внедрением систем антивирусной защиты;
2. Формирование навыков самостоятельного проведения процедур анализа и оценки рисков информационной безопасности;
3. Формирование навыков выполнения анализа технологий обеспечения антивирусной защиты программного обеспечения организации;
4. Формирование навыков разработки внутренних нормативных документов организации в области обеспечения антивирусной защиты.

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

Учебная дисциплина «Методы защиты системного программного обеспечения» реализуется в разделе дисциплина по выбору, вариативной части основной профессиональной образовательной программы «Информационная безопасность» по направлению«10.03.01 «Информационная безопасность» очной формы обучения.

Изучение дисциплины (модуля) «Методы защиты системного программного обеспечения» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Физика», «Теория информационной безопасности и методология защиты информации», «Организационная защита информации», «Технические средства охраны»

Изучение дисциплины (модуля) «Методы защиты системного программного обеспечения ». является базовым для последующего освоения программного материала дисциплины (модуля) «Комплексная защита объектов информатизации»

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-1, ПК-2 в соответствии с основной профессиональной программой «Информационная безопасность» по направлению«10.03.01Информационная 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 компетенции**	**Результаты обучения**
	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.

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 4 зачетных единицы (144 часа).

Вид учебной работы	Всего часов	Семестры				
		7				
Контактная работа обучающихся с педагогическими работниками	**72**	**72**				
Учебные занятия лекционного типа	16	16				
из них: в форме практической подготовки						
Практические занятия	16	16				
из них: в форме практической подготовки						

Лабораторные занятия	8	8				
из них: в форме практической подготовки						
Иная контактная работа	32	32				
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**36**	**36**				
из них: в форме практической подготовки	*7*	*7*				
Контроль промежуточной аттестации	**36**	**36**				
Форма промежуточной аттестации		экзам				
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**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 7)													
Раздел 1.1	27	9	*2*	18		4		4		2		8	
Раздел 1.2	27	9	*2*	18		4		4		2		8	
Раздел 1.3	27	9	*2*	18		4		4		2		8	
Раздел 1.4	27	9	*1*	18		4		4		2		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**144**	**36**	***7***	**72**		**16**		**16**		**8**		**32**	

Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**144**	**36**	***7***	**72**		**16**		**16**		**8**		**32**	

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 7)							
Раздел 1.1	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 1.2	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 1.3	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 1.4	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	**36**	**12**		**16**		**8**	

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

РАЗДЕЛ 1.1 ОБЩИЕ ХАРАКТЕРИСТИКИ КОМПЬЮТЕРНЫХ ВИРУСОВ

Цель: Ввести понятия компьютерные вирусы, программы-агенты, макровирусы, файловые вирусы, загрузочные вирусы.

Перечень изучаемых элементов содержания

Понятие компьютерные вирусы. Классификация компьютерных вирусов. Программы-агенты. Сетевые вирусы. «Черви», «трояны». Макровирусы. Файловые вирусы. Загрузочные вирусы. Пути проникновения вируса в компьютер. Вредоносные действия вирусов. Ущерб и угрозы безопасности, связанные с вредоносными программами. Описание вредоносных действий вирусов. Вирусы Zero-day Руткиты, работающие в user-mode. Атаки на GUI. Методики загрузки информации из Интернета. Троянские программы категории Trojan-Downloader. DDoS атаки. Перегрузка каналов связи. Атака с помощью переполнения пакетами SYN.

Вопросы для самоподготовки:

1. Троянские программы категории Trojan-Downloader. DDoS атаки.
2. Перегрузка каналов связи.
3. Атака с помощью переполнения пакетами SYN.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.1

Форма практического задания: лабораторный практикум.

Лабораторная работа 1. «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 РАЗДЕЛУ 1.1: форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 1.2. ВРЕДОНОСНЫЕ ПРОГРАММЫ

Цель: изучение принципов создания системы управления информационной безопасностью.

Перечень изучаемых элементов содержания

Признаки, характерные для зараженных компьютеров. Явные, косвенные и скрытые проявления вредоносных программ. Способы поиска проявлений вредоносных программ. Признаки заражения сайтов вредоносным ПО. Заражение с помощью методов простой переадресации. Антируткиты. Использование ловушек для антируткитов. Основные методы защиты вредоносных программ от удаления: watchdog, метод троянского потока, блокировка доступа к файлу, пересоздание ключей реестра.

Вопросы для самоподготовки:

1. Технологии блокировки работы антивирусных продуктов.
2. Защита от обнаружения и снятия перехватов.
3. Поведенческое противодействие.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 1.2

Форма практического задания: лабораторный практикум.

Лабораторная работа 2. «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 РАЗДЕЛУ 1.2: форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 2.1. ОБНАРУЖЕНИЕ И ПРОФИЛАКТИКА ВИРУСОВ

Цель: изучение методик разработки документов по информационной безопасности.

Перечень изучаемых элементов содержания

Технологии сигнатурного анализа (реактивной защиты). Технологии вероятностного анализа (проактивной защиты). Эвристический анализ. Метод контроля активности HIPS - размещаемая система предотвращения вторжений. Виртуальные технологии. VIPS – метод контроля активности. Поведенческий анализ. Поведенческие анализаторы. Анализ контрольных сумм. Методы ограничения выполнения операций. Песочница (sandbox).

Методы контроля целостности ПО и ОС. Сканер целостности. Периодическое сканирование при запуске. Экран файловой системы. Экран почты. Веб-экран. Экран P2P. Экран интернет-чатов. Сетевой экран. Экран сценариев. Экран поведения.

Вопросы для самоподготовки:

1. Выборочное или полное сканирование.
2. Сканирование с помощью резидентного модуля.
3. Препятствие проникновению вредоносного ПО в систему.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.1

Форма практического задания: лабораторный практикум.

Лабораторная работа 3. «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 РАЗДЕЛУ 2.1: форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 2.2. АНТИВИРУСНЫЕ СРЕДСТВА И СИСТЕМЫ.

Цель: изучение методологии оценки рисков информационной безопасности.

Перечень изучаемых элементов содержания

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

Вопросы для самоподготовки:

Общие характеристики Антивируса Касперского.

1. Принципы работы компонента Анти-Хакер в Антивирусе Касперского.
2. Приоритезация правил в Анти-Хакере в Антивирусе Касперского. Доверенная зона и локальная сети.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.2

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 РАЗДЕЛУ 2.2: форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 2.3. КОМПЛЕКСНАЯ СИСТЕМА АНТИВИРУСНОЙ ЗАЩИТЫ

Цель: изучение методологии оценки рисков информационной безопасности.

Перечень изучаемых элементов содержания

Модули, содержащие компоненты проактивной защиты, компонент Анти-Шпион в Антивирусе Касперского. Тестовые вирусы. Лечение инфицированных файлов. Файловый Антивирус. Помещение файлов на карантин. Передача вируса по E-mail, почтовый Антивирус. Протоколы, поддерживающиеся Почтовым антивирусом в Антивирусе Касперского. Пути внесения изменений в настройки унаследованной задачи. Использование лицензионного ключа в приложениях Лаборатории Касперского.

Назначение, содержание КСАЗ. Уровень защиты шлюзов. Защита почтовых систем. Уровень защиты серверов и рабочих станций. Классы защищенности средств антивирусной защиты. ГОСТ Р 51188-98. Приказ ФСТЭК России от 20 марта 2012 г. N 28 «Требования к средствам антивирусной защиты». Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами».

Вопросы для самоподготовки:

1. Типы архивов, проверяемые и вылечиваемые задачей проверки по требованию в Антивирусе Касперского.
2. Способы применения политик на клиентских компьютерах существуют в Kaspersky Administration Kit.
3. Задачи, не наследуемые подчиненным Сервером администрирования.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 2.3

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 РАЗДЕЛУ 2.3: форма рубежного контроля – отчет по лабораторной работе.

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,** 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-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических	Знать: основы и особенности установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности информации	Этап формирования знаний
		Уметь: осуществлять установку, настройку и эксплуатацию компонентов технических	Этап формирования умений

	средств защиты информации	систем обеспечения безопасности информации и поддержку их работоспособного состояния	
		Владеть: методами установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности 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 профессиональных задач	Знать: средства защиты информации в правоохранительной сфере	Этап формирования знаний
		Уметь: проектировать, внедрять и использовать системы мониторинга средств защиты информации в правоохранительной сфере	Этап формирования умений
		Владеть: навыками проектирования, внедрения и применения системы мониторинга средств защиты информации	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-1; ПК-2	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-1; ПК-2;	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;
ПК-1; ПК-2;	Этап формирования навыков и	Аналитическое задание *(задачи, ситуационные*	

	получения опыта.	*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.	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.

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

Форма промежуточного контроля знаний -экзамен в устной форме

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

1. Понятие «компьютерные вирусы». Классификация компьютерных вирусов.
2. Программы-агенты. Сетевые вирусы. «Черви», «трояны».
3. Макровирусы. Файловые вирусы. Загрузочные вирусы.
4. Пути проникновения вируса в компьютер.
5. Вредоносные действия вирусов. Ущерб и угрозы безопасности, связанные с вредоносными программами.
6. Примеры вредоносных вирусов и их действий: вирусы Zero-day, руткиты, работающие в user-mode , Kernel-mode руткит, Boot-рутикты, атаки на GUI, методики загрузки информации из Интернета, троянские программы категории Trojan-Downloader.
7. DDoS атаки, перегрузка каналов связи, атака с помощью переполнения пакетами SYN.
8. Признаки, характерные для зараженных компьютеров.
9. Явные, косвенные и скрытые проявления вредоносных программ.
10. Способы поиска проявлений вредоносных программ.
11. Признаки заражения сайтов вредоносным ПО.
12. Заражение с помощью методов простой переадресации.

13. Технологии сигнатурного анализа (реактивной защиты);
14. Эвристический анализ; Метод контроля активности HIPS - размещаемая система предотвращения вторжений.
15. Виртуальные технологии. VIPS – метод контроля активности
16. Поведенческий анализ; Поведенческие анализаторы. Анализ контрольных сумм.
17. Методы ограничения выполнения операций; Песочница (sandbox)
18. Методы контроля целостности ПО и ОС. Сканер целостности.
19. Противодействие вредоносных программ обнаружению.
20. Защита от обнаружения и снятия перехватов.
21. Поведенческое противодействие. Антируткиты.
22. Использование ловушек для антируткитов.
23. Технологии блокировки работы антивирусных продуктов.
24. Основные методы защиты вредоносных программ от удаления: watchdog,
25. Метод троянского потока, блокировка доступа к файлу, пересоздание ключей реестра.
26. Профилактика и обнаружение вирусов в системе.
27. Периодическое сканирование при запуске. Выборочное или полное сканирование. Сканирование с помощью резидентного модуля.
28. Классификации антивирусных средств.
29. Препятствие проникновению вредоносного ПО в систему. Устранение вирусов из компьютерной системы.
30. Пример защитных экранов антивируса Avast .
31. Антивирусные программы: антивирусные блокировщики; ревизоры; полифаги; полифаги-мониторы.
32. Антивирусные комплексы: комплекс для защиты рабочих станций; комплекс для защиты файловых серверов; комплекс для защиты почтовых систем; комплекс для защиты шлюзов.
33. Основные функции антивирусных средств: обнаружение вирусов, дезактивация вируса, лечение, прививка. Примеры антивирусных средств.

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

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 среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433

5.1.2. Дополнительная литература.

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524

2. *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/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
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 защиты системного программного обеспечения**» 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

Обучающиеся 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 дисциплине (модулю)

Для изучения дисциплины (модуля) в рамках реализации основной профессиональной образовательной программы «Информационная безопасность» по направлению10.03.01Информационная безопасность очной формы обучения 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 дисциплине «Системы контроля управления доступом» проводятся 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 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).

5.7. Образовательные технологии

При реализации дисциплины (модуля) **«Методы защиты системного программного обеспечения»** применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение дисциплины (модуля) **«Методы защиты системного программного обеспечения»** 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) «**Методы защиты системного программного обеспечения»** предусмотрено применением электронного обучения.

Учебные часы дисциплины «**Методы защиты системного программного обеспечения»** 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) 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) СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Организация и технологии защиты информации

Уровень образования
ВЫСШЕЕ ОБРАЗОВАНИЕ - УРОВЕНЬ БАКАЛАВРИАТА

Наименование квалификации
БАКАЛАВР

Очная форма обучения

Москва 2022 г.

Рабочая программа дисциплины (модуля) **«Системы контроля и управления доступом»** 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:
к.т.н. Сиротский А.А., ст. преподаватель Мальцев Н.В.

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

(подпись)

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 Н.П. Третьяков
информатики РГСУ

(подпись)

Согласовано И.Г. Маляр
Научная библиотека, директор

(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 и практических навыков по применению систем контроля и управления доступом (СКУД), как функциональной компонентов защиты объектов информатизации от несанкционированного проникновения нарушителей, в том числе с целью деструктивного воздействия на объекты защиты.

Задачи дисциплины (модуля) «Системы контроля и управления доступом» являются:

1) *Формирование теоретических знаний и практических* навыков в сфере профессиональной деятельности по обеспечению информационной безопасности , связанных с применением средств и методов физической защиты объектов информатизации, применительно к СКУД , от несанкционированного проникновения нарушителей и угроз деструктивного воздействия антропогенного и техногенного характера.
2) *Формирование теоретических знаний и практических* навыков по обоснованному выбору функциональных компонентов СКУД, обеспечивающих защиту реального объекта информатизации.
3) Теоретическое и практическое изучение вопросов, связанных с разработкой концепции и внедрением систем контроля и управления доступом для физической защиты информационных ресурсов и информационных систем от несанкционированного проникновения и угроз деструктивного воздействия на объекты защиты.

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

Учебная дисциплина «Системы контроля и управления доступом» реализуется в разделе дисциплина по выбору, вариативной части основной профессиональной образовательной программы «Информационная безопасность» по направлению«10.03.01Информационная безопасность» очной формы обучения.

Изучение дисциплины (модуля) «Системы контроля и управления доступом» базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: «Физика», «Теория информационной безопасности и методология защиты информации», «Организационная защита информации», «Технические средства охраны»

Изучение дисциплины (модуля) «Системы контроля и управления доступом ». является базовым для последующего освоения программного материала дисциплины (модуля) «Комплексная защита объектов информатизации»

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-1, ПК-2 в соответствии с основной профессиональной программой «Информационная безопасность» по направлению«10.03.01Информационная 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 компетенции**	**Результаты обучения**
	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.

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 4 зачетных единиц.

Вид учебной работы	Всего часов	Семестры				
		7				
Контактная работа обучающихся с педагогическими работниками	**72**	**72**				
Учебные занятия лекционного типа	16	16				
из них: в форме практической подготовки						
Практические занятия	16	16				
из них: в форме практической подготовки						

Лабораторные занятия	8	8				
из них: в форме практической подготовки						
Иная контактная работа	32	32				
из них: в форме практической подготовки						
Самостоятельная работа обучающихся	**36**	**36**				
из них: в форме практической подготовки	*7*	*7*				
Контроль промежуточной аттестации	**36**	**36**				
Форма промежуточной аттестации		экзам				
ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЧАСАХ	**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 7)													
Раздел 1.1	27	9	*2*	18		4		4		2		8	
Раздел 1.2	27	9	*2*	18		4		4		2		8	
Раздел 1.3	27	9	*2*	18		4		4		2		8	
Раздел 1.4	27	9	*1*	18		4		4		2		8	
Контроль промежуточной аттестации (час)	**36**												
Общий объем, часов	**144**	**36**	***7***	**72**		**16**		**16**		**8**		**32**	

Форма промежуточной аттестации	**экзамен**												
Общий объем, часов	**144**	**36**	***7***	**72**		**16**		**16**		**8**		**32**	

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 7)							
Раздел 1.1	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 1.2	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 1.3	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 1.4	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	**36**	**12**		**16**		**8**	

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

Раздел 1. Системы физической защиты объектов информатизации

Раздел 1.1 Основы построения системы физической защиты объекта информатизации, с учетом требований нормативных и методических документов различных уровней.

Цель:
Изучение нормативных документов, регламентирующих методы и средства физической защиты объектов информатизации, и основных принципов построения системы охраны объектов от несанкционированного проникновения и деструктивных воздействий.

Перечень изучаемых элементов содержания

1. Основной понятийный аппарат и нормативные документы изучаемой дисциплины.
2. Характеристика основных угроз личности, информации и имуществу, которые призваны нейтрализовать, или минимизировать системы физической защиты.
3. Состав, структура и назначение элементов комплексной системы защиты объектов инженерно-техническими средствами.
4. Основные принципы построения системы физической защиты объекта информатизации.
5. Интегрированные системы охраны (ИСО).
6. Деструктивные средства защиты носителей информации от несанкционированного попадания к нарушителям.

Вопросы для самоподготовки:

1. Классификация и характеристики средств и методов физической защиты объекта информатизации.
2. Зоны и рубежи охраны. Особенности построения.
3. Средства инженерно- технической укрепленности и технические средства охраны объекта информатизации. Назначение и функциональное различие по решаемым задачам.
4. Состав и особенности различных видов интеграции технических средств охраны. Классификация аппаратно- программных и технических средств легального физического уничтожения информации на электронных и бумажных носителях.

Практическое задание к разделу 1.1

Форма практического задания: Выполнение практических мероприятий по моделированию угроз, обоснованному выбору специализированного оборудования и грамотного его применения для защиты объектов информатизации.

Примерные темы практических занятий.

1. Модель нарушителя для заданных исходных условий функционирования коммерческого предприятия, связанных с несанкционированным проникновением нарушителя к объекту информатизации.
2. Модель угроз, для заданных исходных условий функционирования коммерческого предприятия, связанных с несанкционированным проникновением нарушителя к объекту информатизации.

3. Сравнительный анализ различных типов ИСО на коммерческом предприятии, с учетом экономических, технических, потребительских, критериев, а также устойчивости оборудования к воздействующим деструктивным и дестабилизирующим факторам.

Отчет по результатам проведения практического занятия.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.1 форма рубежного контроля – Тестовый опрос

Раздел 1.2 Состав , структура построения и основные характеристики систем контроля и управления доступом

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, классификация и состав СКУД
2. Требования к системам контроля управления доступом
3. Средства идентификации и аутентификации
4. Особенности построения СКУД для различных объектов.
5. Функциональные особенности программного обеспечения для различных объектов.

Вопросы для самоподготовки:

1. Классификация способов идентификации в СКУД.
2. Классификация СКУД по архитектуре и способу управления.
3. Классификация преграждающих устройств.

Практическое задание к разделу 1.2

Форма практического задания:

Выполнение практических занятий по изучению принципов построения и функциональных особенностей СКУД, эксплуатируемых в условиях предприятий различных размеров и форм собственности

Примерные темы практических занятий.

1. Практическое изучение, конструктивных и функциональных особенностей построения СКУД.
2. Практическое изучение средств верификации, аутентификации и идентификации личности и транспортных средств на КПП предприятия.
3. Практическое изучение структуры обеспечения пропускного режима на предприятии с применением СКУД.

Отчет по результатам проведения практического занятия.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.2 форма рубежного контроля – Тестовый опрос

Раздел 1.3 Методы и средств биометрической идентификации

Цель: Изучение конструктивных особенностей и принципов построения средств идентификации личности на основе биометрических признаков.

Перечень изучаемых элементов содержания

1. Классификация методов биометрической идентификации.
2. Конструктивные особенности построения систем идентификации личности на основе биометрических признаков.
3. Примеры защиты устройств биометрической идентификации от случайных или преднамеренных ложных срабатываний.

Вопросы для самоподготовки:

1. Конструктивные особенности современных средств идентификации личности на основе биометрических признаков.
2. Конструктивные особенности считывателей биометрических признаков

Практическое задание к разделу 1.3

Форма практического задания: Выполнение практических мероприятий по изучению основных принципов и критериев, заложенных с систему электронной идентификации личности на основе биометрических признаков.

Примерные темы практических занятий.

1. Практическое и аналитическое изучение построения считывателя идентификационных признаков на основе папиллярного рисунка кожного покров пальцев рук.
2. Практическое и аналитическое изучение построения считывателя идентификационных признаков на основе пространственного анализа геометрии рук и лица.

Отчет по результатам проведения практического занятия.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.3 форма рубежного контроля – Тестовый опрос

Раздел 1.4 Методы и средства идентификации по вещественному и запоминаемым кодам.

Цель: Изучение конструктивных особенностей и принципов построения технических средств идентификации личности на основе вещественного и запоминаемых кодов.

Перечень изучаемых элементов содержания

1. Классификация идентификаторов и считывателей, использующих вещественный код.
2. Методы и средства идентификации на основе PIN-кода.
3. RFID- технология.
4. Особенности выбора и применения считывающих устройств, в зависимости от условий применения.

Вопросы для самоподготовки.

1. Области применения идентификаторов на основе RFID- технологий.
2. Особенности применения идентификаторов на основе вещественного кода.
3. Защита идентификации с использованием запоминаемого кода

Практическое задание к разделу 1.3

Форма практического задания: Выполнение практических мероприятий по изучению методов и средств идентификации личности на основе вещественного и запоминаемого кодов.

Примерные темы практических занятий.

1. Практическое и изучение конструктивных параметров и защищенности контактных и бесконтактных идентификаторов на основе вещественного кода.
2. Практическое и изучение конструктивных параметров и защищенности бесконтактных идентификаторов на основе RFID- технологии.

Отчет по результатам проведения практического занятия.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 1.3 форма рубежного контроля – Тестовый опрос

Раздел 2. **Преграждающие устройства СКУД для обеспечения санкционированного прохода.**

Раздел 2.1
Преграждающие устройства СКУД для обеспечения санкционированного прохода.

Цель: Изучение преграждающих устройств, как компонентов СКУД, обеспечивающих управляемый и контролируемый проход и проезд на охраняемую территорию.

Перечень изучаемых элементов содержания

1. Классификация преграждающих устройств, как исполнительных элементов СКУД.
2. Электрические замки и защелки
3. Турникеты
4. Шлюзовые кабины
5. Автоматические и автоматизированные шлагбаумы
6. Электроуправляемые ворота и калитки.

Вопросы для самоподготовки.

1. Классификация и устройство электроуправляемых замков и защелок , как исполнительных устройств СКУД.
2. Классификация и особенности применения турникетов и шлюзовых кабин на КПП предприятия.
3. Классификация и особенности применения автоматических шлагбаумов.

Примерные темы практических занятий.

1. Практическое изучение, конструктивных особенностей электроуправляемых замков и защелок, применяемых в СКУД.
2. Практическое изучение, устройства поясных и полноростовых турникетов, с учетом их устойчивости к внешним случайным и преднамеренным силовым воздействиям.
3. Практическое изучение конструкции автоматических и автоматизированных шлагбаумов, с учетом климатических условий и устойчивости к внешним преднамеренным силовым воздействиям.
4. Практическое изучение конструкции электроуправляемые ворот и калиток, с учетом климатических условий и устойчивости к внешним преднамеренным силовым воздействиям.

Отчет по результатам проведения практического занятия.

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 2.2 форма рубежного контроля – Тестовый опрос

Раздел 2.2 Прегражданющие устройства СКУД для предотвращения деструктивных угроз криминальной и террористической направленности.

Цель: Изучение специализированных компонентов СКУД, обеспечивающих предотвращения попадания на территорию предприятия **материалов , оборудования и транспортных средств , которые могут быть использованы для деструктивных криминальных или террористических воздействий на персонал, информационные ресурсы и системы, а так же материальные ценности.**

Перечень изучаемых элементов содержания

1. Классификация досмотрового и поискового оборудования, используемого в составе комплексов СКУД
2. Основные типы металлоискателей и основной принцип работы.
3. Организационно- технические и тактические методы использования СКУД для защиты информационных систем от деструктивного преднамеренного силового электромагнитного воздействие .
4. Антитеррористические прегражданющие системы, как специализированные компоненты СКУД..

Примерные темы практических занятий.

1. Ручные и стационарные металлоискатели и газоанализаторы.
2. Досмотровые ренгенотелевизионные установки.
3. **Применения СКУД для пространственного и временного контроля перемещения посетителей и персонала.**
4. Антитеррористические прегражданющие системы.

Раздел 3. Системы контроля и управления доступом

Раздел 1.5 Системы контроля и управления доступом

Цель: Изучение средств и тактических методов защиты объектов информатизации от несанкционированного проноса, провоза и других подобных процессов на территорию защищаемого предприятия материалов и оборудования, которые могут быть использованы для деструктивных воздействий на персонал, информационные ресурсы и системы, а так же материальные ценности.

Перечень изучаемых элементов содержания

1. Изучение основных каналов преднамеренного силового электромагнитного воздействие на объекты информатизации (ПД ЭМВ).
2. Практическое изучения функциональных возможностей и методологии работы технических средств обработки, отображения и анализа видеосигнала, поступающего от видеокамер системы охранного телевидения (СОТ), как

компонента антитеррористической защищенности **персонала, информационных ресурсов и системы, а так же материальных ценностей.**

3. Практическое изучения функциональных возможностей и методологии работы антитеррористических досмотровых средств.
4. Практическое изучения функциональных возможностей и методологии работы антитеррористических преграждающих средств.

Вопросы для самоподготовки.

1. Классификация досмотрового и поискового оборудования.
2. Основные типы металлоискателей и основной принцип работы.
3. Организационно- технические методы защиты информационных систем от преднамеренного силового электромагнитного воздействие.
4. Антитеррористические преграждающие системы.

Примерные темы практических занятий.

1. Изучение возможных направлений воздействия угрозы технологического (кибернетического и электромагнитного) терроризма на информационные системы и методов противодействия этим угрозам средствами физической защиты объектов информатизации.
2. Технические средства выявления несанкционированного проноса на территорию опасных предметов и проезда транспортных средств.

Отчет по результатам проведения практического занятия.

1. **РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3 форма рубежного контроля** – Тестовый опрос

Раздел 4. Интеграция СКУД с техническими средствами обеспечения физической защиты предприятия

Раздел 4.1 Интеграция СКУД с техническими средствами обеспечения физической защиты предприятия.

Цель: Изучение принципов построения интегрированных систем охраны (ИСО), на основе аппаратных и программных средств управления СКУД

Перечень изучаемых элементов содержания

2. Классификация ИСО.
3. Принципы объединения СКУД, сигнализационных систем, Систем охранного телевидения и антитеррористических средств в единую интегрированную систему (ИС).
4. Выбор компонентов ИС.
5. Основные типы металлоискателей и основной принцип работы.
6. Организационно- технические и тактические методы защиты информационных систем, входящих в состав ИСО, от деструктивного воздействия силовых электромагнитных факторов.

Примерные темы практических занятий.

1. Изучение возможных направлений воздействия угрозы технологического (кибернетического и электромагнитного) терроризма на информационные системы и методов противодействия этим угрозам средствами физической защиты объектов информатизации, в том числе с применением СКУД.
2. **Уязвимость компонентов СКУД к деструктивным воздействиям, в том числе к проявлению кибернетического и электромагнитного терроризма.**
3. **Практическое изучение существующих принципов построения ИСО.**
4. Современные аппаратно-программные средства обработки и отображения видеосигнала, поступающего от видеокамер, в составе ИСО, как средство обнаружения террористической угрозы.

   Отчет по результатам проведения практического занятия.

7. **РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 4.1 форма рубежного контроля** – Тестовый опрос

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) является **экзамен,** 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-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-	Знать: основы и особенности установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности информации	Этап формирования знаний

	аппаратных (в том числе криптографических) и технических средств защиты информации	Уметь: осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Этап формирования умений
		Владеть: методами установки, настройки и эксплуатации компонентов технических систем обеспечения безопасности 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 профессиональных задач	Знать: средства защиты информации в правоохранительной сфере	Этап формирования знаний
		Уметь: проектировать, внедрять и использовать системы мониторинга средств защиты информации в правоохранительной сфере	Этап формирования умений
		Владеть: навыками проектирования, внедрения и применения системы мониторинга средств защиты информации	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-1; ПК-2	Этап формирования знаний.	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с

		самостоятельно обобщать и излагать материал	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-1; ПК-2;	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-1; ПК-2;	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. Основной понятийный аппарат изучаемой дисциплины. Нормативные документы, отражающие терминологию.
2. Характеристика основные угрозы личности, информации и имуществу, которые призваны нейтрализовать, или минимизировать системы физической защиты.
3. Система физической защиты организации.
4. Понятие об интегрированных системах охраны.
5. Состав, структура и назначение элементов СКУД.
6. Зоны и рубежи охраны.
7. Роль и место инженерной укрепленности в общей системе безопасности объектов.
8. Способы, средства к технической укрепленности конструктивных элементов зданий и помещений: перекрытия и стеновые панели, дверные и оконные конструкции.
9. Требования руководящих документов и рекомендации по их выбору.
10. Электроуправляемые замки и защелки. Конструктивное исполнение.
11. Классификация СКУД. Централизованные и децентрализованные системы.
12. Требования нормативных документов к системе контроля и управления доступом. Роль и место системы контроля и управления доступом в общей системе безопасности объектов
13. Структура системы контроля и управления доступом. Классификация средств и систем контроля и управления доступом.
14. Принципы построения и функционирования элементов систем контроля и управления доступом.
15. Способы электронной идентификации и их характеристики.
16. Электронная идентификация по вещественному коду.
17. Электронная идентификация по биометрическим признакам.
18. Электронная идентификация по запоминаемому коду.
19. Электронная идентификация на основе RFID технологии.
20. Электронная идентификация на основе трехмерного образа.
21. Выбор считывающие устройства с учетом устойчивости к внешним факторам.
22. Преграждающие устройства.
23. Особенности функционирования считывающих и преграждающих устройств в условиях деструктивного воздействия антропогенных факторов.
24. Принципы построения и функционирования систем контроля и управления доступом на объектах различной сложности.
25. Перспективы развития систем контроля и управления доступом.
26. Роль и место антитеррористических мероприятий в системе обеспечения комплексной безопасности предприятия, в том числе его информационной составляющей.
27. Технические средства антитеррористической защиты, их назначение и основные характеристики
28. Технологический терроризм. Классификация. Обобщенная характеристика методов и средств деструктивного воздействия. Примеры реализации, по материалам открытой печати.
29. Организационно-технические и инженерно-технические методы защиты объекта от субъектов технологического терроризма. на основе ИСО.

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

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

5.1.1. Основная литература

1. *Стасышин, В. М.* Базы данных: технологии доступа : учебное пособие для вузов / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 164 с. — (Высшее образование). — ISBN 978-5-534-08687-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/492177

5.1.2. Дополнительная литература.

1. *Казарин, О. В.* Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524

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

5.2. 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	Полнотекстовая база данных периодических	http://ebiblioteka.ru/

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
	«EastView»	изданий	
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) «**Системы контроля и управления доступом Т**» 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) в рамках реализации основной профессиональной образовательной программы «Информационная безопасность» по направлению10.03.01Информационная безопасность очной формы обучения 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 дисциплине «Системы контроля управления доступом» проводятся 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 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).

5.7. Образовательные технологии

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

Освоение дисциплины (модуля) **«Системы контроля управления доступом»** 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) «**Системы контроля управления доступом»** предусмотрено применением электронного обучения.

Учебные часы дисциплины «**Системы контроля управления доступом»** 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) **«Системы контроля управления доступом»** 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.			