УТВЕРЖДЕНО:
Ученым советом Высшей школы сервиса
Протокол № 12 от «22» мая 2019 г.

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ
Б1.В.ДВ.3.1 ОСНОВЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ

основной профессиональной образовательной программы высшего образования – программы ***бакалавриата***

по направлению подготовки: ***43.03.01 Сервис***

на направленность (профиль): ***Цифровые сервисы для бизнеса***

Квалификация: ***бакалавр***

Год начала подготовки 2019

Разработчик:

должность	ученая степень и звание, ФИО
Доцент, высшей школы сервиса	к.т.н., доцент Деменев А.В.

Рабочая программа согласована и одобрена директором ОПОП:

должность	ученая степень и звание, ФИО
Директор высшей школы сервиса	***к.т.н., доцент Сумзина Л.В.***

1. Аннотация рабочей программы дисциплины (модуля)

Дисциплина Б1.В.ДВ.3.1 «Основы цифровой безопасности» относится к элективным дисциплинам части, формируемой участниками образовательных отношений первого блока программы бакалавриата по направлению подготовки 43.03.01 Сервис, профилю «Цифровые сервисы для бизнеса».

Содержание дисциплины охватывает круг вопросов, связанных с базовыми принципами формирования у обучающихся базовых теоретических знаний в области цифровой безопасности и развитие необходимых практических умений и навыков их применения в будущей профессиональной деятельности и различных предметных областях бизнеса.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК УВ-2 Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия; в части индикаторов достижения компетенции ПК УВ-2.1. (Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации), ПК УВ-2.2. (Осуществляет контроль обеспечения уровня защищенности информационных сервисов), ПК УВ-2.3. (Оценивает защищенность объектов информатизации с помощью типовых программных средств).

Общая трудоемкость освоения дисциплины «Основы цифровой безопасности» составляет 16 зачетных единиц, 576 часов, продолжительностью четыре семестра на 3,4 курсе (5,6,7,8 семестры) для очной формы и на 4,5 курсе (6,7,8,9 семестры) для заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекция с мультимедийными презентациями, практические занятия в форме интерактивного практического занятия с использованием компьютерной техники, самостоятельная работа обучающихся.

Программой дисциплины предусмотрены лекционные занятия – 136 часов, практические работы – 144 часа, самостоятельная работа студента – 280 часов, консультации – 8 часов и промежуточная аттестация – 8 часов.

Программой дисциплины, для заочной формы обучения предусмотрены лекционные занятия – 32 часа, практические работы – 44 часа, самостоятельная работа студента – 484 часа, консультации – 8 часов и промежуточная аттестация – 8 часов.

Целью изучения дисциплины «Основы цифровой безопасности» является формирование у обучающихся базовых теоретических знаний в области цифровой безопасности и развитие необходимых практических умений и навыков, их применения в будущей профессиональной деятельности и различных предметных областях бизнеса

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестов и зашиты практических работ, контроль выполнения самостоятельной работы в форме доклада с презентацией, промежуточная аттестация в форме зачета в 5 семестре и экзаменов в 6,7,8 семестрах для очной формы обучения; в форме зачетов в 6,8 семестрах и экзаменов в 7,8 семестрах для заочной формы обучения.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

№ пп	Индекс компетенции, индикатора достижения компетенции	Планируемые результаты обучения (компетенции, индикатора достижения компетенции)
1.	ПК УВ-2	Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия в части: ПК УВ-2.1. Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации ПК УВ-2.2. Осуществляет контроль обеспечения уровня защищенности информационных сервисов ПК УВ-2.3. Оценивает защищенность объектов информатизации с помощью типовых программных средств.

3. Место дисциплины (модуля) в структуре ОП ОП:

Дисциплина Б1.В.ДВ.3.1 «Основы цифровой безопасности» относится к элективным дисциплинам части, формируемой участниками образовательных отношений первого блока программы бакалавриата по направлению подготовки 43.03.01 Сервис, профилю «Цифровые сервисы для бизнеса».

В результате изучения дисциплины «Основы цифровой безопасности» студенты должны:

знать:

• и иметь представление о вопросах организационно-правового обеспечения информационной безопасности

• организационное обеспечение информационной безопасности

• и иметь представление о технических средствах и методах защиты информации

• иметь представление о назначение и задачах в сфере обеспечения информационной безопасности на уровне государства

• криптографические методы защиты информации

• и иметь представление о работе инфраструктуры открытых ключей

• средства стеганографии для защиты информации

• иметь представление о настройке безопасного сетевого соединения

• иметь представление о информационной безопасности экономических систем в национальной безопасности страны

• антивирусные средства защиты информации

• объектно-ориентированный подход к проектированию программного обеспечения

• иметь представление об таксономии нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование

• иметь представление о жизненном цикле программного обеспечения.

• иметь представление о управлении разработкой ПО.

• структурный подход к проектированию и управление качеством программного обеспечения

• и иметь представление о тестирование, отладке и сборке ПО.

уметь:

• применять знания о организационно-правовом обеспечение информационной безопасности

• применять технические средствах и методах защиты информации

• применять знания о назначение и задачах в сфере обеспечения информационной безопасности на уровне государства

• применять криптографические методы защиты информации

• применять знания о работе инфраструктуры открытых ключей

• применять средства стеганографии для защиты информации

• применять настройки безопасного сетевого соединения

• применять представление о информационной безопасности экономических систем в

национальной безопасности страны

• применять антивирусные средства защиты информации

• применять объектно-ориентированный подход к проектированию программного обеспечения

• применять знания о таксономии нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование

• применять знания о жизненном цикле программного обеспечения.

• применять знания об управлении разработкой ПО.

• применять структурный подход к проектированию и управление качеством программного обеспечения

• применять знания о тестирование, отладке и сборке ПО.

владеть:

• знаниями о организационно-правового обеспечение информационной безопасности

• навыками применения техническими средствами и методами защиты информации

• знаниями о назначении и задачах в сфере обеспечения информационной безопасности на уровне государства

• навыками применения криптографических методов защиты информации

• знаниями о работе инфраструктуры открытых ключей

• навыками применения средств стеганографии для защиты информации

• навыками применения настройки безопасного сетевого соединения

• навыками применения представления о информационной безопасности экономических систем в национальной безопасности страны

• навыками применения антивирусные средства защиты информации

• навыками применения объектно-ориентированным подходом к проектированию программного обеспечения

• знаниями о таксономии нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование

• знаниями о жизненном цикле программного обеспечения.

• знаниями о управлении разработкой ПО.

• навыками применения структурного подхода к проектированию и управлению качеством программного обеспечения

• знаниями о тестирование, отладке и сборке ПО.

Изучение дисциплины «Основы цифровой безопасности» должно способствовать развитию основных профессиональных компетенций, необходимых для изучения последующих дисциплин основной образовательной программы бакалавриата, 43.03.01. «Сервис», профилю «Цифровые сервисы для бизнеса».

Освоение компетенции ПКУВ-2 начинается с изучения дисциплины «Основы цифровой безопасности». Основные положения дисциплины должны быть использованы в дальнейшем при выполнении выпускной квалификационной работы и получении новых знаний по дисциплинам: «Преддипломная практика».

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
Очная форма обучения

Общая трудоемкость дисциплины составляет 16 зачетных единиц / 576 акад.часов.

№ п/п	Виды учебной деятельности		**Семестры**			
		Всего	**5**	**6**	**7**	**8**
1	**Контактная работа обучающихся**	**296**	74	74	74	74
	в том числе:	**-**	-	-	-	-
1.1.	Занятия лекционного типа	**136**	**34**	34	34	34
1.2.	Занятия семинарского типа, в том числе:	**144**	**36**	**36**	**36**	**36**
	Семинары					
	Лабораторные работы					
	Практические занятия	**144**	36	36	36	36
1.3.	Консультации	**8**	2	2	2	2
1.4.	**Промежуточная аттестация**					
2.	**Самостоятельная работа**	**280**	70	70	70	70
3.	**Форма промежуточной аттестации (зачет, экзамен)**	**8**	**зачет** **2**	**экз.** **2**	**экз.** **2**	**экз.** **2**
4	**Общая трудоемкость час**	**576**	144	144	144	144
	з.е.	**16**	4	4	4	4

Заочная форма обучения
Общая трудоемкость дисциплины составляет 16 зачетных единиц / 576акад.часов.

№ п/п	Виды учебной деятельности		**Семестры**			
		Всего	**6**	**7**	**8**	**9**
1	**Контактная работа обучающихся**	**92**	18	18	28	28
	в том числе:	**-**	-	-	-	-
1.1.	Занятия лекционного типа	**32**	**6**	6	10	10
1.2.	Занятия семинарского типа, в том числе:	**44**	**8**	**8**	**14**	**14**
	Семинары					
	Лабораторные работы					
	Практические занятия	**44**	8	8	14	14
1.3.	Консультации	**8**	2	2	2	2
1.4.	**Промежуточная аттестация**					
2.	**Самостоятельная работа**	**484**	126	126	116	116
3.	**Форма промежуточной аттестации (зачет, экзамен)**	**8**	**зачет** **2**	**экз.** **2**	**зачет** **2**	**экз.** **2**
4	**Общая трудоемкость час**	**576**	144	144	144	144
	з.е.	**16**	4	4	4	4

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Разделы (блоки) дисциплины и виды занятий

Для очной формы обучения:

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/5	**Концепция цифровой безопасности**	Тема 1.1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.	8,5	Традиционная лекция	9	Семинар			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/5	**Концепция цифровой безопасности**	Тема 1.2. Организационное обеспечение информационной безопасности.	8,5	Лекция-дискуссия	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				

3,4/5	**Концепция цифровой безопасности**	Тема 1.3.Технические средства и методы защиты информации.	8,5	Лекция-дискуссия	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 3				Устный опрос				
3,4/5	**Концепция цифровой безопасности**	Тема 1.4 Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	8,5	Лекция-дискуссия	9	Дискуссии по актуальным темам и разбор практических кейсов			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 4.				Устный опрос				
	Консультация студентов – 2 часа									
3,4/5	**Промежуточная аттестация – зачет– 2 часа**									

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/6	**Криптографические и стеганографические методы защиты**	Тема 2.1. Криптографические методы защиты информации.	8,5	Традиционная лекция	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/6	**Криптографические и стеганографические методы защиты**	Тема 2.2. Реализация работы инфраструктуры открытых ключей.	8,5	Лекция-дискуссия	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				
3,4/6	**Криптографические и стеганографические методы защиты**	Тема 2.3. Средства стеганографии для защиты информации.	8,5	Лекция-дискуссия	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
3,4/6		**Контрольная точка 3**				Устный оп-				

						рос				
3,4/6	**Криптографические и стеганографические методы защиты**	Тема 2.4. Настройка безопасного сетевого соединения.	8,5	Лекция-дискуссия	9	Семинар			17.5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
3,4/6		**Контрольная точка 4.**				Устный опрос				
	Консультация студентов – 2 часа									
3,4/6	**Промежуточная аттестация – экзамен– 2 часа**									

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/7	**Инстументы защиты информации**	Тема 3.1. Место информационной безопасности экономических систем в национальной безопасности страны.	8,5	Традиционная лекция	9	Дискуссии по актуальным темам и разбор практических кейсов			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/7	**Инстументы защиты информации**	Тема 3.2. Антивирусные средства защиты информации.	8,5	Лекция-дискуссия	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				
3,4/7	**Инстументы защиты информации**	Тема 3.3. Объектно-ориентированный подход к проектированию программного обеспечения.	8,5	Лекция-дискуссия	9	Дискуссии по актуальным темам и разбор практических кейсов			17.5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 3				Устный опрос				
3,4/7	**Инстументы**	Тема 3.4.Таксономия	8,5	Лекция-	9	Практическая			17,5	Самостоятельное

	защиты информации	нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.		дискуссия		работа				изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 4.				Устный опрос				
	Консультация студентов – 2 часа									
3,4/7	**Промежуточная аттестация – экзамен– 2 часа**									

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/8	**Стандартизация, сертификация и управление качеством программного обеспечения**	Тема 4.1. Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного обеспечения.	8.5	Традиционная лекция	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/8	**Стандартизация, сертификация**	Тема 4.2. Управление разработкой ПО	8,5	Лекция-дискуссия	9	Дискуссии по актуальным			17,5	Самостоятельное изучение материала,

	и управление качеством программного обеспечения					темам и разбор практических кейсов				подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				
3,4/8	**Стандартизация, сертификация и управление качеством программного обеспечения**	Тема 4.3. Структурный подход к проектированию и управление качеством программного обеспечения.	8,5	Лекция-дискуссия	9	Дискуссии по актуальным темам и разбор практических кейсов			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 3				Устный опрос				
3,4/8	**Стандартизация, сертификация и управление качеством программного обеспечения**	Тема 4.4. Тестирование, отладка и сборка ПО	8,5	Лекция-дискуссия	9	Практическая работа			17,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 4.				Устный опрос				
	Консультация студентов – 2 часа									
3,4/8	**Промежуточная аттестация – экзамен– 2 часа**									

Для заочной формы обучения:

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/6	**Концепция цифровой безопасности**	Тема 1.1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.	1,5	Традиционная лекция	2	Семинар			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/6	**Концепция цифровой безопасности**	Тема 1.2. Организационное обеспечение информационной безопасности.	1,5	Лекция-дискуссия	2	Практическая работа			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				
3,4/6	**Концепция цифровой безопасности**	Тема 1.3.Технические средства и методы защиты информации.	1,5	Лекция-дискуссия	2	Практическая работа			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с

										использованием ЭБС
		Контрольная точка 3				Устный опрос				
3,4/6	**Концепция цифровой безопасности**	Тема 1.4 Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	1,5	Лекция-дискуссия	2	Дискуссии по актуальным темам и разбор практических кейсов			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 4.				Устный опрос				
	Консультация студентов – 2 часа									
3,4/6	**Промежуточная аттестация – зачет– 2 часа**									

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/7	**Криптографические и стеганографические методы защиты**	Тема 2.1. Криптографические методы защиты информации.	1,5	Традиционная лекция	2	Практическая работа			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с использо-

										ванием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/7	**Криптографические и стеганографические методы защиты**	Тема 2.2. Реализация работы инфраструктуры открытых ключей.	1,5	Лекция-дискуссия	2	Практическая работа			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				
3,4/7	**Криптографические и стеганографические методы защиты**	Тема 2.3. Средства стеганографии для защиты информации.	1,5	Лекция-дискуссия	2	Практическая работа			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
3,4/7		**Контрольная точка 3**				Устный опрос				
3,4/7	**Криптографические и стеганографические методы защиты**	Тема 2.4. Настройка безопасного сетевого соединения.	1,5	Лекция-дискуссия	2	Семинар			31,5	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
3,4/7		**Контрольная точка 4.**				Устный опрос				
	Консультация студентов – 2 часа									
3,4/7	**Промежуточная аттестация – экзамен– 2 часа**									

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/8	**Инстументы защиты информации**	Тема 3.1. Место информационной безопасности экономических систем в национальной безопасности страны.	2,5	Традиционная лекция	3,5	Дискуссии по актуальным темам и разбор практических кейсов			29	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/8	**Инстументы защиты информации**	Тема 3.2. Антивирусные средства защиты информации.	2,5	Лекция-дискуссия	3,5	Практическая работа			29	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				
3,4/8	**Инстументы защиты информации**	Тема 3.3. Объектно-ориентированный подход к проектированию программного обеспечения.	2,5	Лекция-дискуссия	3,5	Дискуссии по актуальным темам и разбор практических кейсов			29	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 3				Устный опрос				
3,4/8	**Инстументы**	Тема 3.4.Таксономия	5,5	Лекция-	3,5	Практическая			29	Самостоятельное

	защиты информации	нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.		дискуссия		работа				изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 4.				Устный опрос				
	Консультация студентов – 2 часа									
3,4/8	**Промежуточная аттестация – зачет– 2 часа**									

Номер курса/ семестр	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО	Виды учебных занятий и формы их проведения							
			Контактная работа обучающихся с преподавателем				Консультации, акад. часов	Форма проведения консультации	СРО, акад.часов	Форма проведения СРО
			Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия				
3,4/9	**Стандартизация, сертификация и управление качеством программного обеспечения**	Тема 4.1. Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного обеспечения.	2,5	Традиционная лекция	3,5	Практическая работа			29	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 1				Устный опрос				
3,4/9	**Стандартизация, сертификация**	Тема 4.2. Управление разработкой ПО	2,5	Лекция-дискуссия	3,5	Дискуссии по актуальным			29	Самостоятельное изучение материала,

	и управление качеством программного обеспечения					темам и разбор практических кейсов				подготовка к практическому занятию с использованием ЭБС.
		Контрольная точка 2				Устный опрос				
3,4/9	**Стандартизация, сертификация и управление качеством программного обеспечения**	Тема 4.3. Структурный подход к проектированию и управление качеством программного обеспечения.	2,5	Лекция-дискуссия	3,5	Дискуссии по актуальным темам и разбор практических кейсов			29	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 3				Устный опрос				
3,4/9	**Стандартизация, сертификация и управление качеством программного обеспечения**	Тема 4.4. Тестирование, отладка и сборка ПО	2,5	Лекция-дискуссия	3,5	Практическая работа			29	Самостоятельное изучение материала, подготовка к практическому занятию с использованием ЭБС
		Контрольная точка 4.				Устный опрос				
	Консультация студентов – 2 часа									
3,4/9	**Промежуточная аттестация – экзамен– 2 часа**									

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Перечень тем самостоятельной работы обучающихся на очной/заочной форме (280/484 часа)

№ п/п	Тема, трудоемкость в акад.ч.	Учебно-методическое обеспечение
1.	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности. (17,5/31,5 часов)	1.Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 413 с.: - (Высшее образование: Бакалавриат) - Режим доступа: http://znanium.com/catalog/product/1022055 2. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 - Режим доступа: http://znanium.com/catalog/product/474838 3. Стандартизация, сертификация и управление качеством программного обеспечения: Учебное пособие / Ананьева Т.Н., Новикова Н.Г., Исаев Г.Н. - М.:НИЦ ИНФРА-М, 2016. - 232 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (П) ISBN 978-5-16-011711-9 - Режим доступа: http://znanium.com/catalog/product/541003 1.Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ "Об информации,информационных технологиях и защите информации" (постатейный) / А.И.Савельев - М.: Статут, 2015. - 320 с.: 60x84 1/16 (Обложка) ISBN 978-5-8354-1150-4 - Режим доступа: http://znanium.com/catalog/product/528227
2.	Организационное обеспечение информационной безопасности. (17,5/31,5 часов)	
3.	Технические средства и методы защиты информации. (17,5/31,5 часов)	
4.	Назначение и задачи в сфере обеспечения информационной (17,5/31,5 часов)	
5.	Криптографические методы защиты информации.	
6.	Реализация работы инфраструктуры открытых ключей. (17,5/31,5 часов)	
7.	Средства стеганографии для защиты информации . (17,5/31,5 часов)	
8.	Настройка безопасного сетевого соединения. (17,5/31,5 часов)	
9.	Место информационной безопасности экономических систем в национальной безопасности страны. (17,5/29 часов)	
10.	Антивирусные средства защиты информации. (17,5/29 часов)	
11.	Объектно-ориентированный подход к проектированию программного обеспечения. (17,5/29 часов)	
12.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. (17,5/29 часов)	
13.	Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного	

	обеспечения. (17,5/29 часов)	
14.	Управление разработкой ПО.. (29 часов)	
15.	Структурный подход к проектированию и управление качеством программного обеспечения. (17,5/29 часов)	
16.	Тестирование, отладка и сборка ПО. (17,5/29 часов)	

7. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине (модулю)

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

№ пп	Индекс компетенции, индикатора достижения компетенции	Содержание компетенции (индикатора достижения компетенции)	Раздел дисциплины, обеспечивающий формирование компетенции (индикатора достижения компетенции)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (индикатора достижения компетенции) обучающийся должен:		
				знать	уметь	владеть
1.	ПК УВ-2	Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия				
		ПК УВ-2.1 Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации	Все разделы	Знает организационные меры по защите информации, основные методы управления защитой информации	Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации	Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации
		ПК УВ-2.2. Осуществляет контроль обеспечения уровня		Знает современные виды информацион-	Контролирует работоспособность и эффективность при-	Владеет методами анализа проект-

		защищенности информационных сервисов		ного взаимодействия, методы анализа исходных данных для проектирования подсистем обеспечения информационной безопасности	меняемых программных, программно-аппаратных и технических средств защиты информации	ных решений по обеспечению защищенности информационных сервисов
		ПК УВ-2.3. Оценивает защищенность объектов информатизации с помощью типовых программных средств.		Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	Владеет принципами формирования политики информационной безопасности объекта информатизации

7.2. Описание показателей и критериев оценивания компетенций на разных этапах их формирования, описание шкал оценивания

Результат обучения по дисциплине	Показатель оценивания	Критерий оценивания	Этап освоения компетенции
Знать организационные меры по защите информации, основные методы управления защитой информации; современные виды информационного взаимодействия, методы анализа исходных данных для проектирования подсистем обеспечения информационной безопасности; программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях. Уметь разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации; контролировать работоспособность и эффективность применяемых программных, программно-аппаратных и технических средств защиты информации; конфигурировать программно-аппаратные средства защиты информации в соответ-	Тестирование, устный опрос, решение выполнение интерактивных практических работ с использованием компьютерной техники	Студент демонстрирует знание организационных мер по защите информации, основных методов управления защитой информации; современных видов информационного взаимодействия, методов анализа исходных данных для проектирования подсистем обеспечения информационной безопасности; программно-аппаратных средств защиты информации в типовых операционных системах, систем управления базами данных, компьютерных сетях. Уметь разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации; контролировать работоспособность и эффективность применяемых программных, программно-аппаратных и технических средств защиты информации; конфигурировать программ-	использование способности знать критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации; осуществлять контроль обеспечения уровня защищенности информационных сервисов; оценивать защищенность объектов информатизации с помощью типовых программных средств.

ствии с заданными политиками безопасности. Владеть навыками выработки рекомендаций для решения о модернизации системы защиты информации; методами анализа проектных решений по обеспечению защищенности информационных сервисов; принципами формирования политики информационной безопасности объекта информатизации.		но-аппаратные средства защиты информации в соответствии с заданными политиками безопасности. Владеть навыками выработки рекомендаций для решения о модернизации системы защиты информации; методами анализа проектных решений по обеспечению защищенности информационных сервисов; принципами формирования политики информационной безопасности объекта информатизации.	

Для оценки учебных достижений обучающихся используется балльно-рейтинговая технология, которая основана на единых требованиях к студентам, предполагающих в процессе изучения дисциплины прохождение фиксированного количества мероприятий текущего контроля успеваемости.

Балльно-рейтинговая технология оценки успеваемости студентов базируется на следующих принципах:

· реализации компетентностного подхода к результатам обучения в образовательном процессе;

· индивидуализации обучения;

· модульном принципе структурирования учебного процесса;

· вариативности форм контроля и гибкой модели оценивания успеваемости студентов;

· открытости процедур контроля и результатов оценки текущей успеваемости студентов;

· единства требований, предъявляемых к работе студентов в ходе освоения программы дисциплины;

· строгом соблюдении исполнительской дисциплины всеми участниками образовательного процесса.

Балльно-рейтинговая система предназначена для повышения мотивации учебной деятельности студентов, для объективности и достоверности оценки уровня их подготовки и используется в качестве одного из элементов управления учебным процессом в университете. Получение баллов позволяет студентам четко понимать механизм формирования оценки по дисциплине, что исключит конфликтные ситуации при получении итоговой

оценки; осознавать необходимость систематической и регулярной работы по усвоению учебного материала; стимулировать саморазвитие и самообразование.

Рейтинговая оценка студентов по дисциплине определяется по 100-балльной шкале в семестре. Распределение баллов рейтинговой оценки между видами контроля устанавливается в следующем соотношении:

- посещение учебных занятий (max 30 баллов)
- текущий контроль успеваемости (max 70 баллов), в том числе:

1 контрольная точка текущего контроля (max 10 баллов)
2 контрольная точка текущего контроля (max 10 баллов) **max**
3 контрольная точка текущего контроля (max 10 баллов) **100 баллов**
4 контрольная точка текущего контроля (max 35 баллов)
бонусные рейтинговые баллы за активность на занятиях по итогам семестра (max 5 баллов)

Посещение лекций (за исключением поточных) и практических занятий оценивается накопительно следующим образом: максимальное количество баллов, отводимых на учет посещаемости (30 баллов), делится на количество лекций (за исключением поточных) и практических занятий по дисциплине. Полученное значение определяет количество баллов, набираемых студентом за посещение одного занятия.

Оценка успеваемости выставляется за выполнение заданий текущего контроля по дисциплине. Всего в семестре 4 мероприятия текущего контроля (4 «контрольных точки»), причем выполнение всех 4 заданий текущего контроля является обязательным для студента. В рамках дисциплины «Основы цифровой безопасности» предусмотрено 1 аудиторное тестирование (оценивается по 10-ти бальной шкале), 2 контрольные работы (оцениваются по 10-ти бальной шкале) и выполнение группового проекта по окончании семестра (оценивается по 35-ти бальной шкале). Аудиторное тестирование предусматривает вопросы с несколькими вариантами ответа. Аттестация по четвертой «контрольной точке» – проводится в период последних двух недель семестра в форме презентации

Практические занятия (между «контрольными точками») проводятся в активной и интерактивной форме (дискуссии по изученному материалу, разбор ситуаций, решение задач, круглый стол, представление презентаций и т.п.), в аудитории или вне аудитории (на выставке, предусмотренной в настоящей программе). Несмотря на то, что преподаватель не оценивает в баллах студента на практических занятиях, в тоже время преподаватель фиксирует активность на занятии и при подведении итогов за семестр начисляет от 0 до 5 **рейтинговых бонусных баллов** за активность на занятиях. Под активностью понимается демонстрация хорошего уровня знаний по дисциплине, что может выражаться в выступлениях на занятиях, ответах на вопросы преподавателя, решении задач, участии в профессиональных мероприятиях и т.д.

Промежуточная аттестация проводится в соответствии с расписанием в экзаменационную сессию (экзамен). Для допуска к промежуточной аттестации необходимо набрать в общей сложности **не менее 41 балла**, успешно пройти все мероприятия текущего контроля по дисциплине (не иметь задолженностей по текущей контролю успеваемости).

Результаты текущего контроля успеваемости учитываются при выставлении оценки в ходе промежуточной аттестации.

Для допуска к промежуточной аттестации обучающийся должен выполнить все мероприятия текущего контроля по дисциплине (не иметь задолженностей по текущей контролю успеваемости) и набрать в общей сложности не менее 51 балла.

Перевод рейтинговых баллов в итоговую 5 – балльную шкалу оценку осуществляется в соответствии с таблицей.

Баллы за семестр	Автоматическая оценка		Баллы за зачет	Баллы за экзамен	Общая сумма баллов	Итоговая оценка
	зачет	экзамен				
90-100*	зачет	5 (отлично)	-	-	90-100	5 (отлично)
71-89*	зачет	4 (хорошо)	-	0-20	71-89 90-100	4 (хорошо) 5 (отлично)
51-70*	зачет	3 (удовлетворительно)	-	0-20	51-70 71-89 90	3 (удовлетворительно) 4 (хорошо) 5 (отлично)
50 и менее	недопуск к зачету, экзамену		-	-	50 и менее	2 (неудовлетворительно), незачет

* при условии выполнения всех заданий текущего контроля успеваемости

Результаты промежуточной аттестации определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно" (форма промежуточной аттестации – экзамен) и "зачтено", "не зачтено" (форма промежуточной аттестации – зачет).

Шкала оценок при промежуточном контроле по балльно-рейтинговой системе.

Наименование формы промежуточной аттестации	**Форма проведения**	**Шкала**
1. Экзамен (6,7,8/7,9* семестр) 2. Зачет(5/6,8* семестр)	устно	не более 50% - 10 б -2 50-65% - 13б – 3 65-80% - 16 б – 4 80-100% - 20б – 5 Менее 65% - 13б – «незачтено» 65-100% - 20б – «зачтено»
	тестирование	не более 50% - 10 б -2 50-65% - 13б – 3 65-80% - 16 б – 4 80-100% - 20б – 5 Менее 65% - 13б – «незачтено» 65-100% - 20б – «зачтено»

*для заочной формы обучения

Виды средств оценивания, применяемых при проведении промежуточной аттестации и шкалы оценки уровня знаний, умений и навыков при их выполнении

Зачет по дисциплине основывается на результатах выполнения индивидуальных заданий (контрольных точек) студента по данной дисциплине. Форма проведения зачета определяется преподавателем, ведущим данную дисциплину, представлен в п.7.4.

Критерии оценки «зачтено» и «незачтено»

Ответ студента на зачете оценивается одной из следующих оценок: «зачтено» и «незачтено», которые выставляются по следующим критериям.

Оценки «зачтено» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебного и нормативного материала, умеющий свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой (п.8), демонстрирующие систематический характер знаний по дисциплине и способные к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

Оценка «незачтено» выставляется студентам, обнаружившим пробелы в знаниях основного учебного материала, допускающим принципиальные ошибки в выполнении предусмотренных программой заданий. Такой оценки заслуживают ответы студентов, носящие несистематизированный, отрывочный, поверхностный характер, когда студент не понимает существа излагаемых им вопросов, что свидетельствует о том, что студент не может дальше продолжать обучение или приступать к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине

Экзамен по дисциплине проводится в устной (по билетам) или письменной форме (в форме тестирования). Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных дисциплинарных компетенций. Типовые вопросы и тестовые задания для экзамена приводятся в разделе 7.4.

Шкала оценки уровня знаний, умений и навыков при проведении промежуточной аттестации в устной форме зачета/экзамена

оценка	Критерии оценивания	Показатели оценивания
«5»	– полно раскрыто содержание материала; – материал изложен грамотно, в определенной логической последовательности; – продемонстрировано системное и глубокое знание программного материала; – точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; – ответ прозвучал самостоятельно, без наводящих вопросов; – продемонстрирована способность творчески применять знание теории к решению профессиональных задач; – продемонстрировано знание современной учебной и научной литературы; – допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию	– Обучающийся показывает всесторонние и глубокие знания программного материала, – знание основной и дополнительной литературы; – последовательно и четко отвечает на вопросы билета и дополнительные вопросы; – уверенно ориентируется в проблемных ситуациях; – демонстрирует способность применять теоретические знания для анализа практических ситуаций, делать правильные выводы, проявляет творческие способности в понимании, изложении и использовании программного материала; – подтверждает полное освоение компетенций, предусмотренных программой
«4»	– вопросы излагаются систематизировано и последовательно; – продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; – продемонстрировано усвоение основной литературы. – ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: – а) в изложении допущены небольшие пробелы, не исказившие со-	– обучающийся показывает полное знание – программного материала, основной и – дополнительной литературы; – дает полные ответы на теоретические вопросы билета и дополнительные вопросы, допуская некоторые неточности; – правильно применяет теоретические положения к оценке практических ситуаций;

	держание ответа; – б) допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; – в) допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя	– демонстрирует хороший уровень освоения материала и в целом подтверждает освоение компетенций, предусмотренных программой
«3»	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; – усвоены основные категории по рассматриваемому и дополнительным вопросам; – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; – при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации; – продемонстрировано усвоение основной литературы	– обучающийся показывает знание основного – материала в объеме, необходимом для предстоящей профессиональной деятельности; – при ответе на вопросы билета и дополнительные вопросы не допускает грубых ошибок, но испытывает затруднения в последовательности их изложения; – не в полной мере демонстрирует способность применять теоретические знания для анализа практических ситуаций; – подтверждает освоение компетенций, предусмотренных программой на минимально допустимом уровне
«2»	– не раскрыто основное содержание учебного материала; – обнаружено незнание или непонимание большей или наиболее важной части учебного материала; – допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов. – не сформированы компетенции, умения и навыки.	– обучающийся имеет существенные пробелы в знаниях основного учебного материала по дисциплине; – не способен аргументировано и последовательно его излагать, допускает грубые ошибки в ответах, неправильно отвечает на задаваемые вопросы или затрудняется с ответом; – не подтверждает освоение компетенций, предусмотренных программой

Шкала оценки уровня знаний, умений и навыков при проведении промежуточной аттестации в форме решения тестовых заданий для зачета/экзамена

Критерии оценки	**оценка**
выполнено верно заданий	«5», если (90 –100)% правильных ответов
	«4», если (70 – 89)% правильных ответов
	«3», если (50 – 69)% правильных ответов
	«2», если менее 50% правильных ответов

Виды средств оценивания, применяемых при проведении текущего контроля и шкалы оценки уровня знаний, умений и навыков при выполнении отдельных форм текущего контроля

Раздел «Концепция цифровой безопасности»

1-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

2-ая контрольная точка, формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

3-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

4-ая контрольная точка – формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

Раздел «Криптографические и стеганографические методы защиты»

1-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

2-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

3-ая контрольная точка в виде обсуждения рефератов, подготовленных студентами.

4-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Презентация

Раздел «Инструменты защиты информации»

1-ая контрольная точка - в форме группового обсуждения рефератов

2-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

3-ая контрольная точка, в виде обсуждения рефератов, подготовленных студентами.

4-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

Раздел «Стандартизация, сертификация и управление качеством программного обеспечения»

1-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся

2-ая контрольная точка - в виде обсуждения рефератов, подготовленных студентами.

3-ая контрольная точка - в виде обсуждения рефератов, подготовленных студентами.

4-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся опрос

Шкала оценки уровня знаний, умений и навыков при устном ответе во время защиты практических работ с использованием компьютерной техники

оценка	Критерии оценивания	Показатели оценивания
«5»	– полно раскрыто содержание материала; – материал изложен грамотно, в определенной логической последовательности; – продемонстрировано системное и глубокое знание программного материала; – точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; – ответ прозвучал самостоятельно, без наводящих вопросов; – продемонстрирована способность творчески применять знание теории к решению профессиональных задач; – продемонстрировано знание современной учебной и научной литературы; – допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию	– Обучающийся показывает всесторонние и глубокие знания программного материала, – знание основной и дополнительной литературы; – последовательно и четко отвечает на вопросы билета и дополнительные вопросы; – уверенно ориентируется в проблемных ситуациях; – демонстрирует способность применять теоретические знания для анализа практических ситуаций, делать правильные выводы, проявляет творческие способности в понимании, изложении и использовании программного материала; – подтверждает полное освоение компетенций, предусмотренных программой
«4»	– вопросы излагаются систематизировано и последовательно; – продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; – продемонстрировано усвоение основной литературы. – ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: – а) в изложении допущены не-	– обучающийся показывает полное знание – программного материала, основной и – дополнительной литературы; – дает полные ответы на теоретические вопросы билета и дополнительные вопросы, допуская некоторые неточности; – правильно применяет теоретические положения к оценке

	большие пробелы, не исказившие содержание ответа; – б) допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; – в) допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя	практических ситуаций; – демонстрирует хороший уровень освоения материала и в целом подтверждает освоение компетенций, предусмотренных программой
«3»	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; – усвоены основные категории по рассматриваемому и дополнительным вопросам; – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; – при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации; – продемонстрировано усвоение основной литературы	– обучающийся показывает знание основного – материала в объеме, необходимом для предстоящей профессиональной деятельности; – при ответе на вопросы билета и дополнительные вопросы не допускает грубых ошибок, но испытывает затруднения в последовательности их изложения; – не в полной мере демонстрирует способность применять теоретические знания для анализа практических ситуаций; – подтверждает освоение компетенций, предусмотренных программой на минимально допустимом уровне
«2»	– не раскрыто основное содержание учебного материала; – обнаружено незнание или непонимание большей или наиболее важной части учебного материала; – допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов. – не сформированы компетенции, умения и навыки.	– обучающийся имеет существенные пробелы в знаниях основного учебного материала по дисциплине; – не способен аргументировано и последовательно его излагать, допускает грубые ошибки в ответах, неправильно отвечает на задаваемые вопросы или затрудняется с ответом; – не подтверждает освоение компетенций, предусмотренных программой

оценочная шкала устного ответа в процентах

Процентный интервал	**оценка**

оценки	
менее 50%	**2**
51% - 70%	**3**
71% - 85%	**4**
86% - 100%	**5**

Расчетно-графическое задание на тему «Создание модели конструктивных элементов» оценивается максимуму на 10 баллов, «хорошо» - 7,2 балла, «удовлетворительно» -5,1балла, «неудовлетворительно» - менее 5,1. Использование электронной презентации приветствуется.

7.2. 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.

Номер недели семестра	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	Вид и содержание контрольного задания	Требования к выполнению контрольного задания и срокам сдачи
1/5(6*)	Концепция цифровой безопасности	1-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
1/5(6*)	Концепция цифровой безопасности	2-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9

			ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
1/5(6*)	Концепция цифровой безопасности	3-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
1/5(6*)	Концепция цифровой безопасности	4-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 35 баллов**
2/ 6(7*)	Криптографические и стеганографические методы защиты	1-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
1/6(7*)	Криптографические и стеганографические методы защиты	2-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опро-	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10

		са обучающихся	контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
1/6(7*)	Криптографические и стеганографические методы защиты	3-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
1/6(7*)	Криптографические и стеганографические методы защиты	4-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся Презентация	Устный опрос выполняется в аудитории. **Суммарный вес 35 баллов**
2/7(8*)	Инстументы защиты информации	1-ая контрольная точка - в форме группового обсуждения рефератов	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.

7/8	Инстументы защиты информации	2-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
7/8	Инстументы защиты информации	3-ая контрольная точка, в форме группового обсуждения рефератов	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
7/8	Инстументы защиты информации	4-ая контрольная точка, - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 35 баллов**
8/9	Стандартизация, сертификация и управление качеством программного обеспечения	1-ая контрольная точка - формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал,

			допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
8/9	Стандартизация, сертификация и управление качеством программного обеспечения	2-ая контрольная точка, в виде Обсуждение рефератов, подготовленных студентами.	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
8/9	Стандартизация, сертификация и управление качеством программного обеспечения	3-ая контрольная точка, в виде Обсуждение рефератов, подготовленных студентами.	Устный опрос выполняется в аудитории. **Суммарный вес 10 баллов.** Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
8/9	Стандартизация, сертификация и управление качеством программного обеспечения	4-ая контрольная точка, формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся	Устный опрос выполняется в аудитории. **Суммарный вес 35 баллов**

7.3.1. Типовые контрольно-измерительные задания текущего контроля для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Контрольно-измерительные материалы по блоку «Концепция цифровой безопасности»

Вопросы для подготовки к устному опросу обучающихся

1. Что понимается под системой управления экономическим объектом?
2. В чем заключается иерархичность систем управления?
3. Что такое информационный контур организации и информационная система?
4. Что такое принятие решения? В чем заключается процесс принятия решения?
5. Как влияют уровни и функции управления на информационную систему организации?
6. Что такое дискретность управления, каково его влияние на частоту получения информации и принятия решений?
7. Что такое информация?
8. Чем отличаются данные от информации?
9. Какая информация является экономической?
10. Охарактеризуйте особенности экономической информации.
11. Перечислите основные характеристики экономической информации.
12. По каким признакам классифицируют экономическую информацию?
13. Перечислите виды экономической информации по функциям управления.
14. Какая информация является входной и выходной для организации?
15. Что такое информация из внешней и внутренней среде организации?
16. Каковы свойства информации?
17. Что такое документ, документооборот?
18. Какова классификация документов?
19. Какие преимущества обеспечивает унификация форм документов?
20. Что понимают под информационными ресурсами?
21. В чем заключается управление информационными ресурсами?

Контрольно-измерительные материалы по блоку «Концепция цифровой безопасности»

Вопросы для подготовки к устному опросу обучающихся

1. Что такое информационная система?
2. Как можно классифицировать информационные системы?
3. Как можно представить процессы, происходящие в информационной системе?
4. Приведите примеры информационных систем, поддерживающих деятельность фирмы.
5. Как Вы представляете структуру информационной системы?
6. Какова миссия информационных систем?

7. Укажите состав и свойства обеспечивающей и функциональных частей автоматизирован-ной информационной системы.
8. Дайте определение функциональным компонентам ИС.
9. Охарактеризуйте основные фазы управления, согласно которым определяется состав функциональных подсистем ИС.

Контрольно-измерительные материалы по блоку «Концепция цифровой безопасности»

Вопросы для подготовки к устному опросу обучающихся

1. Охарактеризуйте жизненный цикл ИС.
2. Каковы основные стадии и этапы разработки ИС?
3. Какова роль заказчика в создании ИС?
4. Назовите основные рекомендации при использовании типовых проектных решений в разработке ИС?

Контрольно-измерительные материалы по блоку «Концепция цифровой безопасности»

Вопросы для подготовки к устному опросу обучающихся

1. Перечислите технические каналы утечки информации.
2. Перечислите средства защиты акустического канала
3. Перечислите средства защиты визуального канала
4. Перечислите средства защиты вибрационного канала
5. Перечислите средства защиты электромагнитного канала
6. Перечислите средства защиты индукционного канала
7. Что такое спец.обследование?
8. Что такое спец.исследование?

Контрольно-измерительные материалы по блоку «Криптографические и стеганографические методы защиты»

Вопросы для подготовки к устному опросу обучающихся

1. Что такое программно-аппаратные средства защиты информации?
2. Что такое программные средства защиты информации?
3. Какие механизмы реализуют программно-аппаратные средства защиты информации?
4. Какие компьютерные угрозы безопасности существуют?
5. Что такое сниффинг? Какие методы защиты против него существуют?
6. Что такое IP-спуффинг? Какие методы защиты против него существуют?
7. Что такое сетевая разведка? Какие методы защиты против нее существуют?
8. Что такое переполнение буффера? Какие методы защиты против него существуют?
9. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
10. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
11. Что такое фишинг? Какие методы защиты против него существуют?
12. Что такое компьютерный вирус? Какие виды вирусов существуют?

13. Опишите механизм работы вируса. Как вирус может проникнуть на компьютер?
14. Какие существуют механизмы работы антивируса? Опишите их.
15. Что такое фаервол?

Контрольно-измерительные материалы по блоку «Криптографические и стеганографические методы защиты»

Вопросы для подготовки к устному опросу обучающихся

1. Что такое шифр?
2. Какие виды шифров существуют?
3. Что такое симметричный шифр? Какие симметричные шифры используются сейчас?
4. Что такое ассиметричный шифр? Какие ассиметричные шифры используются сейчас?
5. Что такое хеш-функция? Какие виды хеш-функций вы знаете?
6. Какие хеш-функции используются сейчас?
7. Что такое цифровая подпись?
8. Что такое инфраструктура открытых ключей?
9. Что такое аутентификация? Что такое идентификация?
10. Какие протоколы аутентификации вы знаете?
11. Какие криптографические протоколы используются в компьютерных сетях? Опишите их.

Контрольно-измерительные материалы по блоку «Криптографические и стеганографические методы защиты»

Вопросы для подготовки к устному опросу обучающихся

1. Какие основные законы в области защиты информации в РФ?
2. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
3. Что такое концепция информационной безопасности?
4. Что такое конфиденциальная информация?
5. Что такое персональные данные?
6. В каких случаях возможно использовать персональные данные без согласия обладателя?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна?
9. Что такое коммерческая тайна?
10. Что такое режим коммерческой тайны?
11. Что такое государственная тайна?
12. Опишите правовой режим государственной тайны.
13. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

Контрольно-измерительные материалы по блоку «Криптографические и стеганографические методы защиты»

Вопросы для подготовки к устному опросу обучающихся

1. Какие основные международные стандарты в области информа-ционной безопасности существуют?
2. Что такое "Единые критерии"
3. Как связаны международные стандарты и стандарты РФ?
4. Какие основные стандарты РФ в области информационной безо-пасности существуют?
5. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
6. Что такое политика безопасности?
7. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

Контрольно-измерительные материалы по блоку «Инстументы защиты информации»

Вопросы для подготовки к устному опросу обучающихся

1. Что такое инженерная защита объектов?
2. Какие виды сигнализаций устанавливаются для обеспечения ин-женерной защиты?
3. Что такое технические каналы утечки информации?
4. Перечислите основные виды технических каналов утечки ин-формации?
5. Перечислите методы защиты информации от утечки по визуаль-ному каналу.
6. Перечислите методы защиты информации от утечки по воздуш-ному каналу.
7. Перечислите методы защиты информации от утечки по вибраци-онному каналу.
8. Перечислите методы защиты информации от утечки по индук-ционному каналу.
9. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
10. Перечислите основные мероприятия по обеспечению защиты информации от утеч-ки по техническим каналам.

Контрольно-измерительные материалы по блоку «Инстументы защиты информации»

Вопросы для подготовки к устному опросу обучающихся

1. Какие виды компьютерных угроз существуют?
2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?
9. Какую роль несет журналирование действий в программно-аппаратных средствах защи-ты информации?
10. Что такое средства стеганографической защиты информации?

Контрольно-измерительные материалы по блоку «Инстументы защиты информации»

Вопросы для подготовки к устному опросу обучающихся

1. Какие виды компьютерных угроз существуют?

2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?
9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
10. Что такое средства стеганографической защиты информации?
"

Контрольно-измерительные материалы по блоку «Инстументы защиты информации»

Вопросы для подготовки к устному опросу обучающихся

Определение и описание архитектуры программного обеспечения. Базовые средства по созданию архитектуры ПО. Способы формального представления знаний. Основы устройства и использование экспертных систем в разработке адаптируемого программного обеспечения. Основные направления интеллектуализации ПО.

Контрольно-измерительные материалы по блоку «стандартизация, сертификация и управление качеством программного обеспечения»

Вопросы для подготовки к устному опросу обучающихся

Перечень тем рефератов:

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

Контрольно-измерительные материалы по блоку «стандартизация, сертификация и управление качеством программного обеспечения»

Вопросы для подготовки к устному опросу обучающихся

"Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного обеспечения. Определение ЖЦ международным стандартом ISO/IEC 12207:1995. Основные процессы ЖЦ ПО. Вспомогательные процессы ЖЦ ПО. Организационные процессы ЖЦ ПО. Взаимосвязь между процессами ЖЦ ПО."

Контрольно-измерительные материалы по блоку «стандартизация, сертификация и управление качеством программного обеспечения»

Вопросы для подготовки к устному опросу обучающихся

"Разработка требований и внешнее проектирование ПО. Анализ и разработка требований к ПО. Определение целей создания ПО. Разработка внешний спецификаций проекта. Использование программной инженерии при разработки ПО. Понятие CASE ? технологии.

Обзор CASE-средств для проектирования ПО. Стандартизация и метрология в разработке программного обеспечения. Понятие качественного ПС и связанные с ним характеристики. Стандартизация показателей качества ПС. Характеристики качества базового международного стандарта ISO 9126:1991. Надежность ПО. Основные количественные показатели надежности. Классификация моделей надежности. "

Контрольно-измерительные материалы по блоку «стандартизация, сертификация и управление качеством программного обеспечения»

Вопросы для подготовки к устному опросу обучающихся

"Определение и принципы тестирования ПО. Категории ошибок. Тестирование и отладка программ. Аксиомы тестирования.Средства тестирования. Анализ рисков как средство тестирования. Процесс тестирования. Методы тестирования программ. Методы проектирования тестовых наборов данных. Сборка программ при тестировании."
"

7.3.2. Типовые контрольно-измерительные задания промежуточной аттестации для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Краткие методические указания по подготовке к промежуточной аттестации (зачёту и экзамену) в процессе освоения образовательной программы

Подготовка к зачёту способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к зачёту, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На зачёте студент демонстрирует то, что он приобрел в процессе обучения по учебной дисциплине.

В период подготовки к зачёту студенты вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

При подготовке к зачёту студентам целесообразно использовать материалы лекций, учебно-методические комплексы, рекомендованные правовые акты, основную и дополнительную литературу.

На зачёт выносится материал в объёме, предусмотренном рабочей программой учебной дисциплины за семестр. Зачёт проводится в устной форме.

Ведущий данную дисциплину преподаватель составляет билеты, которые утверждаются руководителем ОПОП и включают в себя два (три) вопроса включающих ситуационные задачи. Формулировка вопросов совпадает с формулировкой перечня рекомендованных для подготовки вопросов зачёта, доведенного до сведения студентов накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины. В аудитории, где проводится устный зачёт, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего зачёт.

На подготовку к ответу на билет на зачёте отводится 20 минут.

Для прохождения зачёта студенту необходимо иметь при себе зачетную книжку и письменные принадлежности. Зачёт принимает преподаватель, читавший учебную дисциплину в данном учебном потоке (группе). За нарушение дисциплины и порядка студенты могут быть удалены с зачёта.

Вопросы для промежуточной аттестации в форме зачета (устно) , проводимого в 5 семестре очной формы, 6 семестре заочной формы, по блоку Концепция цифровой безопасности

1. Понятие информации
2. Доступ к информации
3. Информационные системы
4. Обработка информации
5. Защита информации
6. Информационная безопасность
7. Какие основные международные стандарты в области информа-ционной безопасности существуют?
8. Что такое "Единые критерии"
9. Как связаны международные стандарты и стандарты РФ?
10. Какие основные стандарты РФ в области информационной безо-пасности существуют?
11. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
12. Что такое политика безопасности?
13. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?
14. Что такое инженерная защита объектов?
15. Какие виды сигнализаций устанавливаются для обеспечения ин-женерной защиты?
16. Что такое технические каналы утечки информации?
17. Перечислите основные виды технических каналов утечки ин-формации?
18. Перечислите методы защиты информации от утечки по визуаль-ному каналу.
19. Перечислите методы защиты информации от утечки по воздуш-ному каналу.
20. Перечислите методы защиты информации от утечки по вибраци-онному каналу.
21. Перечислите методы защиты информации от утечки по индук-ционному каналу.
22. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
23. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.
24. Схема построения информационной безопасности на уровне государства.
25. Назначение и задачи в сфере обеспечения безопасности.
26. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства

Перечень вопросов для промежуточной аттестации в форме устного экзамена , проводимого в 6 семестре очной формы 7 семестре заочной формы по блоку «Криптографические и стеганографические методы защиты»

1.Что такое криптография?
2. Какие используются симметричные алгоритмы шифрования?
3. Какие используются ассиметричные алгоритмы шифрования?
4. Что такое криптографическая хеш-функция?
5. Какие используются криптографические хеш-функции?
6. Что такое цифровая подпись?
7. Что такое инфраструктура открытых ключей?
8. Какие российские и международные стандарты на формирование цифровой подписи существуют?

9. Какие основные криптографические протоколы используются в сетях?
10.Использование средств стеганографии для защиты файлов
11.Методы создания защищенного канала связи средствами виртуальной частной сети.

Перечень вопросов для промежуточной аттестации в форме устного экзамена/зачёта , проводимого в 7 семестре очной формы/ 8 семестре заочной формы по блоку «Инструменты защиты информации»

1. Информационная безопасность страны.
2. Защита экономических систем.
3. Обмен конфиденциальной информацией.
4. Структура банковских
5. информационных систем в области защиты информации.
6. Важность защиты
7. экономических систем.
8. Электронные деньги и безопасность финансовых
9. переводов.
10. Концепция информационной безопасности. Основные сведения и
11. положения.
12. .Какие виды компьютерных угроз существуют?
13. Что такое брандмауэр?
14. Что такое антивирусная программа?
15. Что такое эвристический алгоритм поиска вирусов?
16. Что такое сигнатурный поиск вирусов?
17. Методы противодействия сниффингу?
18. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
19. Что такое механизм контроля и разграничения доступа?
20. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
21. Что такое средства стеганографической защиты информации?
22. Определение и описание архитектуры программного обеспечения.
23. Базовые средства по созданию архитектуры ПО.
24. Способы формального представления знаний.
25. Основы устройства и использование экспертных систем в разработке адаптируемого программного обеспечения.
26. Основные направления интеллектуализации ПО.

Перечень вопросов для промежуточной аттестации в форме устного экзамена , проводимого в 8 семестре очной формы/ 9 семестре заочной формы по блоку «Стандартизация, сертификация и управление качеством программного обеспечения»

1. Жизненный цикл программного обеспечения.
2. Понятие жизненного цикла (ЖЦ) программного обеспечения.
3. Определение ЖЦ международным
4. стандартом ISO/IEC 12207:1995.
5. Основные процессы ЖЦ ПО.
6. Вспомогательные процессы ЖЦ ПО.

7. Организационные процессы ЖЦ ПО.
8. Взаимосвязь между процессами ЖЦ ПО.
9. Разработка требований и внешнее проектирование ПО.
10. Анализ и разработка требований к ПО.
11. Определение целей создания ПО.
12. Разработка внешний спецификаций проекта.
13. Использование программной инженерии при разработки ПО.
14. Понятие CASE технологии.
15. Обзор CASE-средств для проектирования ПО.
16. Стандартизация и метрология в разработке программного обеспечения.
17. Понятие качественного ПС и связанные с ним
18. характеристики.
19. Стандартизация показателей качества ПС.
20. Характеристики качества базового международного стандарта ISO 9126:1991. Надежность ПО.
21. Основные количественные показатели надежности.
22. Классификация моделей надежности.
23. Структурный подход к проектированию программного обеспечения.
24. Характеристика и основные принципы структурного подхода.
25. SADT (Structured Analysis and Design Technique), DFD (Data Flow Diagrams) и ERD (Entity-Relationship Diagrams) модели структурного подхода.
26. Концепции функциональной модели SADT.
27. Состав функциональной модели.
28. Построение иерархии диаграмм моделей стандарта IDEF0.
29. Типы связей между функциями.
30. Определение и принципы тестирования ПО.
31. Категории ошибок.
32. Тестирование и отладка программ.
33. Аксиомы тестирования.
34. Средства тестирования.
35. Анализ рисков как средство тестирования.
36. Процесс тестирования.
37. Методы тестирования программ.
38. Методы проектирования тестовых наборов данных.
39. Сборка программ при тестировании.

7.4. Содержание занятий семинарского типа.

Практическое занятие № 1.

Вид практического занятия: Семинар, контрольная точка 1, в форме устного опроса
Раздел: Концепция цифровой безопасности
Тема и содержание занятия: Тема 1.1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
Практические навыки: Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
Вопросы, выносимые на обсуждение:
Понятие информации
Доступ к информации
Информационные системы
Обработка информации
Защита информации
Информационная безопасность
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 1)

Практическое занятие № 2.

Вид практического занятия: Практическая работа, контрольная точка 2, в форме устного опроса
Раздел: Концепция цифровой безопасности
Тема и содержание занятия: Тема 1.2. Организационное обеспечение информационной безопасности.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия:
Практические навыки:
Вопросы, выносимые на обсуждение:
1. Какие основные международные стандарты в области информа-ционной безопасности существуют?
2. Что такое "Единые критерии"
3. Как связаны международные стандарты и стандарты РФ?
4. Какие основные стандарты РФ в области информационной безо-пасности существуют?
5. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
6. Что такое политика безопасности?
7. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 3.
Вид практического занятия: Практическая работа, контрольная точка 3, в форме устного опроса
Раздел: Концепция цифровой безопасности
Тема и содержание занятия: Тема 1.3.Технические средства и методы защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия:
Практические навыки:

Вопросы, выносимые на обсуждение:
1. Что такое инженерная защита объектов?
2. Какие виды сигнализаций устанавливаются для обеспечения ин-женерной защиты?
3. Что такое технические каналы утечки информации?
4. Перечислите основные виды технических каналов утечки ин-формации?
5. Перечислите методы защиты информации от утечки по визуаль-ному каналу.
6. Перечислите методы защиты информации от утечки по воздуш-ному каналу.
7. Перечислите методы защиты информации от утечки по вибраци-онному каналу.
8. Перечислите методы защиты информации от утечки по индук-ционному каналу.
9. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
10. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 3).

Практическое занятие № 4.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 4, контроль в форме устного опроса.
Раздел: Концепция цифровой безопасности
Тема и содержание занятия: Тема 1.4 Назначение и задачи в сфере обеспечения информационной
безопасности на уровне государства.
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия:
Практические навыки:
Вопросы, выносимые на обсуждение:
Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 4)

Практическое занятие № 5.

Вид практического занятия: Практическая работа, контрольная точка 1, контроль в форме устного опроса.
Раздел: Криптографические и стеганографические методы защиты
Тема и содержание занятия: Тема 2.1. Криптографические методы защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование криптографических средств защиты информации
Практические навыки:
Вопросы, выносимые на обсуждение:
Что такое криптография?
2. Какие используются симметричные алгоритмы шифрования?
3. Какие используются ассиметричные алгоритмы шифрования?

4. Что такое криптографическая хеш-функция?
5. Какие используются криптографические хеш-функции?
6. Что такое цифровая подпись?
7. Что такое инфраструктура открытых ключей?
8. Какие российские и международные стандарты на формирование цифровой подписи существуют?
9. Какие основные криптографические протоколы используются в сетях?

Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 1).

Практическое занятие № 6.

Вид практического занятия: Практическая работа, контрольная точка 2, в форме устного опроса
Раздел:
Тема и содержание занятия: Тема 2.2. Реализация работы инфраструктуры открытых ключей.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование инфраструктуры открытых ключей
Практические навыки:
Вопросы, выносимые на обсуждение:
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 7.

Вид практического занятия: Практическая работа, контрольная точка 3, в форме устного опроса
Раздел:
Тема и содержание занятия: Тема 2.3. Средства стеганографии для защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование средств стеганографии для защиты файлов
Практические навыки: Использование средств стеганографии для защиты файлов
Вопросы, выносимые на обсуждение:
Использование средств стеганографии для защиты файлов
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 3).

Практическое занятие № 8.

Вид практического занятия: Практическая работа, контрольная точка 4, в форме презентации и устного опроса
Раздел:
Тема и содержание занятия: Тема 2.4. Настройка безопасного сетевого соединения.
Практическое занятие, предусматривающее применение кейс технологии, контроль в форме презентации и устного опроса
Цель занятия: создание защищенного канала связи средствами виртуальной частной сети.

Практические навыки: Создание защищенного канала связи средствами виртуальной частной сети.
Вопросы, выносимые на обсуждение:
Методы создания защищенного канала связи средствами виртуальной частной сети.
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 4).

Практическое занятие № 9.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 1, в форме группового обсуждения рефератов
Раздел: Инстументы защиты информации
Тема и содержание занятия: Тема 3.1. Место информационной безопасности экономических систем в национальной безопасности страны.
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия:
Практические навыки:
Вопросы, выносимые на обсуждение:
Информационная безопасность страны. Защита экономических систем.
Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 1)

Практическое занятие № 10.

Вид практического занятия: Практическая работа, контрольная точка 2, в форме устного опроса
Раздел: Инстументы защиты информации
Тема и содержание занятия: Тема 3.2. Антивирусные средства защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки использования настроек средств антивирусной защиты информации
Практические навыки: Изучение настроек средств антивирусной защиты информации
Вопросы, выносимые на обсуждение:
1. Какие виды компьютерных угроз существуют?
2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?

9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
10. Что такое средства стеганографической защиты информации?

Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 11.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 3, в форме группового обсуждения рефератов
Раздел: Инстументы защиты информации
Тема и содержание занятия: Тема 3.3. Объектно-ориентированный подход к проектированию программного обеспечения.
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки использования объектно-ориентированного подхода к проектированию программного обеспечения
Практические навыки: Изучение объектно-ориентированного подхода к проектированию программного обеспечения
Вопросы, выносимые на обсуждение:
Определение и описание архитектуры программного обеспечения. Базовые средства по созданию архитектуры ПО. Способы формального представления знаний. Основы устройства и использование экспертных систем в разработке адаптируемого программного обеспечения. Основные направления интеллектуализации ПО.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 3).

Практическое занятие № 12.

Вид практического занятия: Практическая работа, контрольная точка 4, в форме устного опроса
Раздел: Инстументы защиты информации
Тема и содержание занятия: Тема 3.4.Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки выявления нарушений информационной безопасности
Практические навыки: Изучение объектно-ориентированного подхода к проектированию программного обеспечения
Вопросы, выносимые на обсуждение:
Перечень тем рефератов: 1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними 2. Современные средства защиты информации 3. Современные системы компьютерной безопасности 4. Современные средства противодействия экономическому шпионажу 5. Современные криптографические системы 21 6. Криптоанализ, современное состояние 7. Правовые основы защиты информации 8. Технические аспекты обеспечения защиты информации. Современное

состояние 9. Атаки на систему безопасности и современные методы защиты 10. Современные пути решения проблемы информационной безопасности РФ
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 4)

Практическое занятие № 13.

Вид практического занятия: Практическая работа, контрольная точка 1, контроль в форме устного опроса.
Раздел: Стандартизация, сертификация и управление качеством программного обеспечения
Тема и содержание занятия: Тема 4.1. Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного обеспечения.
Практическое занятие, предусматривающее Обсуждение. Выполнение проектного задания
Цель занятия:
Практические навыки:
Вопросы, выносимые на обсуждение:
Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного обеспечения. Определение ЖЦ международным стандартом ISO/IEC 12207:1995. Основные процессы ЖЦ ПО. Вспомогательные процессы ЖЦ ПО. Организационные процессы ЖЦ ПО. Взаимосвязь между процессами ЖЦ ПО.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 1).

Практическое занятие № 14.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 2, контроль в форме устного опроса.
Раздел: Стандартизация, сертификация и управление качеством программного обеспечения
Тема и содержание занятия: Тема 4.2. Управление разработкой ПО..
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки управления разработкой ПО.
Практические навыки:
Вопросы, выносимые на обсуждение:
Разработка требований и внешнее проектирование ПО. Анализ и разработка требований к ПО. Определение целей создания ПО. Разработка внешний спецификаций проекта. Использование программной инженерии при разработки ПО. Понятие CASE ? технологии. Обзор CASE-средств для проектирования ПО. Стандартизация и метрология в разработке программного обеспечения. Понятие качественного ПС и связанные с ним характеристики. Стандартизация показателей качества ПС. Характеристики качества базового международного стандарта ISO 9126:1991. Надежность ПО. Основные количественные показатели надежности. Классификация моделей надежности.

Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 15.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 3.
Раздел: Стандартизация, сертификация и управление качеством программного обеспечения
Тема и содержание занятия: Тема 4.3. Структурный подход к проектированию и управление качеством программного обеспечения.
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки подхода к проектированию и управлению качеством программного обеспечения
Практические навыки:
Вопросы, выносимые на обсуждение:
Структурный подход к проектированию программного обеспечения. Характеристика и основные принципы структурного подхода. SADT (Structured Analysis and Design Technique), DFD (Data Flow Diagrams) и ERD (Entity-Relationship Diagrams) модели структурного подхода. Концепции функциональной модели SADT. Состав функциональной модели. Построение иерархии диаграмм моделей стандарта IDEF0. Типы связей между функциями.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 3).

Практическое занятие № 16.

Вид практического занятия: Практическая работа, контрольная точка 4, контроль в форме устного опроса.
Раздел: Стандартизация, сертификация и управление качеством программного обеспечения
Тема и содержание занятия: Тема 4.4. Тестирование, отладка и сборка ПО..
Практическое занятие, предусматривающее Обсуждение. Выполнение проектного задания
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки тестирования, отладка и сборки ПО.
Практические навыки:
Вопросы, выносимые на обсуждение:
Определение и принципы тестирования ПО. Категории ошибок. Тестирование и отладка программ. Аксиомы тестирования.
Средства тестирования. Анализ рисков как средство тестирования. Процесс тестирования. Методы тестирования программ. Методы проектирования тестовых наборов данных. Сборка программ при тестировании.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 4).

8. Перечень основной и дополнительной учебной литературы; перечень ресурсов информационно-телекоммуникационной сети «Интернет», перечень информационных технологий, необходимых для освоения дисциплины

8.1 Основная литература

1.Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 413 с.: - (Высшее образование: Бакалавриат) - Режим доступа: http://znanium.com/catalog/product/1022055

2. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 - Режим доступа: http://znanium.com/catalog/product/474838

3. Стандартизация, сертификация и управление качеством программного обеспечения: Учебное пособие / Ананьева Т.Н., Новикова Н.Г., Исаев Г.Н. - М.:НИЦ ИНФРА-М, 2016. - 232 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (П) ISBN 978-5-16-011711-9 - Режим доступа: http://znanium.com/catalog/product/541003

8.2 Дополнительная литература

1.Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ "Об информации,информационных технологиях и защите информации" (постатейный) / А.И.Савельев - М.: Статут, 2015. - 320 с.: 60x84 1/16 (Обложка) ISBN 978-5-8354-1150-4 - Режим доступа: http://znanium.com/catalog/product/528227

8.3. Базы данных, информационно-справочные и поисковые системы

Электронно-библиотечная система «Znanium.com»:http://znanium.com/
Информационная система «Единое окно доступа к образовательным ресурсам»:http://window.edu.ru/
Служба тематических толковых словарей «Глоссарий.ру»:http://www.glossary.ru/
Научная электронная библиотека «КиберЛенинка»:https://cyberleninka.ru/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Microsoft Windows
2. Microsoft Office
3. База данных сервисных центров «Сервисбокс» [профессиональная база данных]: https://www.servicebox.ru/
4. База данных «Российский бизнес-портал «BazaRF.ru» [профессиональная база данных]: http://www.baza-r.ru/enterprises
5. Справочная правовая система КонсультантПлюс
6. Интернет-версия системы Гарант (информационно-правовой портал "Гарант.ру

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

Процесс изучения дисциплины «Основы цифровой безопасности» предусматривает аудиторную (работа на лекциях и практических занятиях) и внеаудиторную (самоподготовка к лекциям и практическим занятиям) работу обучающегося.

В качестве основной методики обучения была выбрана методика, включающая - совокупность приёмов, с помощью которых происходит целенаправленно организованный, планомерно и систематически осуществляемый процесс овладения знаниями, умениями и навыками.

В качестве основных форм организации учебного процесса по дисциплине «Основы цифровой безопасности» в предлагаемой методике обучения выступают лекционные и практические занятия (с использованием интерактивных технологий обучения), а так же самостоятельная работа обучающихся.

Лекции

Лекция с мультимедийными презентациями и применением видеоматериалов, которая предполагает научное выступление лектора с обоснованием процессов и явлений, предусмотренных областью лекционного материала.

Теоретические занятия(лекции) организуются по потокам. На лекциях излагаются темы дисциплины, предусмотренные рабочей программой, акцентируется внимание на наиболее принципиальных и сложных вопросах дисциплины, устанавливаются вопросы для самостоятельной проработки. Конспект лекций является базой при подготовке к практическим занятиям, к экзаменам, а также самостоятельной научной деятельности.

Изложение лекционного материала проводится в мультимедийной форме (презентаций). Смысловая нагрузка лекции смещается в сторону от изложения теоретического материала к формированию мотивации самостоятельного обучения через постановку проблем обучения и показ путей решения профессиональных проблем в рамках той или иной темы. При этом основным методом ведения лекции является метод проблемного изложения материала.

Практические занятия

Практические занятия по дисциплине «Основы цифровой безопасности» проводятся с целью приобретения практических навыков в области разработки разделов компьютерное проектирование сферы сервиса.

Занятия проводятся в форе: интерактивного практического занятия с использованием компьютерной техники. Практическая работа заключается в выполнении студентами, под руководством преподавателя, комплекса учебных заданий направленных на приобретение практических навыков разработки разделов дисциплины «Основы цифровой безопасности». Выполнения практической работы студенты производят в интерактивном виде, в виде презентаций результата преподавателя. Отчет предоставляется преподавателю, ведущему данный предмет, в электронном и печатном виде.

Практические занятия способствуют более глубокому пониманию теоретического материала учебного курса, а также развитию, формированию и становлению различных уровней составляющих профессиональной компетентности студентов.

10. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю):

Учебные занятия по дисциплине «Основы цифровой безопасности» проводятся в следующих оборудованных учебных кабинетах:

Вид учебных занятий по дисциплине	Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий с перечнем основного оборудования
Лекции	Поточная аудитория (видеопроекционная аппаратура с возможностью подключения к ПК, персональный компьютер, экран, доска, учебная мебель)
Практические занятия	Компьютерный класс 1109 или 1409 (персональные компьютеры, доска, учебная мебель)
Самостоятельная работа обучающихся	Читальный зал Научно-технической библиотеки университета Компьютерный класс 1409 (Учебная мебель, 20 компьютеров с возможностью выхода в информационно-телекоммуникационную сеть «Интернет», Экран, 19 компьютеров)