Аннотация к рабочей программе дисциплины «Управление разработкой систем безопасности»

Цель преподавания дисциплины

Цель дисциплины – ознакомление студентов с основными способами, методами, принципами, технологиями и средствами управления, проектирования, создания и модернизации защищённых информационных систем для решения задач профессиональной деятельности проектного, научно-исследовательского и организационно-управленческого типов.

Задачи изучения дисциплины

Задачами дисциплины являются:

1. Изучение основных методов и способов защиты информации, передаваемой в информационных системах и сетях, а также основных принципов, используемых при организации и проведении мероприятий по защите информации на объектах защиты.

2. Изучение принципов работы и основных технических характеристик средств защиты информации, передаваемой в информационных системах и сетях.

3. Овладение навыками по разработке, проектированию и модернизации защищённых информационных систем; навыками проведения теоретических и экспериментальных исследований защищённости информационных систем; навыками организации, планирования и управления коллективами по созданию защищённых информационных систем; навыками управления персоналом, обслуживающим защищённые информационные системы.

4. Изучение обязанностей персонала по разработке и обслуживанию информационных систем; изучение задач при проведении работ по развитию, модернизации защищённой информационной системы.

5. Анализ требований, предъявляемых к программным, программно-аппаратным и техническим средствам и системам защиты информации.

6. Изучение эксплуатационной документации и овладение навыками проведения процедур сертификации и аттестации средств и систем защиты и объектов информатизации; изучение основных нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации.

7. Анализ проблемных ситуаций на основе системного и междисциплинарных подходов.

8. Обеспечение совместно с другими дисциплинами семестра теоретической подготовки обучающихся к производственной эксплуатационной практике
на предприятии-заказчике.

Индикаторы компетенций, формируемые в результате освоения дисциплины

УК-1.4 Разрабатывает и аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.

УК-3.1 Вырабатывает стратегию сотрудничества и на её основе организует отбор членов команды для достижения поставленной цели.

УК-3.2 Планирует и корректирует работу команды с учётом интересов, особенностей поведения и мнений её членов.

УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.

УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям

УК-3.5 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.

УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания.

ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей.

ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем.

ПК-1.3 Разрабатывает техническое задание на проектирование защищённых информационных систем

ПК-3.1 Разрабатывает формальные модели обработки и передачи данных в информационных системах.

ПК-4.1 Согласовывает с уполномоченными федеральными органами исполнительной власти условия поставки средств и систем защиты

ПК-4.2 Организовывает и проводит аттестацию средств и систем защиты

ПК-4.3 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации

Разделы дисциплины

Основные аспекты построения системы информационной безопасности.

Мероприятия по защите информации. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. Оценочные стандарты и технические спецификации. Критерии оценки безопасности информационных технологий. Руководящие документы ФСТЭК России.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«30» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление разработкой систем безопасности
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность,
(шифр и наименование направления подготовки)

направленность (профиль) «Защищенные информационные системы»
(наименование направленности (профиля))

форма обучения очная

ОПОП ВО реализуется по модели дуального обучения

Курск – 2023

Рабочая программа дисциплины составлена:

– в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455;

– на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № 12 от 29.05.2023).

– с учетом заказа-требования от 28.04.2023 на результаты освоения ОПОП ВО – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения в ФГБОУ ВО «Юго-Западный государственный университет», от ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(приложение к общей характеристике ОПОП ВО).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для дуального обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы» на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № 8 от 29.05.2023).

Зав. кафедрой _____ А.Л. Марухленко

Разработчик программы
к.т.н. _____ Е.А. Кулешова

Директор научной библиотеки _____ В.Г. Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО дуального обучения 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № __ от __. __. 20__), на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № __ от __. __. 20__).

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Цель дисциплины – ознакомление студентов с основными способами, методами, принципами, технологиями и средствами управления, проектирования, создания и модернизации защищённых информационных систем для решения задач профессиональной деятельности проектного, научно-исследовательского и организационно-управленческого типов.

1.2 Задачи дисциплины

Задачами дисциплины являются:

1. Изучение основных методов и способов защиты информации, передаваемой в информационных системах и сетях, а также основных принципов, используемых при организации и проведении мероприятий по защите информации на объектах защиты.

2. Изучение принципов работы и основных технических характеристик средств защиты информации, передаваемой в информационных системах и сетях.

3. Овладение навыками по разработке, проектированию и модернизации защищённых информационных систем; навыками проведения теоретических и экспериментальных исследований защищённости информационных систем; навыками организации, планирования и управления коллективами по созданию защищённых информационных систем; навыками управления персоналом, обслуживающим защищённые информационные системы.

4. Изучение обязанностей персонала по разработке и обслуживанию информационных систем; изучение задач при проведении работ по развитию, модернизации защищённой информационной системы.

5. Анализ требований, предъявляемых к программным, программно-аппаратным и техническим средствам и системам защиты информации.

6. Изучение эксплуатационной документации и овладение навыками проведения процедур сертификации и аттестации средств и систем защиты и объектов информатизации; изучение основных нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации.

7. Анализ проблемных ситуаций на основе системного и междисциплинарных подходов.

8. Обеспечение совместно с другими дисциплинами семестра теоретической подготовки обучающихся к производственной эксплуатационной практике на предприятии-заказчике.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.4 Разрабатывает и аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	***Знать:*** принципы построения защищённых систем, методы и средства защиты операционных систем, сетевого оборудования, управления доступом, идентификации и аутентификации, настройки межсетевых экранов, защиты от компьютерных вирусов, вопросы организации системы защиты информации в информационных системах (ИС), этапы построения системы защиты информации, политики безопасности, виды угроз и возможные каналы утечки информации, основы проектирования и построения архитектур систем безопасности, методы, модели и технологии проектирования систем безопасности, требования стандартов и руководящих документов, стадии и этапы создания систем безопасности. ***Уметь:*** правильно эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем правильной

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности. ***Владеть:*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры инфокоммутационных систем и сетевой защиты, поиска и обнаружения уязвимых узлов инфокоммуникационных систем и сетей.
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	УК-3.1 Вырабатывает стратегию сотрудничества и на её основе организует отбор членов команды для достижения поставленной цели.	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию ИС сре-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			ди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
		УК-3.2 Планирует и корректирует работу команды с учётом интересов, особенностей поведения и мнений её членов.	***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых защищённых ИС, этапы разработки типовой прикладной ИС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			перечень РКД, ЭД, ПД, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке прикладных ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов; своевременного внесения корректив в разработанную документацию и устранения замечаний,

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов.
		УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.	***Знать:*** классификацию, назначение, конфигурацию, состав, структуру, принципы функционирования типовых защищенных ИС предприятий; основы управления ИС; виды, состав, назначение, принципы функционирования, функции и взаимосвязь основных элементов и компонентов ИС; понятие, типы, примеры архитектур ИС, принципы работы ИС; типовые архитектуры ИС с точки зрения программно-аппаратной реализации; классификацию архитектур; особенности проектирования распределённых систем; методы и средства защиты информации в ИС, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ИС. ***Уметь:*** проводить сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ИС; оценку вариантов предлагаемых к реализации ар-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			хитектур ИС; выбор наиболее оптимального варианта построения предлагаемой архитектуры ИС; формировать требования к структуре ИС исходя из решаемых задач; разрабатывать регламентирующие документы для принятия решения на технических совещаниях; предложения для технических советов с обоснованием выбора предлагаемой архитектуры прикладной ИС. ***Владеть:*** навыками сравнительного анализа технических средств и оборудования из состава прикладных ИС, оценки предлагаемых к реализации вариантов построения прикладных ИС, выбора оптимальной архитектуры прикладной ИС исходя из решаемых системой задач, разрешения конфликтных ситуаций в ходе выполнения работ по разработке защищённых ИС.
		УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям	***Знать:*** порядок внедрения, отладки и этапы разработки систем обеспечения информационной безопасности ИС. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			Владеть: навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС, организации обсуждений результатов работы команды с привлечением оппонентов разработанным идеям в рамках создания защищённых ИС.
		УК-3.5 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять кон-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			троль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания.	***Знать:*** классификацию программно-аппаратных и телекоммуникационных средств защиты, технические характеристики и возможности сетевого оборудования инфокоммуникационных сетей, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, основные действующие нормативные документы и юридические законы в

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			области защиты информации. ***Уметь:*** проводить анализ защищенности локальной вычислительной сети, настраивать режимы работы межсетевых экранов, проводить анализ информационных рисков, определять оптимальный состав программных и аппаратных средств для построения инфокоммуникационных сетей, применять действующие нормативные документы и юридические законы в области защиты информации. ***Владеть:*** навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов, разработки и установки программных средств защиты инфокоммуникационных сетей, определения действующих нормативных требований и юридических законов в области защиты информации.
ПК-1	Способен формировать проектные решения по созданию и модернизации защищённых инфор-	ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых	***Знать:*** Номенклатуру средств разработки телекоммуникационных систем и сетей. Принципы и средства

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	мационных систем	телекоммуникационных систем и сетей.	разработки защищённых ИС, все этапы, методы и средства проектирования защищённых ИС. ***Уметь:*** Формулировать требования к защищённым ИС, реализовывать основные этапы обеспечения безопасности ИС, самостоятельно ставить задачи по обеспечению ИБ ИС, производить их декомпозицию. ***Владеть:*** Базовыми технологиями обеспечения информационной безопасности, основными методами обеспечения ИБ ИС.
		ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем.	***Знать:*** основные подходы к оценке качества защищённых ИС, методики проведения испытаний защищённых ИС, методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** определять функциональные характеристики отдельных структурных компонентов ИС, определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом, самостоятельно разрабатывать программы и методики испытаний средств и систем обеспе-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			чения информационной безопасности. ***Владеть:*** навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков.
		ПК-1.3 Разрабатывает техническое задание на проектирование защищённых информационных систем	***Знать:*** Основные стандарты ИБ, структуру и содержание стандартов ИБ, структуру, содержание и методологические аспекты, лежащие в основе стандартов ИБ. ***Уметь:*** Соотносить требования стандартов ИБ реальным системам, сопоставлять требования стандартов к целым защищённым информационным системам и их отдельным структурным компонентам, обосновывать применение технологий ЗИ . ***Владеть:*** Навыками использования стандартов ИБ для классификации ИС, применения стандартов ИБ, оценки соответствия защищённых информационных систем требованиям стандартов.
ПК-3	Способен проводить теоретические и экспериментальные исследования защищённости информационных систем.	ПК-3.1 Разрабатывает формальные модели обработки и передачи данных в информационных системах.	***Знать:*** основные подходы к оценке качества защищённых ИС, методики проведения теоретических и экспериментальных исследований защищённо-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			сти ИС, методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** определять функциональные характеристики отдельных структурных компонентов ИС, определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом, самостоятельно разрабатывать программы и методики проведения теоретических и экспериментальных исследований средств и систем обеспечения информационной безопасности. ***Владеть:*** навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков, разработки технического облика средств обработки и передачи данных в информационных системах, разработки методик теоретических и экспериментальных исследований защищённости информационных систем.
ПК-4	Способен управлять отношениями с регуляторами в сфере защиты информации	ПК-4.1 Согласовывает с уполномоченными федеральными органами исполнительной власти условия поставки	***Знать:*** руководящие и методические документы уполномоченных федеральных органов исполнительной

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		средств и систем защиты	власти по защите информации и обеспечения безопасности критической информационной инфраструктуры ***Уметь:*** организовывать получение организацией лицензий на лицензируемые виды деятельности по производству товаров и услуг в сфере обеспечения защиты ***Владеть (****или* ***Иметь опыт деятельности):*** согласование с уполномоченными федеральными органами исполнительной власти условий поставки средств и систем защиты
		ПК-4.2 Организовывает и проводит аттестацию средств и систем защиты	***Знать:*** порядок аттестации ЗТКС на соответствие требованиям защиты информации ***Уметь:*** организовывать получение эксплуатирующей ЗТКС организацией разрешительных документов в соответствии с требованиями нормативных правовых актов ***Владеть (****или* ***Иметь опыт деятельности):*** организация и проведение аттестации ЗТКС в соответствии с требованиями нормативных правовых актов
		ПК-4.3 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых	***Знать:*** нормативные правовые акты в области связи, информатизации и защиты информации ***Уметь:***

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		актов, руководящих и методических документов, предъявляемых к системам защиты информации	проводить мониторинг и анализ нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти ***Владеть (****или* ***Иметь опыт деятельности):*** мониторинг нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты СССЭ от НД и обеспечения безопасности критической информационной инфраструктуры

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Управление разработкой систем безопасности» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения.

Дисциплина изучается на 1 курсе в 1 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной эксплуатационной практики, завершающей данный семестр.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зачетные единицы (з.е.), 180 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	90
в том числе:	
лекции	36
лабораторные занятия	-
практические занятия	54, из них практическая подготовка обучающихся – 4.
Самостоятельная работа обучающихся (всего)	52,85
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен(-а)
экзамен (включая консультацию перед экзаменом)	1,15

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

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Основные аспекты построения системы информационной безопасности.	Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Этапы обеспечения информационной безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
2	Мероприятия по защите информации.	Нормативно-законодательный аспект. Процедурный аспект. Программно-технический аспект.
3	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	Структурирование ЗИС. Анализ безопасности ИС на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Критерии адекватности средств защиты**.** Структура профиля защиты ИТ-продукта. Соотношение эффективности и рентабельности систем информационной безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Зависимость эффективности защиты от величины ущерба на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
4	Оценочные стандарты и технические спецификации.	"Оранжевая книга" как оценочный стандарт. Стандарты информационной безопасности распределенных систем. Механизмы реализации сервисов (функций) безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Администрирование средств безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
5	Критерии оценки безопасности информационных технологий.	Основные понятия. Стандарт "Критерии оценки безопасности информационных технологий" . Иерархия класс-семейство-компонент-элемент. Требования доверия безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
6	Руководящие документы ФСТЭК России.	Требования к защищенности автоматизированных систем. Классы защищённости информационных систем. Аспекты защищённых ИС, фигурирующие в требованиях ФСТЭК. Классификация защищённых информационных систем на примере ООО ЦСБ «ЩИТ-ИНФОРМ».

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Основные аспекты построения системы информационной безопасности.	6	-	1	У-1-5 МУ-1-4	УО, ЗПР, ПЗ 1-3	УК-1 УК-3 УК-6 ПК-1 ПК-3 ПК-4
2	Мероприятия по защите информации.	6	-	2	У-1-5 МУ-1-4	УО, ЗПР, КЗ 5-6	УК-1 УК-3 УК-6 ПК-1 ПК-3 ПК-4
3	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	6	-	3	У-1-5 МУ-1-4	УО, ЗПР 7-9	УК-1 УК-3 УК-6 ПК-1 ПК-3 ПК-4
4	Оценочные стандарты и технические спецификации.	6	-	-	У-1-5 МУ-1-4	УО 10	УК-1 УК-3 УК-6 ПК-1 ПК-3 ПК-4
5	Критерии оценки безопасности информационных технологий.	6	-	-	У-1-5 МУ-1-4	УО 11	УК-1 УК-3 УК-6 ПК-1 ПК-3 ПК-4
6	Руководящие документы ФСТЭК России.	6	-	4	У-1-5 МУ-1-4	УО, ЗПР 12-14	УК-1 УК-3 УК-6 ПК-1 ПК-3 ПК-4

УО – устный опрос; ЗПР – защита практической работы; ПЗ – решение производственных задач; КЗ – решение кейса

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

№ п/п	Наименование практической работы	Объем, час.
1	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.	12, из них практическая подготовка обучающихся – 4
2	Определение показателей защищенности информации при несанкционированном доступе.	14
3	Критерии оценки и выбора CASE-средств.	14
4	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	14
Итого		54, из них практическая подготовка обучающихся – 4

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	2	3	4
1.	Основные аспекты построения системы информационной безопасности.	1-3 недели	9
2.	Мероприятия по защите информации.	5-6 недели	8,85
3.	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	7-9 недели	9
4.	Оценочные стандарты и технические спецификации.	10 неделя	8
5.	Критерии оценки безопасности информационных технологий.	11 неделя	9
6	Руководящие документы ФСТЭК России.	12-14 недели	9
Итого			52,85

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельном изучении отдельных тем и вопросов дисциплины студенты могут пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры *информационной безопасности* в рабочее время, установленное Правилами внутреннего распорядка работников университета.

Учебно-методическое обеспечение самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с учебным планом и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– методических указаний к выполнению практических работ и т.д.

типографией университета:

– посредством оказания помощи авторам в подготовке и издании научной, учебной и методической литературы;

– посредством удовлетворения потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Практическая подготовка обучающихся

Реализация программы магистратуры по модели дуального обучения и компетентностного подхода предусматривают широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных и профессиональных компетенций обучающихся.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	2	3	4
1	Мероприятия по защите информации.	Кейс-технология	4
Итого:			4

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения или практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю) программы магистратуры.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях.

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы[1] формирования компетенций и дисциплины (модули), практики, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Современная философия и методология науки Организация работ по обеспечению безопасности в информационных системах	Управление разработкой систем безопасности	
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Управление информационной безопасностью		Управление разработкой систем безопасности
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Управление информационной безопасностью		Управление разработкой систем безопасности
ПК-1 Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	Технологии распределенных реестров Безопасность распределённых систем		Методы и средства защиты информации в системах электронного документооборота Теоретические основы компьютерной безопасности Управление разработкой систем безопасности Производственная проектно-технологическая практика
ПК-3 Способен прово-	Моделирование технических объектов и		Теоретические ос-

дить теоретические и экспериментальные исследования защищённости информационных систем	систем управления Производственная практика по получению умений и навыков управленческой деятельности		новы компьютерной безопасности Управление разработкой систем безопасности Производственная преддипломная практика
ПК-4 Способен управлять отношениями с регуляторами в сфере защиты информации	Организация аудита информационной безопасности Нормативно-правовое регулирование в сфере информационной безопасности	Производственная практика по получению умений и навыков управленческой деятельности	Методы и средства защиты информации в системах электронного документооборота Управление разработкой систем безопасности Производственная преддипломная практика

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(наименование этапа по таблице 6.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Критерии и шкала оценивания компетенций			
		Недостаточный уровень («неудовл.»)	Пороговый уровень («удовл.»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5	6
УК-1/ завершающий	УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на ос-	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-1. Обучающийся нуждается в постоянных подсказках;	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося имеют поверхностный	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-1. Обучающийся имеет хорошие, но не исчерпывающие зна-	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося являются прочными и глубокими, имеют

	нове системного и междисциплинарных подходов	допускает грубые ошибки, которые не может исправить самостоятельно.	характер, имеют место неточности и ошибки.	ния; допускает неточности.	системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-1.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-1.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-1.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-1.
		Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для УК-1, не развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, развиты на элементарном уровне.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, хорошо развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, доведены до автоматизма.
УК-3/ завершающий	УК-3.1 Вырабатывает стратегию сотрудничества и на её основе организует отбор членов команды для достижения поставленной цели. УК-3.2 Планирует	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-3. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.

	и корректирует работу команды с учётом интересов, особенностей поведения и мнений её членов. УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон. УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям УК-3.5 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.	**Уметь:** демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-3.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-3.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-3.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, доведены до автоматизма.

УК-6/ завершающий	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-6. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-6. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-6. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-6. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-6.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-6.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-6.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-6.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, доведены до автоматизма.

ПК-1/ завершающий	ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем ПК-1.3 Разрабатывает техническое задание на проектирование защищённых информационных систем	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-1. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-1. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-1. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-1. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-1.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-1.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-1.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-1.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-1, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-1, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-1, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-1, доведены до автоматизма.

ПК-3/ завершающий	ПК-3.1 Разрабатывает формальные модели обработки и передачи данных в информационных системах	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-3. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-3.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-3.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-3.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, доведены до автоматизма.

ПК-4/ завершающий	ПК-4.1 Согласовывает с уполномоченными федеральными органами исполнительной власти условия поставки средств и систем защиты ПК-4.2 Организовывает и проводит аттестацию средств и систем защиты ПК-4.3 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-4. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-4. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-4. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-4. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-4.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-4.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-4.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-4.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-4, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-4, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-4, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-4, доведены до автоматизма.

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

Таблица 7.3 - Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные аспекты построения системы информационной безопасности.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-4	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Производственная задача	1-10 1-10 1-10	Согласно табл.7.2
2	Мероприятия по защите информации.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-4	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Кейс	1-10 1-10 1	Согласно табл.7.2
3	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-4	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2
4	Оценочные стандарты и технические спецификации.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-4	лекция, СРС	Вопросы для УО	1-10	Согласно табл.7.2
5	Критерии оценки безопасности информационных технологий.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-4	лекция, СРС	Вопросы для УО	1-10	Согласно табл.7.2
6	Руководящие документы ФСТЭК России.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-4	. лекция, практическое занятие, СРС	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2

КВЗПР – контрольные вопросы для защиты практической работы

7.3.1 Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 5. «Критерии оценки безопасности информационных технологий».

1. Опишите иерархию сущностей в "Критериях оценки безопасности информационных технологий".
2. Назовите основные термины, описанные в "Критериях оценки безопасности информационных технологий".
3. Опишите структуру класса «приватность».
4. Опишите структуру класса «использование ресурсов».
5. Что такое требования доверия безопасности и для чего они нужны?

Контрольные вопросы для защиты практической работы №2:

Определение показателей защищенности информации при несанкционированном доступе.

1. В чем заключаются основные принципы проектирования защищённых систем?
2. Перечислите показатели качества процесса проектирования.
3. Постановка проблемы комплексного обеспечения информационной безопасности защищённых систем.
4. Основы методологии многовариантного планирования процесса проектирования.
5. Методы и методики проектирования комплексных систем информационной безопасности от несанкционированного доступа.

Производственная задача по теме 1

Задача планирования процесса разработки системы безопасности: Вам поручено управлять процессом разработки системы безопасности для нового проекта. Ваша задача - разработать детальный план, включающий определение целей системы безопасности, этапы разработки, ресурсы, сроки и оценку затрат. Учтите различные аспекты, такие как угрозы, требования безопасности и бюджет.

Кейс по теме 2

Компания X решила разработать и внедрить новую систему безопасности для защиты своих информационных ресурсов. Ваша задача - управлять процессом разработки этой системы и обеспечить ее успешное внедрение. Вот описание кейса:

Компания XYZ является крупным провайдером интернет-услуг и хранит значительное количество конфиденциальной информации о своих клиентах. В связи с увеличением числа кибератак и угроз информационной безопасности, компания решила усилить свою систему защиты данных.

Ваша роль - управляющего проектом по разработке и внедрению новой системы безопасности. Вам предоставлены следующие задачи:

1. Определение требований безопасности: Проведите анализ уязвимостей и рисков, связанных с текущей системой безопасности компании. Составьте список требований, которые должна удовлетворять новая система, чтобы обеспечить надежную защиту данных и информационных ресурсов компании.
2. Выбор поставщика и технологий: Исследуйте рынок систем безопасности и выберите подходящих поставщиков и технологии. Оцените их опыт, репутацию, функциональность и соответствие требованиям компании. Составьте план закупки и сотрудничества с поставщиками.
3. Управление процессом разработки: Разработайте план процесса разработки новой системы безопасности. Определите этапы разработки, ресурсы, сроки и задачи для каждого этапа. Управляйте командой разработчиков, обеспечивая их синхронную работу, контролируйте выполнение плана и решайте возникающие проблемы.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

7.3.2 Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. На промежуточной аттестации по дисциплине применяется механизм квалификационного экзамена. Экзамен имеет структуру квалификационного экзамена и состоит из 2 частей:

– теоретической (компьютерное тестирование);
– практической (решение компетентностно-ориентированной задачи).

На теоретической части экзамена (тестировании) проверяются знания и частично – умения и навыки обучающихся. Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

– закрытой (с выбором одного или нескольких правильных ответов),
– открытой (необходимо вписать правильный ответ),
– на установление правильной последовательности,
– на установление соответствия.

На практической части экзамена проверяются результаты практической подготовки: *компетенции, включая умения, навыки (или опыт деятельности)*). Результаты практической подготовки *(компетенции, включая умения, навыки (или опыт деятельности))* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных, кейс-задач или кейсов) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

а) Примеры типовых заданий для теоретической части экзамена (тестирования)

Задание в закрытой форме:

1. Руководитель, оценивая результаты создания системы безопасности, прежде всего, должен обратить внимание на:

А) Экономический эффект от внедрения системы.

Б) Функциональную полноту, адаптивность, корректность работы системы.

В) Эффективность использования системой существующей инфраструктуры.

Г) Степень достижения поставленных целей.

Задание в открытой форме:

1. Элементом архитектуры системы безопасности организации является…….

2. Архитектура информационных систем организации включает в себя……..

3. Формальное описание архитектуры предприятия впервые было сформулировано в……...

4. В системном проектировании существуют следующие уровни представления архитектуры ……

Задание на установление правильной последовательности.

Установите последовательность этапов проектирования и разработки защищённой ИС:

1. Внедрение
2. Эксплуатация и модификация
3. Разработка
4. Выявление требований

Задание на установление соответствия между ИТ- ресурсами защищённой ИС и описаниями функционирования её элементов

1	Информация	А	Автоматизированные пользовательские системы, которые собирают, хранят, обрабатывают и распространяют информацию
2	Инфраструктура	Б	Данные во всех формах ввода, хранения, обработки и вывода с помощью информационных систем, в любых формах, которые используются для принятия управленческих решений
3	Персонал	В	Средства (аппаратное и программное обеспечение, системы управления базами данных, сеть, мультимедиа, среда, в которой все это функционирует), которые делают возможным работу приложений
		Г	Люди (специалисты), требующиеся для планирования, организации, установки, эксплуатации и развития информационных систем и сервисов, нанимаемые по контрактам

б) Примеры типовых заданий для практической части экзамена

Компетентностно-ориентированная задача:

Разработайте подробный план проекта разработки системы безопасности, который включает в себя определение этапов, задач, сроков выполнения и ресурсов. Установите ключевые моменты, на которых будет осуществляться контроль прогресса проекта.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– положение П 02.207 «Проектирование и реализация основных профессиональных программ высшего образования – программ магистратуры по модели дуального обучения»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Практическая работа № 1	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по работе	4	Выполнил, правильно и полно ответил на все вопросы по работе
Практическая работа № 2	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по работе	4	Выполнил, правильно и полно ответил на все вопросы по работе
Практическая работа № 3	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по работе	4	Выполнил, правильно и полно ответил на все вопросы по работе
Практическая работа № 4	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по работе	4	Выполнил, правильно и полно ответил на все вопросы по работе
Устный опрос по темам 1-6	8	Не ответил или неполно ответил на какой-либо вопрос	16	Правильно и полно ответил на все вопросы

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Производственная задача	4	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	8	Выполнил, правильно и полно ответил на все вопросы
Кейс	4	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	8	Выполнил, правильно и полно ответил на все вопросы
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

Для проведения промежуточной аттестации обучающихся (теоретической части и практической части) используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов для тестирования и одна компетентностно-ориентированная задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов по промежуточной аттестации – 36.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 с. — ISBN 978-5-4497-0328-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89443.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. Пользователе

2. Милославская, Н. Г. Управление информационной безопасностью. Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2020. — 534 с. — ISBN 978-5-7262-2694-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/125513.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.2 Дополнительная учебная литература

3. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87643.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

4. Газизов, А. Р. Управление информационной безопасностью : учебное пособие / А. Р. Газизов, С. Б. Петренкова, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2019. — 115 с. — ISBN 978-5-7890-1775-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/117771.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/117771

5. Аверченков, В. И. Служба защиты информации. Организация и управление : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. — Брянск : Брянский государственный технический университет, 2012. — 186 с. — ISBN 5-89838-138-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/7008.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.3 Перечень методических указаний

1. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение : методические указания по выполнению практической работы: [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 16 с. - Текст : электронный.

2. Определение показателей защищенности информации при несанкционированном доступе : методические указания по выполнению практической работы: [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

3. Критерии оценки и выбора CASE-Средств : методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2022. - 11 с. - Загл. с титул. экрана. - Текст : электронный.

4. Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
4. Электронно-библиотечная система IQLib – http://www.iqlib.ru
5. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и практические занятия.

На лекциях излагаются и разъясняются основные понятия и положения каждой новой темы; важные положения аргументируются и иллюстрируются примерами из практики; объясняется практическая значимость изучаемой

темы; делаются выводы; даются рекомендации для самостоятельной работы по данной теме. На лекциях необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных вопросов. В ходе лекции студент должен конспектировать учебный материал. Конспектирование лекций – сложный вид работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это лично студентом в режиме реального времени в течение лекции. Не следует стремиться записать лекцию дословно. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем кратко записать ее. Желательно заранее оставлять в тетради пробелы, куда позднее, при самостоятельной работе с конспектом, можно внести дополнительные записи. Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, который преподаватель дает в начале лекционного занятия. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале.

Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологией. Работу с конспектом лекции целесообразно проводить непосредственно после ее прослушивания, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях. Работа с конспектом лекции предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Некоторые вопросы выносятся за рамки лекций. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы, указанной в п.8.2.

Изучение наиболее важных тем или разделов дисциплины продолжается на практических занятиях, которые обеспечивают контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. При работе с источниками и литературой необходимо:

– сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;

– обобщать полученную информацию, оценивать прочитанное;

– фиксировать основное содержание прочитанного текста; формулировать устно и письменно основную идею текста; составлять план, формулировать тезисы.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю. Обязательным элементом самостоятельной работы по дисциплине является самоконтроль. Одной из важных задач обучения студентов способам и приемам самообразования является формирование у них умения самостоятельно контролировать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями самоконтроля приучает студентов к планированию учебного труда, способствует углублению их внимания, памяти и выступает как важный фактор развития познавательных способностей. Самоконтроль включает:

– оперативный анализ глубины и прочности собственных знаний и умений;

– критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заметить и исправить свои ошибки. Формы самоконтроля могут быть следующими:

– устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;

– составление плана, тезисов, формулировок ключевых положений текста по памяти;

– пересказ с опорой на иллюстрации, чертежи, схемы, таблицы, опорные положения.

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допускаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

При подготовке к промежуточной аттестации по дисциплине необходимо повторить основные теоретические положения каждой изученной темы и основные термины, самостоятельно решить несколько типовых компетентностно-ориентированных задач.

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

Информационные технологии:

1. Средства для просмотра презентаций;
2. Средства для проведения онлайн-конференций.
3. Электронно-образовательная среда ЮЗГУ

Программное обеспечение:

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

Информационные справочные системы:

1. Научно-информационный портал ВИНИТИ РАН. Режим доступа: свободный.
2. База данных "Патенты России". Режим доступа: свободный.
3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: по подписке.
4. Электронная библиотека диссертаций и авторефератов РГБ. Режим доступа: свободный.
5. Электронный каталог Научной библиотеки ЮЗГУ. Режим доступа: свободный.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудиторные занятия по дисциплине проводятся в учебной аудитории для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенных стандартной учебной мебелью (столы и стулья для обучающихся; стол и стул для преподавателя; доска).

Для организации образовательного процесса применяются технические средства обучения: Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24.

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности:

1. Класс ПЭВМ - Asus-P7P55LX-/DDR34096Mb/Coree i3-540/SATA-11 500 Gb Hitachi/PCI-E 512Mb, Монитор TFT Wide 23.
2. Мультимедиацентр: ноутбук ASUS X50VL PMD - T2330/14"/1024Mb/ 160Gb/ сумка/проектор inFocus IN24+ .
3. Экран мобильный Draper Diplomat 60x60.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			