Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Управление информационной безопасностью
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления

по направленности Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта

факультет Компьютерных технологий и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность и программная инженерия
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 2 семестр (ы) 3
очная

г. Махачкала – 2026

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению подготовки и программе магистратуры «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Разработчик _____ Мирземагомедова М.М., к.т.н.
(подпись) (ФИО уч. степень, уч. звание)

« 02 » февраля 2026 г.

Зав. кафедрой, за которой закреплена дисциплина

_____ Качаева Г.И., к.э.н.
(подпись) (ФИО уч. степень, уч. звание)

« 03 » февраля 2026 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности и программной инженерии от « 05 » февраля 2026 года, протокол № 6/1

Зав. выпускающей кафедрой по данному направлению подготовки

_____ Качаева Г.И. к.э.н.
(подпись) (ФИО уч. степень, уч. звание)

« 05 » февраля 2026 г.

Программа одобрена на заседании Методического совета факультета компьютерных технологий и энергетики от « 10 » февраля 2026 г., протокол № 5/1

Председатель Методического совета факультета КТиЭ

_____ Исабекова Т.И.. к.ф.-м.н., доцент
(подпись) (ФИО уч. степень, уч. звание)

« 10 » февраля 2026 г.

Декан факультета _____ Т.А. Рагимова
(подпись) (ФИО)

Начальник УО _____ Л.Н. Мусаева
(подпись) (ФИО)

Проректор по УР _____ А.Ф. Демирова
(подпись) (ФИО)

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ 4
1.1. Место дисциплины в структуре ОПОП 4
1.2. Цели и задачи освоения дисциплины 4
1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины 4
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 5
2.1. Объем дисциплины и виды учебной работы 5
2.2. Содержание дисциплины 6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 12
3.1. Материально-техническое обеспечение 12
3.2. Учебно-методическое и информационное обеспечение программы 12
3.2.1. Печатные издания 13
3.2.2. Основные электронные издания 14
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 15

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре ОПОП

Дисциплина «Управление информационной безопасностью» входит в обязательную часть учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Предшествующими дисциплинами являются: Защищенные информационные системы, Технологии обеспечения информационной безопасности, Системы мониторинга и управления инцидентами информационной безопасности, Интеллектуальные системы и технологии.

Дисциплина «Управление информационной безопасностью» является основополагающей для изучения следующих дисциплин: Производственная (проектно-технологическая) практика, Преддипломная практика, Государственная итоговая аттестация.

1.2. Цели и задачи освоения дисциплины

Дисциплина «Управление информационной безопасностью» способствует формированию у обучающихся компетенций, предусмотренных данной рабочей программой в соответствии с требованиями ФГОС ВО и ОПОП ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом специфики направленности подготовки «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта».

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Управление информационной безопасностью» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование общепрофессиональной компетенции	**Код и наименование индикаторов достижения компетенции**
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	ОПК-3.1 Применяет отечественные стандарты при сертификации средств защиты и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки организационно-распорядительных документов
	ОПК-3.2 Разрабатывает технические задания на создание подсистем обеспечения информационной безопасности
	ОПК-3.3 Исследует эффективность и проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.3 Структурирует информацию по теме исследования, владеет методикой создания технического задания и технического проекта при организации научно-исследовательских и опытно-конструкторских работ (НИОКР)

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Таблица 2.

Вид учебной работы	**Форма обучения**
	очная
Объем образовательной программы дисциплины (ЗЕТ/ в часах)	3/108
В том числе:	**Объем в часах**
Лекции	34
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа	4
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме экзамена**,** семестр	3
Часы на экзамен	36

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Системы управления информационной безопасности			
Тема 1.1 Введение в дисциплину	Предмет дисциплины, структура и место курса в подготовке специалиста. Понятие информационной безопасности. Основные составляющие информационной безопасности.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Организационное проектирование. Создание структуры организационно-распорядительной документации с использованием офисных пакетов.		
	Самостоятельная работа обучающихся: Анализ современных стандартов управления ИБ		
Тема 1.2 Основные понятия информационной безопасности	Управление информационной безопасностью как механизм обеспечения безопасности предприятия. Важность и сложность проблемы информационной безопасности.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Анализ формальных моделей. Исследование и анализ простых сценариев контроля доступа с использованием принципов модели HRU.		
	Самостоятельная работа обучающихся: Проектирование системы ролевого управления доступом.		
Тема 1.3 Основные составляющие государственной системы защиты информации	Информационная безопасность и ее место в системе национальной безопасности РФ. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Современные тенденции в развитии организационно-правового обеспечения информационной безопасности.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Построение ролевой модели. Разработка матрицы доступа на основе ролей для условной организации.		
	Самостоятельная работа обучающихся: Разработка профиля угроз для объекта информатизации**.**	**1**	

Раздел 2. Угрозы и стандарты в информационной безопасности			
Тема 2.1 Угрозы информационной безопасности в информационных системах	Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Вредительские программы.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Разработка профиля угроз. Разработка и оформление профиля угроз для заданного объекта защиты на основе классификации.		
	Самостоятельная работа обучающихся: Технико-экономическое обоснование выбора СЗИ		
Тема 2.2 Оценочные стандарты в информационной безопасности	Роль стандартов ИБ. " Оранжевая книга" как оценочный стандарт. Международный стандарт ISO/IES 15408. Критерии оценки безопасности информационных систем.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Разработка политики парольной аутентификации. Анализ и настройка локальной политики безопасности ОС.		
	Самостоятельная работа обучающихся: Аудит настроек локальной политики безопасности ОС		
Тема 2.3 Стандарты управления информационной безопасностью	Стандарты управления информационной безопасностью BS7799 и ISO/IES 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Анализ требований стандарта и сопоставление с конфигурацией условной системы.		
	Самостоятельная работа обучающихся: Составление плана внутреннего аудита ИБ	**1**	
Раздел 3. Методы и технологии информационной безопасности			
Тема 3.1 Организационно-правовые основы защиты информации на предприятии	Основные направления, принципы и условия организационной защиты информации. Цели и значение защиты информации. Основные составляющие информационной безопасности. Основные подходы и требования к организационной составляющей защиты информации. Основные методы, силы и средства, используемые для организации защиты информации.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Анализ инструментов ИБ. Обзор и сравнительный анализ функциональности систем управления ИБ или SIEM-платформ.		

	Самостоятельная работа обучающихся: Картирование мер защиты на матрицу MITRE ATT&CK/D3FEND		
Тема 3.2 Создание СУИБ на предприятии	Этапы разработки и внедрения системы управления ИБ на предприятии. Содержание этапов разработки и внедрения системы управления ИБ.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Проектирование мер защиты. Разработка фрагмента технического задания на организационно-технические мероприятия по защите помещения от утечки информации.		
	Самостоятельная работа обучающихся: Анализ инцидента ИБ и разработка регламента реагирования		
Тема 3.3 Управление безопасности и обеспечения непрерывностью бизнеса предприятия. инцидентами информационной безопасности	Событие и инцидент ИБ. Система управления инцидентами ИБ. Этапы процесса управления инцидентами ИБ. Обнаружение событий ИБ и инцидентов ИБ и оповещение о них. Обработка событий ИБ и инцидентов ИБ. Реагирование на инциденты ИБ. Документация системы управления инцидентами ИБ. Группа реагирования на инциденты ИБ. Обеспечение осведомленности и обучение в области инцидентов ИБ. Средства управления событиями ИБ.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Категорирование объектов. Проведение категорирования условного объекта информатизации и определение требуемого уровня защищенности.		
	Самостоятельная работа обучающихся: Категорирование информационных активов		
Тема 3.4 Методика оценки рисков информационной безопасности	Основы управления рисками. Обоснование необходимости инвестиций в информационную безопасность компании. Методика FRAP. Методика OCTAVE. Методика RiskWatch.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Проактивные меры защиты. Разработка регламента действий администратора безопасности по предотвращению программно-математических воздействий.		
	Самостоятельная работа обучающихся: Исследование моделей управления ИБ «Security as a Service»	**1**	
Раздел 4. Информационной безопасности на предприятии			

Тема 4.1 Правовые меры обеспечения информационной безопасности на предприятии	Основные направления обеспечения информационной безопасности на предприятии. Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Разработка плана реагирования. Создание плана первоочередных действий по минимизации последствий инцидента.		
	Самостоятельная работа обучающихся: Проектирование системы защиты от утечки по техническим каналам		
Тема 4.2 Разработка СУИБ организации	Разработка корпоративной методики анализа рисков. Организационные меры обеспечения безопасности компьютерных информационных систем.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Разработка и документирование сценариев восстановления после сбоев для критических информационных систем организации		
	Самостоятельная работа обучающихся: Систематизация полученных теоретических знаний, их углубление и расширение на уровне межпредметных связей. Развитие познавательных способностей.		
Тема 4.3 Условия и требования лицензирования и сертификации в области защиты информации, способствующие информационной безопасности объектов критической информационной инфраструктуры	Понятия объект и субъект критической информационной инфраструктуры. Лицензирование объектов критической информационной инфраструктуры. Требования сертификации средств защиты информации	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Анализ условной инфраструктуры предприятия, определение и обоснование значимости ее объектов с точки зрения национальной безопасности		
	Самостоятельная работа обучающихся: Систематизация полученных теоретических знаний, их углубление и расширение на уровне межпредметных связей. Развитие познавательных способностей.		

Тема 4.4 Создание информации объектов критической информационной инфраструктуры модели потенциальных каналов и методов несанкционированного доступа к информации объектов критической информационной инфраструктуры	Выполнение требований закона №187-ФЗ.Разработка организационных и технических мер по обеспечению безопасности значимого объекта КИИ. Анализ угроз безопасности информации и разработка модели потенциальных каналов и методов несанкционированного доступа к информации. Создание модели потенциальных каналов и методов несанкционированного доступа к информации объектов КИИ. Описание объекта защиты. Определение источников угроз. Формирование списка уязвимостей объекта защиты. Определение перечня потенциальных каналов и методов несанкционированного доступа к информации объектов критической информационной инфраструктуры. Описание потенциальных каналов и методов несанкционированного доступа к информации объектов критической информационной инфраструктуры. Определение возможных последствий.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Формализованное описание векторов атаки, уязвимостей и возможных последствий для выбранного объекта защиты		
	Самостоятельная работа обучающихся: Систематизация полученных теоретических знаний, их углубление и расширение на уровне межпредметных связей. Развитие познавательных способностей.		
Тема 4.5 Создание системы управления непрерывностью бизнеса на предприятии в условиях дестабилизирующего воздействия на информационную безопасность предприятия	Методы и подходы к созданию систем управления непрерывности бизнеса в условиях дестабилизирующего воздействия на информационную безопасность. Жизненный цикл процесса управления непрерывностью бизнеса. Инициация проекта. Анализ воздействия на бизнес. Оценка рисков. Разработка стратегий непрерывности бизнеса. Разработка и внедрение планов непрерывности бизнеса. Методология разработки планов. Тестирование и пересмотр планов.	**2**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**2**	
	Создание структурированного ТЗ, включающего требования к политикам, процедурам и средствам защиты информации		
	Самостоятельная работа обучающихся: Систематизация полученных теоретических знаний, их углубление и расширение на уровне межпредметных связей. Развитие познавательных способностей		

Тема 4.6 Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях	Проблемы построения корпоративной информационной системы. Причины возникновения уязвимостей в безопасности. Оценка рисков уязвимостей. Методы обнаружения уязвимостей. Тестирование на проникновение. Этапы проведения тестирования. Виды тестирования на проникновение. Симуляция нарушений и атак (BAS). Антивирусный мониторинг. Управление конфигурацией (SCM). Этапы внедрения метода (SCM). Программные комплексы обнаружения уязвимостей. Платные инструменты сканирования и обнаружения уязвимостей. Бесплатные инструменты сканирования и обнаружения уязвимостей.	**4**	ОПК-3; ОПК-4
	в том числе лабораторных занятий:	**4**	
	Проверка комплекта организационно-распорядительных документов (политик, инструкций) на полноту, актуальность и соответствие стандартам		
	Самостоятельная работа обучающихся: Систематизация полученных теоретических знаний, их углубление и расширение на уровне межпредметных связей. Развитие познавательных способностей.	**1**	
Итого за 3 семестр:			
Лекции		**34**	
Лабораторные работы		**34**	
Самостоятельная работа		**4**	
Промежуточная аттестация в форме экзамена		**36**	
Всего:		**108**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Управление информационной безопасностью» включает:

Наименование помещения	Перечень основного оборудования
Лаборатория программно-аппаратных средств защиты информации	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор интерактивная доска Программное и программно-аппаратное обеспечение: Сетевой сканер «Ревизор Сети»; Система защиты информации от НСД «Страж NT»; Система резервного копирования Кибер Бэкап Расширенная редакция для универсальной платформы; Программный комплекс по предотвращению утечек данных (DLP) Кибер Протего; Персональный идентификатор iButton (арт. 930300); Право на использование СПО ПАК СЗИ НСД «Аккорд-Win64»; Служебный носитель «Секрет Особого Назначения» криптографический с быстрым процессором, 32Гб (арт. 620520); ПАК «Мобильный носитель лицензий»; OpenGRC, SimpleRisk, OWASP DefectDojo; OpenSCAP, CIS-CAT
Аудитория для проведения занятий лекционного типа	Аудитория для проведения занятий лекционного типа; Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска
Аудитория для самостоятельной работы обучающихся	Аудитория для самостоятельной работы обучающихся: Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска

3.2. Учебно-методическое и информационное обеспечение программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями

3.2.1. Печатные издания

Основная литература:

1. Зырянова, Т. Ю. Управление информационной безопасностью: учебное пособие / Т. Ю. Зырянова. — Екатеринбург: 2023. — 96 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482.
2. Капгер, И. В. Управление информационной безопасностью: учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь: ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889.
3. Поздняк, И. С. Управление информационной безопасностью: учебное пособие / И. С. Поздняк, И. С. Макаров. — Самара: ПГУТИ, 2023. — 104 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/463619
4. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2020. - 44 с. – Режим доступа: https://e.lanbook.com/book/130179
5. Крюков Д. А. Информационная безопасность [Электронный ресурс]: Метод. указ. по выполнению практ. занятий для студентов. - М.: МИРЭА, 2016. - – Режим доступа: http://library.mirea.ru/secret/ab/1352.iso
6. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]: - Санкт-Петербург: Лань, 2020. - 124 с. – Режим доступа: https://e.lanbook.com/book/133924
7. Гродзенский Я. С. Информационная безопасность:учебное пособие. - М.: Проспект, 2020. - 144 с.

Дополнительные источники:

1. Дешко, И. П. Управление ИТ-услугами по ITIL 4: учебное пособие для вузов / И. П. Дешко. — 4-е изд., стер. — Санкт-Петербург: Лань, 2026. — 228 с. — ISBN 978-5-507-54585-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/509851.
2. Дешко, И. П. Библиотека инфраструктуры информационных технологий. Практики управления ITIL 4: учебное пособие для вузов / И. П. Дешко. — 4-е изд., стер. — Санкт-Петербург: Лань, 2026. — 224 с. — ISBN 978-5-507-54437-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/508553.
3. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Серия «Вопросы управление информационной безопасностью". Выпуск 2 [Электронный ресурс]: - Москва: Горячая линия-Телеком, 2012. - 130 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5179
4. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Серия «Вопросы управление информационной безопасностью". Выпуск 5 [Электронный ресурс]: - Москва: Горячая линия-Телеком, 2012. - 166 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5182
5. Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс]: - Москва: Горячая линия-Телеком, 2012. - 244 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5178

3.2.2. Основные электронные издания

1. Информационный портал Российского научного фонда http://www.rscf.ru
2. Информационно-правовой портал ГАРАНТ http:// www.garant.ru
3. ИСС "Гарант" http://www.internet.garant.ru/
4. ЭБС «IPR Books» http://www.iprbookshop.ru/
5. Библиоклуб.ру http://biblioclub.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения	**Критерии оценки**	**Методы оценки**
- применяет отечественные стандарты при сертификации средств защиты и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки организационно-распорядительных документов - разрабатывает технические задания на создание подсистем обеспечения информационной безопасности - исследует эффективность и проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности - структурирует информацию по теме исследования, владеет методикой создания технического задания и технического проекта при организации научно-исследовательских и опытно-конструкторских работ (НИОКР)	*Шкала оценивания для экзамена* *«Отлично»* Показывает высокий уровень сформированности компетенций, т.е.: - демонстрирует высокое и прочное освоение материала; - исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; - правильно формирует определения; - демонстрирует умения самостоятельной работы с нормативно-правовой литературой; - умеет делать выводы по излагаемому материалу. *«Хорошо»* Показывает достаточный уровень сформированности компетенций, т.е.: - демонстрирует достаточно полное знание материала, основных теоретических положений; - достаточно последовательно, грамотно и логически стройно излагает теоретический материал; - демонстрирует умения ориентироваться в нормативно-правовой литературе; - умеет делать достаточно обоснованные выводы по излагаемому материалу. *«Удовлетворительно»* Показывает пороговый уровень сформированности компетенций, т.е.: - демонстрирует общее знание изучаемого материала; - испытывает затруднения при ответах на дополнительные вопросы; - знает основную рекомендуемую литературу; - умеет строить ответ в соответствии со структурой излагаемого материала. *Неудовлетворительно»* Ставится в случае: - незнания значительной части программного материала; - невладения понятийным аппаратом дисциплины; - допущения существенных ошибок при изложении учебного материала; - неумения строить ответ в соответствии со структурой излагаемого вопроса; - неумения делать выводы по излагаемому материалу.	Текущий контроль при проведении: - письменного/устного опроса; - тестирования; - оценки результатов самостоятельной работы (докладов, рефератов). Промежуточная аттестация в форме: -экзамена, - письменных/ устных ответов, - тестирования.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;

- приказа Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене