

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Баламирзоев Назим Лиодинович  
Должность: Ректор  
Дата подписания: 2025.04.11  
Уникальный программный ключ:  
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

**Министерство науки и высшего образования РФ**

**Федеральное государственное бюджетное образовательное учреждение  
высшего образования**

**«Дагестанский государственный технический университет»**

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Дисциплина Теория обнаружения вторжения с применением искусственного интеллекта  
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность  
код и полное наименование специальности

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 1 семестр (ы) 2.  
очная

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 «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Разработчик   
(подпись)

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

« 02 » февраля 2026 г.

Зав. кафедрой, за которой закреплена дисциплина

  
(подпись)

Качаева Г.И., к.э.н.  
(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

  
(подпись)

Качаева Г.И. к.э.н.  
(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

  
(подпись)

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

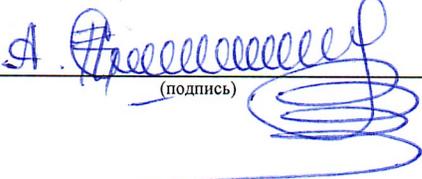
« 10 » февраля 2026 г.

Декан факультета   
(подпись)

Т.А. Рагимова  
(ФИО)

Начальник УО   
(подпись)

Л.Н. Мусаева  
(ФИО)

Проректор по УР   
(подпись)

А.Ф. Демирова  
(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 «Теория обнаружения вторжении с применением искусственного интеллекта» .....	6
3.	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ.....	11
3.1.	Материально-техническое обеспечение.....	11
3.2.	Учебно-методическое и информационное обеспечению программы .....	11
3.2.1.	Печатные издания .....	11
3.2.2.	Основные электронные издания .....	12
4.	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	13

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## 1.1. Место дисциплины в структуре ОПОП

Дисциплина «Теория обнаружения вторжении с применением искусственного интеллекта» входит в часть, формируемую участниками образовательных отношений учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Предшествующими дисциплинами, формирующими начальные знания, являются: интеллектуальные системы и технологии, специальные разделы математики, библиотеки машинного обучения, технологии машинного обучения в кибербезопасности, система для сбора событий и логов, защищенные информационные системы, логика и методология науки.

Последующими дисциплинами, формирующими начальные знания, являются: системы мониторинга и управления инцидентами информационной безопасности, принятие решений на основе проактивного поиска и обнаружения угроз, интеллектуальные системы информационной безопасности в промышленных системах/здравоохранении, анализ защищенности систем искусственного интеллекта.

## 1.2. Цели и задачи освоения дисциплины

Дисциплина «Теория обнаружения вторжении с применением искусственного интеллекта» имеет своей целью способствовать 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 «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта».

## 1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Теория обнаружения вторжении с применением искусственного интеллекта» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	Код и наименование индикаторов достижения компетенции
ПК-1. Способен разрабатывать и применять процедуры и интеллектуальные средства информационно-аналитических систем поддержки принятия решений по обеспечению информационной безопасности	ПК-1.1 Способен решать задачи анализа данных в целях обеспечения информационной безопасности
	ПК-1.2 Способен интерпретировать и использовать результаты решения информационно-аналитических задач обеспечения информационной безопасности
ПК-2. Способен выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности	ПК-2.1 Способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности
ПК-4. Способен разрабатывать и применять методы и алгоритмы машинного обучения для решения задач искусственного интеллекта	ПК-4.1 Ставит задачи по разработке или совершенствованию методов и алгоритмов для решения комплекса задач предметной области

## 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)	4/144
<b>В том числе:</b>	<b>Объем в часах</b>
Лекции	34
Практические занятия	
Лабораторные занятия	34
Самостоятельная работа	40
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме экзамена, семестр	2 семестр
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
<b>Раздел 1. Основы теории искусственного интеллекта</b>			
<b>Тема 1. Искусственный интеллект и проблемы представления знаний.</b>	Краткая история развития вычислительных машин и искусственного интеллекта. Основные направления исследований в области искусственного интеллекта. Прикладные интеллектуальные системы	<b>2</b>	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	<b>2</b>	
	Лабораторная работа № 1. Применение библиотек машинного обучения, использование пакетов ggplot2 для визуализации расчетов.		
	<b>Самостоятельная работа обучающихся:</b> Сравнительный анализ отечественных и зарубежных стандартов в области обнаружения вторжений.	<b>2</b>	
<b>Тема 2. Логические модели представления знаний.</b>	Логические модели представления знаний. Исчисление предикатов первого порядка. Дедуктивный вывод в логических моделях. Прямой, обратный и смешанный логический вывод. Метод резолюции.	<b>2</b>	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	<b>2</b>	
	Лабораторная работа № 2. Последовательность шагов работы аналитика на примере разбора практической задачи по обнаружению вторжения на защищаемую ИТ-инфраструктуру		
	<b>Самостоятельная работа обучающихся:</b> Исследование эволюции моделей угроз и их влияние на архитектуру IDS.	<b>2</b>	
<b>Тема 3. Модели представления знаний.</b>	Сетевая модель. Понятие семантической сети. Классификация семантических сетей. Основные виды отношений. Функциональная сеть. Формальные и программные системы продукций. Структура программной системы продукций. Цикл работы системы продукций. Конфликтное множество правил. Способы разрешения конфликта. Управляющие стратегии. Стратегии применения правил	<b>2</b>	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	<b>2</b>	
	Лабораторная работа № 3. Применение нечетких моделей для построения интеллектуальных систем.		
	<b>Самостоятельная работа обучающихся:</b> Обзор и классификация современных коммерческих и open-source IDS/IPS.	<b>2</b>	

<b>Тема 4. Инструментарий искусственного интеллекта.</b>	Представление нечетких знаний. Понятие лингвистической переменной. Нечеткие множества. Основные операции над нечеткими множествами. Нечеткие отношения. Технологии разработки программного обеспечения – цели, принципы, парадигмы. Методологии создания и модели жизненного цикла интеллектуальных систем. Инструментарий ИИ.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 4. Решение задач подготовки обучающей выборки. Получение данных сетевого трафика.		
	<b>Самостоятельная работа обучающихся:</b> Изучение методов синтеза и генерации тестовых данных для обучения и оценки IDS.	2	
<b>Раздел 2. Теория и технологии обнаружения вторжений</b>			
<b>Тема 5. Понятие и виды угроз информационной безопасности.</b>	Модель зрелости поиска угроз ИБ. Threat hunting framework. Применение data science в процессе обнаружения вторжений.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 5. Обнаружение вредоносных событий на Linux-инфраструктуру.		
	<b>Самостоятельная работа обучающихся:</b> Анализ проблем интерпретируемости моделей ML в IDS. Методы объяснения решений.	2	
<b>Тема 6. Модели преднамеренных угроз информационной безопасности.</b>	Модели MITRE, PTES, Lockheed martin Cyber kilchain, Mandiant Attack Lifecycle	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 6. Установка и настройка IDS Snort. Создание новых правил обнаружения вредоносных событий.		
	<b>Самостоятельная работа обучающихся:</b> Исследование применения методов обучения с подкреплением для адаптивного реагирования IDS.	2	
<b>Тема 7. Источники сведений системы мониторинга информационной безопасности.</b>	Основные источники сведений системы мониторинга. DLP-системы, IDS-системы, журналы событий домена. Достоинства и недостатки. Описание технического решения Threat Intelligence	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 7. Организация и настройка IDS-системы в информационно-коммуникационной сети организации.		

	<b>Самостоятельная работа обучающихся:</b> Написание скрипта для автоматической разметки сетевого датасета на основе известных сигнатур.	2	
<b>Тема 8. Обзор современных технических решений мониторинга информационной безопасности.</b>	Основные понятия и определения. Классификация технических средств мониторинга ИБ. Описание процесса сбора и обработки сведений в реальном времени. Основные компоненты ИАС мониторинга.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 8. Создание типового отчета об угрозах на основе решений класса Threat Intelligence Platform.		
	<b>Самостоятельная работа обучающихся:</b> Проектирование feature engineering pipeline для логов веб-приложений.	2	
<b>Раздел 3. Применение искусственного интеллекта в интеллектуальных системах обнаружения</b>			
<b>Тема 9. Организация интеллектуальной вторжений системы обнаружения вторжений.</b>	Компоненты системы интеллектуальной системы обнаружения вторжений и их функции.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 9. Разработка программы интеллектуального анализа событий безопасности домена на основе алгоритма Change Finder и временных рядов.		
	<b>Самостоятельная работа обучающихся:</b> Сравнительный анализ метрик качества для задач с крайне несбалансированными данными.	2	
<b>Тема10. Особенности организации интеллектуальной системы обнаружения вторжений от АРТ-атак.</b>	Исследование интеллектуальной системы обнаружения вторжений на предмет источников данных для мониторинга. Создание технического проекта. Обучение технического персонала.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 10. Разработка программы интеллектуального анализа событий информационной безопасности Linux-серверов на основе машинного обучения.		
	<b>Самостоятельная работа обучающихся:</b> Изучение фреймворка MITRE ATT&CK и его использование для таксономии детектируемых ИСОВ техник.	2	
<b>Тема11. Интеллектуальный анализ событий информационной безопасности домена.</b>	Обзор источников событий безопасности домена. Журнал Security.evtx. Журнал LocalSessionManager.evtx.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 11. Глубокий анализ сетевого трафика с помощью парадигмы MAP-REDUCE		

	<b>Самостоятельная работа обучающихся:</b> Разработка концепции гибридной ИСОВ, сочетающей сигнатурный анализ, ML и правила корреляции.	2	
<b>Тема 12. Интеллектуальный анализ событий информационной безопасности Linux-серверов.</b>	Журналирование событий безопасности в Linux-подобных ОС. Выявление аномального поведения пользователей.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 12. Журналирование событий безопасности в Linux-подобных ОС. Выявление аномального поведения пользователей.		
	<b>Самостоятельная работа обучающихся:</b> Анализ требований 152-ФЗ и приказов ФСТЭК к средствам обнаружения вторжений (СОВ).	2	
<b>Раздел 4. Искусственный интеллект</b>			
<b>Тема 13. Основы разработки информационно-аналитической системы в сфере ИБ.</b>	Основные этапы разработки информационно-аналитических систем. Разработка концепции ИАС. Проектирование инфраструктуры.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 13. Расширение их функционала возможностями типовых BI-инструментов для обработки OLAP-кубов и использования средств Data mi		
	<b>Самостоятельная работа обучающихся:</b> Разработка проекта «Положения о порядке внедрения и эксплуатации ИСОВ» в организации.	4	
<b>Тема 14. Этапы разработки информационно-аналитической системы в сфере ИБ.</b>	Проектирование информационной базы. Подключение возможностей готового программного обеспечения. Разработка специализированных аналитических инструментов. Внедрение и расширение ИАС.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 14. Расширение их функционала возможностями типовых BI-инструментов для обработки OLAP-кубов и использования средств Data m		
	<b>Самостоятельная работа обучающихся:</b> Исследование методов online-обучения и адаптации ML-моделей в IDS к дрейфу данных.	4	
<b>Тема 15. Применение моделей машинного обучения для анализа трафика.</b>	Основные модели машинного обучения. Линейные модели, модели логистического обеспечения, регрессионные модели, кластеризованный анализ. Подготовка обучающей выборки для классификации трафика.	2	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	2	
	Лабораторная работа № 15. Настройка функций отчетности и формирования запросов		

	<b>Самостоятельная работа обучающихся:</b> Оценка ресурсоемкости различных ML-моделей для IDS и выбор оптимальной для edge-развертывания.	<b>4</b>	
<b>Тема 16. Применение методов машинного обучения для анализа трафика.</b>	Наивный байесовский классификатор. Метод опорных векторов. Метод k-ближайших соседей. Деревья принятия решений. Методы бэггинга (случайный лес). Методы бустинга.	<b>4</b>	ПК-1 ПК-2 ПК-4
	<b>в том числе лабораторных занятий:</b>	<b>4</b>	
	Лабораторная работа № 16. Настройка функций отчетности и формирования запросов		
	<b>Самостоятельная работа обучающихся:</b> Критический разбор научной статьи из журнала IEEE S&P, Usenix Security и др. по тематике ИИ для IDS.	<b>4</b>	
<b>Итого за 2 семестр:</b>			
<b>Лекции</b>		<b>34</b>	
<b>Лабораторные работы</b>		<b>34</b>	
<b>Самостоятельная работа</b>		<b>40</b>	
<b>Промежуточная аттестация в форме экзамена</b>		<b>36</b>	
<b>Всего:</b>		<b>144</b>	

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

#### 3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Теория обнаружения вторжении с применением искусственного интеллекта» включает:

Наименование помещения	Перечень основного оборудования
Лаборатория 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 обеспечение: Elastic Stack (Elasticsearch, Logstash, Kibana + Machine Learning); Wazuh, Security Onion; Tcpreplay, CICFlowMeter, CTU-13 dataset;
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:	Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска

#### 3.2. Учебно-методическое и информационное обеспечению 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. Полтавцева, М. А. Высокопроизводительные системы обнаружения вторжений: учебное пособие / М. А. Полтавцева, Д. С. Лаврова. — 2-е изд. — Москва, Вологда: Инфра-Инженерия, 2023. — 152 с. — ISBN 978-5-9729-1213-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/132855.html>
2. Тумбинская М. В., Петровский М. В. Комплексное обеспечение информационной безопасности на предприятии [Электронный ресурс]: учебник. - Санкт-Петербург: Лань, 2019. - 344 с. – Режим доступа: <https://e.lanbook.com/book/125739>

3. Остроух А. В., Суркова Н. Е. Системы искусственного интеллекта [Электронный ресурс]: монография. - Санкт-Петербург: Лань, 2019. - 228 с. – Режим доступа: <https://e.lanbook.com/book/113401>

**Дополнительные источники:**

1. Шелухин, О. И. Системы обнаружения вторжений в компьютерные сети: учебное пособие / О. И. Шелухин, А. Н. Руднев, А. В. Савелов. — Москва: Московский технический университет связи и информатики, 2013. — 88 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/63360.html>.
2. Практикум по дисциплине Системы обнаружения вторжений в инфокоммуникациях / . — Москва: Московский технический университет связи и информатики, 2014. — 28 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/61545.html>.
3. Практикум по дисциплине Иммитационное моделирование систем обнаружения вторжений / составители Д. В. Костин. — Москва: Московский технический университет связи и информатики, 2016. — 29 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/61478.html>.
4. Щерба Е.В. Противодействие сетевым атакам в локальных сетях: учебное пособие / Щерба Е.В., Щерба М.В., Магазев А.А.. — Омск : Омский государственный технический университет, 2021. — 119 с. — ISBN 978-5-8149-3250-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124874.html>

**3.2.2. Основные электронные издания**

1. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации <https://digital.gov.ru/>
2. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) <https://fstec.ru/>
3. MITRE ATT&CK Framework (База знаний о тактиках и техниках киберпротивников) <https://attack.mitre.org/>

#### 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
<p>- способен решать задачи анализа данных в целях обеспечения информационной безопасности;</p> <p>- способен интерпретировать и использовать результаты решения информационно-аналитических задач обеспечения информационной безопасности;</p> <p>- способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности;</p> <p>- ставит задачи по разработке или совершенствованию методов и алгоритмов для решения комплекса задач предметной области.</p>	<p><i>Шкала оценивания для экзамена</i></p> <p><b>«Отлично»</b> Показывает высокий уровень сформированности компетенций, т.е.:</p> <ul style="list-style-type: none"> <li>- демонстрирует высокое и прочное освоение материала;</li> <li>- исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал;</li> <li>- правильно формирует определения;</li> <li>- демонстрирует умения самостоятельной работы с нормативно-правовой литературой;</li> <li>- умеет делать выводы по излагаемому материалу.</li> </ul> <p><b>«Хорошо»</b> Показывает достаточный уровень сформированности компетенций, т.е.:</p> <ul style="list-style-type: none"> <li>- демонстрирует достаточно полное знание материала, основных теоретических положений;</li> <li>- достаточно последовательно, грамотно и логически стройно излагает теоретический материал;</li> <li>- демонстрирует умения ориентироваться в нормативно-правовой литературе;</li> <li>- умеет делать достаточно обоснованные выводы по излагаемому материалу.</li> </ul> <p><b>«Удовлетворительно»</b> Показывает пороговый уровень сформированности компетенций, т.е.:</p> <ul style="list-style-type: none"> <li>- демонстрирует общее знание изучаемого материала;</li> <li>- испытывает затруднения при ответах на дополнительные вопросы;</li> <li>- знает основную рекомендуемую литературу;</li> <li>- умеет строить ответ в соответствии со структурой излагаемого материала.</li> </ul> <p><b>«Неудовлетворительно»</b> Ставится в случае:</p> <ul style="list-style-type: none"> <li>- незнания значительной части программного материала;</li> <li>- невладения понятийным аппаратом дисциплины;</li> <li>- допущения существенных ошибок при изложении учебного материала;</li> <li>- неумения строить ответ в соответствии со структурой излагаемого вопроса;</li> <li>- неумения делать выводы по излагаемому материалу.</li> </ul>	<p>Текущий контроль при проведении:</p> <ul style="list-style-type: none"> <li>- письменного/устного опроса;</li> <li>- тестирования;</li> <li>- оценки результатов самостоятельной работы (докладов, рефератов).</li> </ul> <p>Промежуточная аттестация в форме:</p> <ul style="list-style-type: none"> <li>- экзамена,</li> <li>- письменных/устных ответов,</li> <li>- тестирования.</li> </ul>

## **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