Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Анализ защищенности систем искусственного интеллекта
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления

по направленности Кибеpразведка 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 _____ Качаева Г.И., к.э.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 «Анализ защищенности систем искусственного интеллекта» 6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 10
3.1. Материально-техническое обеспечение 10
3.2. Учебно-методическое и информационное обеспечение программы 10
3.2.1. Печатные издания 10
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 «Анализ защищенности систем искусственного интеллекта» входит в часть, формируемую участниками образовательных отношений учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Кибербразведка 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, теория обнаружения вторжений с применением ИИ.

Дисциплина «Интеллектуальные системы информационной безопасности в здравоохранении» является основополагающей для изучения следующих дисциплин: Производственная (проектно-технологическая) практика, Преддипломная практика, Государственная итоговая аттестация.

1.2. Цели и задачи освоения дисциплины

Дисциплина «Анализ защищенности систем искусственного интеллекта» 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 «Анализ защищенности систем искусственного интеллекта» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	Код и наименование индикаторов достижения компетенции
ПК-2 Способен выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности	ПК-2.2 Способен разрабатывать процедуры мониторинга обстановки в сфере информационной безопасности
ПК-6 Способен выбирать, разрабатывать и проводить экспериментальную проверку работоспособности программных компонентов систем искусственного интеллекта по обеспечению требуемых критериев эффективности и качества функционирования	ПК-6.2 Проводит экспериментальную проверку работоспособности систем искусственного интеллекта

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
В том числе:	**Объем в часах**
Лекции	34
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа	40
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме экзамена**,** семестр	3 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
1. Введение			
Тема1.1 Введение в угрозы систем искусственного интеллекта	Основные понятия, определения. Утечки информации в системах искусственного интеллекта. Источники угроз	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 1. Развертывание тестовой среды для анализа защищенности ML-моделей.		
	Самостоятельная работа обучающихся: Анализ и сравнение таксономий угроз ИИ.	**4**	
Тема 1.2 Таксономия угроз ИИ	Модель нарушителя в контексте ИИ: цели, возможности, векторы атак.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 2. Развертывание тестовой среды для анализа защищенности ML-моделей.		
	Самостоятельная работа обучающихся: Исследование реальных кейсов успешных атак на промышленные системы ИИ.	**4**	
Тема 1.3 Индустриальная практика анализа защищённости систем искусственного интеллекта ч.1	Аспекты практической компьютерной безопасности. Средства анализа защищенности систем искусственного интеллекта.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 3. Разработка и применение методов обнаружения отравленных данных.		
	Самостоятельная работа обучающихся: Обзор методов Robust Learning и их математических основ.	**4**	
Тема 1.4 Индустриальная практика анализа защищённости систем искусственного интеллекта ч.2	Аспекты практической компьютерной безопасности. Средств анализа защищенности систем искусственного интеллекта	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 4. Генерация состязательных примеров методом FGSM.		

	Самостоятельная работа обучающихся: Изучение атак категории "Model Inversion" на генеративные модели.	**2**	
Тема 1.5 Эксплуатационные атаки	Состязательные атаки. Методы FGSM, PGD, Carlini & Wagner.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 5. Генерация состязательных примеров методом PGD		
	Самостоятельная работа обучающихся: Сравнение инструментов для генерации состязательных примеров: CleverHans, Foolbox, ART.	**2**	
Тема 1.6 Защита на этапе инференса	Adversarial training, детектирование состязательных примеров, использование GAN для генерации защищенных данных.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 6. Применение Adversarial Training для повышения устойчивости модели.		
	Самостоятельная работа обучающихся: Анализ компромисса между приватностью и точностью модели.	**2**	
Тема 1.7 Атаки на конфиденциальность моделей	Атаки на тренировочные данные: Membership Inference, Model Inversion, Attribute Inference.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 7. Реализация Membership Inference Attack.		
	Самостоятельная работа обучающихся: Исследование методов физических состязательных атак.	**2**	
Тема 1.8 Методы обеспечения приватности моделей	Дифференциальная приватность для ML, федеративное обучение.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 8. Внедрение дифференциальной приватности в процесс обучения.		
	Самостоятельная работа обучающихся: Поиск и описание уязвимостей в популярных ML-библиотеках	**2**	
Тема 1.9 Атаки на целостность и доступность моделей	Атаки на подавление работы модели.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 9. Проведение Model Extraction Attack.		

	Самостоятельная работа обучающихся: Проектирование безопасного MLOps-конвейера с учетом принципа наименьших привилегий.	**2**	
Тема 1.10 Защита от экстракции и саботажа	Предсказание с уверенностью, водяные знаки для моделей, мониторинг API-запросов.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 10. Наложение цифрового водяного знака на модель.		
	Самостоятельная работа обучающихся: Анализ требований к безопасности ИИ в проекте "Единые принципы регулирования ИИ".	**2**	
2. Методы анализа данных			
Тема 2.1 Анализ уязвимостей в конвейерах MLOps и инфраструктуре	Уязвимости в библиотеках, контейнерах, оркестраторах.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 11. Статический анализ кода ML-пайплайна на уязвимости.		
	Самостоятельная работа обучающихся: Разработка модели угроз для системы кибербразведки, использующей NLP для анализа текстов.	**2**	
Тема 2.2 Безопасность supply chain в ML	Анализ уязвимостей в предобученных моделях и датасетах.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 12. Анализ зависимостей ML-проекта на наличие известных уязвимостей.		
	Самостоятельная работа обучающихся: Написание скрипта для мониторинга аномальной активности при обращении к ML-модели в production.	**2**	
Тема 2.3 Анализ защищенности ИИ в предметных областях: кибербразведка и промышленные системы	Угрозы для систем обнаружения вторжений на основе ИИ.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 13. Анализ защищенности системы обнаружения вторжений на основе ИИ.		
	Самостоятельная работа обучающихся: Обзор рынка коммерческих решений для защиты систем ИИ.	**2**	
Тема 2.4 Анализ защищенности ИИ в	Последствия атак на диагностические системы и системы распознавания.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	

предметных областях: здравоохранение и биометрия	Лабораторная работа № 14. Создание состязательного примера для системы распознавания лиц.		
	Самостоятельная работа обучающихся: Изучение методов атак на системы reinforcement learning.	**2**	
Тема 2.5 Методологии аудита безопасности систем ИИ	Разработка плана тестирования на основе таксономий. Инструменты для автоматизированного аудита.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 15. Разработка сценария автоматизированного тестирования ML-API.		
	Самостоятельная работа обучающихся: Подготовка плана тестирования на проникновение для голосового ассистента с ИИ.	**2**	
Тема 2.6 Нормативно-правовое регулирование безопасности ИИ	Требования к надежному ИИ.Сертификация и стандартизация.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 16. Проведение комплексного аудита предобученной модели с Hugging Face.		
	Самостоятельная работа обучающихся: Разработка чек-листа для базового аудита безопасности системы машинного обучения.	**2**	
Тема 2.7 Формирование отчетов и управление рисками	Структура отчета об анализе защищенности. Приоритизация рисков и рекомендации по remediation.	**2**	ПК-2; ПК-6
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 17. Оформление технического отчета по результатам тестирования.		
	Самостоятельная работа обучающихся: Формулировка тезисов для научной публикации по результатам одной из лабораторных работ.	**2**	
Итого за 3 семестр:			
Лекции		**34**	
Лабораторные работы		**34**	
Самостоятельная работа		**40**	
Промежуточная аттестация в форме экзамена		**36**	
Всего:		**144**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Анализ защищенности систем 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 и программно-аппаратное обеспечение: Служебный носитель «Секрет Особого Назначения» криптографический с быстрым процессором, 32Гб (арт. 620520); Adversarial Robustness Toolbox (ART), Foolbox, CleverHans; MLSec, Counterfit
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 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. Ложников, П. С. Безопасность систем искусственного интеллекта. Ч. 2: Доверенный искусственный интеллект: учебное пособие / П. С. Ложников, А. Е. Самотуга, С. С. Жумажанова, А. Е. Сулавко. — Омск: ОмГТУ, 2023. — 74 с. — ISBN 978-5-8149-3731-5. — Текст: электронный // ЭБС «IPR SMART»: [сайт]. — URL: https://www.iprbookshop.ru/
2. Калинин, М. О. Основы искусственного интеллекта. Безопасность искусственного интеллекта: учебное пособие / М. О. Калинин, В. М. Крундышев. — Санкт-Петербург:

ПОЛИТЕХ-ПРЕСС, 2024. — 88 с. — Текст: электронный // ЭБС «Лань»: [сайт]. — URL: https://e.lanbook.com/
3. Чио, К. Машинное обучение и безопасность: защита систем с помощью данных и алгоритмов: практическое руководство / К. Чио, Д. Фримэн; пер. с англ. А. В. Снастина. — Москва: ДМК Пресс, 2020. — 388 с.: ил. — ISBN 978-5-97060-713-8. — Текст: электронный // ЭБС «Лань»: [сайт]. — URL: https://e.lanbook.com/book/131707
4. Митяков Е. С., Шмелева А. Г., Ладынин А. И. Искусственный интеллект и машинное обучение [Электронный ресурс]: учебное пособие для спо. - Санкт-Петербург: Лань, 2025. - 252 с. – Режим доступа: https://e.lanbook.com/book/450830
5. Золкин А. Л. Инструментальные средства разработки интеллектуальных информационных систем [Электронный ресурс]: учебник для спо. - Санкт-Петербург: Лань, 2025. - 140 с. – Режим доступа: https://e.lanbook.com/book/450845
6. Макшанов А. В., Журавлев А. Е., Тындыкарь Л. Н. Большие данные. Big Data [Электронный ресурс]: учебник для спо. - Санкт-Петербург: Лань, 2023. - 188 с. – Режим доступа: https://e.lanbook.com/book/341255
7. Колмогорова С. С. Обработка данных алгоритмами искусственного интеллекта в системе интернета вещей [Электронный ресурс]: учебное пособие для вузов. - СанктПетербург: Лань, 2023. - 104 с. – Режим доступа: https://e.lanbook.com/book/327356
8. Тюгашев А. А. Интеллектуальные системы [Электронный ресурс]: учебное пособие. - Самара: СамГУПС, 2020. - 151 с. – Режим доступа: https://e.lanbook.com/book/161308
9. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:. - Санкт-Петербург: Лань, 2022. - 124 с. – Режим доступа: https://e.lanbook.com/book/185333
10. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум [Электронный ресурс]: - Санкт-Петербург: Лань, 2022. - 44 с. – Режим доступа: https://e.lanbook.com/book/187645

Дополнительные источники:

1. Платонов, В. В. Технологии машинного обучения в кибербезопасности : учебное пособие / В. В. Платонов. — Москва, Вологда: Инфра-Инженерия, 2024. — 140 с. — ISBN 978-5-9729-2048-8. — Текст: электронный // Цифровой образовательный ресурс «IPR SMART» : [сайт]. — URL: https://www.iprbookshop.ru/144586.html
2. Менисов, А. Б. Киберщит. Искусственный интеллект и кибербезопасность / А. Б. Менисов. — Москва: Ай Пи Ар Медиа; Алматы: EDP Hub (Идипи Хаб), 2024. — 166 с. — ISBN 978-5-4497-2336-9. — Текст: электронный // ЭБС «IPR SMART»: [сайт]. — URL: https://www.iprbookshop.ru/
3. Ложников, П. С. Безопасность систем искусственного интеллекта. Ч. 1: Этика и правовые проблемы искусственного интеллекта: учебное пособие / П. С. Ложников, С. С. Жумажанова, А. Е. Сулавко, А. Е. Самотуга. — Омск: ОмГТУ, 2023. — 42 с. — ISBN 978-5-8149-3615-8. — Текст: электронный // ЭБС «Лань»: [сайт]. — URL: https://e.lanbook.com/books/1537
4. Котенко, И. В. Атаки и методы защиты в системах машинного обучения: анализ современных исследований / И. В. Котенко, И. Б. Саенко, О. С. Лаута, Н. А. Васильев, В. Е. Садовников // Вопросы кибербезопасности. — 2024. — № 1. — С. 24–37. — DOI: 10.21681/2311-2024-1-24-37. — Текст: электронный // Cyberrus.info: [сайт]. — URL: https://cyberrus.info/wp-content/uploads/2024/02/vokib-2024-1-st03-s024-037.pdf

3.2.2. Основные электронные издания

1. CyberHoot. 10 новых угроз на основе искусственного интеллекта, к которым должен быть готов каждый бизнес / CyberHoot. — 2026. — URL: https://cyberhoot.com/ru/blog/top-10-emerging-ai-based-threats-every-business-must-prepare-for/
2. Canadian Centre for Cyber Security (CCCS). Generative artificial intelligence - ITSAP.00.041 / CCCS. — URL: https://www.cyber.gc.ca/en/guidance/generative-artificial-intelligence-ai-itsap00041

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**
- Способен разрабатывать процедуры мониторинга обстановки в сфере информационной безопасности; - Проводит экспериментальную проверку работоспособности систем искусственного интеллекта	*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