

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Баламирзоев Назим Лиодинович  
Должность: И.о. ректора  
Дата подписания: 09.11.2025 16:06:08  
Уникальный программный ключ:  
2a04bb882d7edb7f479cb266eb4aaaaedebee849

**Министерство науки и высшего образования РФ**

**Федеральное государственное бюджетное образовательное учреждение  
высшего образования**

**«Дагестанский государственный технический университет»**

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Дисциплина Методы оценки безопасности компьютерных систем  
наименование дисциплины по ОПОП

для направления 10.03.01 Информационная безопасность  
код и полное наименование специальности

по профилю Безопасность автоматизированных систем

факультет Компьютерных технологий, вычислительной техники и энергетики  
наименование факультета, где ведется дисциплина

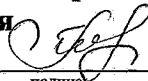
кафедра Информационная безопасность  
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, очно-заочная курс 4 семестр (ы) 7(8)  
очная, очно-заочная, заочная


г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению 10.03.01 Информационная безопасность и профилю Безопасность автоматизированных систем.


Разработчик  Качаева Г.И.  
подпись (ФИО уч. степень, уч. звание)  
« 18 » 09 2021г.


Зав. кафедрой, за которой закреплена дисциплина (модуль) Машинно-зависимые языки программирования  Качаева Г.И.  
подпись (ФИО уч. степень, уч. звание)  
« 18 » 09 2021г.

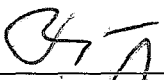
Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 20 сентября 2021 года, протокол № 2


Зав. выпускающей кафедрой по данному направлению (специальности, профилю)  Качаева Г.И., к.э.н.  
подпись (ФИО уч. степень, уч. звание)  
« 20 » 09 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от 18.10 2021 года, протокол № 1.

Председатель Методического совета факультета КТВТиЭ  Шаабетова Ш.А.  
подпись (ФИО уч. степень, уч. звание)  
« 18 » 10 2021г.

Декан факультета  Юсуфов Ш.А.  
подпись ФИО

Начальник УО  Магомаева Э.В.  
подпись ФИО

И.о проректора по УР  Баламирзоев Н.Л.  
подпись ФИО

## **1. Цели и задачи освоения дисциплины.**

Целями освоения учебной дисциплины «Методы оценки безопасности компьютерных систем» являются формирование компетенций по основным разделам данного курса, изучение студентами основных методов оценки безопасности компьютерных систем, стандартов в этой области; получение представления об организации и принципах обеспечения информационной безопасности компьютерных систем.

Студенты должны научиться применять современные методы оценки безопасности компьютерных систем. Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):

Эксплуатационной:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта;
- участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологической:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

Организационно-управленческой:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

Экспериментально-исследовательской:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
  - проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств.

## **2. Место дисциплины в структуре ОПОП**

Дисциплина «Методы оценки безопасности компьютерных систем» относится к блоку I (Обязательная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Основы информационной безопасности, Математическая логика и теория алгоритма.

Последующими дисциплинами являются: Управление информационной безопасностью, Защита программ и данных, Обеспечение ИБ в интеллектуальных системах.

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

В результате освоения дисциплины «Методы оценки безопасности компьютерных систем» студент должен овладеть следующими компетенциями:

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
УК-2.	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1.1 знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности
		УК-2.2.1 умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1.1 знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации
		ОПК-5.2.1 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.3 знает цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью
		ОПК-10.2.3 умеет оценивать информационные риски объекта информатизации
ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.2.2 умеет проводить физический эксперимент, обрабатывать его результаты, формировать отчет и делать выводы о проделанной исследовательской работе
		ОПК-11.2.2 умеет проводить физический эксперимент, обрабатывать его результаты, формировать отчет и делать выводы о проделанной исследовательской работе

#### 4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно- заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	2/72	2/72	
Семестр	8	9	
Лекции, час	16	8	
Практические занятия, час	-		
Лабораторные занятия, час	16	8	
Самостоятельная работа, час	40	56	
Курсовой проект (работа), РГР, семестр	8	9	
Зачет (при заочной форме <b>4 часа</b> отводится на контроль)	+	+	
Часы на экзамен (при очной, очно-заочной формах <b>1 ЗЕТ – 36 часов</b> , при заочной форме <b>9 часов</b> отводится на контроль)	-	-	

4.1.Содержание дисциплины (модуля) «Методы оценки безопасности компьютерных систем»

№ п/п	Раздел дисциплины, тема лекции и вопросы	Очная форма				Очно-заочная форма				Заочная форма			
		ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР
1	<p><u>Тема 1: Базовые сведения о и оценке уровня безопасности компьютерных систем</u></p> <p>1. Проверки и оценки уровня ИБ организации                  2. Оценка уязвимостей компьютерной системы                  3. Разновидности проверок и оценок уровня ИБ организации. Рынок аналитических услуг в сфере ИБ.                  4. Место и роль аудита в модели обеспечения ИБ.</p>	2	-	2	8	1	-	1	10	-	-	-	-
2	<p><u>Тема 2: Оценка уровня безопасности компьютерных систем: общие понятия и определения</u></p> <p>1. Базовые определения                  2. Принципы и формы аудита ИБ организации                  3. Оценка уязвимостей компьютерной                  4. Особенности автоматизированных информационных систем как объектов аудита ИБ.                  5. Исходная концептуальная схема (парадигма) проведения аудита ИБ.</p>	2	-	2	8	1	-	1	10	-	-	-	-

3	<p><u>Тема 3 Стандарты проведения оценки уровня безопасности компьютерных систем</u></p> <ol style="list-style-type: none"> <li>1. Законодательная и нормативная база аудита ИБ.</li> <li>2. Структура международных стандартов по ИБ. Область применения.</li> <li>3. Процессная модель управления ИБ.</li> <li>4. Оценка зрелости системы управления ИБ.</li> <li>5. ISO 27001 (B 7799 - 2:2005). ISO 27002 (BS 7799 - 1:2005).</li> <li>6. Стандарты ISO/IEC и ГОСТ ИСО/МЭК 27005, BS 7799-3.</li> <li>7. Анализ рисков ИБ.</li> <li>8. Общие критерии (ГОСТ Р ИСО/МЭК 15408).</li> <li>9. Руководящие документы</li> <li>10. ФСТЭК России аудит в целях сертификации средств защиты и аттестации объектов информатизации.</li> <li>11. Ста Банка России СТО БР ИББС- 1.1.</li> <li>12. CoBit. Стандарт аудита PCI DSS.</li> <li>13. Соответствие и взаимодействие международного и российского подходов и методов аудита безопасности.</li> <li>14. Стандарт аудита PCI DSS.</li> </ol>	4	-	4	8	2	-	2	12	-	-	-	-	-
---	---	---	---	---	---	---	---	---	----	---	---	---	---	---

4	<p><u>Тема 4 Методология оценки уровня безопасности компьютерных систем. Организация процесса оценки уровня безопасности компьютерных систем.</u></p> <ol style="list-style-type: none"> <li>1. Основные этапы и методы работ по проведению аудита ИБ.</li> <li>2. Программа аудита ИБ</li> <li>3. Сбор свидетельств (исходной информации) для проведения аудита ИБ.</li> <li>4. Рекомендации по планированию аудита ИБ.</li> <li>5. Рекомендации по моделированию.</li> <li>6. Этапы проведения внутреннего и внешнего аудитов ИБ: общее и различия.</li> <li>7. Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование.</li> <li>8. Договор о проведении внешнего аудита ИБ.</li> <li>9. Порядок планирования аудита.</li> <li>10. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника.</li> </ol>	4	-	4
	<ol style="list-style-type: none"> <li>11. Методы сбора исходных данных: опрос, наблюдение,</li> <li>12. анализ.</li> <li>13. Методы анализа собранных свидетельств.</li> <li>14. Аудиторская группа: состав, права и обязанности, роли, привлечение технических специалистов.</li> <li>15. Обязанности проверяемой организации во время аудита ИБ.</li> </ol>			



8	2	-	2	12	-	-	-	-

5	Тема 5 Инструментальные средства оценки уровня безопасности компьютерных систем 1. Методы и инструментальные средства проведения аудита ИБ 2. Программные средства анализа и управления 3. Оценка уязвимостей компьютерной системы средствами Dallas Lock 4. Инструментарий базового уровня - справочные и методические материалы. 5. Инструментарий для обеспечения повышенного уровня безопасности. 6. ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия СПВ, их применение и примеры систем. 7. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.	4	-	4	8	2	-	2	12	-	-	-	-	
	Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)	Входная конт. работа 1 аттестация 1-5 тема 2 аттестация 6-10 тема 3 аттестация 11-15 тема			Входная конт. работа 1 аттестация 1-5 тема 2 аттестация 6-10 тема 3 аттестация 11-15 тема									
	Форма промежуточной аттестации (по семестрам)	Экзамен			Экзамен									
	<b>Итого</b>	<b>16</b>	<b>-</b>	<b>16</b>	<b>40</b>	<b>8</b>	<b>-</b>	<b>8</b>	<b>56</b>		<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>

*К видам учебной работы в вузе отнесены: лекции, консультации, семинары, практические занятия, лабораторные работы, контрольные работы, коллоквиумы, самостоятельные работы, научно- исследовательская работа, практики, курсовое проектирование (курсовая работа). Вуз может устанавливать другие виды учебных занятий.*

*\* - Разделы, тематику и вопросы по дисциплине следует разделить на три текущие аттестации в соответствии со сроками проведения текущих аттестаций. По материалу программы, пройденному студентом после завершения 3-ей аттестации до конца семестра (2-3 недели), контроль успеваемости осуществляется при сдаче зачета или экзамена.*

#### 4.2. Содержание лабораторных (практических) занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов			Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Очно-заочно	Заочно	
1	2	3	4	5	6	7
1.	№1	Оценка уязвимостей компьютерной системы	2	1	-	№№ 1-8
2.	№2	Схема проведения аудита ИБ	2	1	-	№№ 1-8
3.	№3	Этапы проведения внутреннего внешнего аудитов ИБ: общее различия.	2	1	-	№№ 1-8
4.	№4	Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование.	2	1	-	№№ 1-8
5.	№5	Договор о проведении внешнего аудита ИБ. Порядок планирования аудита.	2	1	-	№№ 1-8
6.	№6	Оценка уязвимостей компьютерной системы средствами Dallas Lock	2	1	-	№№ 1-8
7.	№7	Инструментарий базового уровня справочные методические материалы. Инструментарий для обеспечения повышенного уровня безопасности.	2	1	-	№№ 1-8
8.	№8	ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия	2	1	-	№№ 1-8
<b>ИТОГО</b>			<b>16</b>	<b>8</b>		

#### 4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
		Очно	Очно-заочно	Заочно		
1	2	1	4	5	6	7
1	Обеспечение информационной	6	6	-	№№ 1-8	Опрос, реферат, статья

	безопасности					
2	Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга).	6	10	-	№№ 1-8	Опрос, реферат, статья
3	Критерии безопасности компьютерных систем STCPEC	8	10	-	№№ 1-8	Опрос, реферат, статья
4	Гармонизированные критерии оценки безопасности информационных технологий ITSEC.	8	10	-	№№ 1-8	Опрос, реферат, статья
5	Рекомендации X.800 для распределенных систем	6	10	-	№№ 1-8	Опрос, реферат, статья
6	Общие критерии оценки безопасности информационных технологий.	6	10	-	№№ 1-8	Опрос, реферат, статья
<b>ИТОГО</b>		<b>40</b>	<b>56</b>		-	

**7. Учебно-методическое и информационное обеспечение дисциплины Методы  
оценки безопасности компьютерных систем**  
Рекомендуемая литература и источники информации (основная и дополнительная)  
Зав. библиотекой / *И.И.И.* Алиева Ж.А.

п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы	Количество изданий	
			В библиотеке	На кафедре
<b>Основная</b>				
1.	лк, пз, срс	Вагина, Н. Д. Диагностика и прогнозирование угроз организации : учебно-методическое пособие / Н. Д. Вагина. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2018. — 102 с. — ISBN 978-5-00137-036-9. — Текст : электронный // Лань : электронно-библиотечная система.	URL: <a href="https://e.lanbook.com/book/115101">https://e.lanbook.com/book/115101</a>	
2.	лк, пз, срс	Кондрашова, Е. А. Финансовая безопасность предприятия : учебно-методическое пособие / Е. А. Кондрашова. — Донецк : ДонНУ, 2020. — 190 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: <a href="https://e.lanbook.com/book/179971">https://e.lanbook.com/book/179971</a>	
3.	лк, пз, срс	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система.	URL: <a href="https://e.lanbook.com/book/156401">https://e.lanbook.com/book/156401</a>	
<b>Дополнительная</b>				
4.	лк, пз, срс	Международное сотрудничество в области охраны окружающей среды : учебное пособие / Ю. А. Мандра, Е. Е. Степаненко, Т. Г. Зеленская, О. А. Поспелова. — Ставрополь : СтГАУ, 2015. — 68 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: <a href="https://e.lanbook.com/book/82242">https://e.lanbook.com/book/82242</a>	
5.	лк, пз, срс	Шилер, А. В. Обеспечение информационной безопасности корпоративных информационных сетей на базе программного комплекса SecureTower : учебно-методическое пособие / А. В. Шилер, А. А. Елизаров, Е. А. Степанова. — Омск : ОмГУПС, 2020. — 23 с. — Текст : электронный // Лань : электронно-	URL: <a href="https://e.lanbook.com/book/165730">https://e.lanbook.com/book/165730</a>	

		библиотечная система.	
6.	лк, пз, срс	Информационная безопасность : учебное пособие / В. Н. Яснев, А. В. Дорожкин, А. Л. Сочков, О. В. Яснев ; под редакцией В. Н. Яснева. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2017. — 198 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: <a href="https://e.lanbook.com/book/153011">https://e.lanbook.com/book/153011</a>

## **8. Материально-техническое обеспечение дисциплины (модуля) «Методы оценки безопасности компьютерных систем»**

Материально-техническое обеспечение дисциплины включает:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет (лаборатории по автоматизированным информационным системам, оснащенные современной электронно-вычислительной техникой с соответствующим программным обеспечением);
- аудитории, оборудованные проекционной техникой.

Для проведения практических занятий используются компьютерные классы кафедры ИБ, оборудованные современными персональными компьютерами, характеристики которых не ниже:

Pentium 4, DDR 1 Gb, HDD – 150 GB, Video Card – 126 MB, CD/DVD, USB -2.

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

На компьютере предустанавливается ОС Windows XP/Vista/7 и программное обеспечение MS Office 2010, Borland C++ , Borland C++ Builder 6 и др. Приложение командной строки dumpasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumpasn1.rar (Windows, x86).

КриптоПро ОСPCOM (версия 1.05.0726).

КриптоПро TSPCOM (версия 1.05.0972).

8.4. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

При проведении лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

Microsoft Office (Word, Excel, PowerPoint, Access)

ЭБС <http://library.mirea.ru/>.

Дистрибутив КриптоПро WinLogon и КриптоПро EAP-TLS;

Дистрибутив КриптоПро JCP и КриптоПро JTLS

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

## **5. Образовательные технологии**

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий.

Аудиторная работа включает: лекции, практические занятия, мастер-классы, консультации.

В курсе лекций использованы наглядные, иллюстрированные материалы, обширная информация в табличной и графической формах, а также электронные ресурсы сети Интернет. Разработаны продвинутые лекции (с визуализацией) в формате презентаций, с использованием пакета прикладных программ MS Power Point.

Внеаудиторная работа призвана для формирования и развития профессиональных навыков обучающихся. Самостоятельная работа включает: выполнение домашних заданий, подготовка рефератов, участие в дискуссиях, работа в информационно-образовательной среде. В конце обучения проводится экзамен.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

## **6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов**

Оценочные средства приведены в ФОС (Приложение А)



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 05.04.2017 № 301 «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 оснащённости 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