Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Информационная безопасность открытых 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 энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, очно-заочная курс 3 семестр (ы) 5(6)
очная, очно-заочная, заочная

г. Махачкала 2024

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., к.э.н.
подпись (ФИО уч. степень, уч. звание)

«27» сентября 2024г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)

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

«15» сентября 2024 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности от 15 октября2024 года, протокол № 3.

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)

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

«15» октября 2024 г.

Программа одобрена на заседании Методического Совета факультета компьютерных технологий и энергетики от 17 октября 2024 года, протокол № 2.

Председатель Методического совета факультета КТиЭ _____ Т.И. Исабекова, к.ф.-м.н., доцент
подпись (ФИО уч. степень, уч. звание)

Декан факультета _____ Т.А. Рагимова
подпись ФИО

Начальник УО _____ М.Т. Муталибов
подпись ФИО

Проректор по УР _____ А.Ф. Демирова
подпись ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) « Информационная безопасность открытых систем» является приобретение студентами фундаментальных представлений о функциях современной ИБОС и о структуре ее функциональных компонентов, дается определение задач ИБОС и ее границ, говорится об адекватном позиционировании и средствах интеграции ИБОС в современной ИТ структуре.

Современная проблема обеспечения безопасности информационных систем компаний, фирм, производств, Госучреждений является довольно сложным комплексом и объективными причинами появления этой проблемы и ее решения являются внутренние (сбои техники и программного обеспечения, ошибки и недоработки в проектировании, наладке систем, недостатки масштабировании, обслуживания системы, администрирования мониторинга, аудита систем, преднамеренные и целенаправленные действия обслуживающего персонала, ведущие к нарушению сохранности информации), внешние (наличие объективных причин уязвимостей действующих систем и, как следствие, хакерские атаки и взлом систем) причины.

В курсе делается попытка создания единой системы обеспечения безопасности начиная от идеи создания такой системы, проектирования ее, наладке, эксплуатации и масштабирования. Отдельной темой будет раскрытие понятий, что такое система, информация ,безопасность, открытые и закрытые системы.

Цели изучения дисциплины.

•Уметь анализировать классы задач и процессов, создания защищенных информационных систем и навыков их поддержания ;

•Описывать основные функциональные подсистемы и их взаимодействие в рамках комплексной БОИС;

•Владеть методикой выбора средств автоматизации и методология процесса внедрения системы;

•Знать разницу решения данной проблемы в отечественных организациях и зарубежных компаниях;

•Понимать, персоналу разрешено все, что не запрещено, строгое соблюдение инструкций и этапов выполнение работ, уяснения понятия важности каждой должности в едином организме фирмы, справедливой системы материального поощрения;

• Приобретение навыков в диагностировании работы алгоритмов, техники, протоколов, коррекция инструкций и положений;

•Единое требование к безопасности всеобщая система двойной парольной защиты, хранение любой информации в зашифрованном формате и система допуска к технике, программному обеспечению и атрибутам информации.

2.Место дисциплины в структуре ОПОП

Дисциплина « Информационная безопасность открытых систем » относится к блоку 1 (Обязательная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Основы информационной безопасности, Математическая логика и теория алгоритма, знание основ курса “Криптографические основы защиты информации”.

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 « Информационная безопасность открытых систем» студент должен овладеть следующими компетенциями:

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности
		ОПК-5.2.2 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1.1 знает систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации
		ОПК-6.2.1 умеет определить политику контроля доступа работников к информации ограниченного доступа
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-10.1.2 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации
		ОПК-10.1.5 знает принципы организации информационных систем в соответствии с требованиями по защите информации
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144	4/144	
Семестр	5	6	
Лекции, час	34	17	
Практические занятия, час	-		
Лабораторные занятия, час	34	17	
Самостоятельная работа, час	40	74	
Курсовой проект (работа), РГР, семестр	-	-	
Зачет (при заочной форме **4 часа** отводится на контроль)	-	-	
Часы на экзамен (при очной, очно-заочной формах **1 ЗЕТ – 36 часов**, при заочной форме **9 часов** отводится на контроль)	**1 ЗЕТ – 36 часов**	**1 ЗЕТ – 36 часов**	

4.1.Содержание дисциплины (модуля) « Информационная безопасность открытых 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	Лекция 1: Архитектура безопасности ИТС 1. Источники и последствия реализации угроз ИБ 2. Функция, способы и средства обеспечения ИБ 3. Архитектура безопасности ЭМВОС	2	-	2	4	2	-	-	8				
2	Лекция 2: Концепции обеспечения информационной безопасности 1. Общие концепции обеспечения ИБ 2. Общая информация для обеспечения безопасности 3. Общие средства обеспечения безопасности. 4. Взаимосвязи между СПБ	4	-	4	4	2	-	1	8				
3	Лекция 3: Теоретические основы аутентификации 1. Общие положения 2. Вспомогательная информация и средства аутентификации 3. Свойства способов аутентификации 4. Способы аутентификации 5. Взаимодействие с другими службами и способами обеспечения безопасности 6. Персонификация (аутентификация пользователей) 7. Аутентификация в ЭМВОС и Интернет-архитектуре 8. Практические аспекты парирования атак типа «повторная передача» на основе применения уникальных чисел или встречных запросов 9. Защита процедуры аутентификации 10. Примеры способов аутентификации	4	-	4	4	2	-	1	8				

4	Лекция 4: Теоретические основы управления доступом 1. Общие положения 2. Политики УД 3. Вспомогательная информация и средства УД 4. Классификация способов УД 5. Взаимодействие с другими СЛБ и СПБ 6. Обмен СЕРТ|УД между компонентами 7. Управление доступом в ЭМВОС и Интернет-архитектуре 8. Проблема уникальности (неединственность) параметров подлинности для УД 9. Распределение компонентов УД 10. Сравнительный анализ УДПР и УДПП 11. Способ обеспечения ретрансляции ВИУД через инициатора	4	-	4	4	2	-	1	8				
5	Лекция 5: Теоретические основы обеспечения неотказуемости 1. Общие положения 2. Политики обеспечения неотказуемости 3. Вспомогательная информация и средства обеспечения неотказуемости 4. Способы обеспечения неотказуемости 5. Взаимосвязи с другими СЛБ И СПБ 6. СЛНТ в системах ЭМВОС и Интернет-архитектуры 7. СЛНТ в системах хранения и ретрансляции 8. Восстановление в СЛНТ 9. Взаимодействие со Службой единого каталога	4	-	4	4	2	-	1	8				

6	Лекция 6: Теоретические основы обеспечения конфиденциальности 1. Общие положения 2. Политики обеспечения конфиденциальности 3. .Вспомогательная информация и средства обеспечения конфиденциальности 4. Способы обеспечения конфиденциальности 5. Взаимодействие с другими СЛБ и СПБ 6. Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре 7. Форматы представления информации 8. Скрытые каналы передачи	4	-	4	5	2	-	1	8				
7	Лекция 7: Теоретические основы обеспечения целостности 1. Общие положения 2. Политики обеспечения целостности 3. Вспомогательная информация и средства обеспечения целостности 4. Классификация способов обеспечения целостности 5. Взаимосвязи с другими СЛБ и СПБ 6. Обеспечение целостности в ЭМВОС и Интернет-архитектуре 7. Целостность внешних данных	4	-	4	5	2	-	1	9				

8	Лекция 8: Теоретические основы аудита безопасности и оповещения об опасности 1. Общие положения 2. Политики и другие аспекты аудита безопасности и оповещения об опасности 3. Вспомогательная информация и средства для аудита безопасности и оповещения об опасности 4. Способы проведения АДБ и применения СОП 5. Взаимосвязи с другими СЛБ и СПБ 6. Общие принципы АДБ и СОП в ЭМВОС и Интернет - архитектуре 7. Реализация модели АДБ и СОП 8. Регистрация времени возникновения событий, подлежащих аудиторскому контролю	4	-	4	5	2	-	1	9				
9	Лекция 9: Теоретические основы обеспечения ключами 1. Общая модель обеспечения ключами 2. Основные концепции обеспечения ключами 3. Концептуальные модели распределения ключей между двумя взаимодействующими сторонами 4. Провайдеры специализированных услуг 5. Угрозы системе обеспечения ключами 6. Информационные объекты в службе обеспечения ключами 7. Классы прикладных криптографических систем 8. Обеспечение жизненного цикла СЕРТ|ОК	4	-	4	5	1	-	1	8				
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 (36 ч)				Экзамен (36 ч)							
Итого		**34**	**-**	**34**	**40**	**17**	**-**	**17**	**74**				

-

* -

3- *(2-3*

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	Изучение и опробование системы крипто-защиты WinApi	2	1		№№ 1-8
2	№2	Настройка экранов. Брандмауэров, антивирусная защита	2	1		№№ 1-8
3	№3	Разработка Config клиентов и серверов OpenVPN	2	1		№№ 1-8
4	№4	Построение сетей в терминальных классах.	2	1		№№ 1-8
5	№5	Организация систем удаленного доступа	2	1		№№ 1-8
6	№ 6	Построение сетей на оборудовании домашних компьютеров	2	1		№№ 1-8
7	№7	Администрирование, масштабирование, настройка БИС	2	1		№№ 1-8
8	№8	Разработка сети в пакете Cisko Packet Tracer	2	1		№№ 1-8
ИТОГО			**16**	**8**		

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	Основные положения управление доступа к элементам информации	2	8	-	№№ 1-8	Опрос, реферат, статья
2	Понятие положений конфиденциальности, сохранности, ответственности и авторства информации	4	8	-	№№ 1-8	Опрос, реферат, статья

3	Криптографические основы БИС	2	10	-	№№ 1-8	Опрос, реферат, статья
4	Архитектура и основы БИС	4	10	-	№№ 1-8	Опрос, реферат, статья
5	Концепция БИС	2	10	-	№№ 1-8	Опрос, реферат, статья
6	Понятие положений конфиденциальности, сохранности, ответственности и авторства информации	4	10	-	№№ 1-8	Опрос, реферат, статья
7	Обеспечение основ мониторинга и аудита БИС	2	10	-	№№ 1-8	Опрос, реферат, статья
8	Философское трактование понятий открытых и закрытых систем и подсистем	4	10	-	№№ 1-8	Опрос, реферат, статья
ИТОГО		**24**	**76**	-		

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)

7. Учебно-методическое и информационное обеспечение дисциплины
Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой  **Сулейманова О.Ш.**

п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы	Количество изданий	
			В библиотеке	На кафедре
1	2	3	4	5
Основная				
1.	лк, лб, срс	Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. — 2-е изд. — Москва : ФЛИНТА, 2014. — 448 с. — ISBN 978-5-9765-1613-7. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/48368	
2.	лк, лб, срс	Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2016. — 201 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/155246	
3.	лк, лб, срс	Основы работы в программе CISCO PACKET TRACER : учебно-методическое пособие / составители Г. В. Абрамов [и др.]. — Воронеж : ВГУ, 2017. — 31 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/154795	
Дополнительная				
4.	лк, лб, срс	Космачева, И. М. Проектирование защищенных баз данных : учебное пособие / И. М. Космачева, Н. В. Давидюк. — Санкт-Петербург : Интермедия, 2020. — 144 с. — ISBN 978-5-4383-0191-2. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/161362	
5.	лк, лб, срс	Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/216425	
6.	лк, лб, срс	Трошин, А. В. Конфигурирование коммутаторов Cisco : методические указания / А. В. Трошин. — Самара : ПГУТИ, 2021. — 24 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/301205	
7.	лк, лб, срс	Паршин, К. А. Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / К. А. Паршин. — Екатеринбург : , 2018. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/121337	

8.	лк, лб, срс	Основы построения объединенных сетей по технологиям CISCO : учебное пособие. — 2-е изд. — Москва : ИНТУИТ, 2016. — 285 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/100313
ИНТЕРНЕТ - РЕСУРСЫ			
9.	лк, лб, срс	Cisco Learning Network (www.cisco.com/c/en/us/training-events/training-certifications/learning-network.html) — это онлайн сообщество уроков и видеоуроков на различные темы, связанные с устройствами Cisco.	
10.	лк, лб, срс	Курсы Cisco Networking Academy (www.netacad.com) —программа, разработанная Cisco для обучения студентов	
11.	лк, лб, срс	https://securelist.ru/enciklopediya Энциклопедия информационной безопасности.	
12.	лк, лб, срс	http://www.citforum.ru/security/ CITFORUM — информационная безопасность	
13.	лк, лб, срс	http://www.infoforum.ru/ Национальный форум информационной безопасности "ИНФОФОРУМ" — электронное периодическое издание по вопросам информационной безопасности	
14.	лк, лб, срс	http://saferunet.ru/ Центр Безопасного Интернета в России посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Вопросы Интернет-угроз, технологий, способов эффективного противодействия им в отношении пользователей	
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ			
15.	лк, лб, срс	ОС Windows XP/ 7 / 8/10	
16.	лк, лб, срс	ОС Windows XP/ 7 / 8/10, Microsoft Office 2013/2016	
17.	лк, лб, срс	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017	

8. Материально-техническое обеспечение дисциплины (модуля) « Информационная безопасность открытых 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 OCSPCOM (версия 1.05.0726).

КриптоПро TSPCOM (версия 1.05.0972).

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

При проведения 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)

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 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