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 специальности 10.05.03 Информационная безопасность автоматизированных систем
код и полное наименование специальности

по специализации Безопасность открытых информационных 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 курс 5 семестр (ы) А
очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем с учетом рекомендаций и ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

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

«18» 09 2021г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)_____
_____ Качаева Г.И.,к.э.н._____
подпись (ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

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» сентября 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от «18» октября 2021 г., протокол № 2

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

от «18» октября 2021 г.

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 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.

Задачами дисциплины являются: получение студентами знаний о классах задач и процессах создания защищенных информационных систем и навыков их поддержании. Научить: описывать основные функциональные подсистемы и их взаимодействие в рамках комплексной БОИС; владеть методикой выбора средств автоматизации и методология процесса внедрения системы; 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.

2.Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность открытых систем» относится к обязательной части учебного плана.

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: ОПК-4; ОПК-5.2.; ОПК-5.3.

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.2.6 умеет осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий
ОПК-5.2	Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ОПК-5.2.1.1 знает методы и средства обеспечения информационной безопасности открытых информационных систем;
		ОПК-5.2.1.2 знает методы контроля, разработки эксплуатационной документации, обслуживания систем защиты информации открытых информационных систем;
		ОПК-5.2.2.1 умеет применять методы и средства защиты информации открытых информационных систем;
		ОПК-5.2.2.2 умеет разрабатывать эксплуатационную документацию, требования по эксплуатации систем защиты открытых информационных систем;
ОПК-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ОПК-5.3.1.1 знает основные информационные технологии, используемые в автоматизированных системах;
		ОПК-5.3.1.2 знает системы управления информационной безопасностью открытой информационной системы;
		ОПК-5.3.2.1 умеет работать с интегрированной средой разработки программного обеспечения;
		ОПК-5.3.2.2 умеет анализировать представленную в общедоступных источниках информацию о современных тенденциях в области информационных систем;

Компетенции кот. прописав. в учеб. плане.

ОПК-6 ОПК-5.3

ОПК-8

ОПК-5.1

ОПК-5.2.

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	6/216		
Семестр	А		
Лекции, час	68		
Практические занятия, час	-		
Лабораторные занятия, час	51		
Самостоятельная работа, час	61		
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)	**36**		

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 Источники и последствия реализации угроз ИБ. Функция, способы и средства обеспечения ИБ. Архитектура безопасности ЭМВОС	2	-	2	2								
2	Лекция 2: Концепции обеспечения информационной безопасности. Общие концепции обеспечения ИБ. Общая информация для обеспечения безопасности	2	-	2	2								
3	Лекция 3: Концепции обеспечения информационной безопасности. Общие средства обеспечения безопасности. Взаимосвязи между СПБ.	2	-	1	2								
4	Лекция 4: Теоретические основы аутентификации Общие положения. Вспомогательная информация и средства аутентификации. Свойства способов аутентификации.	2	-	2	2								
5	Лекция 5: Теоретические основы аутентификации Взаимодействие с другими службами и способами обеспечения безопасности. Персонификация (аутентификация пользователей) . Аутентификация в ЭМВОС и Интернет-архитектуре.	2	-	1	2								
6	Лекция 6: Теоретические основы аутентификации Практические аспекты парирования атак типа «повторная передача» на основе применения уникальных чисел или встречных запросов. Защита процедуры аутентификации. Примеры способов аутентификации	2	-	2	2								
7	Лекция 7: Теоретические основы управления доступом Общие положения. Политики УД. Вспомогательная информация и средства УД . Классификация способов УД. Взаимодействие с другими СЛБ и СПБ. Обмен СЕРТ|УД между компонентами. Управление доступом в ЭМВОС и Интернет-архитектуре.	2	-	1	2								

8	Лекция 8: Теоретические основы управления доступом Проблема уникальности (неединственность) параметров подлинности для УД. Распределение компонентов УД. Сравнительный анализ УДПР и УДПП. Способ обеспечения ретрансляции ВИУД через инициатора.	2	-	2	2								
9	Лекция 9: Теоретические основы обеспечения неотказуемости. Общие положения. Политики обеспечения неотказуемости. Вспомогательная информация и средства обеспечения неотказуемости. Способы обеспечения неотказуемости..	2	-	1	2								
10	Лекция 10: Теоретические основы обеспечения неотказуемости Взаимосвязи с другими СЛБ И СПБ. СЛНТ в системах ЭМВОС и Интернет-архитектуры. СЛНТ в системах хранения и ретрансляции. Восстановление в СЛНТ. Взаимодействие со Службой единого каталога.	2	-	2	2								
11	Лекция 11: Теоретические основы обеспечения конфиденциальности Общие положения. Политики обеспечения конфиденциальности. Вспомогательная информация и средства обеспечения конфиденциальности.	2	-	1	2								
12	Лекция 12: Теоретические основы обеспечения конфиденциальности Способы обеспечения конфиденциальности. Взаимодействие с другими СЛБ и СПБ.	2	-	2	2								
13	Лекция 13: Теоретические основы обеспечения конфиденциальности. Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре. Форматы представления информации. Скрытые каналы передачи.	2	-	1	2								
14	Лекция 14: Теоретические основы обеспечения целостности. Общие положения. Политики обеспечения целостности. Вспомогательная информация и средства обеспечения целостности.	2	-	2	2								
15	Лекция 15: Теоретические основы обеспечения целостности. Классификация способов обеспечения целостности. Взаимосвязи с другими СЛБ и СПБ. Обеспечение целостности в ЭМВОС и Интернет-архитектуре. Целостность внешних данных	2	-	1	2								

16	Лекция 16: Теоретические основы аудита безопасности и оповещения об опасности. Общие положения. Политики и другие аспекты аудита безопасности и оповещения об опасности. Вспомогательная информация и средства для аудита безопасности и оповещения об опасности. Способы проведения АДБ и применения СОП.	2	-	2	2								
17	Лекция 17: Теоретические основы аудита безопасности и оповещения об опасности. Взаимосвязи с другими СЛБ и СПБ. Общие принципы АДБ и СОП в ЭМВОС и Интернет –архитектуре. Реализация модели АДБ и СОП. Регистрация времени возникновения событий, подлежащих аудиторскому контролю.	2	-	1	2								
18	Лекция 18: Теоретические основы обеспечения ключами. Общая модель обеспечения ключами. Основные концепции обеспечения ключами. Концептуальные модели распределения ключей между двумя взаимодействующими сторонами. Провайдеры специализированных услуг.	2	-	2	2								
19	Лекция 19: Теоретические основы обеспечения ключами. Угрозы системе обеспечения ключами. Информационные объекты в службе обеспечения ключами. Классы прикладных криптографических систем . Обеспечение жизненного цикла СЕРТ|ОК	2	-	1	2								
20	Лекция 20. Стандартизация и модельное представление открытых информационных систем. Роль стандартов в технологии открытых систем. Основные группы стандартов и организации по стандартизации.	2	-	2	2								
21	Лекция 21. Стандартизация и модельное представление открытых информационных систем. Модель OSI и POSIX.	2	-	1	2								
22	Лекция 22. Интранет как открытая система. Разработка и управление Политикой использования ресурсов интранета.	2	-	2	2								
23	Лекция 23. Уязвимость открытых систем на примере интранета Анализ угроз ИБ ресурсам интранета и причины их реализации.	2	-	1	2								
24	Лекция 24. Уязвимость открытых систем на примере интранета Уязвимости операционных систем, серверов, рабочих станций, каналов связи.	2	-	2	2								

25	Лекция 25. Уязвимость открытых систем на примере интранета Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, WorldWideWeb, Команды удаленного выполнения, Sendmail и электронная почта.	2	-	1	2								
26	Лекция 26. Атаки на открытые системы. Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.	2	-	2	2								
27	Лекция 27. Атаки на открытые системы. Этапы реализации и уровни атак. Атаки с использованием сетевых протоколов.	2	-	1	2								
28	Лекция 28. Обеспечение информационной безопасности в открытых системах. Разработка Политики безопасности для открытых систем.	2	-	2	1								
29	Лекция 29. Обеспечение информационной безопасности в открытых системах. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.	2	-	1	1								
30	Лекция 30. Аутентификация субъектов и объектов взаимодействия в открытых системах. Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа.	2	-	1	1								
31	Лекция 31. Аутентификация субъектов и объектов взаимодействия в открытых системах. Анализ типовой модели аутентификации.	2	-	2	1								
32	Лекция 32. Виртуальные вычислительные сети. Виды ВЧВС в зависимости от решаемых задач: Intranet VPN, Client/server VPN, Extranet VPN, RemoteAccess VPN.	2	-	1	1								

33	Лекция 33. Межсетевые экраны. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений. Типы межсетевых экранов: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, межсетевые экраны экспертного уровня, персональные межсетевые экраны.	2	-	2	1								
34	Лекция 34. Межсетевые экраны. Сетевой сканер XSpider. Система обнаружения вторжений Cisco IPS.	2	-	1	1								
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; Контрольная работа			
Форма промежуточной аттестации (по семестрам)		Экзамен				Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого		68	-	51	61								

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	Изучение и опробование системы крипто-защиты WinApi	6			№№ 1-14
2	№2	Настройка экранов. Брандмауэров, антивирусная защита	6			№№ 1-14
3	№3	Разработка Config клиентов и серверов OpenVPN	6			№№ 1-14
4	№ 4	Построение сетей в терминальных классах.	6			№№ 1-14
5	№5	Организация систем удаленного доступа	6			№№ 1-14

6	№6	Построение сетей на оборудовании домашних компьютеров	8			№№ 1-14
7	№7	Администрирование, масштабирование, настройка БИС	6			№№ 1-14
8	№8	Разработка сети в пакете Cisko Packet Tracer	7			№№ 1-14
ИТОГО			51			

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	3	4	5	6	7
1.	Основные положения управление доступа к элементам информации	6			№№ 1-14	Опрос, реферат
2.	Понятие положений конфиденциальности, сохранности, ответственности и авторства информации	8			№№ 1-14	Опрос, реферат
3.	Криптографические основы БИС	8			№№ 1-14	Опрос, реферат
4.	Архитектура и основы БИС	8			№№ 1-14	Опрос, реферат
5.	Концепция БИС	8			№№ 1-14	Опрос, реферат
6.	Понятие положений конфиденциальности, сохранности, ответственности и авторства информации	8			№№ 1-14	Опрос, реферат
7.	Обеспечение основ мониторинга и аудита БИС	8			№№ 1-14	Опрос, реферат
8.	Философское трактование понятий открытых и закрытых систем и подсистем	7			№№ 1-14	Опрос, реферат
ИТОГО		**61**				

7. Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой _____ **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
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. —	URL: https://e.lanbook.com/book/121337	

		Текст : электронный // Лань : электронно-библиотечная система. —	
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

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).

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/.

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