Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Криптографические протоколы и стандарты
наименование дисциплины по ОПОП

для специальности 10.05.03 Информационная безопасность автоматизированных систем
код и полное наименование направления (специальности)

по специализации Безопасность открытых информационных систем

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

кафедр Информационной безопасности.
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 4 семестр (ы) 7.
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)

«17» 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.

Целью освоения дисциплины (модуля) Криптографические протоколы и стандарты являются ознакомление существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

Задачи дисциплины: обучить студентов принципам работы основных протоколов; привить студентам навыки реализации криптографических протоколов с использованием ЭВМ; дать студентам представление об анализе стойкости протоколов к атакам.

2.Место дисциплины в структуре ОПОП

Дисциплина «Криптографические протоколы и стандарты» относится к обязательной части учебного плана.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Алгебра и геометрия», «Дискретная математика», «Операционные системы».

Последующими дисциплинами являются: «Управление информационной безопасностью», «Информационная безопасность открытых систем».

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

В результате освоения дисциплины Криптографические протоколы и стандарты студент должен овладеть следующей компетенцией: ОПК-5.1.

Код компетенции	**Наименование компетенции**	**Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)**
ОПК-5.1	Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ОПК-5.1.1.1. знает основные криптографические протоколы и стандарты;
		ОПК-5.1.1.2 знает критерии оценки и контроля эффективности используемых криптографических протоколов и стандартов;
		ОПК-5.1.2.1 умеет выбирать криптографические протоколы и стандарты, для обеспечения информационной безопасности открытых информационных систем;
		ОПК-5.1.2.2 умеет осуществлять контроль эффективности средств защиты, реализующих используемые криптографические протоколы и стандарты;

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144		
Семестр	8		
Лекции, час	34		
Практические занятия, час			
Лабораторные занятия, час	34		
Самостоятельная работа, час	40		
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) Криптографические протоколы и стандарты

№ 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.	Тема №1: Общие сведения о криптографических протоколах.	2	-	2	2								
2.	Тема №2: Основные понятия. Анализ безопасности простейших протоколов. Классификация атак. Анализ протоколов цифровых подписей. Анализ DSA и ГОСТ.	2	-	2	2								
3.	Тема №3: Привязка к биту и электронная жеребьевка. Компьютерная реализация схем электронной жеребьевки и привязки к биту.	2	-	2	2								
4.	Тема №4: Разделение секрета. Реализация пороговых схем разделения секрета и СРС для произвольной структуры доступа.	2	-	2	2								
5.	Тема №5: Разделение секрета. Проверяемое разделение секрета и конфиденциальные вычисления.	2	-	2	3								
6.	Тема №6: Идентификация и аутентификация. Парольные схемы. Одноразовые пароли.	2	-	2	2								
7.	Тема №7: Идентификация и аутентификация. Схемы рукопожатия.	2	-	2	2								
8.	Тема №8: Протоколы идентификации с нулевым разглашением. Интерактивные системы доказательства.	2	-	2	3								
9.	Тема №9: Протоколы идентификации с нулевым разглашением Имитационное моделирование протоколов идентификации на основе ИСД с нулевым разглашением.	2	-	2	2								

10.	Тема №10: Протоколы открытых сделок. Компьютерная реализация схем слепой подписи и скрытого канала. Компьютерная реализация протокола «Покер по телефону» для 3-х игроков. Имитационное моделирование схемы электронных денег с монетами одинакового достоинства.	2	-	2	3								
11.	Тема №11: Протоколы обмена ключами	2	-	2	2								
12.	Тема №12: Развитые протоколы обмена ключами с аутентификацией сторон.	2	-	2	3								
13.	Тема №13: Инфраструктура открытых ключей. Изучение работы с удостоверяющим центром при помощи CryptoPro. Формирование и проверка сертификата с использованием CryptoPro.	2	-	2	2								
14.	Тема №14: Управление ключами. Компьютерная реализация протокола передачи секретного ключа через доверенный центр (работа в группах). Компьютерная реализация протокола передачи секретного ключа средствами асимметричной криптографии(работа в группах).	2	-	2	3								
15.	Тема №15: Типичные атаки на протоколы аутентификации. Протоколы защиты данных в сети Internet.	2	-	2	2								
16.	Тема №16: Депонирование ключей и возможность контроля информационного взаимодействия.	2	-	2	3								
17.	Тема №17: Прикладные протоколы. Протоколы семейства KriptoKnight для различных сетевых конфигураций и условий применения. Протоколы семейства IPSec. Протоколы семейства SSL/TLS.	2	-	2	2								
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная Конт. Работа 1 аттестация 1-4 тема 2 аттестация 5-7 тема 3 аттестация 8-10 тема								Входная Конт. Работа; Контрольная работа			
Форма промежуточной аттестации (по семестрам)		экзамен				Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого		34		34	40								

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.	4	Идентификация и аутентификация Содержание занятия: Реализация пороговых схем разделения секрета, оценка размеров долей секрета для каждого участника, оценка вероятности угадывания секрета для заданной неразрешенной группы доступа	4			
2.	4	Протоколы обмена ключами Содержание занятия: Реализация схем подбрасывания монеты и атаки на них.	4			
3.	5	Протоколы обмена ключами Содержание занятия: Реализация парольных схем и протоколов рукопожатия. Реализация интерактивных схем аутентификации и атаки на них.	4			
4.	6	Протоколы обмена ключами Содержание занятия: Реализация схем цифровой подписи. Имитация скрытого канала на основе схемы цифровой подписи.	2			
5.	7	Развитые протоколы обмена ключами с аутентификацией сторон Содержание занятия: Схемы управления ключами – выработка и распределения сеансового секретного ключа между двумя не доверяющими друг другу пользователями. Распределение секретного ключа при помощи двухключевой криптосистемы	4			

6.	8	Депонирование ключей и возможность контроля информационного взаимодействия Содержание занятия: Протокол “Kerberos”. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей.	4			
7.	9	Инфраструктура открытых ключей. Схемы обязательств Содержание занятия: Протокол Диффи-Хеллмана. Протоколы STS, MTI	2			
8.	10	Инфраструктура открытых ключей. Схемы обязательств Содержание занятия: KDP(n,q)-схема предварительного распределения ключей	4			
ИТОГО			34			

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.	Общие сведения о криптографических протоколах.	2				Опрос, реферат, статья
2.	Основные понятия. Анализ безопасности простейших протоколов.	2				Опрос, реферат, статья
3.	Привязка к биту и электронная жеребьевка.	2				Опрос, реферат, статья
4.	Разделение секрета.	2				Опрос, реферат, статья
5.	Разделение секрета.	3				Опрос, реферат, статья
6.	Идентификация и аутентификация.	2				Опрос, реферат, статья
7.	Идентификация и аутентификация.	2				Опрос, реферат, статья
8.	Протоколы идентификации с нулевым разглашением.	3				Опрос, реферат, статья
9.	Протоколы идентификации с нулевым разглашением.	2				Опрос, реферат, статья
10.	Протоколы открытых сделок.	3				Опрос, реферат, статья

11.	Протоколы обмена ключами	2				Опрос, реферат, статья
12.	Развитые протоколы обмена ключами с аутентификацией сторон.	3				Опрос, реферат, статья
13.	Инфраструктура открытых ключей.	2				Опрос, реферат, статья
14.	Управление ключами.	3				Опрос, реферат, статья
15.	Типичные атаки на протоколы аутентификации.	2				Опрос, реферат, статья
16.	Депонирование ключей и возможность контроля информационного взаимодействия.	3				Опрос, реферат, статья
17.	Прикладные протоколы. сетевых конфигураций и условий применения.	2				Опрос, реферат, статья
ИТОГО		**40**				

5. Образовательные технологии

Чтение лекций и практические занятия по данной дисциплине проводятся традиционным способом. При работе используется диалоговая форма ведения лекций и практики с постановкой и решением проблемных задач, обсуждением дискуссионных моментов и т.д. При проведении контрольных работ студентам предлагается ответить на некоторые теоретические вопросы по курсу лекций и решить задачи, содержащие элементы научных исследований, которые могут потребовать углубленной самостоятельной проработки теоретического материала. При организации внеаудиторной самостоятельной работы по данной дисциплине преподавателю рекомендуется использовать следующие ее формы:

- решение студентом самостоятельных задач обычной сложности, направленных на закрепление знаний и умений;
- выполнение индивидуальных заданий повышенной сложности, направленных на развитие у студентов научного мышления и инициативы.

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 _____ **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
		Основная		
1.	лк, пз, срс	Косолапов, Ю. В. Криптографические протоколы на основе линейных кодов : учебное пособие / Ю. В. Косолапов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 98 с. — ISBN 978-5-9275-3316-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/100176.html	
2.	лк, пз, срс	Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/97571.html	
3.	лк, пз, срс	Алексеев, В. А. Методы и средства криптографической защиты информации : методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / В. А. Алексеев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2009. — 16 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/17710.html	
		Дополнительная		
4.	лк, пз, срс	Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 95 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/17925.html	
5.	лк, пз, срс	Отрыванкина, Т. М. Криптографические свойства булевых функций : методические указания / Т. М. Отрыванкина, А. Н. Благовисная. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2014. — 55 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/51536.html	
6.	лк, пз, срс	Морозова, Е. И. Изучение протоколов IP-телефонии с помощью пакета Telelogic TAU : методические указания по выполнению цикла лабораторных работ / Е. И. Морозова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2013. 34 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/55476.html	

7.	лк, пз, срс	Деарт, В. Ю. Мультисервисные сети связи. Протоколы и системы управления сеансами (Softswitch/IMS) / В. Ю. Деарт. — Москва : Московский технический университет связи и информатики, 2010. — 198 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/61507.html
8.	лк, пз, срс	Буранова, М. А. Конфигурация протокола динамической маршрутизации OSPF на основе оборудования Cisco : учебное пособие / М. А. Буранова, Н. В. Киреева. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. — 82 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/71848.html
9.	лк, пз, срс	Методы получения дополнительных сведений при анализе протоколов и журналов : методические указания к выполнению лабораторных работ / составители А. А. Кречетов. — Йошкар-Ола : Поволжский государственный технологический университет, 2015. — 35 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/75436.html
10.	лк, пз, срс	еменов, Ю. А. Протоколы и алгоритмы маршрутизации в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 998 с. — ISBN 978-5-4497-1652-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/120488.html
11.	лк, пз, срс	Семенов, Ю. А. Алгоритмы телекоммуникационных сетей. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 757 с. — ISBN 978-5-4497-1634-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/120470.html
12.	лк, пз, срс	Косолапов, Ю. В. Протоколы защищенных вычислений на основе линейных схем разделения секрета : учебное пособие / Ю. В. Косолапов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 112 с. — ISBN 978-5-9275-3317-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/100193.html
13.	лк, пз, срс	Берлин, А. Н. Основные протоколы интернет : учебное пособие / А. Н. Берлин. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 601 с. — ISBN 978-5-4497-0337-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/89452.html
14.	лк, пз, срс	Шерстнева, О. Г. Интерфейсы и протоколы цифровых систем коммутации : учебное пособие / О. Г. Шерстнева, А. А. Шерстнева. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2018. — 149 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/84067.html

8. Материально-техническое обеспечение дисциплины (модуля) «Криптографические протоколы и стандарты»

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