Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Защита информации в сетях VPN
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 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)

«16» 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) «Защита информации в сетях VPN» являются формирование у обучающихся знаний и практических навыков изучения существующих технологий и программно- аппаратных средств защиты компьютерных сетей. В содержание дисциплины входят пять основных направлений: обнаружения компьютерных атак, межсетевое экранирование, организация виртуальных частных сетей, технологии защищенной обработки информации и аудита информационной безопасности в компьютерных сетях.

Задачами освоения дисциплины (модуля) «Защита информации в сетях VPN» являются: овладение механизмами построения систем безопасности сетей; изучение принципов работы VPN; - усвоение основных стандартов построения и защиты беспроводных сетей.

2.Место дисциплины в структуре ОПОП

Дисциплина «Защита информации в сетях VPN» относится к обязательной части учебного плана.

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Сети и системы передачи информации, Безопасность сетей ЭВМ.

Последующими дисциплинами являются: Основы управленческой деятельности, Защита программ и данных, Организация работы администратора автоматизированных систем, Защита информации от утечки по техническим каналам, Программно-аппаратные средства защиты информации, Виртуальные частные сети.

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

В результате освоения дисциплины «Защита информации в сетях VPN» студент должен овладеть следующими компетенциями: ОПК-9; ОПК-10; ОПК-12.

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-9.	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.2.1 умеет анализировать основные характеристики и возможности телекоммуникационных систем
ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2.3 умеет проводить анализ угроз безопасности в локальных вычислительных сетях
		ОПК-10.1.3 знает основные протоколы, используемые для защиты информации в вычислительных сетях
ОПК-12.	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1.2 знает принципы построения и функционирования локальных и глобальных вычислительных сетей
		ОПК-12.1.3 знает последовательность и содержание этапов построения локальных вычислительных сетей

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	6/216		
Семестр	7		
Лекции, час	68		
Практические занятия, час	-		
Лабораторные занятия, час	68		
Самостоятельная работа, час	44		
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) «Защита информации в сетях VPN»

№ 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: Обнаружение компьютерных атак	2	-	2	1								
2	Тема №2: Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак.	2	-	2	1								
3	Тема №3 Технологии обнаружения и предотвращения вторжений	2	-	2	1								
4	Тема №4: Протоколы защищенных каналов	2	-	2	1								
5	Тема №5: Технология межсетевого экранирования	2	-	2	1								
6	Тема №6: Стратегии и средства межсетевого экранирования.	2	-	2	1								
7	Тема №7: Технологии виртуальных защищенных сетей VPN	2	-	2	1								
8	Тема №8: Защита удаленного доступа	2	-	2	1								
9	Тема №9: Системы предотвращения утечек данных (DLP)	2	-	2	1								
10	Тема №10: Управление информацией и событиями ИБ (SIEM)	2	-	2	1								
11	Тема №11: Протоколы SSL, TLS, SOCKS.	2	-	2	1								
12	Тема №12: Организация удаленного доступа. Управление идентификацией и доступом.	2	-	2	1								
13	Тема №13: Средства управления доступом. Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	2	-	2	1								
14	Тема №14: Фильтрация пакетов. Критерии и правила фильтрации.	2	-	2	1								
15	Тема №15: Шлюзы прикладного уровня.	2	-	2	1								
16	Тема №16: Организация виртуальных частных сетей.	2	-	2	1								
17	Тема №17: Задачи, решаемые VPN. Туннелирование в VPN.	2	-	2	1								
18	Тема №18 Уровни защищенных каналов. Защита данных на канальном уровне.	2	-	2	1								
19	Тема №19 Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.	2	-	2	1								

20	Тема №20 Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec.	2	-	2	1								
21	Тема №21 Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей.	2	-	2	1								
22	Тема №22 Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec.	2	-	2	1								
23	Тема №23 Организация VPN средствами СЗИ «StrongNet». Описание системы.	2	-	2	1								
24	Тема №24 Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения.	2	-	2	1								
25	Тема №25 Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003	2	-	2	2								
26	Тема №26 Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения.	2	-	2	2								
27	Тема №27 Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP.	2	-	2	2								
28	Тема №28 Защищенный обмен электронной почтой.	2	-	2	2								
29	Тема №29 Технологии защищенной обработки информации	2	-	2	2								
30	Тема №30 Применение технологии терминального доступа. Общие сведения о технологии терминального доступа.	2	-	2	2								
31	Тема №31 Обеспечение безопасности сервера ОС Windows Server 2003 Настройка сервера MSTS. Настройка протокола RDP.	2	-	2	2								
32	Тема №32 Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.	2	-	2	2								
33	Тема №33 Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.	2	-	2	2								
34	Тема №34: Аудит информационной безопасности в компьютерных сетях	2	-	2	2								

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	-	68	44								

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	Обнаружение компьютерных атак	2			№№ 1-6
2	№2	Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак.	2			№№ 1-6
3	№3	Технологии обнаружения и предотвращения вторжений	2			№№ 1-6
4	№ 4	Протоколы защищенных каналов	2			№№ 1-6
5	№5	Технология межсетевого экранирования	2			№№ 1-6
6	№6	Стратегии и средства межсетевого экранирования.	2			№№ 1-6
7	№7	Технологии виртуальных защищенных сетей VPN	2			№№ 1-6
8	№8	Защита удаленного доступа	2			№№ 1-6
9	№9	Системы предотвращения утечек данных (DLP)	2			№№ 1-6
10	№10	Управление информацией и событиями ИБ (SIEM)	2			№№ 1-6
11	№ 11	Протоколы SSL, TLS, SOCKS.	2			№№ 1-6
12	№ 12	Организация удаленного доступа. Управление идентификацией и доступом.	2			№№ 1-6

13	№ 13	Средства управления доступом. Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	2			№№ 1-6
14	№ 14	Фильтрация пакетов. Критерии и правила фильтрации.	2			№№ 1-6
15	№ 15	Шлюзы прикладного уровня.	2			№№ 1-6
16	№ 16	Организация виртуальных частных сетей.	2			№№ 1-6
17	№ 7	Задачи, решаемые VPN. Туннелирование в VPN.	2			№№ 1-6
18	№ 18	Уровни защищенных каналов. Защита данных на канальном уровне.	2			№№ 1-6
19	№ 19	Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.	2			№№ 1-6
20	№ 20	Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec.	2			№№ 1-6
21	№ 21	Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей.	2			№№ 1-6
22	№ 22	Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec.	2			№№ 1-6
23	№ 23	Организация VPN средствами СЗИ «StrongNet». Описание системы.	2			№№ 1-6
24	№ 24	Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения.	2			№№ 1-6
25	№ 25	Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003	2			№№ 1-6
26	№ 26	Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения.	2			№№ 1-6
27	№ 27	Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP.	2			№№ 1-6
28	№ 28	Защищенный обмен электронной почтой.	2			№№ 1-6
29	№ 29	Технологии защищенной обработки информации	2			№№ 1-6
30	№ 30	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа.	2			№№ 1-6
31	№ 31	Обеспечение безопасности сервера ОС Windows Server 2003	2			№№ 1-6

		Настройка сервера MSTS. Настройка протокола RDP.				
32	№ 32	Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.	2			№№ 1-6
33	№ 33	Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.	2			№№ 1-6
34	№ 34	Аудит информационной безопасности в компьютерных сетях	2			№№ 1-6
ИТОГО			68			

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.	Обнаружение компьютерных атак	1			№№ 1-6	Опрос, реферат
2.	Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак.	1			№№ 1-6	Опрос, реферат
3.	Технологии обнаружения и предотвращения вторжений	1			№№ 1-6	Опрос, реферат
4.	Протоколы защищенных каналов	1			№№ 1-6	Опрос, реферат
5.	Технология межсетевого экранирования	1			№№ 1-6	Опрос, реферат
6.	Стратегии и средства межсетевого экранирования.	1			№№ 1-6	Опрос, реферат
7.	Технологии виртуальных защищенных сетей VPN	1			№№ 1-6	Опрос, реферат
8.	Защита удаленного доступа	1			№№ 1-6	Опрос, реферат
9.	Системы предотвращения утечек данных (DLP)	1			№№ 1-6	Опрос, реферат
10.	Управление информацией и событиями ИБ (SIEM)	1			№№ 1-6	Опрос,

						реферат
11.	Протоколы SSL, TLS, SOCKS.	1			№№ 1-6	Опрос, реферат
12.	Организация удаленного доступа. Управление идентификацией и доступом.	1			№№ 1-6	Опрос, реферат
13.	Средства управления доступом. Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	1			№№ 1-6	Опрос, реферат
14.	Фильтрация пакетов. Критерии и правила фильтрации.	1			№№ 1-6	Опрос, реферат
15.	Шлюзы прикладного уровня.	1			№№ 1-6	Опрос, реферат
16.	Организация виртуальных частных сетей.	1			№№ 1-6	Опрос, реферат
17.	Задачи, решаемые VPN. Туннелирование в VPN.	1			№№ 1-6	Опрос, реферат
18.	Уровни защищенных каналов. Защита данных на канальном уровне.	1			№№ 1-6	Опрос, реферат
19.	Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.	1			№№ 1-6	Опрос, реферат
20.	Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec.	1			№№ 1-6	Опрос, реферат
21.	Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей.	1			№№ 1-6	Опрос, реферат
22.	Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec.	1			№№ 1-6	Опрос, реферат
23.	Организация VPN средствами СЗИ «StrongNet». Описание системы.	1			№№ 1-6	Опрос, реферат
24.	Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения.	1			№№ 1-6	Опрос, реферат
25.	Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003	2			№№ 1-6	Опрос, реферат
26.	Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения.	2			№№ 1-6	Опрос, реферат

27.	Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP.	2			№№ 1-6	Опрос, реферат
28.	Защищенный обмен электронной почтой.	2			№№ 1-6	Опрос, реферат
29.	Технологии защищенной обработки информации	2			№№ 1-6	Опрос, реферат
30.	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа.	2			№№ 1-6	Опрос, реферат
31.	Обеспечение безопасности сервера ОС Windows Server 2003 Настройка сервера MSTS. Настройка протокола RDP.	2			№№ 1-6	Опрос, реферат
32.	Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.	2			№№ 1-6	Опрос, реферат
33.	Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.	2			№№ 1-6	Опрос, реферат
34.	Аудит информационной безопасности в компьютерных сетях	2			№№ 1-6	Опрос, реферат
ИТОГО		**44**				

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности 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 30% 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
Защита информации в сетях VPN
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	Информационные технологии. Базовый курс : учебник для вузов / А. В. Костюк, С. А. Бобонец, А. В. Флегонтов, А. К. Черных. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 604 с. — ISBN 978-5-8114-8776-9. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/180821	
2.	лк, пз, срс	Сети ЭВМ и средства коммуникаций : учебное пособие / составители В. Г. Брежнев, Е. В. Беляева. — Ульяновск : УИ ГА, 2019. — 170 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/162527	
3.	лк, пз, срс	Видин, Д. В. Защита интеллектуальной собственности : учебное пособие / Д. В. Видин, К. П. Петренко, Д. Б. Шатько. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2020. — 160 с. — ISBN 978-5-00137-186-1. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/163562	-
Дополнительная				
4.	лк, пз, срс	Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. — Санкт-Петербург : Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/118646	-
5.	лк, пз, срс	Гвоздева, Т. В. Проектирование информационных систем. Стандартизация : учебное пособие для вузов / Т. В. Гвоздева, Б. А. Баллод. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 252 с. — ISBN 978-5-8114-7963-4. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/169810	-
6.	лк, пз, срс	Трофимова, М. В. Менеджмент в сфере информационных технологий : учебное пособие / М. В. Трофимова. — Ставрополь : СКФУ, 2015. — 195 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/155578	-

8. Материально-техническое обеспечение дисциплины (модуля) «Защита информации в сетях VPN»

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