57.0.31

Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Безопасность сетей ЭВМ»
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 «Компьютерные технологии, вычислительная техника и энергетика»,
наименование факультета, где ведется дисциплина

кафедра «Информационная безопасность».
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, курс 3,4 семестр (ы) 6,7.
очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС 3++ ВО по специальности10.05.03 «Информационная безопасность автоматизированных систем» с учетом рекомендаций и ОПОП ВО по специализации «Безопасность открытых информационных систем»,

Разработчик _____ Фейламазова С.А., б/с
подпись (ФИО уч. степень, уч. звание)

«18» 09 2021 г.

Зав. кафедрой, за которой закреплена дисциплина (модуль) «Информационная безопасность»

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

«18» 09 2021 г.

Программа одобрена на заседании выпускающей кафедры
от «20» 09 2021года, протокол № 2.

Зав. выпускающей кафедрой по данной специальности

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

«20» 09 2021г.

Программа одобрена на заседании Методического Совета факультета компьютерных технологий, вычислительной техники и энергетики
от «18» 10 2021г. года, протокол № 1.

Программа одобрена на заседании Методического Совета факультета компьютерных технологий, вычислительной техники и энергетики

_____ Т.И. Исабекова,к.ф-м.н., доцент.
подпись (ФИО уч. степень, уч. звание)

«18» 10 2021.

Декан факультета _____ Ш.А. Юсуфов., к.т.н., доцент
подпись ФИО

Начальник УО _____ Э.В. Магомаева
подпись ФИО

И.о. проректор по УР _____ Н.Л. Баламирзоев
подпись ФИО

Программа составлена в соответствии с требованиями ФГОС 3++ ВО по специальности10.05.03 «Информационная безопасность автоматизированных систем» с учетом рекомендаций и ОПОП ВО по специализации «Безопасность открытых информационных систем»,

Разработчик _____ Фейламазова С.А., б/с
подпись (ФИО уч. степень, уч. звание)

«18» 09 2021 г.

Зав. кафедрой, за которой закреплена дисциплина (модуль) «Информационная безопасность»

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

«18» 09 2021 г.

Программа одобрена на заседании выпускающей кафедры от «10» сентября 2021 года, протокол № 1.

Зав. выпускающей кафедрой по данной специальности

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

«20» 09 2021г.

Программа одобрена на заседании Методического Совета факультета компьютерных технологий, вычислительной техники и энергетики
от «18» 10 2021г. года, протокол № 1.

Председатель Методической комиссии факультета компьютерных технологий, вычислительной техники и энергетики

_____ Т.И. Исабекова,к.ф-м.н., доцент.
подпись (ФИО уч. степень, уч. звание)

«28» 10 2021.

Декан факультета _____ Ш.А. Юсуфов., к.т.н., доцент
подпись ФИО

Начальник УО _____ Э.В. Магомаева
подпись ФИО

И.о. проректор по УР _____ Н.Л. Баламирзоев
подпись ФИО

1. Цели и задачи освоения дисциплины

Целью освоения дисциплины «Безопасность сетей ЭВМ» является изучение принципов и методов защиты информации в сетях, изучение принципов и алгоритмов обеспечения и построения безопасных сетей ЭВМ.

Задачи дисциплины:

- Изучение основных угроз в сетях ЭВМ и методов противодействия им;
- Овладения механизмами построения систем безопасности сетей ЭВМ;
- Изучение мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- Изучить защищенные протоколы и межсетевые экраны;

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «Безопасность сетей ЭВМ» входит в обязательную часть.

Программа базируется на дисциплинах: «Сети и системы передачи информации», «Теория кодирования», «Теоретические основы компьютерной безопасности».

Входными знаниями для освоения данной дисциплины являются знания основы сетей передачи данных, полученные при освоении дисциплины «Сети и системы передачи информации».

3. Компетенции формируемые в результате освоения дисциплины (модуля)

В результате освоения дисциплины «Безопасность сетей ЭВМ» *студент должен овладеть следующими компетенциями: (перечень компетенций и индикаторов их достижения относящихся к дисциплинам, указан в соответствующей ОПОП).*

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-10.	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2.Умеет проводить анализ угроз безопасности в локальных вычислительных сетях ОПК-10.2.1.3нает основную эксплуатационную и проектную документацию на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса ОПК-10.3.1.3знает основные системы и способы тестирования на проникновение
ОПК-12.	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.	ОПК-12.1.2знает принципы построения и функционирования локальных и глобальных вычислительных сетей
ОПК-15.	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1.3знает программные средства, позволяющие вести автоматизированный аудит

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	8 ЗЕТ/288ч.		
Лекции, час	17/68	-	-
Практические занятия, час	-		
Лабораторные занятия, час	34/34	-	-
Самостоятельная работа, час	57/42	-	-
Курсовой проект (работа), РГР, семестр	-		-
Зачет (при заочной форме **4 часа** отводится на контроль)	зачет	-	-
Часы на экзамен (при очной, очно-заочной формах **1 ЗЕТ – 36 часов**, при заочной форме **9 часов**)	36 часов	-	-

4.1 Содержание дисциплины (модуля)

№ 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. Тема 1: Введение в сетевую безопасность** 1. Основные понятия и определения 2. Нейтрализация угроз. Области сетевой безопасности 3. Общие рекомендации по сетевой безопасности. 4. Типы атак.	2		4	9								
2	**Лекция №2 Тема 2: Аудит информационной безопасности** 1. Основные виды аудита безопасности 2. Экспертный аудит 3. Инструментальный анализ защищенности. **4.** Основные этапы работ при проведении аудита.	2		4	9								
3	**Лекция №3 Тема 3: Протоколы сетевой аутентификации. Модели разграничения доступа. Вредоносное программное обеспечение.** 1. Локальная аутентификация Windows 2. Протоколы сетевой аутентификации.	2		4	9								
4	**Лекция №4 Тема 4: Системы предотвращения утечек информации. Системы анализа трафика. Файрвол веб-приложений** 1. DLP-системы. 2. DMZ –системы 3. DPI- системы. 4. WAF-системы.	3		6	10								
5	**Лекция №5,6 Тема 5: Системы обнаружения и предотвращения вторжений (ISD/IPS)** 1. Что такое системы обнаружения вторжений (IDS). 2. Сетевые ISD (NIDS) 3. Проблемы NIDS 4. Системы предотвращения вторжений (IPS).	4		4	10								

6	**Лекция №7,8 Тема 6: Угрозы безопасности на канальном уровне 2** 1. Атака на таблицу MAC. 2. Атаки на сети VLAN. 3. Атаки, связанные с DHCP. 4. ARP атаки. **5.** Атаки с подменой адреса.	4		8	10								
	Итого за 6 семестр	**17**		**34**	**57**								
7	**Лекция № 8,10 Тема 7: Настройка параметров безопасности коммутатора cisco.** 1. Защита не используемых портов. 2. Нейтрализация атак таблицы MAC-адресов. 3. Ограничение и изучение MAC-адресов. **4.** Режимы нарушения безопасности порта.	4		2	2								
8	**Лекция №11,12. Тема 8: Обеспечение безопасности сетевых устройств** 1. Защита доступа к устройствам. 2. Назначение административных ролей. 3. Простой протокол сетевого управления SNMP.	4		2	2								
9	**Лекции №13,14. Тема 9:Межсетевые экраны** 1. Определение типов межсетевых экранов. 2. Разработка конфигурации межсетевого экрана. 3. Построение набора правил межсетевого экрана. **4.** Выявление различий между межсетевыми экранами различных типов.	4		2	2								
10	**Лекция №15 Тема 10: Дополнительные возможности Wireshark для графического представления получаемых результатов.** 1. Конечные точки и сетевые диалоги. 2. Выявление наиболее активных сетевых узлов с помощью конечных точек и диалогов	2		4	2								

11	**Лекция №16,17 Тема11: Методы сбора информации.** 1. Общедоступные сайты, которые можно использовать для сбора информации о целевом домене. Использование общих ресурсов. 2. Информация о регистрации домена. 3. Анализ DNS. 4. Информация о маршруте. 5. Использование поисковой системы.	4		2	2								
12	**Лекция №18,19 Тема 12: Уязвимости по приложениям** 1. SSTI. 2. XXE-атака. 3. XSS-атаки. 4. Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet .xssFilter.	4		2	2								
13	**Лекция №20 Тема 13: Атака на сервер компьютерной сети** 1. SSRF атака	2		2	2								
14	**Лекция №21 Тема 14: Способы обхода авторизации** 1. BruteForce. 2. SQL инъекции. 3. Cookie.	2		2	2								
15	**Лекция №22,23 Тема 15: Sql инъекции** 1. Принцип атаки внедрения SQL. 2. Типы SQLi. 3. Защита от SQLi. 4. Классические атаки. 5. Комментирование, Манипуляции со строками, Обход аутентификации. 6. Union injection.	4		2	2								

16	**Лекция №24,25 Тема 16: Sql инъекции** 1. Последовательные запросы 2. Error-Based 3. Слепые инъекции 4. Условные выражения 5. Boolean-based 6. Time Based SQL-injection 7. Stacked Query Based SQL-injections 8. JSQ injection.	4		2	2								
17	**Лекция №26,27 Тема 17: Защита от SQL-инъекций** 1. Функция mysql(i)_real_escape_string 2. Приведение к числу 3. Использование анализатора sqlmap.	4		2	2								
18	**Лекция №28 Тема 18: Алгоритмы взлома корпоративной сети** 1. захват учетных записей 2. атака протокола отладки Java Debug Wire Protocol 3. веб-уязвимости 4. Социальная инженерия. 5. Log4j	2			2								
19	**Лекция №29,30 Тема 19: Анализ защищённости веб-приложений** 1. Методология тестирования на проникновение: Метод черного ящика (black box), Метод белого ящика (white box), Метод серого ящика (gray box) 2. Анализ защищённости веб-приложений путём внешних проверок (автоматизированных и ручных). 3. Этапы теста на проникновение: 4. Тестирование на проникновение с помощью Burp 5. Nikto – сканер веб-серверов 6. NSLOOKUP – утилита для поиска DNS-серверов	4		2	2								

20	**Лекция № 31,32 Тема 20: Инструменты Kali Linux.** 1. Разведка сайтов. Поиск каталогов и файлов. Dirb, Dirhunt, DirBuster. 2. dirsearch —инструмент командной строки, предназначенный для брут-форса (поиска путём полного перебора) директорий и файлов в веб-сайтах. 3. DVCS-Ripper 4. SQLmap 5. WPScan — это сканер уязвимостей WordPress.	4		2	2								
21	**Лекция №33,34. Тема 21: Методы сканирования и уклонения в Kali Linux** 1. Описание метода обнаружения цели. 2. Как с помощью инструментов Kali Linux распознать целевую машину. 3. Шаги, которые необходимо выполнить для поиска операционных систем целевых машин (получение отпечатков операционной системы). 4. Автоматическое сканирование с помощью Striker. 5. Сокрытие с помощью Nipe. 6. Сканирование nmap. 7. Sql map 8. NetCat	4		2	2								
22	**Лекция №35 Тема 22: Инструментальные средства командной строки для анализа пакетов**	2		2	2								
23	**Лекция №36 Тема 23: Процесс выявления и анализа критических недостатков безопасности в Kali Linux**	2			2								
24	**Лекция №37,38 Тема 24: Python для тестирования на проникновение** 1. Понимание сокетов и создание TCP-сервера 2. Создание TCP-клиента 3. Разработка сканера Nmap	4		4	2								
25	**Лекция №39,40 Тема 25: Исследование сетей с Python** 1. Сканер сети библиотеки scapy 2. Использование веб-библиотек. Взаимодействие с веб-сервисами -библиотека urllib2. 3. Форензика с Python 4. Библиотека requests 5. Пакеты lxml и BeautifulSoup.	4		2	3								

26	**Лекция №41,42 Тема 26: Безопасность беспроводных сетей.** 1. WEP-атаки на конфиденциальность проводных сетей 2. Протоколы WPA и AES 3. Заблуждения о безопасности беспроводной сети 4. Беспроводные атаки и защита от них 5. Проектирование безопасной сети с помощью беспроводной связи. 6. Создание широковещательного трафика базе ESP8266 для подавления активности беспроводной сети.	4			3								
	Итого за 7 семестр	**68**		**34**	**42**								
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт. работа 1 аттестация 1-5 темы 2 аттестация 6-10 темы 3 аттестация 11-15 темы											
Форма промежуточной аттестации (по семестрам)		Экзамен (5сем.) Экзамен (6сем.)											
Итого		**85**	**0**	**68**	**99**								

1.2 Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного 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	Нейтрализация угроз.	4			1-7
2.	2	Аудит информационной безопасности.	4			1-7
3.	3	Локальная аутентификация Windows.	4			1-7
4.	4	DLP-системы. DMZ –системы. DPI- системы. WAF-системы	6			1-7
5.	5	Системы обнаружения и предотвращения вторжений	4			1-7
6.	6	Угрозы безопасности на уровне 2	8			1-7
7.	7	Настройка параметров безопасности коммутатора cisco.	2			1-7
8.	8	Простой протокол сетевого управления SNMP.	2			1-7
9.	9	Межсетевые экраны.	2			1-7
10.	10	Анализатор протоколов Wireshark	4			1-7
11.	11	Утилита NSLOOKUP	2			1-7

12.	12	Уязвимости по приложениям.	2			1-7
13.	13	Уязвимости по приложениям.	2			1-7
14.	14,	Способы обхода авторизации	2			1-7
15.	15,16	Sql инъекции	4			1-7
16.	17	Защита от SQL-инъекций	2			1-7
17.	18	Анализ защищённости веб-приложений	2			1-7
18.	19,20	Инструменты Kali Linux	4			1-7
19.	21,22	Инструментальные средства командной строки для анализа пакетов.	2			1-7
20.	23, 24	Python для тестирования на проникновение	6			1-7
Итого			**68**			

1.3 Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения
1	2
1.	Нейтрализация угроз. Области сетевой безопасности.
2.	Экспертный аудит
3.	Протоколы сетевой аутентификации
4.	WAF-системы
5.	Сетевые ISD (NIDS)
6.	Режимы нарушения безопасности порта.
7.	Защита доступа к устройствам.
8.	Выявление различий между межсетевыми экранами различных типов.
9.	Конечные точки и сетевые диалоги.
10.	Информация о регистрации домена.
11.	Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet .xssFilter.
12.	Атака на сервер компьютерной сети
13.	Комментирование, Манипуляции со строками, Обход аутентификации.
14.	Слепые инъекции.
15.	Защита от SQL-инъекций
16.	Захват учетных записей.
17.	Этапы теста на проникновение.
18.	Разведка сайтов.
19.	Описание метода обнаружения цели.
20.	Инструментальные средства командной строки для анализа пакетов.
21.	Создание TCP-клиента.
22.	Python для тестирования на проникновение.

Количество часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
Очно	Очно-заочно	Заочно		
3	4	5	6	7
9			1-7	Контрольная работа
9			1-7	Контрольная работа,
9			1-7	Контрольная работа
10			1-7	Контрольная работа,
10			1-7	Контрольная работа
10			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
4			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
4			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа
2			1-7	Контрольная работа

23.	Исследование сетей с Python.	3			1-7	Контрольная работа
24.	WEP-атаки на конфиденциальность проводных сетей.	3			1-7	Контрольная работа
Итого		**99**				

5. Образовательные технологии

Используется технология учебного исследования:

При выполнении лабораторных работ используется программа Packet Tracer - симулятор сети передачи данных, выпускаемый фирмой Cisco Systems, а также оборудование фирмы CISCO: коммутаторы 260, маршрутизаторы 2800.

При чтении лекций используются активные формы, то есть привлекаются студенты в качестве экспертов для ответов на вопросы при рассмотрении принципов работы устройств сети. Это позволяет более детально понять излагаемый материал.

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

Оценочные средства по дисциплине приведены в приложении к рабочей программе в приложении А «Фонд оценочных средств»

Зав. библиотекой _____ *Алиева Ж.А.*

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

№п/п	Виды занятий	Комплект необходимойучебной литературы подисциплине	Автор(ы)	Издательство игод издания	Количество экземпляров	
					В библио-теке	На каф ед - ре
1	2	3	4	5	6	7
ОСНОВНАЯ						
1	КР,СР	Сети ЭВМ и телекоммуникации. Архитектура и организация: учебное пособие / С. С. Гельбух. — Санкт-Петербург: Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текс: электронный // Лань: электронно-библиотечная система.	Гельбух, С. С.	Лань, 2019.	URL: https://e.lanbook.com/book/118646	
2	КР,СР	Безопасность сетей ЭВМ: учебное пособие / Ю. И. Синицын, Е. И. Ряполова. — Оренбург: ОГУ, 2017. — 189 с. — ISBN 978-5-7410-1886-6. — Текст : электронный // Лан : электронно-библиотечная система. —		Оренбург: ОГУ, 2017	URL: https://e.lanbook.com/book/110613	
3	ЛК, СР, ЛБ	Основы построения компьютерных сетей: учебное пособие / М. В. Левин, И. А. Ушаков, А. Ю. Цветков, П. А. Исаченков. — Санкт-Петербур: СПбГУТ им. М.А. Бонч-Бруевича, 2016. — 55 с. — Текст: электронный // Лань: электронно-библиотечная система.	М. В. Левин, И. А. Ушаков, А. Ю. Цветков, П. А. Исаченков.	Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016.	URL: https://e.lanbook.com/book/180098	
4	ЛК, СР, ЛБ	Компьютерные сети. Анализ и диагностика: учебное пособие / С. П. Борисов. — Москва: РТУ МИРЭА, 2021 — Часть 1 — 2021. — 67 с. — Текст:электронный //Лань: электронно-библиотечная система.	Борисов, С. П.	Москва : РТУ МИРЭА, 2021	URL: https://e.lanbook.com/book/176562	
5	ЛК, СР	Безопасность сетей ЭВМ: методические указания / А. Г. Лютов, Н. Н. Чернышев. — Москва: РТУ МИРЭА, 2021. — 83 с. — Текст: электронный //Лань: электронно-библиотечная система.	Лютов, А. Г.	Москва : РТУ МИРЭА, 2021.	URL: https://e.lanbook.com/book/182523	
6	ЛК, СР	Основы локальных компьютерных сетей: учебное пособие для вузов / А. Н. Сергеев. — 3-е изд., стер. — Санкт-Петербург: Лань, 2021. — 184 с. — ISBN 978-5-8114-6855-3. — Текст: электронный // Лань:	Сергеев, А. Н.	Санкт-Петербург : Лань, 2021.	URL: https://e.lanbook.com/book/152651	-

		электронно-библиотечная система.				
ДОПОЛНИТЕЛЬНАЯ						
7	ЛК, СР	Ракитин, Р. Ю. Компьютерные сети: учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул: АлтГПУ, 2019. — 340 с. — ISBN 978-5-.88210-942-3. — Текст: электронный // Лань: электронно-библиотечная система.	Ракитин, Р. Ю.	Барнаул: АлтГПУ, 2019.	URL: https://e.lanbook.com/book/139182	-
8	ЛК, СР	Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст: электронный // Лань: электронно-библиотечная систем.	Краковский, Ю. М.		URL: https://e.lanbook.com/book/156401	

8. Материально-техническое обеспечение дисциплины (модуля)

Для проведения лабораторных работ используются персональные компьютеры, на которых установлена виртуальная машина с ОС Kali Linux.

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

9. Лист изменений и дополнений к рабочей программе

Дополнения и изменения в рабочей программе на 2021/2022 учебный год.

В рабочую программу вносятся следующие изменения:

1. нет изменений;
2. ……;
3. ……;
4. ……;
5. ……

или делается отметка о нецелесообразности внесения каких-либо изменений или дополнений на данный учебный год.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ от 20.09.21 года, протокол № 2.

Заведующий кафедрой ИБ _____ Г.И. Качаева, к.э.н.

(название кафедры) (подпись, дата) (ФИО, уч. степень, уч. звание)

Согласовано:

Декан (директор) _____ Юсуфов Ш.А, к.т.н, доцент

(подпись, дата) (ФИО, уч. степень, уч. звание)

Председатель МС факультета _____ Т.И. Исабекова, д.ф-м.н., доцент

(подпись, дата) (ФИО, уч. степень, уч. звание)