Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Основы информационной безопасности
наименование дисциплины по ОПОП

для специальности 38.05.01 – Экономическая безопасность
код и полное наименование направления (специальности)

факультет информационных систем в экономике и управлении
наименование факультета, где ведется дисциплина

кафедра экономической безопасности и таможенного дела
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, заочная курс 1,2,3 семестр(ы) 2,3,4,5
очная, очно-заочная, заочная

г. Махачкала 2023

Программа составлена в соответствии с требованиями ФГОС ВО по направлению **38.05.01- Экономическая безопасность** с учетом рекомендаций и ОПОП ВО по специализации **«Экономико-правовое обеспечение экономической безопасности»**.

Разработчик _____ Раджабова З.Р., к.э.н., доцент
подпись (ФИО уч. степень, уч. звание)

«09» 09 2023г.

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

«19» 09 2023г.

Программа одобрена на заседании выпускающей кафедры финансов, аудита и бухгалтерского учета от _____2023 года, протокол № _____.

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

подпись _____ Шахбанова И.К. к.э.н., доцент
(ФИО уч. степень, уч. звание)

«18» 09 2023 г.

Программа одобрена на заседании Методического совета комиссии направления факультета информационных систем в экономике и управлении
от 18.09 2023 года, протокол № 1

Председатель Методического совета факультета ИСвЭиУ

_____ Бабаева Д.Р., к.э.н., доцент
подпись (ФИО уч. степень, уч. звание)

«18» 09 2023 г.

Декан факультета _____ Раджабова З.Р.
подпись ФИО

Начальник УО _____ Магомаева Э.В.
подпись ФИО

И.о. ректора _____ Баламирзоев Н.Л.
подпись ФИО

1. Цели и задачи освоения дисциплины

Целью дисциплины «Основы информационной безопасности» является формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Приобретенные знания позволят студентам правильно ориентироваться в категориях защищаемых информационных ценностей и приобрести минимально необходимый кругозор в проблемах информационной безопасности. На основе данной дисциплины предполагается более подробно изучать различные направления защиты компьютерной безопасности.

Задачами изучения дисциплины являются:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации, использовании современной научно-технической литературой для решения задач по вопросам защиты информации;
- приобретение навыков анализа информационной инфраструктуры государства с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» относится к обязательной части направления 38.05.01- Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности». Для освоения дисциплины обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения таких предметов как: информатика, математика.

Освоение дисциплины «Основы информационной безопасности» является необходимой основой для последующего изучения дисциплин учебного плана: Безопасность операционных систем.

Результаты освоения дисциплины также могут быть использованы при выполнении выпускной квалификационной работы и в профессиональной деятельности.

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

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-2	Способен осуществлять сбор, анализ и использование данных хозяйственного, налогового и бюджетного учетов, учетной документации бухгалтерской (финансовой), налоговой и статистической отчетности в целях оценки эффективности и прогнозирования финансово-хозяйственной деятельности хозяйствующего субъекта, а также выявления, предупреждения, локализации и нейтрализации внутренних и внешних угроз и рисков.	ОПК-2.1. Знает сущность, цель и задачи бухгалтерского учета; принципы ведения бухгалтерского учета и формирования отчетности; инструменты и методы экономического анализа и прогнозирования деятельности хозяйствующего субъекта, выявления угроз и оценки рисков ОПК-2.2. Умеет правильно идентифицировать, классифицировать и систематизировать факты хозяйственной деятельности организации в соответствии с их экономико-правовым содержанием; регистрировать, обрабатывать и обобщать данные бухгалтерского, налогового, бюджетного учетов. ОПК-2.3. Анализирует эффективность деятельности и ресурсов организации; обосновывает оперативные и стратегические решения в условиях риска и неопределенности ОПК-2.4. Владеет приемами и методами оценки активов и обязательств в коммерческой организации; способами организации бухгалтерского налогового, бюджетного учетов на предприятии; навыками формирования бухгалтерской отчетности; навыками применения методов экономического анализа и прогнозирования
ПК-6	Способен определять и контролировать цели, основные мероприятия и ключевые индикаторы на основе	ПК-6.1. Знает основные положения теории рисков. теории корпоративных финансов: принципы и индикаторы

	отчетности по вопросам обеспечения системы управления рисками, экономической безопасности и устойчивого развития социально-экономических систем и процессов организации.	устойчивого развития организации и социальной ответственности; структуру программы управления рисками, последовательность применения контрольных процедур управления рисками. ПК-6.2. Выявляет причины отклонений, владеет навыками устранения нарушений и недостатков системы управления рисками. ПК-6.3. Умеет анализировать и объединять потенциальные возможности управления рисками с точки зрения социального, экономического, нормативно-законодательного, экологического и технологического контекста для создания долгосрочной стоимости. ПК-6.4. Владеет навыками контроля и мониторинга исполнения стратегии развития, направленной на долгосрочное устойчивое развитие с учетом принципов социальной ответственности.

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	2/72 5/180	2/72 5/180
Семестр	2,3	4,5
Лекции, час	17,17	4.4
Практические занятия, час	34	9
Лабораторные занятия, час	34,34	9,9
Самостоятельная работа, час	21,59	55,149
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)	Зачет (2 семестр) Экзамен(3 семестр)	Зачет (4 семестр) Экзамен(5 семестр)

4.1. Содержание дисциплины (модуля)

№ пп	Раздел дисциплины, тема лекции и вопросы	Очная форма				Заочная форма			
		ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР
		2 семестр				4 семестр			
1.	**Лекция № 1** **Тема: «Понятие составляющие и система формирования режима информационной безопасности»** 1. Определение понятия "информационная безопасность" 2. Доступность ,целостность и конфиденциальность информации	2	-	4	3	1	-	2	6
2.	**Лекция №2** **Тема: «Понятие составляющие и система формирования режима информационной безопасности»** 1. Задачи информационной безопасности общества. 2. Уровни формирования режима информационной безопасности	2	-	4	3	-	-	-	6
3.	**Лекции №3** **Тема: «Нормативно-правовые основы информационной безопасности в РФ».** 1. Правовые основы информационной безопасности общества. 2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. 3. Ответственность за нарушения в сфере информационной безопасности.	2	-	4	3	1	-	2	7

4.	**Лекция №4** **Тема: «Стандарты информационной безопасности».** 1. Стандарты информационной безопасности: "Общие критерии". 2. Стандарты информационной безопасности распределенных систем	2	-	4	2	1	-	2	6
5.	**Лекция №5** **«Стандарты информационной безопасности».** 1 Стандарты информационной безопасности в РФ.	2	-	4	2	-	-	1	6
6.	**Лекция №6** **Тема: «Административный уровень обеспечения информационной безопасности»** 1. Цели, задачи и содержание административного уровня. 2. Разработка политики информационной безопасности.	2	-	4	2	-	-	-	6
7.	**Лекции №7** **Тема: «Классификация угроз "информационной безопасности"»** 1. Классы угроз информационной безопасности. 2.Каналы несанкционированного доступа к информации	2	-	4	2	1	-	2	6
8.	**Лекция №8** **Тема: «Вирусы как угроза информационной безопасности».** 1. Компьютерные вирусы и информационная безопасность. 2. Характерные черты компьютерных вирусов.	2	-	4	2	-	-	-	6
9.	**Лекция №9** **Тема: «Классификация компьютерных вирусов»** 1. Классификация компьютерных вирусов по среде обитания. 2. Классификация компьютерных вирусов по	1	-	2	2	-	-	-	6

	особенностям алгоритма работы. 3. Классификация компьютерных вирусов по деструктивные возможностям								
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 1-3 тема 2 аттестация 4-6 тема 3 аттестация 7-9 тема							
Форма промежуточной аттестации (по семестрам)		Зачет				Зачет			
ИТОГО		**17**	**-**	**34**	**21**	**4**	**-**	**9**	**55**
		3 семестр				**5 семестр**			
10.	**Лекция № 10** **Тема: «Характеристика "вирусоподобных" программ. Антивирусные программы»** 1. Виды "вирусоподобных" программ. 2. Характеристика "вирусоподобных" программ Государственное экономическое регулирование. Объекты и цели ГРЭ 3. Утилиты скрытого администрирования	2	4	4	8	1	2	2	20
11.	**Лекция № 11** **Тема: «Характеристика "вирусоподобных" программ. Антивирусные программы»** 1."Intended"-вирусы. 2. Особенности работы антивирусных программ. Классификация антивирусных программ 3. Факторы, определяющие качество антивирусных программ	2	4	4	8	-	-	-	18
12.	**Лекция № 12** **Тема: «Профилактика компьютерных вирусов. Обнаружение неизвестного вируса».** 1. Характеристика путей проникновения вирусов в компьютеры. 2. Правила защиты от компьютерных вирусов	2	4	4	7	1	2	2	20

	3. Обнаружение загрузочного и резидентного вируса, макровируса 4. Общий алгоритм обнаружения вируса								
13.	**Лекция № 13** **Тема: «Информационная безопасность вычислительных сетей».** 1. Особенности обеспечения информационной безопасности в компьютерных сетях 2. Сетевые модели передачи данных. 3. Модель взаимодействия открытых систем OSI/ISO. 4. Адресация в глобальных сетях.	4	8	8	12	1	2	2	19
14.	**Лекция № 14** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Классификация удаленных угроз в вычислительных сетях 2. Типовые удаленные атаки и их характеристика	2	4	4	6	-	-	-	18
15.	**Лекция № 15** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Причины успешной реализации удаленных угроз в вычислительных сетях 2. Принципы защиты распределенных вычислительных сетей	2	4	4	6	-	-	-	18
16.	**Лекция № 16** **Тема: «Механизмы обеспечения "информационной безопасности"»** 1. Идентификация и аутентификация 2. Криптография и шифрование 3. Методы разграничение доступа	2	4	4	6	1	2	2	18
17.	**Лекция № 17** **Тема: «Механизмы обеспечения "информационной**	1	2	2	6	-	1	1	18

	безопасности"» 1. Регистрация и аудит 2. Межсетевое экранирование 3. Технология виртуальных частных сетей (VPN)								
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 10-12 тема 2 аттестация 13-15 тема 3 аттестация 16-17 тема							
Форма промежуточной аттестации (по семестрам)		Экзамен				Экзамен			
ИТОГО		**17**	**34**	**34**	**59**	**4**	**9**	**9**	**149**

4.2. Содержание лабораторных (практических) занятий (5 семестр)

4.2. Содержание практических занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	Количество часов		Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Заочно	
1	2	3	4	5	6
			3 семестр	5 семестр	
1.	10	Характеристика "вирусоподобных" программ. Антивирусные программы	4	2	
2.	11	Характеристика "вирусоподобных" программ. Антивирусные программы	4	-	
3.	12	Профилактика компьютерных вирусов. Обнаружение неизвестного вируса	4	2	
4.	13	Информационная безопасность вычислительных сетей	8	2	
5.	14	Удаленные угрозы в вычислительных сетях	4	-	
6.	15	Удаленные угрозы в вычислительных сетях	4	-	
7.	16	Механизмы обеспечения "информационной безопасности"	4	2	
8.	17	Механизмы обеспечения "информационной безопасности"	2	1	
ИТОГО			34	9	

4.3. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	Количество часов		Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Заочно	
1	2	3	4	5	6
			2 семестр	**4 семестр**	
1.	1	Понятие составляющие и система формирования режима информационной безопасности	4	2	
2.	2	Понятие составляющие и система формирования режима информационной безопасности	4	-	
3.	3	Нормативно-правовые основы информационной безопасности в РФ	4	2	
4.	4	Стандарты информационной безопасности	4	2	
5.	5	Стандарты информационной безопасности	4	1	
6.	6	Административный уровень обеспечения информационной безопасности	4	-	
7.	7	Классификация угроз "информационной безопасности"	4	2	
8.	8	Вирусы как угроза информационной безопасности	4	-	
9.	9	Классификация компьютерных вирусов	2	-	
ИТОГО			**34**	**9**	
			3 семестр	**5 семестр**	
10.	10	Характеристика "вирусоподобных" программ. Антивирусные программы	4	2	
11.	11	Характеристика "вирусоподобных" программ. Антивирусные программы	4	-	
12.	12	Профилактика компьютерных вирусов. Обнаружение неизвестного вируса	4	2	
13.	13	Информационная безопасность вычислительных сетей	8	2	

14.	14	Удаленные угрозы в вычислительных сетях	4	-	
15.	15	Удаленные угрозы в вычислительных сетях	4	-	
16.	16	Механизмы обеспечения "информационной безопасности"	4	2	
17.	17	Механизмы обеспечения "информационной безопасности"	2	1	
ИТОГО			**34**	**9**	

4.4. 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	Заочно		
1	2	3	4	5	6
		2 семестр	**4семестр**		
1.	Понятие составляющие и система формирования режима информационной безопасности	3	6		Реферат
2.	Понятие составляющие и система формирования режима информационной безопасности	3	6		Доклад
3.	Нормативно-правовые основы информационной безопасности в РФ	3	7		Доклад
4.	Стандарты информационной безопасности	2	6		Доклад
5.	Стандарты информационной безопасности	2	6		Реферат
6.	Административный уровень обеспечения информационной безопасности	2	6		Реферат
7.	Классификация угроз "информационной безопасности"	2	6		Доклад
8.	Вирусы как угроза информационной безопасности	2	6		Реферат
9.	Классификация компьютерных вирусов	2	6		Доклад
ИТОГО		**21**	**55**		Реферат
		3 семестр	**5семестр**		
10.	Характеристика "вирусоподобных" программ. Антивирусные программы	8	20		Реферат
11.	Характеристика "вирусоподобных" программ. Антивирусные программы	8	18		Доклад
12.	Профилактика компьютерных вирусов. Обнаружение неизвестного вируса	7	20		Реферат
13.	Информационная безопасность вычислительных сетей	12	19		Доклад

14.	Удаленные угрозы в вычислительных сетях	6	18		Реферат
15.	Удаленные угрозы в вычислительных сетях	6	18		Доклад
16.	Механизмы обеспечения "информационной безопасности"	6	18		Реферат
17.	Механизмы обеспечения "информационной безопасности"	6	18		Доклад
ИТОГО		**59**	**149**		Реферат

5. Образовательные технологии

В рамках курса «Основы информационной безопасности» уделяется особое внимание установлению межпредметных связей, демонстрации возможности применения полученных знаний в практической деятельности.

В лекционных занятиях используются следующие инновационные методы:

- **групповая форма обучения** - форма обучения, позволяющая обучающимся эффективно взаимодействовать в микрогруппах при формировании и закреплении знаний;
- **компетентностный подход к оценке знаний** - это подход, акцентирующий внимание на результатах образования, причем в качестве результата рассматривается не сумма усвоенной информации, а способность человека действовать в различных проблемных ситуациях;
- **личностно-ориентированное обучение-** это такое обучение, где во где во главу угла ставится личность обучаемого, ее самобытность, самоценность, субъективный опыт каждого сначала раскрывается, а затем согласовывается с содержанием образования;
- **междисциплинарный подход-** подход к обучению, позволяющий научить студентов самостоятельно «добывать» знания из разных областей, группировать их и концентрировать в контексте конкретной решаемой задачи;
- **развивающее обучение-** ориентация учебного процесса на потенциальные возможности человека и их реализацию. В концепции развивающего обучения учащийся рассматривается не как объект обучающих воздействий учителя, а как самоизменяющийся субъект учения.

В процессе выполнения практических занятий используются следующие методы:

- **исследовательский метод обучения** – метод обучения, обеспечивающий возможность организации поисковой деятельности обучаемых по решению новых для них проблем, процессе которой осуществляется овладение обучаемыми методами научными познания и развитие творческой деятельности;
- **метод рейтинга** - определение оценки деятельности личности или события. В последние годы начинает использоваться как метод контроля и оценки в учебно-воспитательном процессе;
- **проблемно-ориентированный подход-** подход, к обучению позволяющий сфокусировать внимание студентов на анализе и разрешении, какой-либо конкретной проблемной ситуации, что становится отправной точкой в процессе обучения.

Удельный вес занятий, проводимых в интерактивной форме, составляет не менее 20% аудиторных занятий (10 ч.).

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

Фонд оценочных средств является обязательным разделом РПД (разрабатывается как приложение А к рабочей программе дисциплины).

Зав. Библиотекой_____ **(Сулейманова О.Ш.)**

(подпись)

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

№ п/п	Виды занятия	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Автор (ы)	Издательство, год издания	Количество изданий	
					в библиотеке	на кафедре
1	2	3	4	5	6	7
ОСНОВНАЯ						
1.	ЛЗ, ПЗ, ЛБ, СРС	Основы информационной безопасности: учебное пособие https://e.lanbook.com/book/118233	Гультяева Т. А.	Новосибирск: НГТУ, 2018.	Электронный ресурс	
2.	ЛЗ, ПЗ, ЛБ, СРС	Основы информационной безопасности: учебник для вузов https://e.lanbook.com/book/165837	Нестеров С. А	Санкт-Петербург: 2021.	Электронный ресурс	
3.	ЛЗ, ПЗ, ЛБ, СРС	Теоретические основы защиты информации: учебное пособие https://e.lanbook.com/book/155247	Петренко В. И.	Ставрополь: СКФУ, 2015.	Электронный ресурс	
ДОПОЛНИТЕЛЬНАЯ						
4.	ЛЗ, ПЗ, ЛБ, СРС	Основы информационной безопасности: учебное пособие https://e.lanbook.com/book/129192	Мызникова Т. А.	Омск: ОмГУПС, 2017	Электронный ресурс	
5.	ЛЗ, ПЗ, ЛБ, СРС	Комплексное обеспечение информационной безопасности на предприятии: учебник https://e.lanbook.com/book/125739	Тумбинская М. В.	Санкт-Петербург: Лань, 2019	Электронный ресурс	
6.	ЛЗ, ПЗ, ЛБ, СРС	Анализ рынка информационных систем и технологий: учебное пособие https://e.lanbook.com/book/182310	Н.Н. Секлетова, А.С. Тучкова, О. И. Захарова	Самара: ПГУТИ, 2018.	Электронный ресурс	
7.	ЛЗ, ПЗ, ЛБ, СРС	Разработка защищенных программных средств информатизации производственных процессов предприятия: учебное пособие https://e.lanbook.com/book/193486	Бабушкин В. М.	Казань: КНИТУ-КАИ, 2020	Электронный ресурс	
8.	ЛЗ, ПЗ, ЛБ, СРС	Основы безопасности прикладных информационных технологий и систем: учебное пособие https://e.lanbook.com/book/167606	А. А. Криулин, В. С. Нефедов, С. И. Смирнов	Москва: РТУ МИРЭА, 2020	Электронный ресурс	

8. Материально-техническое обеспечение дисциплины (модуля)

На факультете Компьютерных технологий, вычислительной техники и энергетики ФГБОУ ВО «Дагестанский государственный технический университет» имеются аудитории, оборудованные интерактивными, мультимедийными досками, проекторами, что позволяет читать лекции в формате презентаций, разработанных с помощью пакета прикладных программ MSPowerPoint, использовать наглядные, иллюстрированные материалы, обширную информацию в табличной и графической формах, а также электронные ресурсы сети Интернет.

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 20___/20___ учебный год.

В рабочую программу вносятся следующие изменения:

1. ……..;
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 _____ от _____ года, протокол № _____.

Заведующий кафедрой _____ _____ _____

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

Согласовано:

Декан (директор)_____ _____

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

Председатель МС факультета _____ _____

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