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 направления 10.03.01 Информационная безопасность

код и полное наименование направления (специальности)

по профилю Безопасность автоматизированных систем

факультет Компьютерных технологий, вычислительной техники и энергетики

наименование факультета, где ведется дисциплина

кафедра информационной безопасности

Форма обучения очная, очно-заочная курс 1 семестр (ы) 1.

очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению 10.03.01 Информационная безопасность и профилю подготовки Безопасность автоматизированных систем.

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

«__» _____ 2021г.

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

«__» _____ 2021г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности от _____2021 года, протокол № _____.

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)
_____ Качаева Г.И., к.э.н.
подпись (ФИО уч. степень, уч. звание)

«__» _____ 2021 г.

Программа одобрена на заседании Методического совета факультета компьютерных технологий, вычислительной техники и энергетики от _____2021 года, протокол № _____.

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

«__» _____ 20__ 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 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 УП ВО. 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.

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

В результате освоения дисциплины Основы информационной безопасности 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)***
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач. УК-1.2. Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности. УК-1.3. Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений.
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации ОПК-1.2. Умеет классифицировать и оценивать угрозы информационной безопасности ОПК-1.3. Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в	ОПК-8.1. Знает принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной

	целях решения задач профессиональной деятельности;	информацией ОПК-8.2. Умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно-справочными системами ОПК-8.3. Владеет навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы, нормативных и методических документов

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	3/108	3/108	
Семестр	1	1	
Лекции, час	34	17	
Практические занятия, час	17	9	
Лабораторные занятия, час	-	-	
Самостоятельная работа, час	57	82	
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)	–	-	

4.1. Содержание дисциплины (модуля)

№ пп	Разлел 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: «Понятие составляющие и система формирования режима информационной безопасности»** 1. Определение понятия "информационная безопасность" 2. Доступность ,целостность и конфиденциальность информации	2	2	-	3	1	1	-	4				
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	1	-	-	4				
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	2	-	3	1	1	-	4				

4.	**Лекция №4** **Тема: «Стандарты информационной безопасности».** 1. Стандарты информационной безопасности: "Общие критерии". 2. Стандарты информационной безопасности распределенных систем	2	-	-	4	1	-	-	4				
5.	**Лекция №5** **«Стандарты информационной безопасности».** 1 Стандарты информационной безопасности в РФ.	2	2	-	3	1	1	-	4				
6.	**Лекция №6** **Тема: «Административный уровень обеспечения информационной безопасности»** 1. Цели, задачи и содержание административного уровня. 2. Разработка политики информационной безопасности.	2	-	-	4	1	-	-	4				
7.	**Лекции №7** **Тема: «Классификация угроз "информационной безопасности"»** 1. Классы угроз информационной безопасности. 2.Каналы несанкционированного доступа к информации	2	2	-	3	1	1	-	4				
8.	**Лекция №8** **Тема: «Вирусы как угроза информационной безопасности».** 1. Компьютерные вирусы и информационная безопасность. 2. Характерные черты	2		-	4	1	-	-	4				

	компьютерных вирусов.												
9.	**Лекция №9** **Тема: «Классификация компьютерных вирусов»** 1. Классификация компьютерных вирусов по среде обитания. 2. Классификация компьютерных вирусов по особенностям алгоритма работы. 3. Классификация компьютерных вирусов по деструктивные возможностям	2	2		3	1	1	-	5				
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	1	-	-	5				
11.	**Лекция № 11** **Тема: «Характеристика "вирусоподобных" программ. Антивирусные программы»** 1."Intended"-вирусы. 2. Особенности работы антивирусных программ. Классификация антивирусных программ	2	2		3	1	2	-	5				

	3. Факторы, определяющие качество антивирусных программ												
12.	**Лекция № 12** **Тема: «Профилактика компьютерных вирусов. Обнаружение неизвестного вируса».** 1. Характеристика путей проникновения вирусов в компьютеры. 2. Правила защиты от компьютерных вирусов 3. Обнаружение загрузочного и резидентного вируса, макровируса 4. Общий алгоритм обнаружения вируса	2	-		4	1	-	-	5				
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.	2	2		3	1	1	-	5				
14.	**Лекция № 14** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Классификация удаленных угроз в вычислительных сетях 2. Типовые удаленные атаки и их характеристика	2	-		3	1	-	-	5				

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	2		3	1	-	-	6				
16.	**Лекция № 16** **Тема: «Механизмы обеспечения "информационной безопасности"»** 1. Идентификация и аутентификация 2. Криптография и шифрование 3. Методы разграничение доступа	2	-		3	1	-	-	6				
17.	**Лекция № 17** **Тема: «Механизмы обеспечения "информационной безопасности"»** 1. Регистрация и аудит 2. Межсетевое экранирование 3. Технология виртуальных частных сетей (VPN)	2	1		3	1	1	-	6				
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 1-6 тема 2 аттестация 7-12 тема 3 аттестация 13-17 тема				Входная конт.работа 1 аттестация 1-6 тема 2 аттестация 7-12 тема 3 аттестация 13-17 тема							
Форма промежуточной аттестации (по семестрам)		Зачет				Зачет							
ИТОГО		**34**	**17**	**-**	**57**	**17**	**9**	**-**	**82**				

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

№	№ 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.	1	«Ответственность за нарушения в сфере информационной безопасности»	2	1	-	1-8
2.	2,3	«Стандарты информационной безопасности РФ»	2	1	-	1-8
3.	4,5	«Разработка политики информационной безопасности»	2	1	-	1-8
4.	6,7	«Каналы несанкционированного доступа к информации	2	1		1-8
5.	8,9	«Характерные черты компьютерных вирусов»	2	1		1-8
6.	10,11	«Факторы, определяющие качество антивирусных программ «	2	2	-	1-8
7.	12,13	«Адресация в глобальных сетях»	1	1	-	1-8
8.	14,15	«Принципы защиты распределенных вычислительных сетей»	2	-	-	1-8
9.	16,17	«Технология виртуальных частных сетей (VPN)»	2	1		1-8
	Итого:		17	9	-	

4.3. Тематика для самостоятельной работы студента

№	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
		очно	Очно-заочно	заочно		
1.	**Лекция № 1** **Тема: «Понятие составляющие и система формирования режима информационной безопасности»** 1 Определение понятия "информационная безопасность" 2. Доступность ,целостность и конфиденциальность информации	3	4	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
2.	**Лекция №2** **Тема: «Понятие составляющие и система формирования режима информационной безопасности»** 1. Задачи информационной безопасности общества. 2. Уровни формирования режима информационной безопасности	4	4	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
3.	**Лекция №3** **Тема: «Нормативно-правовые основы информационной**	3	4	-	1-8	изучение основной и дополнительной литературы,

	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.					подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
4.	**Лекция №4** **Тема: «Стандарты информационной безопасности».** 1. Стандарты информационной безопасности: "Общие критерии". 2. Стандарты информационной безопасности распределенных систем	4	4	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
5.	**Лекция №5** **«Стандарты информационной безопасности».** 1 Стандарты информационной безопасности в РФ.	3	4	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение

						домашних заданий
6.	**Лекция №6** **Тема: «Административный уровень обеспечения информационной безопасности»** 1. Цели, задачи и содержание административного уровня. 2. Разработка политики информационной безопасности.	4	4	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
7.	**Лекции №7** **Тема: «Классификация угроз "информационной безопасности"»** 1. Классы угроз информационной безопасности. 2.Каналы несанкционированного доступа к информации	3	4	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
8.	**Лекция №8** **Тема: «Вирусы как угроза информационной безопасности».** 1. Компьютерные вирусы и информационная безопасность. 2. Характерные черты компьютерных вирусов.	4	4	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником,

						изучение дополнительных тем занятий, выполнение домашних заданий
9.	**Лекция №9** **Тема: «Классификация компьютерных вирусов»** 1. Классификация компьютерных вирусов по среде обитания. 2. Классификация компьютерных вирусов по особенностям алгоритма работы. 3. Классификация компьютерных вирусов по деструктивные возможностям	3	5	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
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	4	5	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
11.	**Лекция № 11** **Тема: «Характеристика "вирусоподобных" программ. Антивирусные программы»** 1."Intended"-вирусы. 2. Особенности работы антивирусных программ. Классификация антивирусных программ	3	5	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка

	3. Факторы, определяющие качество антивирусных программ					презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
12.	**Лекция № 12** **Тема: «Профилактика компьютерных вирусов. Обнаружение неизвестного вируса».** 1. Характеристика путей проникновения вирусов в компьютеры. 2. Правила защиты от компьютерных вирусов 3. Обнаружение загрузочного и резидентного вируса, макровируса 4. Общий алгоритм обнаружения вируса	4	5	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
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.	3	5	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
14.	**Лекция № 14** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Классификация удаленных угроз в вычислительных сетях 2. Типовые удаленные атаки и	3	5	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе,

	их характеристика					докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
15.	**Лекция № 15** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Причины успешной реализации удаленных угроз в вычислительных сетях 2. Принципы защиты распределенных вычислительных сетей	3	6	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
16.	**Лекция № 16** **Тема: «Механизмы обеспечения "информационной безопасности"»** 1. Идентификация и аутентификация 2. Криптография и шифрование 3. Методы разграничение доступа	3	6	-	1-8	изучение основной и дополнительной литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
17.	**Лекция № 17** **Тема: «Механизмы**	3	6	-	1-8	изучение основной и дополнительной

	обеспечения "информационной безопасности"» 1. Регистрация и аудит 2. Межсетевое экранирование 3. Технология виртуальных частных сетей (VPN)					литературы, подготовка к семинарам, подготовка эссе, докладов и рефератов, тестирование, подготовка презентаций, работа с электронным учебником, изучение дополнительных тем занятий, выполнение домашних заданий
	ИТОГО:	57	82	-		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки реализации компетентностного подхода в процессе изучения дисциплины «Гуманитарные аспекты информационной безопасности» используются как традиционные, так и инновационные технологии, активные и интерактивные методы и формы обучения: практические занятия тренинг речевых умений, разбор конкретных ситуаций, коммуникативный эксперимент, коммуникативный тренинг. Творческие задания для самостоятельной работы, информационно-коммуникативные технологии. Удельный вес, проводимых в интерактивных формах составляет не менее 30% аудиторных занятий (28 ч.).

В рамках учебного курса предусмотрены встречи со специалистами в области информационной безопасности региона, коммерческих, государственных и общественных организаций, экспертов и специалистов в области информационных технологий.

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

Зав. библиотекой _____ *(Алиева Ж.А.)*
(подпись)

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

№ п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Количество изданий	
			В библиотеке	На кафедре
1	2	3	4	5
ОСНОВНАЯ				
1	лк, пз, срс	Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118233 — Режим доступа: для авториз. пользователей.	
2	лк, пз, срс	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный //	Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 — Режим доступа: для авториз. пользователей.	
ДОПОЛНИТЕЛЬНАЯ				
3	лк, пз, срс	Петренко, В. И. Теоретические основы защиты информации: учебное пособие / В. И. Петренко. — Ставрополь: СКФУ, 2015. — 222 с. — Текст: электронный //	Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/155247 — Режим доступа: для авториз. пользователей.	-
4	лк, пз, срс	Мызникова, Т. А. Основы информационной безопасности: учебное пособие / Т. А. Мызникова. — Омск: ОмГУПС, 2017. — 82 с. — ISBN	Лань : электронно-библиотечная система. —	-

		978-5-949-41160-5. — Текст: электронный //	URL: https://e.lanbook.com/book/129192 — Режим доступа: для авториз. пользователей.	
5	лк, пз, срс	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст: электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739 — Режим доступа: для авториз. пользователей.	-
6	лк, пз, срс	Секлетова, Н. Н. 1Анализ рынка информационных систем и технологий: учебное пособие / Н. Н. Секлетова, А. С. Тучкова, О. И. Захарова. — Самара : ПГУТИ, 2018. — 215 с. — Текст : электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182310 — Режим доступа: для авториз. пользователей.	-
7	лк, пз, срс	Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия: учебное пособие / В. М. Бабушкин. — Казань: КНИТУ-КАИ, 2020. — 256 с. — ISBN 978-5-7579-2463-2. — Текст: электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/193486 — Режим доступа: для авториз. пользователей.	-
8	лк, пз, срс	Криулин, А. А. Основы безопасности прикладных информационных технологий и систем: учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва: РТУ МИРЭА, 2020. — 136 с. — Текст: электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606 — Режим доступа: для авториз. пользователей.	-

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)