Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Комплексное обеспечение информационной безопасности в АС

для направления 10.03.01 Информационная безопасность
код и полное наименование специальности

по профилю Безопасность автоматизированных 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, очно-заочная курс 4 семестр (ы) 8.
очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС 3++ ВО по направлению подготовки 10.03.01 «Информационная безопасность» с учетом рекомендаций и ОПОП ВО по направлению и профилю - «Информационная безопасность», «Безопасность автоматизированных систем»

Разработчик _____ Качаева Г.И._____
подпись (ФИО уч. степень, уч. звание)

«_18_» сентября 2021 г.

И.о.зав. кафедрой, за которой закреплена практика

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

«_18_» сентября 2021 г.

Программа одобрена на заседании выпускающей кафедры _ИБ_____
от 20 сентября 2021 года, протокол № 2____.

И.о.зав. выпускающей кафедрой по данному направлению (специальности, профилю)

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

«_20_» __09_____ 2021_ г.

Программа одобрена на заседании Методического совета факультета КТВТиЭ
от «18» 10 2021 года, протокол № __1____.

Председатель Методического совета факультета КТВТиЭ

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

«_18_» _10____ 2021___ г.

Декан факультета _____ Ш.А. Юсуфов
подпись ФИО

Начальник УО _____ Э.В.Магомаева
подпись ФИО

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

1. Цели и задачи освоения дисциплины

Учебная дисциплина «Комплексное обеспечение информационной безопасности в АС» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом.

Дисциплина « Комплексное обеспечение информационной безопасности в АС» изучает вопросы, связанные с приобретением необходимых знаний, умений и навыков в области современных информационных технологий, применяемых для обеспечения информационной безопасности.

Целью изучения дисциплины является обучение студентов комплексному подходу к обеспечению информационной безопасности; формирование у них представлений об видах, практических методах и средств проведения аудита информационных технологий и систем обеспечения информационной безопасности.

Задачи дисциплины:

- получить представление об основных угрозах информационной безопасности и методах противодействия данным угрозам;
- изучить основные формальные математические модели, используемые для анализа защищенности автоматизированных систем;
- изучить методологию проектирования и построения защищенных автоматизированных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина «Комплексное обеспечение информационной безопасности в АС» относится к вариативной части УП ВО. Для освоения дисциплины обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения таких предметов как: «Основы обеспечение информационной безопасности» «Управление информационной безопасностью», «Программно-аппаратные средства защиты информации».

Знания и практические навыки, полученные из дисциплины «Комплексное обеспечение информационной безопасности в АС», используются обучающимися при разработке выпускных квалификационных работ.

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

В результате освоения дисциплины Комплексное обеспечение информационной безопасности в АС 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)**
ПК-1	Способен проводить оценивание уровня безопасности компьютерных систем и сетей	

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144	-	-
Семестр	10	-	-
Лекции, час	34	-	-
Практические занятия, час	34	-	-
Лабораторные занятия, час	-	-	-
Самостоятельная работа, час	76	-	-
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	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, 2** **Тема 1: «Основы построения систем информационной безопасности»** 1. Цель и задачи информационной безопасности (ИБ) 2. Угрозы ИБ и их источники 3. Модель построения системы информационной безопасности предприятия 4. Разработка концепция обеспечения ИБ	4	4	-	10	-	-	-	-	-	-	-	-
2.	**Лекция № 3, 4** **Тема 2: «Аудит безопасности и методы его проведения»** 1. Методы анализа данных при аудите ИБ 2. Понятие аудита безопасности 3. Анализ информационных рисков предприятия 4. Методы оценивания информационных рисков 5. Управление информационными рисками	4	4	-	10	-	-	-	-	-	-	-	-
3.	**Лекции № 5, 6, 7** **Тема 3: «Стандарты информационной безопасности»** 1. Предпосылки создания стандартов ИБ Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)	6	6	-	10	-	-	-	-	-	-	-	-

№ пп	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
	2. Гармонизированные критерии Европейских стран 3. Германский стандарт BS1 4. Британский стандарт BS 7799 5. Международный стандарт ISO 17799 6. Международный стандарт ISO 15408 «Общие критерии» 7. Стандарт COBIT 8. Стандарты по безопасности информационных технологий в России												
4.	**Лекции № 8, 9** **Тема 4: «Оценка безопасности информационных технологий на основе «Общих критериев»** 1. Предпосылки введения международного стандарта ISO 15408 2. Основные понятия общих критериев 3. Методология оценки безопасности информационных технологий по общим критериям 4. Оценка уровня доверия функциональной безопасности информационной технологии 5. Обзор классов и семейств ОК	4	4	-	10	-	-	-	-	-	-	-	-
5.	**Лекция № 10, 11,12,13** **Тема 5: «Международный стандарт управления информационной безопасностью ISO 17799 »**	8	8	-	12								

№ пп	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. Назначение стандарта ISO 17799 для управления информационной безопасностью 2. Практика прохождения аудита и получения сертификата ISO 17799 3. Политика безопасности 4. Организационные меры по обеспечению информационной безопасности 5. Классификация ресурсов и их контроль 6. Безопасность персонала Раздел 5. Физическая безопасность 7. Администрирование компьютерных систем и вычислительных сетей 8. Управление доступом к системам 9. Разработка и сопровождение информационных систем 10. Планирование бесперебойной работы организации 11. Соответствие системы основным требованиям.												
6.	**Лекция № 14** **Тема 6: «Программные средства для проведения аудита информационной безопасности»** 1. Анализ видов используемых программных продуктов 2. Система CRAMM 3. Система КОНДОР 4. Сетевые сканеры	2	2	-	12								

№ пп	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
7.	**Лекция № 15, 16,17** **Тема 7: «Методика проведения аудита информационной безопасности на предприятии»** 1. Три подхода к проведению аудита ИБ 2. Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятий к проведению аудита ИБ 3. Планирование процедуры аудита ИБ 4. Организация и проведения работ по аудиту 5. Алгоритм проведения аудита безопасности предприятия 6. Перечень и систематизация данных, необходимых для проведения аудита ИБ 7. Выработка рекомендаций и подготовка отчетных документов 8. Экономическая оценка обеспечения ИБ	6	6	-	12								
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 1-3 тема 2 аттестация 4-5 тема 3 аттестация 6-7 тема											
Форма промежуточной аттестации (по семестрам)		Зачет				-							
ИТОГО		**34**	**34**	**-**	**76**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

4.2. Содержание лабораторных (практических) занятий (1,2 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.	**Лекция № 1, 2**	**Тема 1: «Основы построения систем информационной безопасности»** 1. Цель и задачи информационной безопасности (ИБ) 2. Угрозы ИБ и их источники 3. Модель построения системы информационной безопасности предприятия 4. Разработка концепция обеспечения ИБ	4	-	-	1-8
2.	**Лекция № 3, 4**	**Тема 2: «Аудит безопасности и методы его проведения»** 1. Методы анализа данных при аудите ИБ 2. Понятие аудита безопасности 3. Анализ информационных рисков предприятия 4. Методы оценивания информационных рисков 5. Управление информационными рисками	4	-	-	1-8
3.	**Лекции № 5, 6, 7**	**Тема 3: «Стандарты информационной безопасности»** 1. Предпосылки создания стандартов ИБ Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга) 2. Гармонизированные критерии Европейских стран 3. Германский стандарт BS1 4. Британский стандарт BS 7799 5. Международный стандарт ISO 17799 6. Международный стандарт ISO 15408 «Общие	6	-	-	1-8

		критерии» 7. Стандарт COBIT 8. Стандарты по безопасности информационных технологий в России				
4.	**Лекции № 8, 9**	**Тема 4: «Оценка безопасности информационных технологий на основе «Общих критериев»** 1. Предпосылки введения международного стандарта ISO 15408 2. Основные понятия общих критериев 3. Методология оценки безопасности информационных технологий по общим критериям 4. Оценка уровня доверия функциональной безопасности информационной технологии 5. Обзор классов и семейств ОК	4	-		1-8
5.	**Лекция № 10, 11,12,13**	**Тема 5: «Международный стандарт управления информационной безопасностью ISO 17799 »** 1. Назначение стандарта ISO 17799 для управления информационной безопасностью 2. Практика прохождения аудита и получения сертификата ISO 17799 3. Политика безопасности 4. Организационные меры по обеспечению информационной безопасности 5. Классификация ресурсов и их контроль 6. Безопасность персонала Раздел 5. Физическая безопасность 7. Администрирование компьютерных систем и вычислительных сетей 8. Управление доступом к	8	-		1-8

		системам 9. Разработка и сопровождение информационных систем 10. Планирование бесперебойной работы организации 11. Соответствие системы основным требованиям.				
6.	**Лекция № 14**	**Тема 6: «Программные средства для проведения аудита информационной безопасности»** 1. Анализ видов используемых программных продуктов 2. Система CRAMM 3. Система КОНДОР 4. Сетевые сканеры	2	-	-	1-8
7.	**Лекция № 15, 16,17**	**Тема 7: «Методика проведения аудита информационной безопасности на предприятии»** 1. Три подхода к проведению аудита ИБ 2. Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятий к проведению аудита ИБ 3. Планирование процедуры аудита ИБ 4. Организация и проведения работ по аудиту 5. Алгоритм проведения аудита безопасности предприятия 6. Перечень и систематизация данных, необходимых для проведения аудита ИБ 7. Выработка рекомендаций и подготовка отчетных документов 8. Экономическая оценка обеспечения ИБ	8	-	-	1-8
	Итого:		34	-	-	

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.	**Тема 1: «Основы построения систем информационной безопасности»**	10	-	-	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.	**Тема 2: «Аудит безопасности и методы его проведения»**	10	-	-	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.	**Тема 3: «Стандарты информационной безопасности»**	10	-	-	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
4.	**Тема 4: «Оценка безопасности информационных технологий на основе «Общих критериев»**	10	-	-	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.	**Тема 5: «Международный стандарт управления информационной безопасностью ISO 17799 »**	12	-	-	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.	**Тема 6: «Программные средства для проведения аудита информационной безопасности»**	12	-	-	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.	**Тема 7: «Методика проведения аудита информационной безопасности на предприятии»**	12	-	-	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
	ИТОГО:	76	-	-		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки реализации компетентностного подхода в процессе изучения дисциплины «Комплексное обеспечение информационной безопасности в АС» 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	Гулак М.Л. Аудит информационной безопасности. Прикладная статистика: учебное пособие / Гулак М.Л., Рытов М.Ю., Голембиовская О.М.. — Москва: Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0713-0. — Текст: электронный //	IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97630.html — Режим доступа: для авторизир. пользователей	
2	лк, пз, срс	Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / Нестеров С.А.. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 250 с. — ISBN 978-5-4497-0300-2. — Текст: электронный //	IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89416.html — Режим доступа: для авторизир. пользователей	
ДОПОЛНИТЕЛЬНАЯ				
3	лк, пз, срс	Шинаков К.Е. Анализ рисков безопасности информационных систем персональных данных: монография / Шинаков К.Е., Рытов М.Ю., Голембиовская О.М.. — Москва: Ай Пи Ар Медиа, 2020. — 236 с. — ISBN 978-5-4497-0535-8. — Текст: электронный //	IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95150.html — Режим доступа: для авторизир. пользователей	-
4	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.	-
5	лк, пз,	Компьютерные информационные	Лань:	-

	срс	технологии в документационном обеспечении управления : учебное пособие / Е. Э. Попова, А. М. Назаренко, О. Л. Липницкая [и др.]. — Минск : БГУ, 2019. — 167 с. — ISBN 978-985-566-623-4. — Текст : электронный //	электронно-библиотечная система. — URL: https://e.lanbook.com/book/180431 — Режим доступа: для авториз. пользователей.	
6	лк, пз, срс	Федин, Ф. О. Информационная безопасность баз данных: учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 133 с. — Текст: электронный //	Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/167605 — Режим доступа: для авториз. пользователей.	-
7	лк, пз, срс	Гаенко В.П. Безопасность технических систем. Методологические аспекты теории, методы анализа и управления безопасностью : монография / Гаенко В.П., Костюков В.Е., Фомченко В.Н.. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2020. — 329 с. — ISBN 978-5-9515-0452-4. — Текст: электронный //	IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101918.html — Режим доступа: для авторизир. пользователей	-
8	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. 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