МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Гробова Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Комплексное обеспечение информационной безопасности автоматизированных систем

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	А

Разработано
Пелешенко Т.А., доцент кафедры вычислительной математики и кибернетики.

Ставрополь 2026 г.

Цель и задачи освоения дисциплины:

Целью освоения дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» понимания основных методов, реализации успешной командной работы, применение ИТ-технологий для эффективного взаимодействия в команде и развития проектной деятельности.

Задачи дисциплины:

- изучение теоретических основ формирования и развития навыков командной работы и проектной деятельности;
- формирование умений удаленного управления групповыми проектами;
- овладение навыками эффективного социального взаимодействия, создания благоприятной и конструктивной атмосферы в команде средствами доступных онлайн-инструментов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к части, формируемой участниками образовательных отношений дисциплинам (модулям) обязательной части. Ее освоение происходит во 9 семестре.

3. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-1. Способен оценивать уровень безопасности компьютерных систем и сетей	ИД-1$_{ПК-1}$ Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Предоставляет детальный отчёт по результатам Проведения контрольных проверок работоспособности и эффективности применяемых программно- аппаратных средств защиты информации
	ИД-2$_{ПК-1}$ Разрабатывает требования по защите, формирование политик безопасности компьютерных систем и сетей.	Предоставляет детальный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей

	ИД-3$_{ПК-1.}$ Проводит анализ безопасности компьютерных систем.	Предоставляет детальный отчёт по результатам проведения анализа безопасности компьютерных систем.
	ИД-4$_{ПК-1}$ Проводит сертификацию программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет детальный Отчёт п результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов
	ИД-5$_{ПК-1}$ Проводит инструментальный мониторинг защищенности компьютерных систем и сетей.	Предоставляет детальный Отчёт по результатам проведения инструментального Мониторинга защищенности компьютерных систем и сетей
	ИД-6$_{ПК-1}$ Проводит экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет детальный Отчёт по результатам Проведения экспертизы При расследовании Компьютерных преступлений, правонарушений и инцидентов
ПК-8. Способен разрабатывать системы защиты информации автоматизированных систем	ИД-1$_{ПК-8}$ Тестирует системы защиты информации автоматизированных систем.	Предоставлен детальный отчёт с результатами тестирования систем защиты информации автоматизированных систем.
	ИД-2$_{ПК-8}$ Разрабатывает проектные решения по защите информации в автоматизированных системах.	Предоставлен детальный отчёт с результатами разработки проектных решений по защите информации в автоматизированных системах.
	ИД-3$_{ПК-8}$ Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.	Предоставлен детальный отчёт с результатами разработки эксплуатационной документации на системы защиты информации автоматизированных систем.
	ИД-4$_{ПК-8}$ Разрабатывает программные и программно-аппаратные средства для систем	Предоставлен детальный отчёт с результатами разработки программных и

	защиты информации автоматизированных систем.	программно-аппаратных средств для систем защиты информации автоматизированных систем.
ПК-9. Способен формировать требования к защите информации в автоматизированных системах	ИД-1$_{ПК-9}$ Обосновывает необходимость защиты информации в автоматизированной системе.	Предоставляет детальный отчет с обоснованием необходимости защиты информации в автоматизированной системе.
	ИД-2$_{ПК-9}$ Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет детальный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.
	ИД-3$_{ПК-9}$ Разрабатывает архитектуру системы защиты информации автоматизированной системы.	Предоставляет детальный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.
	ИД-4$_{ПК-9}$ Моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Предоставляет детальный Отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

4. Объем учебной дисциплины (модуля) и формы контроля *

Объем занятий: всего: 5 з.е. 180 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	36/0
Лабораторных работ/из них практическая подготовка	54/0
Практических занятий/из них практическая подготовка	-
Самостоятельная работа	36
Формы контроля	
Экзамен А семестр	54
Зачет	-
Зачет с оценкой	-
Курсовая работа А семестр	есть

* Дисциплина (модуль) предусматривает применение электронного обучения, дистанционных образовательных технологий

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Формы текущего контроля успеваемости
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		

1.	**Понятие национальной безопасности. Понятие информационной безопасности.** В данной теме студентам предстоит изучить понятия национальной безопасности и информационной безопасности, их взаимосвязь и значение для государства. Особое внимание будет уделено основным аспектам и задачам обеспечения информационной безопасности в контексте национальных интересов. В конце изучения темы студент будет знать ключевые определения, цели и направления политики в области национальной и информационной безопасности.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	8	4	Собеседование
2.	**Государственная информационная политика. Понятие и виды информации, свойства информации и систем ее обработки.** В данной теме студентам предстоит изучить основы государственной информационной политики, а также понятие информации, её виды и свойства. Особое внимание будет уделено системам обработки информации и их роли в управлении данными на государственном уровне. В конце изучения темы студент будет знать ключевые понятия, классификацию информации и основные принципы формирования государственной информационной политики.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	6	4	Собеседование

3.	**Проблемы информационной войны. Компьютерные системы в сфере государственного и муниципального управления.** В данной теме студентам предстоит изучить проблемы информационной войны и особенности использования компьютерных систем в государственном и муниципальном управлении. Особое внимание будет уделено угрозам и вызовам, связанным с кибербезопасностью в управленческих структурах. В конце изучения темы студент будет знать основные риски информационных атак и методы защиты компьютерных систем в государственных и муниципальных органах.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	6	4	Собеседование
4.	**Современная постановка задачи защиты информации. Организационно-правовое обеспечение информационной безопасности. Анализ угроз информационной безопасности.** В данной теме студентам предстоит изучить современную постановку задачи защиты информации, а также организационно-правовые аспекты обеспечения информационной безопасности. Особое внимание будет уделено методам анализа угроз информационной безопасности и оценке возможных рисков. В конце изучения темы студент будет знать основные принципы защиты информации, нормативные требования и способы выявления угроз для эффективного обеспечения безопасности.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	6	4	Собеседование

5.	**Причины, виды и каналы утечки информации. Функции и задачи защиты информации. Стратегии защиты информации.** В данной теме студентам предстоит изучить причины, виды и каналы утечки информации, а также функции, задачи и стратегии защиты информации. Особое внимание будет уделено анализу потенциальных угроз и выбору эффективных способов предотвращения утечек. В конце изучения темы студент будет знать основные источники угроз, принципы построения систем защиты информации и методы обеспечения её сохранности.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	6	4	Собеседование
6.	**Методы обеспечения информационной безопасности. Способы и средства защиты информации.** В данной теме студентам предстоит изучить методы обеспечения информационной безопасности, а также способы и средства защиты информации. Особое внимание будет уделено классификации и практическому применению технических, программных и организационных средств защиты. В конце изучения темы студент будет знать, какие методы используются для предотвращения несанкционированного доступа, и как применять различные средства защиты в зависимости от уровня угроз.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	6	4	Собеседование

7.	**Электронные деньги. Анализ существующих методик определения требований к защите информации.** В данной теме рассматриваются понятие и принципы функционирования электронных денег, их виды и особенности использования в цифровой экономике. Также проводится анализ существующих методик определения требований к защите информации, применяемых в финансовой сфере. Студент изучит, как обеспечивается конфиденциальность, целостность и доступность информации в системах электронных платежей, а также какие стандарты и нормативные документы регламентируют защиту информации в этой области.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	6	4	Собеседование
8.	**Криптографические методы защиты информации. Архитектура систем защиты информации.** В рамках данной темы изучаются основные криптографические методы защиты информации: симметричное и асимметричное шифрование, электронная подпись, хэш-функции и протоколы распределения ключей. Рассматриваются их принципы работы, области применения и устойчивость к криптоанализу. Также изучается архитектура систем защиты информации, включая ее основные компоненты (средства идентификации и аутентификации, шифрования, контроля доступа, регистрации событий безопасности и т. д.), модели построения защищенных систем и подходы к интеграции криптографических механизмов в инфраструктуру организации.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	6	4	Собеседование

9.	**Криптографические методы защиты информации. Архитектура систем защиты информации.** В рамках данной темы изучаются основные криптографические методы защиты информации: симметричное и асимметричное шифрование, электронная подпись, хэш-функции и протоколы распределения ключей. Рассматриваются их принципы работы, области применения и устойчивость к криптоанализу. Также изучается архитектура систем защиты информации, включая ее основные компоненты (средства идентификации и аутентификации, шифрования, контроля доступа, регистрации событий безопасности и т. д.), модели построения защищенных систем и подходы к интеграции криптографических механизмов в инфраструктуру организации.	ПК-1 ИД-1$_{ПК-1}$, ИД-2$_{ПК-1}$, ИД-3$_{ПК-1}$, ИД-4$_{ПК-1}$, ИД-5$_{ПК-1}$, ИД-6$_{ПК-1}$, ПК-8 ИД-1$_{ПК-8}$, ИД-2$_{ПК-8}$, ИД-3$_{ПК-8}$, ИД-4$_{ПК-8}$, ПК-9 ИД-1$_{ПК-9}$, ИД-2$_{ПК-9}$, ИД-3$_{ПК-9}$, ИД-4$_{ПК-9}$	4	-	4	4	Собеседование
	ИТОГО за 9 семестр		36	-	54	36	
	ИТОГО		36	-	54	36	

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств (ФОС) по дисциплине (модулю) базируется на перечне осваиваемых компетенций с указанием индикаторов. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины (модуля).

7.Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимый для освоения дисциплины

8.1.1. Перечень основной литературы:

1. Жигулин, Г. П.
    Организационное и правовое обеспечение информационной безопасности Электронный ресурс : Учебное пособие / Г. П. Жигулин. - Организационное и правовое обеспечение информационной безопасности,2022-10-01. - Санкт- Петербург : Университет ИТМО, 2014. - 174 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 2227-8397

2. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности : защита конфиденциальной информации : учебное пособие для студентов вузов / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2014. - 256 с. : ил. - (Высшее образование. Бакалавриат). - Гриф: Рек. УМО. - Библиогр.: с. 251-253. - ISBN 978-5- 91134-856-4. - ISBN 978-5-16-009578-3

3. Каторин, Ю. Ф.
    Защита информации техническими средствами Электронный ресурс : Учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак ; ред. Ю. Ф. Каторин. - Защита информации техническими средствами,2022-10-01. - Санкт-Петербург : Университет ИТМО, 2012. - 417 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 2227-8397

4. Обеспечение информационной безопасности бизнеса Электронный ресурс : энциклопедия / Н.А. Голдуев / В.Б. Голованов / С.Л. Зефиров / В.В. Андрианов ; ред. А.П.

Курило. - Москва : ЦИПСиР, 2011. - 373 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-9614-1364-9

5. Чипига, А. Ф. (СевКавГТУ). Многоканальные измерительные системы для мониторинга безопасности объектов : учеб. пособие / А. Ф. Чипига, В. В. Федоренко, И. В. Федоренко ; ФБГОУ Сев.-Кав. гос. техн. ун-т. - Ставрополь : Издательство СевКавГТУ, 2012. - 126 с. : ил. - Библиогр.: с. 123-128 (58 назв.)

8.1.2. Перечень дополнительной литературы:

6. Быкова, А. В. Лидерство и управление командами : учебное пособие / А. В. Быкова. — Москва : РТУ МИРЭА, 2020. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163921

7. Фютик, И. Г. Управление персоналом : учебное пособие / И. Г. Фютик. — Новосибирск : СГУВТ, 2022. — 130 с. — ISBN 978-5-8119-0909-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293378

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Основы информационной безопасности». Ставрополь : СКФУ, 2026.
2. Методические указания к практическим занятиям по дисциплине «Обеспечение информационной безопасности на объектах критической информационной инфраструктуры». Ставрополь : СКФУ, 2026.

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. www.biblioclub.ru - Электронная библиотечная система «Университетская библиотека онлайн»
2. www.eLibrary.ru - Научная электронная библиотека
3. www.iprbookshop.ru - Электронно-библиотечная система IPRbooks

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На практических занятиях студенты защищают отчеты по работам, которые они выполняют самостоятельно или в команде с применением компьютерной техники и Интернет-технологий

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2	https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
	https://spravochnick.ru/psihologiya/ – Справочник по психологии

Программное обеспечение:

1	Операционная система: Microsoft Windows 8: Бессрочная лицензия. Договор № 01-эа/13 от 25.02.2013
2	Операционная система: Microsoft Windows 10: Бессрочная лицензия. Договор № 544-21 от 08.06.2021.
3	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). Microsoft Office Standard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензия Microsoft Office https://support.microsoft.com/ru-ru/lifecycle/search/16674

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Практические занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета

11. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
- индивидуальное равномерное освещение не менее 300 люкс,
- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются: способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование); ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»; для синхронного обучения - время проведения онлайн-занятий и преподаватели; для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнауки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а

также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.