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

Обеспечение информационной безопасности на объектах критической информационной инфраструктуры

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	9

Разработано
Песков М.В., 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-1ПК-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-2ПК-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-3ПК-1. Проводит анализ безопасности компьютерных систем.	Предоставляет детальный отчёт по результатам проведения анализа безопасности компьютерных систем.
	ИД-4ПК-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-5ПК-1 Проводит инструментальный мониторинг защищенности компьютерных систем и сетей.	Предоставляет детальный Отчёт по результатам проведения инструментального Мониторинга защищенности компьютерных систем и сетей
	ИД-6ПК-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-2. Способен разрабатывать программно-аппаратные средства защиты информации компьютерных систем и сетей	ИД-1ПК-2 Разрабатывает требования к программно- аппаратным средствам защиты информации компьютерных систем и сетей.	Специалист способен профессионально разрабатывать программно-аппаратные средства защиты информации для компьютерных систем и сетей. Он демонстрирует компетентность в формировании и обосновании требований к таким средствам защиты, учитывая современные угрозы информационной безопасности и технологические особенности защищаемых систем.
	ИД-2ПК-2 Проектирует программно-аппаратные средства защиты информации компьютерных систем и сетей.	Специалист способен разрабатывать и проектировать программно-аппаратные средства защиты информации для компьютерных систем и сетей. Он демонстрирует комплексное владение технологиями разработки программно-аппаратных комплексов
	ИД-3ПК-2 Разрабатывает и тестирует средства защиты информации компьютерных систем и сетей.	Специалист способен разрабатывать программно-аппаратные средства защиты информации для компьютерных систем и сетей, а также проводить их комплексное тестирование. Результат отражает способность специалиста не только создавать, но и всесторонне проверять средства защиты информации, обеспечивая их надежность и соответствие современным стандартам информационной безопасности.

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

Объем занятий: всего:4 з.е. 144 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	36/0
Лабораторных работ/из них практическая подготовка	36/0
Практических занятий/из них практическая подготовка	0
Самостоятельная работа	72
Формы контроля	
Экзамен	-
Зачет 9 семестр	+
Зачет с оценкой	-
Курсовая работа	нет

* 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. Обеспечение информационной безопасности на объектах критической информационной инфраструктуры.** В данной теме студентам предстоит изучить понятие национальной безопасности и его значение для государства, особое внимание будет уделено ее компонентам, включая политическую, экономическую, военную и информационную безопасность. В конце изучения темы студент будет знать, как информационная безопасность входит в систему национальной безопасности и влияет на устойчивость и защиту общества.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование

2.	**Государственная информационная политика. Понятие и виды информации, свойства информации и систем ее обработки. Создание комиссии по категорированию объектов КИИ.** В данной теме студентам предстоит изучить государственную информационную политику, понятие и виды информации, а также свойства информации и систем её обработки. Особое внимание будет уделено процедуре создания комиссии по категорированию объектов критической информационной инфраструктуры. В конце изучения темы студент будет знать основы государственной информационной политики, типы информации, принципы обработки данных и порядок формирования комиссии по категорированию объектов КИИ.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование
3.	**Проблемы информационной войны. Компьютерные системы в сфере государственного и муниципального управления. Формирование перечня объектов КИИ и их категорирование.** В данной теме студентам предстоит изучить проблемы информационной войны и использование компьютерных систем в сфере государственного и муниципального управления. Особое внимание будет уделено процессу формирования перечня объектов критической информационной инфраструктуры и их категорированию. В конце изучения темы студент будет знать основные угрозы информационной войны, принципы работы информационных систем в управлении и порядок категорирования объектов КИИ.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование
4.	**Современная постановка задачи защиты информации. Организационно-правовое обеспечение информационной безопасности. Анализ угроз информационной безопасности.. Анализ возможных действий нарушителей в отношении объектов КИИ.** В данной теме студентам предстоит изучить современную постановку задачи защиты информации, включая организационно-правовые основы обеспечения информационной безопасности и анализ угроз. Особое внимание будет уделено анализу возможных действий нарушителей в отношении объектов критической информационной инфраструктуры. В конце изучения темы студент будет знать правовые и организационные механизмы защиты информации, методы выявления и оценки угроз, а также подходы к анализу потенциальных нарушителей в контексте КИИ.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование

5.	**Причины, виды и каналы утечки информации. Функции и задачи защиты информации. Стратегии защиты информации. Разработка модели угроз для объектов КИИ.** В данной теме студентам предстоит изучить причины, виды и каналы утечки информации, а также функции и задачи защиты информации. Особое внимание будет уделено стратегиям защиты информации и разработке модели угроз для объектов критической информационной инфраструктуры. В конце изучения темы студент будет знать основные факторы риска утечки данных, способы их предотвращения, а также методы построения эффективных моделей угроз для обеспечения безопасности КИИ.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование
6.	**Методы обеспечения информационной безопасности. Способы и средства защиты информации. Оценка уязвимостей объектов КИИ.** В данной теме студентам предстоит изучить методы обеспечения информационной безопасности, а также различные способы и средства защиты информации. Особое внимание будет уделено оценке уязвимостей объектов критической информационной инфраструктуры. В конце изучения темы студент будет знать основные методы защиты информации, инструменты для их реализации и подходы к выявлению и анализу уязвимых мест в системах КИИ.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование
7.	**Электронные деньги. Оценка рисков для объектов КИИ** В данной теме студентам предстоит изучить понятие электронных денег и особенности их функционирования. Особое внимание будет уделено анализу существующих методик определения требований к защите информации в системах электронных платежей. В конце изучения темы студент будет знать основные принципы работы электронных денег, а также способы и стандарты защиты информации, применяемые для обеспечения безопасности таких систем.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование

8.	**Выбор и обоснование средств защиты информации** В данной теме студентам предстоит изучить криптографические методы защиты информации и принципы их применения. Особое внимание будет уделено архитектуре систем защиты информации и организации их работы. В конце изучения темы студент будет знать основные криптографические алгоритмы и компоненты, а также уметь описывать структуру современных систем защиты информации.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование
9.	**Разработка организационно-распорядительных документов по ИБ на объектах КИИ** В данной теме студентам предстоит изучить криптографические методы защиты информации, включая шифрование, аутентификацию и целостность данных. Особое внимание будет уделено архитектуре систем защиты информации, способам их построения и взаимодействия компонентов. В результате изучения темы студент будет понимать принципы работы криптографических систем и уметь описывать структуру и функции основных элементов систем защиты информации.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2	-	2	4	Собеседование
10.	**Реализация мер по идентификации и аутентификации пользователей** Тема охватывает разработку и внедрение методов идентификации и аутентификации пользователей, включая использование логинов и паролей, биометрических данных, идентификационных карт и токенов, а также различных факторов аутентификации, таких как однофакторная, двухфакторная и многофакторная аутентификация, с целью обеспечения безопасности систем и защиты данных от несанкционированного доступа.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	

11.	**Управление доступом к информационным ресурсам объектов КИИ** Тема охватывает методы контроля и управления доступом к информационным ресурсам критически важных объектов, включая назначение и мониторинг привилегий пользователей, разграничение прав доступа и соблюдение нормативных требований для предотвращения несанкционированного доступа и обеспечения безопасности информационных систем.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	
12.	**Организация аудита безопасности объектов КИИ** Тема включает в себя процесс комплексного обследования и оценки безопасности объектов критической информационной инфраструктуры, направленный на выявление уязвимостей, проверку соответствия нормативным требованиям, анализ текущего уровня защищенности информационных систем и разработку рекомендаций по устранению выявленных недостатков для повышения уровня безопасности и минимизации рисков.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	
13	**Реагирование на компьютерные инциденты на объектах КИИ** Тема описывает комплекс мероприятий по выявлению, анализу и устранению компьютерных инцидентов на объектах критической информационной инфраструктуры, включая разработку планов реагирования, взаимодействие с уполномоченными органами, своевременное информирование о нарушениях, принятие мер по ликвидации последствий атак и обеспечение непрерывности функционирования систем в условиях инцидентов.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	

14	**Применение антивирусной защиты и средств предотвращения вторжений** Тема охватывает использование комплексного подхода к обеспечению безопасности информационных систем, включающего установку антивирусного ПО, применение систем обнаружения и предотвращения вторжений, анализ сетевого трафика, мониторинг поведения устройств и пользователей, а также реализацию мер по защите от вредоносного ПО и несанкционированного доступа для повышения уровня кибербезопасности и минимизации рисков кибератак.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	
15	**Обеспечение целостности и доступности информации на объектах КИИ** Тема охватывает комплекс организационных и технических мер, направленных на защиту информации на объектах критической информационной инфраструктуры, включая предотвращение несанкционированного доступа, модификацию или уничтожение данных, обеспечение непрерывного функционирования систем, восстановление после инцидентов, а также контроль и мониторинг процессов для поддержания целостности и доступности критически важной информации.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	
16	**Защита технических средств и каналов передачи данных** Тема включает в себя совокупность методов и средств, направленных на обеспечение безопасности технических устройств и каналов передачи данных, включая криптографическую защиту, межсетевое экранирование, фильтрацию трафика и использование сертифицированных средств защиты для предотвращения несанкционированного доступа, перехвата и модификации информации при её передаче, а также создание единой точки управления системой защиты всей корпоративной сети.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	

17	**Оценка эффективности системы обеспечения ИБ на объектах КИИ** Тема охватывает процесс анализа и измерения уровня защищенности информационных систем на объектах критической информационной инфраструктуры, включающий оценку выполнения требований безопасности, мониторинг защищенности от актуальных угроз, расчет показателей защищенности, таких как Кзи, и разработку рекомендаций по улучшению мер безопасности для достижения необходимого уровня защиты и соответствия нормативным требованиям.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	
18	**Ознакомление с нормативно-правовой базой в области защиты КИИ** Тема включает изучение совокупности федеральных законов, постановлений и приказов, регулирующих деятельность в сфере защиты критической информационной инфраструктуры, определяющих обязанности субъектов КИИ, требования к обеспечению безопасности информационных систем, порядок категорирования объектов, взаимодействие с государственными органами, такими как ФСТЭК и ФСБ, а также меры ответственности за нарушение установленных требований.	ПК-1 ИД-1ПК-1, ИД-2ПК-1, ИД-3ПК-1, ИД-4ПК-1, ИД-5ПК-1, ИД-6ПК-1, ПК-2 ИД-1ПК-2, ИД-2ПК-2, ИД-3ПК-2,	2		2	4	
	ИТОГО за 9 семестр		36	-	36	72	
	ИТОГО		36	-	36	72	

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. Нестеров С.А.
    Основы информационной безопасности Электронный ресурс : учебное пособие / Нестеров С.А. - Основы информационной безопасности,2021-03-25. - Санкт-Петербург : Санкт-Петербургский политехнический

8.1.2. Перечень дополнительной литературы:

1. 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
2. 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 «Обеспечение информационной безопасности на объектах критической информационной инфраструктуры». 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	https://www.garant.ru/
2	http://www.consultant.ru/

Программное обеспечение:

1.	Альт Рабочая станция 10
2.	Альт Рабочая станция К
3.	Альт «Сервер»
4.	Пакет офисных программ - Р7-Офис

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.
Лабораторная работа	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.