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
Управление информационной безопасностью

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 В.С. доцент кафедры
вычислительной математики и
кибернетики.

Ставрополь 2026 г.

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Управление информационной безопасностью» является выработка у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» навыков по обнаружению, оповещению об инцидентах информационной безопасности и их оценки; обучение реагировать на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и восстановления после негативных воздействий; анализ инцидентов информационной безопасности, введение превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

Задачи освоения дисциплины:

1. обнаруживать события информационной безопасности и эффективно их обрабатывать, также определять относятся или не относятся данные события к инцидентам информационной безопасности;
2. давать оценку инцидентам информационной безопасности;
3. минимизировать воздействие инцидентов информационной безопасности на защищенные автоматизированные системы управления.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к части, формируемой участниками образовательных отношений дисциплинам (модулям) обязательной части. Ее освоение происходит в А 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
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1ОПК-6 Нормативно-правовые механизмы лицензирования, сертификации и аттестации; принципы организационного обеспечения информационной безопасности; основные угрозы информационной безопасности на объекте (в организации); порядок организации службы безопасности на объекте; типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; роль персонала в обеспечении информационной безопасности на объекте; основы организационной защиты информации, ее современные проблемы и терминологию; основные	Разработал и описал детальный проект по обеспечению информационной безопасности согласно нормативно-правовым механизмам лицензирования, сертификации и аттестации; принципам организационного обеспечения информационной безопасности; основным документам по обеспечению режима и конфиденциальности на объекте; основным документам, регламентирующим

	руководящие документы по обеспечению режима и конфиденциальности на объекте; основные документы, регламентирующие организационную безопасность на объекте.	организационную безопасность на объекте. Учитывая основные угрозы информационной безопасности на объекте (в организации); порядок организации службы безопасности на объекте; типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; роль персонала в обеспечении информационной безопасности на объекте; основы организационной защиты информации, ее современные проблемы и терминологию
	ИД-2ОПК-6 Эффективно применять знания теории и методики курса при раскрытии компьютерных преступлений, при работе с конфиденциальной информацией и государственной тайной, при работе с организационно-правовым обеспечением, при работе с ЭП, при защите авторского и международного права, при проведении экспертизы преступлений в сфере компьютерной информации; применять нормативно-правовые акты при защите информации; оценивать состояние организационной защиты информации на объекте	Разработал и описал детальный проект с эффективным применением знаний теории и методик курса при раскрытии компьютерных преступлений, при работе с конфиденциальной информацией и государственной тайной, при работе с организационно-правовым обеспечением, при работе с ЭП, при защите авторского и международного права, при проведении экспертизы преступлений в сфере компьютерной информации. Проект должен соответствовать нормативно-правовым актам по защите информации. Предоставлен отчёт с детальным анализом и оценкой состояния организационной защиты информации на объекте.
	ИД-3ОПК-6 Способностью при решении профессиональных задач организовывать защиту информации ограниченного доступа вавтоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному	Предоставляет детальный отчёт с демонстрацией способности при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами

	контролю.	Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	ИД-1ОПК-7.3 Способен определять требования по безопасности, предъявляемые к разрабатываемому программному обеспечению.	Предоставляет детальный отчёт с демонстрацией способности определять требования по безопасности, предъявляемые к разрабатываемому программному обеспечению.
	ИД-2ОПК-7.3 Формулирует основные угрозы безопасности информации и модели нарушителя в информационных системах.	Предоставляет детальный отчёт с демонстрацией основных угроз безопасности информации и модели нарушителя в информационных системах.
	ИД-3ОПК-7.3 Способен создавать и реализовывать план внедрения процесса разработки безопасного программного обеспечения.	Предоставляет детальный отчёт с демонстрацией способности создавать и реализовывать план внедрения процесса разработки безопасного программного обеспечения.

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	0
Самостоятельная работа	36
Формы контроля	
Экзамен **семестр А**	54
Зачет	-
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	**Введение в дисциплину "Управление Информационной безопасностью". Основные понятия. Анализ задач управления АИС и информационной безопасностью.** В данной теме студентам предстоит изучить основы курса «Управление информационной безопасностью», особое внимание будет уделено ключевым понятиям, определениям и задачам в области ИБ. В конце изучения темы студент будет знать, что представляет собой управление информационной безопасностью и каковы его цели.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4.0	2,0	Собеседование
2	**Общие положения менеджмента инцидентов информационной безопасности. Анализ задач управления АИС и информационной безопасностью.** В данной теме студентам предстоит изучить общие положения менеджмента инцидентов информационной безопасности, особое внимание будет уделено основным этапам процесса реагирования и основным функциям участников. В конце изучения темы студент будет знать структуру и принципы организации управления ИБ-инцидентами.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	2,0	2,0	Собеседование

3	**Преимущества структурного подхода и ключевые вопросы менеджмента инцидентов информационной безопасности автоматизированных систем управления. Анализ задач управления АИС и информационной безопасностью.** В данной теме студентам предстоит изучить преимущества структурного подхода и ключевые вопросы менеджмента инцидентов информационной безопасности автоматизированных систем управления, особое внимание будет уделено подходам к формализации процессов реагирования. В конце изучения темы студент будет знать, как структурный подход позволяет повысить эффективность управления инцидентами в АСУ.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	2,0	2,0	Собеседование
4	**Причины инцидентов информационной безопасности. Реализация системы управления средствами безопасности** В данной теме студентам предстоит изучить причины инцидентов информационной безопасности, особое внимание будет уделено техническим, организационным и человеческим факторам. В конце изучения темы студент будет знать основные источники возникновения инцидентов ИБ.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	2,0	2,0	Собеседование
5	**Основные инциденты информационной безопасности. Реализация системы управления средствами безопасности** В данной теме студентам предстоит изучить основные инциденты информационной безопасности, особое внимание будет уделено классификации и примерам типичных инцидентов в защищённых системах. В конце изучения темы студент будет знать, какие виды инцидентов ИБ наиболее распространены и как они распознаются.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование
6	**Планирование и подготовка менеджмента инцидентов информационной безопасности защищенных автоматизированных систем управления. Реализация системы управления средствами безопасности** В данной теме студентам предстоит изучить процессы планирования и подготовки менеджмента инцидентов информационной безопасности защищённых автоматизированных систем управления, особое внимание будет уделено процедурам выработки стратегий и распределения обязанностей. В конце изучения темы студент будет знать, как организуется предварительная подготовка к возможным инцидентам.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	2,0	2,0	Собеседование

7	**Программа менеджмента инцидентов информационной безопасности. Технология анализа защищенности** В данной теме студентам предстоит изучить программу менеджмента инцидентов информационной безопасности, особое внимание будет уделено структуре документа, его целям, задачам и механизмам реализации. В конце изучения темы студент будет знать, как составляется и используется программа управления ИБ-инцидентами.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование
8	**Планирование и подготовка менеджмента инцидентов. Этап "Использование". Технология анализа защищенности** В данной теме студентам предстоит изучить этап "Использование" в процессе планирования и подготовки менеджмента инцидентов, особое внимание будет уделено реагированию на инциденты и задействованию ресурсов. В конце изучения темы студент будет знать действия, необходимые на этапе непосредственного использования плана реагирования.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование
9	**Обнаружение и оповещение о событиях информационной безопасности защищенных автоматизированных систем управления. Технология анализа защищенности** В данной теме студентам предстоит изучить процессы обнаружения и оповещения о событиях информационной безопасности защищённых автоматизированных систем управления, особое внимание будет уделено средствам мониторинга и каналам передачи информации. В конце изучения темы студент будет знать, как осуществляется оперативное выявление и фиксация событий ИБ.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	2,0	2,0	Собеседование
10	**Планирование и подготовка менеджмента инцидентов. Элементы обобщенной модели взаимодействия ПДС. Технология анализа защищенности.** В данной теме студентам предстоит изучить общие аспекты планирования и подготовки менеджмента инцидентов, особое внимание будет уделено процессам управления рисками, выработке политик и созданию инструкций. В конце изучения темы студент будет знать базовые действия, формирующие основу системы реагирования.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование

11	**Планирование и подготовка менеджмента инцидентов. Этап “Анализ”. Элементы обобщенной модели взаимодействия ПДС** В данной теме студентам предстоит изучить этап “Анализ” в планировании и подготовке менеджмента инцидентов, особое внимание будет уделено процедурам оценки причин, последствий и уязвимостей. В конце изучения темы студент будет знать, как проводится анализ инцидентов и выработка рекомендаций по их предотвращению.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование
12	**Планирование и подготовка менеджмента инцидентов. Этап “Улучшение”. Элементы обобщенной модели взаимодействия ПДС.** В данной теме студентам предстоит изучить этап “Улучшение” в рамках менеджмента инцидентов, особое внимание будет уделено методам оценки эффективности и внедрению корректирующих мер. В конце изучения темы студент будет знать, как совершенствуется система управления ИБ-инцидентами на основе полученного опыта.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	2,0	2,0	Собеседование
13	**Планирование и подготовка менеджмента инцидентов. Этап “Внедрение”** В данной теме студентам предстоит изучить этап “Внедрение” менеджмента инцидентов, особое внимание будет уделено развертыванию политик, регламентов и организационных решений в защищённой инфраструктуре. В конце изучения темы студент будет знать, как происходит практическое внедрение системы реагирования в АС.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование
14	**Определение уровня информационной безопасности АС.** В данной теме студентам предстоит изучить методы определения уровня информационной безопасности автоматизированных систем, особое внимание будет уделено подходам к комплексной оценке защищенности. В конце изучения темы студент будет знать, как проводится анализ уровня ИБ в АС.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование

15	**Определение уровня информационной безопасности АС с использованием общих показателей ИБ.** В данной теме студентам предстоит изучить определение уровня информационной безопасности АС с использованием общих показателей ИБ, особое внимание будет уделено методике расчёта и интерпретации результатов. В конце изучения темы студент будет знать, как общие показатели используются для оценки состояния ИБ.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	2,0	2,0	Собеседование
16	**Определение уровня информационной безопасности АС с использованием частных показателей ИБ.** В данной теме студентам предстоит изучить определение уровня информационной безопасности АС с использованием частных показателей ИБ, особое внимание будет уделено оценке конкретных аспектов защищенности, включая уязвимости и меры защиты. В конце изучения темы студент будет знать, как с помощью частных показателей анализируются отдельные элементы системы ИБ.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	2,0	-	4,0	2,0	Собеседование
17	**Подготовка к экзамену по дисциплине: “Управление информационной безопасностью”.** В данной теме студентам предстоит подготовка к экзамену по дисциплине “Управление информационной безопасностью”, особое внимание будет уделено обобщению полученных знаний, повторению ключевых тем и отработке практических задач. В конце изучения темы студент будет готов продемонстрировать понимание теоретических и прикладных аспектов управления ИБ.	ОПК-6, ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК6 ОПК-7.3 ИД-1ОПК-7.3 ИД-2ОПК-7.3 ИД-3ОПК-7.3	4,0	-	4,0	4,0	Собеседование
	ИТОГО за А семестр		**36.0**	**-**	**54.0**	**36.0**	
	ИТОГО		**36.0**	**-**	**54.0**	**36.0**	

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. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482 (дата обращения: 04.05.2026). — Режим доступа: для авториз. пользователей.

2. Поздняк, И. С. Управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2023. — 104 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463619 (дата обращения: 04.05.2026). — Режим доступа: для авториз. пользователей.

8.1.2. Перечень дополнительной литературы:

1. Пелешенко, В. С. (СКФУ).
    Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина ; Сев.-Кав. федер. ун- т. - Ставрополь : СКФУ, 2016. - 86 с.

2. Шилов, А. К.
    Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего

образования РФ ; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; Институт компьютерных технологий и информационной безопасности. - Ростов-на-Дону|Таганрог : Издательство Южного федерального университета, 2018. - 121 с. : ил. - http://biblioclub.ru/. - Библиогр.: с. 81-82. - ISBN 978-5-9275-

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

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Управление информационной безопасностью». Ставрополь : СКФУ, 2026.
2. Методические указания к практическим занятиям по дисциплине «Управление информационной безопасностью». Ставрополь : СКФУ, 2026.

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

www.biblioclub.ru - Электронная библиотечная система «Университетская библиотека онлайн»

www.eLibrary.ru - Научная электронная библиотека

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.
Лабораторные 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.