Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Дата подписания: 17.06.2026 16:06:56
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c81619d42de79a7

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
Т.А. Гробова
Ф.И.О.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Организационно-правовое обеспечение информационной безопасности

Направление подготовки	10.04.01 «Информационная безопасность»
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	Очная
Реализуется в семестре	1

Разработано
доцент кафедры
(должность разработчика)
Ванина А.Г.
Ф.И.О.

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины «Организационно-правовое обеспечение информационной безопасности» является формирование профессиональной компетенции будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем» для осуществления деятельности в области защиты киберфизических систем, а также создания новых объектов киберфизических систем, а также теоретическая и практическая подготовленность магистра для проведения работ по обеспечению организационной и правовой безопасности информации в соответствии с современными требованиями.

Основными задачами дисциплины является:

– изучение основ правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизмы их реализации;

– изучение основных понятий и видов защищаемой информации, согласно законодательству РФ;

– изучение основ правового регулирования отношений в области государственной тайны, конфиденциальной информации и интеллектуальной собственности, методов и способов защиты такой информации;

– изучение сущности и содержания организационных мероприятий по защите информации;

– обучение студентов основам расследования преступлений в информационной и компьютерной сферах;

– приобретение студентами знаний, умений и практических навыков по правовому и организационному обеспечению защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Организационно-правовое обеспечение информационной безопасности» Б1.В.04) относится к дисциплинам части, формируемой участниками образовательных тношений. Её освоение происходит в 1 семестре.

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

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	ИД-1 ПК-3 состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	Имеет понимание состава и порядка функционирования системы управления информационной безопасностью киберфизических систем
	ИД-2 ПК-3 анализ уязвимости и построение модели угроз для киберфизических систем	Умеет строить модель угроз для киберфизических систем
	ИД-3 ПК-3 выбора и реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	Владеет навыками реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем

	ИД-4 ПК-3 осуществляет анализ предложений по совершенствованию системы управления информационной безопасностью киберфизических систем	Перечисляет и кратко характеризует основные нормативные документы, определяющие требования к системе управления информационной безопасностью киберфизических систем

4 Объем учебной дисциплины (модуля) и формы контроля *

Объем занятий: всего: 4 з.е. 144 акад.ч.	ОФО, в акад. часах
Контактная работа:	72
Лекции/из них практическая подготовка	36
Лабораторных работ/из них практическая подготовка	-
Практических занятий/из них практическая подготовка	36
Самостоятельная работа	18
Формы контроля	
Экзамен	54

* Дисциплина (модуль) предусматривает применение электронного обучения, дистанционных образовательных технологий *(если иное не установлено образовательным стандартом)*

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества 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	Лабораторные		
1 семестр							
1	Государственная система защиты информации Российской Федерации 1. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции 2. Элементы государственной системы защиты информации в Российской Федерации. Федеральная служба безопасности 3. Элементы государственной системы защиты информации в Российской Федерации. Федеральная служба по техническому и экспортному контролю	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	2.00	Собеседование
2	Организационные системы обеспечения безопасности информации 1. Основные принципы и условия организационной защиты информации 2. Основные подходы и требования к организации системы защиты информации 3. Основные силы и средства, используемые для организации защиты информации ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-			
3	Концептуальные положения организационного обеспечения информационной безопасности 1. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации 2. Основные направления, принципы и условия организационной защиты информации	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-		

	3. Угрозы информационной безопасности объекта 4. Организационные источники и каналы утечки информации 5. Модели нарушителей информационной безопасности на объекте						
4	Организация службы безопасности объекта 1. Основные функции, задачи и особенности службы безопасности объекта 2. Принципы организации службы безопасности объекта 3. Типовая структура службы безопасности 4. Основные документы, регламентирующие деятельность службы безопасности объекта	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	2.00	Собеседование
5	Структура и деятельность службы безопасности 1. Основные функции службы безопасности объекта 2. Способы и формы участия сотрудников в организационной защите информации 3. Способы и формы взаимодействия службы безопасности объекта с контрразведывательными и правоохранительными органами 4. Подразделения службы безопасности объекта	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-		
6	Организация охраны объектов 1. Виды и способы охраны 2. Организация пропускного и внутриобъектового режима 3. Требования к помещениям, в которых циркулирует защищаемая информация 4. Пропуск сотрудников, посетителей на объект и в выделенные (категорированные) помещения. обеспечение режима в выделенных помещениях ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-			
7	Технологические меры поддержания информационной безопасности объектов 1. Специальные технические средства охраны. охрана периметра 2. Технические средства видеонаблюдения объекта 3. Оружие, используемое для охраны объектов. индивидуальная защита от оружия нападения 4. Противопожарная охрана	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-		
8	Организация контрольно-пропускного режима 1. Общие положения организации контрольно-пропускного режима 2. Подготовка исходных данных для разработки контрольно-пропускного режима. разработка инструкции о пропускном режиме 3. Атрибутные и биометрические идентификаторы людей. виды пропусков 4. Оборудование КПП. порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	2.00	Собеседование
9	Правовые механизмы информационной безопасности Российской Федерации 1. Развитие права в сфере информационной безопасности 2. Предмет информационного права в информационной безопасности 3. Общая характеристика законодательства Российской Федерации в области информационной безопасности	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	2.00	Собеседование

10	Правовое регулирование отдельных видов информации 1. Правовое обеспечение защиты государственной тайны 2. Система защиты государственной тайны 3. Правовое обеспечение защиты банковской, профессиональной и служебной тайны 4. Правовое обеспечение защиты коммерческой тайны 5. Правовое обеспечение защиты персональных данных 6. Правовое обеспечение защиты интеллектуальной собственности 7. Правовая охрана и защита патентного и авторского права	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	4.00	4.00	-		
11	Правовое регулирование деятельности по защите информации 1. Документы Гостехкомиссии России. Единые критерии, стандарты. Общая характеристика «Руководящих документов Гостехкомиссии России» 2. Общие сведения об «Единых критериях безопасности информационных технологий» и ГОСТ Р ИСО\МЭК 15408 3. Характеристика основных положений «Единых критериев» 4. Анализ требований безопасности компонентов автоматизированных систем в рамках «Единых критериев»	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	2.00	Собеседование
12	Нарушения правового характера в сфере информационной безопасности 1. Понятие компьютерных преступлений и их классификация 2. Способы совершения компьютерных преступлений	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-		
13	Правовые основы и особенности расследования преступлений в сфере информационной безопасности 1. Раскрытие понятий, виды и элементы состава преступления 2. Характеристика международного и российского законодательства в сфере информации, информатизации и защиты информации 3. Уголовно-правовая характеристика преступлений в сфере компьютерной информации	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	4.00	Собеседование
14	Борьба с компьютерными преступлениями 1. Классификация компьютерных преступлений 2. Криминалистическая характеристика преступлений в сфере компьютерной информации 3. Возможности использования специальных познаний в ходе расследования преступлений в сфере компьютерной информации 4. Виды судебных экспертиз, проводимых по делам о преступлениях в сфере компьютерной информации 5. Задачи, решаемые в ходе компьютерных экспертиз	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	2.00	Собеседование
15	Административная и уголовная ответственность в сфере в сфере информационной безопасности 1. Административная ответственность за правонарушения в сфере информационной безопасности 2. Уголовная ответственность за правонарушения в сфере информационной безопасности 3. Выявление компьютерных преступлений 4. Методики проведения следственных действий по расследованию компьютерных	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-		

	преступлений						
16	Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию 1. Общие принципы лицензирования деятельности в области защиты информации 2. Порядок лицензирования деятельности предприятий в области защиты информации, подлежащих лицензированию ФСБ России 3. Порядок лицензирования деятельности предприятий в области защиты информации, подлежащих лицензированию ФСТЭК России	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-	2.00	Собеседование
17	Порядок сертификации средств защиты информации 1. Общие сведения о сертификации средств защиты информации 2. Положение о сертификации средств защиты информации 3. Порядок проведения сертификации средств защиты информации по требованиям безопасности информации 4. Аттестация объектов информатизации в области защиты информации	ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	2.00	2.00	-		
	ИТОГО за 1 семестр		36.00	36.00	-	18.00	
	ИТОГО		36.00	36.00	-	18.00	

6. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю) «Организационно-правовое обеспечение информационной безопасности» базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля). 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;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины (модуля).

ФОС является приложением к данной программе дисциплины (модуля).

Описание шкалы оценивания

Рейтинговой системы оценивания не предусмотрена. Оценивание осуществляется по 5-ти балльной шкале в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента не предусмотрена. Оценивание осуществляется по 5-ти балльной шкале

Промежуточная аттестация в форме экзамена в 1 семестре.

7. Методические указания для обучающихся по освоению дисциплины

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

Дисциплина (модуль) 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, необходимой для освоения дисциплины (модуля)

8.1.1. Перечень основной литературы:

1. Аверченков В.И. Служба защиты информации: организация и управления: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 186 с. - ISBN 978-5-9765-1271-9. - Текст: электронный
2. Аверченков В.И. Защита персональных данных в организации: монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 124 с. - ISBN 978-5-9765-1273-3. - Текст: электронный
3. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва: Издательство Юрайт, 2022. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8.

8.1.2. Перечень дополнительной литературы:

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для. студ. учреждений сред. проф. образования / Е. Б. Белов, В. Н. Пржегорлинский. М.: Издательский центр «Академия», 2017. -336 с.

2. Солодянников А.В. Международные и российские акты и стандарты по информационной безопасности: учебное пособие / А.В. Солодянников. – СПб.: Изд-во СПбГЭУ, 2017. – 87 с.
3. Рагозин Ю.Н., Мельник В.А. Организация и управление подразделением защиты информации на предприятии: Учебное пособие / Ю.Н. Рагозин, В.А. Мельник – СПб: Издательский центр «Интермедия», 2019. – 240 с.
4. Ковалева Н.Н. Информационное право: учебник для вузов / Н.Н. Ковалева [и др.]; под редакцией Н. Н. Ковалевой. – Москва: Издательство Юрайт, 2022. – 353 с. – (Высшее образование). – ISBN 978-5-534-13786-6.
5. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст: электронный

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

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Организованное и правовое обеспечение информационной безопасности»
2. Методические рекомендации по практическим занятиям студентов по учебной дисциплине «Организованное и правовое обеспечение информационной безопасности»
3. Привалов А.А. Организованное и правовое обеспечение информационной безопасности: Учебно-методическое пособие к практической работе. -М.: РУТ(МИИТ), 2018. - 58 с.

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

1	Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/
2	Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/
3	Официальный сайт Федерального агентства по техническому регулированию и метрологии (Росстандарт). – URL: http://www.gost.ru/wps/portal/
4	Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/
5	Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/
6	Интернет портал Защита-информации.SU http://www.iso27000.ru/
7	Научная электронная библиотека eLIBRARY.RU http://elibrary.ru
8	Консорциум сетевых электронных библиотек ЭБС «Лань» https://e.lanbook.com/
9	ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/
10	ЭБС IPR SMART https://www.iprbookshop.ru/
11	ЭБС Znanium https://znanium.com/
12	ЭБС «Юрайт» http://www.biblio-online.ru
13	Поисковые интернет-системы Яндекс, Rambler, Google и др.

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

При чтении лекций используется компьютерная техника, демонстрация презентационных мультимедийных материалов, программное обеспечение для проведения веб-конференции.

При проведении практических занятий используются информационно-справочные системы, интерактивная доска для совместной работы команд и сервис для совместной работы.

При реализации дисциплины с применением электронного обучения и дистанционных образовательных технологий материал может размещаться в системе электронного обучения.

Для обеспечения удаленного доступа, в том числе в случае применения электронного обучения, дистанционных образовательных технологий, используется программное обеспечение для проведения

веб-конференции, виртуализации рабочих столов и система электронного обучения.

Информационные справочные системы:

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

1	Государственный реестр сертифицированных средств защиты информации https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00
2	Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/588-perechen-ispytatelnykh-laboratorij-n-ross-ru-0001-01bi00
3	Реестр операторов, осуществляющих обработку персональных данных https://pd.rkn.gov.ru/operators-registry/operators-list/
4	Common Vulnerabilities and Exposures/ База данных общеизвестных уязвимостей информационной безопасности https://cve.mitre.org/
5	MITRE ATT&CK® база знаний о тактике и методах противника https://attack.mitre.org/

Программное обеспечение:

1	Интерактивная онлайн-доска для совместной работы команд https://workspace.vk.ru/
2	Открытое программное обеспечение для проведения веб-конференции МТС Линк https://mts-link.ru/
3	Платформа для создания онлайн-курсов https://el.ncfu.ru/
4	Российский пакет офисных приложений Р7-Офис https://r7-office.ru/
5	Сервис для совместной работы TEAMLY https://teamly.ru/
6	Альт виртуализация https://www.basealt.ru/alt-virtualization
7	Продукт Positive Technologies – Система MaxPatrol https://www.ptsecurity.com/ru-ru/products/mp8/

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

Материально-техническая база обеспечивает проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, научно-исследовательской работы обучающихся (переносной ноутбук, переносной проектор, компьютеры с необходимым программным обеспечением и выходом в интернет).

Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа, оснащенная оборудованием и техническими средствами обучения: доска магнитно-маркерная, проектор, компьютер с необходимым комплектом лицензионного программного обеспечения.
Практические занятия	Учебная аудитория, оснащенная средствами вычислительной техники, обеспечивающая практическую подготовку в соответствии с направленностью (профилем) программы магистратуры «Информационная безопасность киберфизических систем». Лаборатория на 15 посадочных мест, в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации, в том числе, отечественного производства.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с подключением к сети «Интернет» с необходимым комплектом лицензионного программного обеспечения и доступом в электронную информационно-образовательную среду 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 Минобрнаки 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