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: 19.06.2026 15:33:13
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
Гробова Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность операционных систем

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	7

Разработано
Ляхов А.В., - доцент кафедры вычислительной математики и кибернетики

Ставрополь 2026 г.

Цель и задачи освоения дисциплины

Цель дисциплины: формирование набора универсальных и общепрофессиональных компетенций будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем

Задачи дисциплины:

- изучение назначения и функций ОС;
- приобретение навыков управления ресурсами и задачами в ОС;
- освоение администрирования ОС;
- изучение требований к защите ОС;
- изучение методов и средств разграничения доступа в ОС;
- изучение аудита в ОС;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности ОС;
- приобретение навыков эффективной и безопасной эксплуатации ОС автоматизированных систем;
- приобретение навыков эффективного применения информационно-технологических ресурсов ОС;
- формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы;
- формирование теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций

2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем» относится к дисциплинам обязательной части. Ее освоение происходит в 7 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-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ИД-1ОПК-12 Осуществляет анализ и диагностику операционных систем; выбирает оптимальные критерии оценки эффективности и надежности средств защиты операционных систем; понимает базовые принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; анализирует функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.	Предоставляет детальный отчёт с описанием операционных систем; критериев оценки эффективности и надежности средств защиты операционных систем; принципов организации и структуры подсистем защиты операционных систем семейства UNIX и Windows; функций операционных систем, основных концепций управления процессорами, памятью, вспомогательной памятью, устройствами.
	ИД-2 ОПК-12 Использует	Предоставляет детальный отчёт с

	средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивает эффективность и надёжность защиты операционных систем; планирует политику безопасности операционных систем.	демонстрацией способности использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.
	ИД-3 ОПК-12 Способен применять знания в области безопасности операционных систем при разработке автоматизированных систем.	Предоставляет детальный отчёт с демонстрацией способности применять знания в области безопасности операционных систем при разработке автоматизированных систем.
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИД-1 ОПК-13 Оценивает вероятность возникновения потенциальных угроз информационной безопасности предприятия (организации); использует методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации; определяет основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений; использует методы расследования компьютерных преступлений и инцидентов.	Предоставляет детальный отчет с полным пояснением в котором демонстрирует основные угрозы информационно й безопасности предприятия (организации), а так же методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений с использованием методов расследования компьютерных преступлений и инцидентов
	ИД-2ОПК-13 Проводит диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений; выявляет следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.	Предоставляет детальный отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений и выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.
	ИД-3ОПК-13 Способен организовывать и проводить диагностику и тестировать системы защиты информации	Предоставляет детальный отчет в которым показывает свою способность организовывать и проводить диагностику и

	автоматизированных систем, проводит анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов.	тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов.

4. Объем учебной дисциплины 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	36/0
Практических занятий/из них практическая подготовка	0
Самостоятельная работа	**108**
Формы контроля	
Экзамен	-
Зачет	-
Зачет с оценкой **7 семестр**	+
Курсовая работа	нет

***** Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий

5. Содержание дисциплины, 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 занятия	Лабораторные работы		
	7 СЕМЕСТР						
1.	**Запуск и конфигурирование ОС.** В рамках курса по запуску и конфигурированию операционных систем студенты изучают основные этапы установки ОС, настройку аппаратных и программных компонентов для обеспечения стабильной работы системы. Особое внимание уделяется конфигурации операционных систем на базе популярных платформ, таких как Windows и Linux, включая настройку сетевых интерфейсов, безопасности, учетных записей и системных служб. Студенты осваивают инструменты для оптимизации производительности, управления обновлениями и мониторинга состояния системы.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	2.00	-	2.00	8.00	Защита лабораторной работы

2.	**Управление процессами. Изучение работы системных функций** В рамках курса по управлению процессами и изучению системных функций студенты осваивают методы организации и оптимизации бизнес-процессов, а также изучают работу системных компонентов операционных систем и программных платформ. Они изучают принципы автоматизации процессов, моделирование рабочих потоков, а также инструменты контроля и управления ресурсами системы. В ходе практических занятий студенты знакомятся с системными вызовами, управлением памятью, файловыми системами, процессами и потоками, а также механизмами межпроцессного взаимодействия.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	4.00	-	4.00	10.00	Защита лабораторной работы
3.	**Команды управления процессами**. Сигналы, каналы. Взаимодействие процессов систем. В рамках дисциплины по управлению процессами студенты изучают основные команды и инструменты для контроля и управления процессами в операционных системах. Это включает работу с командами для запуска, приостановки, возобновления и завершения процессов	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	2.00	-	2.00	8.00	Защита лабораторной работы
4.	**Способы организации ввода-вывода.** Произвольный доступ к файлу. Библиотека стандартного ввода-вывода систем. Способы организации ввода-вывода (I/O) в операционных системах являются важной частью обеспечения эффективной работы программ и систем в целом. Они включают различные модели и методы взаимодействия с устройствами хранения данных и периферийными устройствами.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	4.00	-	4.00	10.00	Защита лабораторной работы

5.	**Файловая система. Доступ к файлам. Работа с файлами и каталогами. Изучение типов файлов. Поиск системных журналов систем.** В рамках данного курса/темы мы будем изучать основы файловых систем, их структуру и типы, а также механизмы доступа к файлам и каталогам. Мы познакомимся с методами создания, удаления, переименования и перемещения файлов и папок, научимся навигировать по каталогам и управлять их содержимым. Также мы разберёмся с различными типами файлов, включая обычные файлы, каталоги, символьные и жесткие ссылки, а также специальные файлы устройств.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	4.00	-	4.00	10.00	Защита лабораторной работы
6.	**Структура реестра ОС.** Изучение работы реестра систем. Изучение структуры и работы системного реестра операционных систем охватывает комплексный анализ архитектуры, функциональных возможностей и практического использования реестра как централизованной базы данных настроек ОС	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	4.00	-	4.00	10.00	Защита лабораторной работы
7.	**Изучение базовых прав доступа.** Переход в режим суперпользователя. Изучение базы данных пользователей. Добавление и удаление пользователей систем. Изучение управления пользователями и правами доступа в операционных системах охватывает ключевые аспекты администрирования учетных записей и контроля безопасности.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	2.00	-	2.00	8.00	Защита лабораторной работы
8	**Управление сетью. Сетевые службы. Изучение основных команд для работы в сети систем.** Управление сетью и сетевыми службами охватывает комплексное изучение настройки, диагностики и администрирования сетевых подключений в операционных системах	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	2.00	-	2.00	8.00	Защита лабораторной работы

9	**Обеспечение безопасности операционной системы.** Изучение программных и системных угроз и типов сетевых атак систем. Обеспечение безопасности операционной системы включает комплексное изучение программных и системных угроз, а также методов защиты от них. Основное внимание уделяется анализу вредоносного ПО (вирусы, трояны, руткиты), уязвимостей нулевого дня и эксплойтов, а также системным угрозам, таким как несанкционированный доступ, атаки на ядро ОС и цепочку загрузки (bootkit, UEFI-вирусы).	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	2.00	-	2.00	8.00	Защита лабораторной работы
10	**Архивирование. Восстановление.** Дисциплина «Архивирование и восстановление данных» изучает методы создания резервных копий информации, техники сжатия и хранения данных, а также процедуры восстановления данных в случае их потери или повреждения. Основная цель — обеспечить безопасность, целостность и доступность информации.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	2.00	-	2.00	8.00	Защита лабораторной работы
11	**Реализация простых сценариев.** Дисциплина «Архивирование и восстановление данных» изучает методы создания резервных копий, техники сжатия и хранения информации, а также процессы восстановления данных при их потере или повреждении. В рамках курса также реализуются простые сценарии резервного копирования и восстановления для закрепления практических навыков и обеспечения безопасности и целостности данных.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	4.00	-	4.00	10.00	Защита лабораторной работы
12	**Реализация сложных сценариев.** Дисциплина «Архивирование и восстановление данных» изучает методы создания резервных копий, техники сжатия и хранения информации, а также процессы восстановления данных при их потере или повреждении. В рамках курса реализуются как простые, так и сложные сценарии резервного копирования и восстановления для приобретения практических навыков обеспечения безопасности и целостности данных.	ОПК-12 ИД-1ОПК-12 ИД-2ОПК-12 ИД-3ОПК-12 ОПК-13 ИД-1ОПК-13 ИД-2ОПК-13 ИД-3ОПК-13	4.00	-	4.00	10.00	Защита лабораторной работы
	ИТОГО за 7 семестр		**36.00**	**-**	**36.00**	**108.00**	
	ИТОГО		**36.00**	**-**	**36.00**	**108.00**	

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) по дисциплине 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.

7. Методические указания для обучающихся по освоению дисциплины

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

Дисциплина «Безопасность операционных систем» построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

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

Лабораторные работы направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным 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

8.1.1. Перечень основной литературы:

1. Окороков, В. А. Безопасность операционных систем / В. А. Окороков. — Санкт-Петербург : Лань, 2024. — 228 с. — ISBN 978-5-507-48297-9.
2. Киренберг А. Г. Информационная безопасность современных операционных систем : учебное пособие / Киренберг А. Г. - Кузбасский государственный технический университет имени Т. Ф. Горбачева, 2022. - ISBN 978-5-00137-320-9.
3. Т. Б. Ларина Механизмы аппаратной поддержки операционных систем: учебное пособие для бакалавров направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : учебное пособие / Т. Б. Ларина. - Москва : Российский университет транспорта (РУТ (МИИТ)), 2021. - 109 с.
4. Т. Б. Ларина Сетевые средства операционных систем: учебное пособие для магистров направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : учебное пособие / Т. Б. Ларина. - Москва : Российский университет транспорта (РУТ (МИИТ)), 2021. - 107 с

8.1.2. Перечень дополнительной литературы:

1. Проскурин, В. Г. Защита в операционных системах : учебное пособие / В. Г. Проскурин. — Москва : Горячая линия-Телеком, 2016. — 192 с. — ISBN 978-5-9912-0379-1.

2. Виртуализация операционных систем: учебное пособие для бакалавров направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : учебное пособие / Т. Б. Ларина. - Москва : Российский университет транспорта (РУТ (МИИТ)), 2020. - 66 с.
3. Администрирование операционных систем. Управление системой: учебное пособие для студентов направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : учебное пособие / Т. Б. Ларина. - Москва : Российский университет транспорта (РУТ (МИИТ)), 2020. - 72 с.
4. Т. Б. Ларина Администрирование операционных систем. Управление системой: учебное пособие для студентов направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : учебное пособие / Т. Б. Ларина. - Москва : Российский университет транспорта (РУТ (МИИТ)), 2020. - 72 с.

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

1. Методические указания по выполнению лабораторных работ по дисциплине "Безопасность операционных систем" (электронный ресурс) – Ставрополь, СКФУ, 2026.

2. Методические указания по организации и проведению самостоятельной работы по дисциплине "Безопасность операционных систем" (электронный ресурс) – Ставрополь, СКФУ, 2026.

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

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Безопасность операционных систем»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

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

На лабораторных занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

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

1	КонсультантПлюс - 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 занятий лекционного типа укомплектована специализированной мебелью и техническими средствами обучения, служащими для представления учебной

	информации большой аудитории: ноутбук, проектор. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин.
Лабораторные[1] занятия	Помещения для проведения лабораторных и практических работ (компьютерные классы), оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета
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 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 обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины 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 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;

[1] Перечень лабораторий используемых в учебном процессе представлен https://www.ncfu.ru/sveden/objects/

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.