

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Антоновна

Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова

Дата подписания: 22.09.2026 11:01:35

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

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

УТВЕРЖДАЮ
Декан факультета математики и
компьютерных наук
имени профессора Н.И. Червякова
Т.А. Грובה

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Защита программ и данных

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)	Математическое и программное обеспечение защиты информации
Год начала обучения	2026
Форма обучения	<u>очная</u>
Реализуется в семестре	<u>1</u>

Разработано
Гусева Л.Л., доцент кафедры
вычислительной математики и кибернетики

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины

Целью изучения дисциплины «Защита программ и данных» является формирование набора профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность», содействие фундаментализации образования, развитию логического мышления, формированию научного мировоззрения.

Задачами дисциплины являются:

- формирование навыков экспертизы качества и надёжности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;
- формирование навыков анализа программных реализаций на предмет наличия недокументированных возможностей;
- развитие навыков организации антивирусной защиты.

Цели образовательного процесса достигаются посредством применения инновационных образовательных технологий в обеспечении компетентностного подхода.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита программ и данных» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, – Б1.В.ДВ.01.01. Дисциплина реализуется в 1 семестре 1 курса.

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 (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-3 Способен проводить инструментальный анализ защищённости компьютерной системы и осуществлять поиск уязвимостей программного обеспечения	ИД-2 ПК-3 выполняет анализ защищённости сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Знает правила, процедуры, практические приёмы, принципы и методы, средства обеспечения защиты информации в компьютерной системе. Умеет выполнять анализ защищённости сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей. Владеет навыками инструментального анализа защищённости
	ИД-3 ПК-3 осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения	Знает методы поиска уязвимостей и недокументированных возможностей программного обеспечения. Умеет применять инструментальные средства статического и динамического анализа. Владеет навыками оформления результатов поиска уязвимостей
ПК-4 Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ИД-3 ПК-4 выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать её автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Знает методы выявления индивидуальных признаков программы, позволяющих идентифицировать её автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы. Умеет выявлять такие признаки. Владеет навыками их документирования

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
	ИД-5 ПК-4 устанавливает участников события, их роли, места, условия, при которых была создана, модифицирована или удалена информация, устанавливает соответствие либо несоответствие действий с информацией специальному регламенту (правилам)	Знает методы определения участников события, их ролей, мест и условий, при которых была создана, модифицирована или удалена информация. Умеет устанавливать соответствие либо несоответствие действий с информацией специальному регламенту (правилам). Владеет навыками подготовки экспертного заключения

4. Объём учебной дисциплины и формы контроля

Объём занятий: всего 4 з.е., 144 акад. ч. (108 астр. ч.)	ОФО, в астр. часах
Всего часов по дисциплине (модулю)	108
Контактная работа:	54
Лекции / из них практическая подготовка	27 / 0
Лабораторных работ / из них практическая подготовка	0 / 0
Практических занятий / из них практическая подготовка	27 / 0
в том числе занятия, проводимые в интерактивной форме	13,5 (18 акад. ч.)
Самостоятельная работа	54
Часы на контроль (промежуточная аттестация)	0
Формы контроля	
Экзамен	–
Зачёт	+ (1 семестр)

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

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем / из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	
1 семестр						
1	Тема 1. Введение в теорию и практику защиты программного обеспечения. <i>Краткое содержание:</i> Программное обеспечение (ПО) как объект защиты. Угрозы безопасности ПО на этапах жизненного цикла: разработка, распространение, эксплуатация, сопровождение. Понятия уязвимости, недекларированных (недокументированных) возможностей, программной закладки. Классификация вредоносного ПО. Субъекты и объекты защиты, модель нарушителя. Нормативная база Российской Федерации в	ИД-2 ПК-3 ИД-3 ПК-3 ИД-3 ПК-4 ИД-5 ПК-4	4 / 0	4 / 0	–	8

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем / из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	
	области защиты ПО. Место дисциплины в системе обеспечения информационной безопасности.					
2	Тема 2. Основания теории и практики защиты программного обеспечения. <i>Краткое содержание:</i> Формальные модели безопасности компьютерных систем применительно к программному обеспечению. Модели программных закладок и скрытых каналов. Понятие доверенного программного обеспечения; требования доверия ФСТЭК России и уровни доверия. Жизненный цикл безопасной разработки ПО (ГОСТ Р 56939). Формальная верификация, статический и динамический анализ как основа доказательной защиты. Критерии оценки защищённости (ГОСТ Р ИСО/МЭК 15408).	ИД-2 ПК-3 ИД-3 ПК-3 ИД-3 ПК-4 ИД-5 ПК-4	4 / 0	4 / 0	–	8
3	Тема 3. Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения. <i>Краткое содержание:</i> Технологическая безопасность: контроль исходных текстов, управление сборкой, защита цепочки поставки ПО, доверенный репозиторий. Эксплуатационная безопасность: контроль целостности, разграничение доступа, изоляция процессов, доверенная загрузка, замкнутая программная среда. Средства антивирусной защиты и защиты от несанкционированного доступа. Управление уязвимостями и обновлениями; работа с банком данных угроз безопасности информации ФСТЭК России.	ИД-2 ПК-3 ИД-3 ПК-3 ИД-3 ПК-4 ИД-5 ПК-4	5 / 0	5 / 0	–	10
4	Тема 4. Защита программ от анализа и модификации. <i>Краткое содержание:</i> Статический и динамический анализ программ: дизассемблеры, отладчики, эмуляторы, средства трассировки. Методы противодействия дизассемблированию и отладке.	ИД-2 ПК-3 ИД-3 ПК-3 ИД-3 ПК-4 ИД-5 ПК-4	5 / 0	5 / 0	–	10

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем / из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	
	Обфускация кода и данных, шифрование и упаковка исполняемых модулей, самогенерируемый код. Контроль целостности и электронная подпись исполняемого кода. Защита от копирования: программные и программно-аппаратные механизмы, эмуляция ключей и методы противодействия ей. Оценка стойкости механизмов защиты.					
5	Тема 5. Исследование программного обеспечения на предмет отсутствия недекларированных возможностей. <i>Краткое содержание:</i> Требования по контролю отсутствия недекларированных возможностей, уровни контроля. Статический анализ исходных текстов: контроль полноты и отсутствия избыточности, маршрутов выполнения функциональных объектов, потоков данных. Динамический анализ: покрытие кода, трассировка, фаззинг. Инструментальные средства анализа защищённости и поиска уязвимостей. Выявление индивидуальных признаков программы и идентификация авторства кода. Оформление результатов исследования и подготовка экспертного заключения.	ИД-2 ПК-3 ИД-3 ПК-3 ИД-3 ПК-4 ИД-5 ПК-4	5 / 0	5 / 0	–	10
6	Тема 6. Краткое описание отечественных нормативных актов, регламентирующих деятельность в области защиты программного обеспечения. <i>Краткое содержание:</i> Федеральный закон «Об информации, информационных технологиях и о защите информации»; Доктрина информационной безопасности Российской Федерации. Приказы и руководящие документы ФСТЭК России, требования по безопасной разработке ПО. Национальные стандарты: ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р ИСО/МЭК 15408. Порядок сертификации средств защиты	ИД-2 ПК-3 ИД-3 ПК-3 ИД-3 ПК-4 ИД-5 ПК-4	4 / 0	4 / 0	–	8

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем / из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	
	информации. Единый реестр российских программ для ЭВМ и баз данных, требования по переходу на отечественное ПО. Ответственность за правонарушения в сфере компьютерной информации (ст. 272–274.1 УК РФ).					
ИТОГО за 1 семестр			27 / 0	27 / 0	–	54
ИТОГО по дисциплине (модулю), астр. ч.			54			54

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) «Защита программ и данных» 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 рабочей программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

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

Дисциплина (модуль) построена по тематическому принципу, каждая тема представляет собой логически завершённый раздел.

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

Самостоятельная работа обучающихся направлена на самостоятельное изучение дополнительного материала, подготовку к практическим занятиям, а также выполнение 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. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С.

Забабурин. – Москва : Издательство Юрайт, 2023. – 312 с. – (Высшее образование). – ISBN 978-5-9916-9043-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: <https://urait.ru/bcode/491249>

2. Проскурин, В. Г. Защита программ и данных : учеб. пособие для вузов / В. Г. Проскурин. – М. : Академия, 2012. – 208 с. – (Высшее профессиональное образование. Бакалавриат). – Гриф: Доп. УМО. – Библиогр.: с. 195–196. – ISBN 978-5-7695-9288-1

3. Хаулет, Т. Инструменты безопасности с открытым исходным кодом / Т. Хаулет. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 566 с. – (Основы информационных технологий). – ISBN 978-5-94774-629-7

8.1.2. Перечень дополнительной литературы:

1. Девянин, П. Н. Модели безопасности компьютерных систем : учебное пособие / П. Н. Девянин. – М. : Академия, 2005. – 144 с. – (Высшее профессиональное образование). – Библиогр.: с. 139

2. Хаулет, Т. Защитные средства с открытыми исходными текстами : практическое руководство по защитным приложениям : учебное пособие / Т. Хаулет. – Москва : БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2007. – 608 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 978-5-9556-0087-1

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

Методические указания по организации самостоятельной работы и выполнению практических работ по дисциплине «Защита программ и данных» для обучающихся по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Математическое и программное обеспечение защиты информации» (электронный документ).

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

1. <http://catalog.ncfu.ru/catalog/ncfu> – Электронный каталог научной библиотеки СКФУ.

2. <http://biblioclub.ru> – ЭБС «Университетская библиотека онлайн».

3. <https://urait.ru> – Образовательная платформа «Юрайт».

4. <https://bdu.fstec.ru> – Банк данных угроз безопасности информации ФСТЭК России.

5. <https://fstec.ru> – Официальный сайт ФСТЭК России (нормативные и методические документы).

6. <https://reestr.digital.gov.ru> – Единый реестр российских программ для электронных вычислительных машин и баз данных.

7. <https://safe-surf.ru> – Национальный координационный центр по компьютерным инцидентам.

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

При осуществлении образовательного процесса по дисциплине используются технологии электронного обучения на базе электронной информационно-образовательной среды СКФУ, мультимедийные технологии представления учебного материала, технологии совместной работы с документами. На практических занятиях обучающиеся представляют презентации, подготовленные ими в часы самостоятельной работы.

9.1. Российское программное обеспечение, включённое в Единый реестр российских программ для ЭВМ и баз данных:

1. Операционная система Astra Linux Special Edition (ООО «РусБИТех-Астра»), реестровая запись № 369.
2. Операционная система «РЕД ОС» (ООО «РЕД СОФТ»).
3. Офисный пакет «Р7-Офис. Профессиональный (десктопная версия)» (АО «Р7») / «МойОфис Стандартный» (ООО «Новые облачные технологии»).
4. Kaspersky Endpoint Security для бизнеса (АО «Лаборатория Касперского») – средство антивирусной защиты.
5. Dr.Web Enterprise Security Suite (ООО «Доктор Веб») – средство антивирусной защиты.
6. «Сканер-ВС» (АО «НПО «Эшелон») – средство анализа защищённости и поиска уязвимостей.
7. Программно-аппаратный комплекс «АК-ВС 3» (АО «НПО «Эшелон») – средство контроля отсутствия недеklarированных возможностей и анализа исходных текстов программ.
8. AppChecker (АО «НПО «Эшелон») – статический анализатор исходного кода.
9. PT Application Inspector (АО «Позитив Текнолоджиз») – средство анализа защищённости приложений.
10. Solar appScreener (ГК «Солар») – средство статического и бинарного анализа кода.
11. Secret Net Studio (ООО «Код Безопасности») – средство защиты информации от несанкционированного доступа.
12. КриптоПро CSP (ООО «КРИПТО-ПРО») – средство криптографической защиты информации.
13. ViPNet CSP / ViPNet Client (АО «ИнфоТеКс») – средства криптографической и сетевой защиты информации.

9.2. Свободно распространяемое программное обеспечение, используемое в учебных целях:

1. HxD – шестнадцатеричный редактор.
2. x64dbg – отладчик приложений пользовательского режима.
3. Cutter (radare2) – среда обратной разработки и дизассемблирования.
4. Detect It Easy (DIE) – средство определения типа упаковщика и компилятора исполняемых файлов.

9.3. Информационные справочные и информационно-правовые системы:

1. Справочная правовая система «КонсультантПлюс» (ООО «КонсультантПлюс»), реестровое российское ПО.
2. Информационно-правовое обеспечение «Гарант» (ООО «НПП «Гарант-Сервис»), реестровое российское ПО.
3. Банк данных угроз безопасности информации ФСТЭК России (<https://bdu.fstec.ru>).
4. Единый реестр российских программ для ЭВМ и баз данных Минцифры России (<https://reestr.digital.gov.ru>).
5. Электронный каталог научной библиотеки СКФУ; ЭБС «Университетская библиотека онлайн»; образовательная платформа «Юрайт».

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

Вид занятий	Аудитория	Оснащение
Лекционные занятия	9-431	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: переносной ноутбук, проектор, доска магнитно-маркерная. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочей программе дисциплины
Практические занятия	9-523	Короткофокусный мультимедиа-проектор Epson EB-536Wi с настенным креплением ELPMB45 и набором кабелей

Вид занятий	Аудитория	Оснащение
	9-429	Монитор ЖК 21,5" DELL E2216H (TN, VGA, DP, 1920×1080); персональные компьютеры с установленным отечественным программным обеспечением и доступом к сети «Интернет»
Самостоятельная работа	9-410	ПК преподавателя Dell OptiPlex 3040 i3-6100 3.7 ГГц, 4 ГБ DDR3L 1600 МГц, 500 ГБ, GMA HD 440, DVD+RW, с клавиатурой со считывателем смарт-карт и телефонно-микрофонной гарнитурой
	9-302	Тонкий клиент Dell Wyse 5030 для систем виртуализации рабочих столов на базе VMWare Horizon с аппаратной реализацией протокола PCoIP, с монитором DELL E2416H, клавиатурой со считывателем смарт-карт и телефонно-микрофонной гарнитурой

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде образовательной организации. Материально-техническая база обеспечивает проведение всех видов дисциплинарной и междисциплинарной подготовки, а также научно-исследовательской работы обучающихся.

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 (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 учётом 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, оказывающего обучающемуся необходимую техническую помощь с учётом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть 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 обучающемуся для выполнения задания предоставляется увеличивающее устройство;
- 2) для лиц с ограниченными возможностями здоровья по слуху:
 - присутствие ассистента, оказывающего обучающемуся необходимую техническую помощь с учётом индивидуальных особенностей;

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

– обеспечивается предоставление надлежащих звуковых средств воспроизведения информации;

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

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

– по желанию обучающегося 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.