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)
Технологии выявления следов киберпреступлений и инцидентов

Направление подготовки	10.04.01 «Информационная безопасность»
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	Очная
Реализуется в семестре	3

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

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины «Технологии выявления следов киберпреступлений и инцидентов» является формирование профессиональных компетенций 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.

Основными задачами дисциплины является теоретическое и практическое освоение основных понятий и методов работы по следующим направлениям:

– основные навыки современных технологий поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий;

– прочное усвоение слушателями фундаментальных основ современных технологий цифровой криминалистики, поиска цифровых доказательств и обеспечения кибербезопасности, практики применения данных технологий;

– совершенствование умений и навыков с учетом специализации профессиональной деятельности;

– повышения профессионального уровня в рамках имеющейся квалификации.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Технологии выявления следов киберпреступлений и инцидентов» (Б1.В.ДВ.02.02) относится к дисциплинам части, формируемой участниками образовательных отношений. Её освоение происходит в 3 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 (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-4 Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности	ИД-2 ПК-4 порядок определение уязвимости и уровня защищённости киберфизических систем	умеет определять уязвимости киберфизических систем, а также их уровень защищённости
	ИД-4 ПК-4 реализация организационно-технических мероприятия по обеспечению защиты киберфизических систем	владеет навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем
	ИД-5 ПК-4 управляет инцидентами информационной безопасности киберфизических систем	Применяет специализированное программное обеспечение для управления инцидентами кибербезопасности

4 Объем учебной дисциплины (модуля) и формы контроля *

Объем занятий: всего: 4 з.е. 144 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	36

Лабораторных работ/из них практическая подготовка	36
Практических занятий/из них практическая подготовка	-
Самостоятельная работа	72
Формы контроля	
Зачет с оценкой	+

* 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		
3 семестр							
1	Компьютерно-техническая экспертиза – виды и статусы. 1. Понятие судебной экспертизы. 2. Понятие компьютерно-технической экспертизы. 3. Понятие экспертной методики. 4. Требования законодательства к методике и методам производства экспертизы.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
2	Построение методики модели производства компьютерно-технической экспертизы. 1. Базовые критерии классификации методик компьютерно-технической экспертизы. 2. Содержание модели методики производства компьютерно-технической экспертизы. 3. Применение методов компьютерно-технической экспертизы. 4. Правила расчёта трудозатрат при производстве комплексной экспертизы. ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование	
3	Унифицированная методика производства компьютерно-технической экспертизы. 1. Стадии проведения компьютерно-технической экспертизы. 2. Формирование выводов и правила написания заключения эксперта.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
4	Методики производства компьютерно-технической экспертизы. 1. Аппаратно-компьютерная экспертиза (пример экспертизы № 1). 2. Программно-компьютерная экспертиза (пример экспертизы № 2). 3. Экспертиза данных (пример экспертизы № 3).	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование

	4. Компьютерно-сетевая экспертиза (пример экспертизы № 4).						
5	Фишинг-атаки – методы реализации и противодействия. 1. Фишинг-атака со стороны пользователя на примере электронного почтового ящика. 2. Роль социальной инженерии в фишинг-атаке. 3. Фишинг изнутри. Анализ используемых для атаки инструментов.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
6	Комбинированные атаки с использованием фишинга. 1. Подготовка к персонализированной фишинговой атаке. Некоторые специфические способы сбора информации. 2. Атака с использованием «заброса» вредоносных программ. 3. Атака с использованием маскировки под легальное программное обеспечение или файлы. 4. Атака на мобильные телефоны.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
7	Особенности киберпреступлений. 1. Мистика киберпреступности. 2. Характеристика киберпреступления, проблемы идентификации и трудности перевода. 3. Доступность инструментов анонимной связи и управления ресурсами.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
8	Противодействие и защита от различных типов киберпреступлений. 1. Правоохранительная система. 2. Некоторые национальные особенности борьбы с киберпреступлениями. 3. Традиционная защита и рыночные тенденции 4. Советы по защите информации, правила реагирования на инцидент.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
9	Обзор «Чёрного рынка» информационных услуг в РФ 1. Мобильная и стационарная связь. 2. Хищение логинов и паролей, доступ к аккаунтам. 3. Проверка различных персональных данных и данных государственных информационных систем. 4. Специальные технические устройства	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
10	Основы перехвата и анализа трафика. 1. Перехват трафика с помощью ARP-спуфинга. 2. Анализ перехваченного трафика. 3. Создание TCP-оболочек и ботнетов.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
11	Криптосистемы и программы вымогатели. 1. Криптография и программы-вымогатели. 2. Протокол TLS и алгоритм Диффи-Хеллмана.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
12	Основы социальной инженерии в киберпреступлениях. 1. Фишинг и дипфейки. 2. Сбор информации.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
13	Поиск и эксплуатация уязвимостей. 1. Поиск уязвимостей нулевого дня. 2. Создание троянов.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
14	Захват контроля над сетью: принципы и методы противодействия.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$	2.00	-	2.00	4.00	Собеседовани

	1. Проброс трафика и повышение привилегий. 2. Перемещение по корпоративной сети Windows. 3. Дальнейшие шаги по захвату контроля над сетью.	ИД-5$_{ПК-4}$					е
15	Тестирование сетей на проникновение. 1. Тестирование сетей на проникновение. 2. Обнаружение сетевых хостов.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
16	Целенаправленное проникновение. 1. Атака на уязвимые веб-сервисы. 2. Атака на уязвимые службы баз данных.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
17	Постэксплуатация и повышение привилегий как метод проникновения. 1. Эскалация привилегий. 2. Инструменты подбора пароля.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
18	Документирование следов проникновения и построение плана противодействия. 1. Очистка среды после проникновения. 2. Написание качественного отчёта о проникновении.	ИД-2$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	Собеседование
	ИТОГО за 3 семестр		36.00	-	36.00	72.00	
	ИТОГО		36.00	-	36.00	72.00	

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) «Технологии выявления следов киберпреступлений и инцидентов» 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

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. Масалков А.С. Особенности киберпреступлений: инструменты нападения и защиты информации / А.С. Масалков. – М.: ДМК Пресс, 2018. – 226 с. – ISBN 978-5-97060-651-3. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/105842 (дата обращения: 23.10.2022). – Режим доступа: для авториз. пользователей.
2. Шелупанов А.А. Форензика. Теория и практика расследования киберпреступлений: монография / А.А. Шелупанов, А.Р. Смолина. – М.: Горячая линия – Телеком, 2018. – 104 с. – ISBN 978-5-9912-0769-0.
3. Грэм Дэниел Г. Этичный хакинг. Практическое руководство по взлому.СПб.: Питер, 2022. – 384 с.: ил. – (Серия «Библиотека программиста»). ISBN 978-5-4461-1952-3
4. Дэвис Р. Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК Пресс, 2021. – 310 с.: ил. ISBN 978-5-97060-529-5

8.1.2. Перечень дополнительной литературы:

1. Уголовный кодекс РФ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.
2. Уголовно-процессуальный кодекс РФ. URL:

http://www.consultant.ru/document/cons_doc_LAW_34481/.
3. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_31871/.
4. Black Hat Python: программирование для хакеров и пентестеров. 2-е изд. – СПб.: Питер, 2022. – 256 с.: ил. – (Серия «Библиотека программиста»). ISBN 978-5-4461-3935-4
5. GHIDRA. Полное руководство / пер. с анг. А. А. Слинкина. – М.: ДМК Пресс, 2022. – 750 с.: ил.

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

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Технологии выявления следов киберпреступлений и инцидентов».
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Технологии выявления следов киберпреступлений и инцидентов».

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 Федеральной службы безопасности Российской Федерации http://www.fsb.ru/
4	Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/
5	Интернет портал Защита-информации.SU http://www.iso27000.ru/
6	Научная электронная библиотека eLIBRARY.RU http://elibrary.ru
7	Консорциум сетевых электронных библиотек ЭБС «Лань» https://e.lanbook.com/
8	ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/
9	ЭБС IPR SMART https://www.iprbookshop.ru/
10	ЭБС Znanium https://znanium.com/
11	ЭБС «Юрайт» http://www.biblio-online.ru
12	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

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