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)
Менеджмент инцидентов кибербезопасности
название дисциплины (модуля)

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

Разработано
доцент кафедры
(должность разработчика)
Орёл Д.В
Ф.И.О.

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины: 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.

Задачи освоения дисциплины:

1. Планирование системы управления инцидентами информационной безопасности;
2. Управление инцидентами отказа в обслуживании;
3. Планирование системы управления инцидентами отказа в обслуживании;
4. Управление инцидентами внедрения вредоносного кода;
5. Планирование системы управления инцидентами внедрения вредоносного кода;
6. Управление инцидентами сбора информации;
7. Планирование системы управления инцидентами сбора информации;
8. Устранение инцидента и восстановление после инцидента сбора информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Менеджмент инцидентов кибербезопасности» относится к дисциплинам части, формируемой участниками образовательных отношений.

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-3 ПК-4 выбор оптимального набора технических мер для повышения защищённости киберфизических систем	умеет выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем
	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 занятия	Лабораторные работы		
3 семестр							
1	**Система управления инцидентами кибербезопасности** 1 Инциденты кибербезопасности 2 Процессы управления инцидентами	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
2	**Планирование системы управления инцидентами информационной безопасности** 1 Формирование политики управления инцидентами информационной безопасности 2 Формирование процедур управления инцидентами информационной безопасности 3 Создание группы реагирования на инциденты информационной безопасности 4 Подготовка к обработке инцидентов 5 Формирование последовательности действий при обработке инцидентов 6 Классификация инцидентов по значимости 7 Обеспечение осведомленности и обучение управлению инцидентами	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
3	**Использование системы управления инцидентами информационной безопасности** 1 Последовательность действий при обработке инцидента	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	

	2 Обнаружение и анализ инцидента 3 Реагирование на инциденты						
4	**Анализ обработки инцидентов** 1 Изучение полученного опыт 2 Определение улучшения безопасности 3 Определение улучшения системы управления инцидентами	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
5	**Улучшение системы управления инцидентами** 1 Улучшение оценки рисков и управления информационной безопасностью 2 Улучшение безопасности 3 Улучшение системы управления инцидентами	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
6	**Управление инцидентами неавторизованного доступа** 1 Определение инцидента неавторизованного доступа 2 Цели инцидента неавторизованного доступа	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
7	**Планирование системы управления инцидентами неавторизованного доступа** 1 Подготовка к обработке инцидента 2 Выбор защитных мер 3 Формирование последовательности действий при обработке инцидентов неавторизованного доступа 4 Формирование порядка обработки инцидента неавторизованного доступа	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
8	**Использование системы управления инцидентами неавторизованного доступа** 1 Обнаружение и анализ инцидента неавторизованного доступа 2 Сдерживание инцидента неавторизованного доступа 3 Устранение инцидента неавторизованного доступа и восстановление после него 4 Сбор и обработка свидетельств инцидента неавторизованного доступа	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
9	**Управление инцидентами отказа в обслуживании** 1 Определение инцидента отказа в обслуживании 2 Примеры инцидентов отказа в обслуживании	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
10	**Планирование системы управления инцидентами отказа в обслуживании** 1 Подготовка к обработке инцидента 2 Выбор защитных мер 3 Формирование последовательности действий при обработке	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	

	инцидентов отказа в обслуживании 4 Формирование порядка обработки инцидента отказа в обслуживании						
11	**Использование системы управления инцидентами отказа в обслуживании** 1 Обнаружение и анализ инцидента отказа в обслуживании 2 Сдерживание, устранение инцидента отказа в обслуживании и восстановление после него 3 Сбор и обработка свидетельств инцидента отказа в обслуживании	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
12	**Управление инцидентами внедрения вредоносного кода** 1 Определение инцидента внедрения вредоносного кода 2 Примеры атак, связанных с внедрением вредоносного кода	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
13	**Планирование системы управления инцидентами внедрения вредоносного кода** 1 Подготовка к обработке инцидента 2 Выбор защитных мер 3 Формирование последовательности действий при обработке инцидентов внедрения вредоносного кода 4 Формирование порядка обработки инцидента внедрения вредоносного кода	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
14	**Использование системы управления инцидентами внедрения вредоносного кода** 1 Обнаружение и анализ инцидента внедрения вредоносного кода 2 Сдерживание и устранение инцидента внедрения вредоносного кода 3 Восстановление после инцидента внедрения вредоносного кода 4 Сбор и обработка свидетельств инцидента внедрения вредоносного кода	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
15	**Управление инцидентами сбора информации** 1 Определение инцидента сбора информации 2 Цели инцидента сбора информации	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
16	**Планирование системы управления инцидентами сбора информации** 1 Подготовка к обработке инцидента 2 Выбор защитных мер 3 Формирование последовательности действий при обработке инцидентов сбора информации 4 Формирование порядка обработки инцидента сбора информации	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	

17	**Использование системы управления инцидентами сбора информации** 1 Обнаружение и анализ инцидента сбора информации 2 Сдерживание инцидента сбора информации	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
18	**Устранение инцидента и восстановление после инцидента сбора информации устранение и восстановление инцидента после сбора информации** 1 Сбор и обработка свидетельств инцидента 2 Устранение и восстановление инцидента после сбора информации	ИД-3$_{ПК-4}$ ИД-4$_{ПК-4}$ ИД-5$_{ПК-4}$	2.00	-	2.00	4.00	
	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) «Менеджмент инцидентов кибербезопасности» 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).

7. Методические указания для обучающихся по освоению дисциплины (модуля)

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.

Лабораторные работы направлены на приобретение опыта практической работы 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. Кибербезопасность цифровой индустрии / Зегжда Д.П. Москва: Горячая линия - Телеком, 2022. — 556, [3] с. ил.; 24. — ISBN 978-5-9912-0827-7.

2. Управление инцидентами кибербезопасности: учеб. пособие / С. Л. Зефиров, А. Ю. Щербакова. – Пенза: Изд-во ПГУ, 2012. – 104 с.

3. Investigation of information security incidents: a manual / I.N. Vasilyeva. – Saint Petersburg: Publishing house of Saint Petersburg State University of Economics, 2019. – 113 p.

8.1.2. Перечень дополнительной литературы:

1. Баркалов Ю.М., Гайдин А.И., Потанина И.В. Процессуальные и организационно-тактические особенности фиксации доказательственной информации, обнаруженной в сети Интернет. Метод. рекомендации. −Воронеж: Воронежский институт МВД России, 2016. – 52 с.

2. Баркалов Ю.М., Нестеровский О.И., Лиходедов Д.Ю. Организационно-техническое обеспечение специальных мероприятий. Метод. рекомендации. – Воронеж: Воронежский институт МВД России, 2016. – 82 с.

3. Введенская О.Ю. Расследование преступлений в сфере компьютерной информации: лекции, 2016. – Краснодар: Краснодарский ун-т МВД РФ. Кафедра криминалистики. – 126 с.

4. R.C. Arkin and T. Balch. AuRA: Principles and practice in review. Journal of

Experimental and Theoretical Artificial Intelligence, 9(2-3):175–189, 1997.

5. Khalid, A.; Kirisci, P.; Khan, Z.H.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. Security framework for industrial collaborative robotic cyber–physical systems. Comput. Ind. 2018, 97, 132–145.

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

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Менеджмент инцидентов кибербезопасности».
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Менеджмент инцидентов кибербезопасности».

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

Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/ -

Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/ -

Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/

Интернет портал Защита-информации.SU http://www.iso27000.ru/

Научная электронная библиотека eLIBRARY.RU http://elibrary.ru

Консорциум сетевых электронных библиотек ЭБС«Лань» https://e.lanbook.com/

ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/ -

ЭБС IPR SMART https://www.iprbookshop.ru/

ЭБС Znanium https://znanium.com/

ЭБС «Юрайт» http://www.biblio-online.ru

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 лабораторных работ 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 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 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.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

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.