МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Зам. директора по учебной работе
Пятигорского института (филиал)
СКФУ
М.В. Мартыненко

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Методы и средства криптографической защиты информации

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Безопасность компьютерных систем
Год начала обучения	2023
Форма обучения	очная
Реализуется в семестре	5,6

Разработано
Доцент кафедры СУиИТ
_____ Битюцкая Н.И.

Пятигорск 2023 г.

1. Цель и задачи освоения дисциплины

Цель дисциплины: формирование набора универсальных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

Задачи дисциплины: ознакомить студентов с современными системами шифрования на основе симметричных и асимметричных алгоритмов; научить выбирать параметры псевдослучайных последовательностей для генерирования криптостойких ключей; изучить стандарты систем шифрования; изучить криптографические протоколы.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части образовательной программы. Ее освоение происходит в 5 и 6 семестрах.

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
ОПК-3: Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ИД-1 ОПК-3. Знает необходимые математические методы для решения задач обеспечения защиты информации. ИД-2 ОПК-3. Уметь: применять совокупность необходимых математических методов для решения задач обеспечения защиты информации. ИД-3 ОПК-3 Наделен навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.	Умеет использовать необходимые математические методы для решения задач профессиональной деятельности. Умеет применять информационно-коммуникационные технологи, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности, использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности, применять средства криптографической защиты информации для решения задач профессиональной деятельности. Умеет при решении профессиональных задач организовывать защиту информации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федерации службы по техническому и экспортному контролю,
ОПК-7: Способен использовать языки программирования и технологии разработки программах средств для решения задач профессиональной деятельности	ИД-1 ОПК-7 Знает языки программирования и системы разработки программных средств для решения профессиональных задач. ИД-2 ОПК-7 Способен выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач. ИД-3 ОПК-7 Обладает навыками применения языков программирования и систем разработки программных средств для решения профессиональных задач.	
ОПК-9: Способен	ИД-1 ОПК-9 Понимать	

применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	корректность криптографической алгоритмов в современных программных комплексах. ИД-2 ОПК-9 Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. ИД-3ОПК-9 Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений, участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

4. Объем учебной дисциплины (модуля) и формы контроля

Объем занятий: всего: 8 з.е.216 астр.ч.	ОФО, в астр. часах	ЗФО, в астр. часах	ОЗФО, в астр. часах
Контактная работа:	126		
Лекции/из них практическая подготовка	51		
Лабораторных работ/из них практическая подготовка	51		
Практических занятий/из них практическая подготовка	24		
Самостоятельная работа	63		
Формы контроля			
Экзамен	6 (контроль 27)		
Зачет			
Зачет с оценкой	5		
Расчетно-графические работы			
Курсовые работа			
Контрольные работы			

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				заочная форма				очно-заочная форма			
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы		Лекции	Практические	Лабораторные работы		Лекции	Практические занятия	Лабораторные работы	
5 семестр														
1	Тема 1. Основные понятия и термины криптографии. Методы защиты информации. Криптография и криптоанализ. Понятие шифра и ключа. Симметричные и ассиметричные алгоритмы шифрования.	ОПК-3	1,5		3	3								

2	Тема 2. Основы теории делимости. Основные понятия теории делимости целых чисел. Алгоритм Евклида нахождения наибольшего общего делителя. Расширенный алгоритм Евклида. Решение линейных диофантовых уравнений.	ОПК-3	1,5		3	3								
3	Тема 3. Модульная арифметика. Операции по модулю. Система вычетов. Сравнение по модулю. Свойства оператора mod. Аддитивная и мультипликативная инверсии чисел. Применение расширенного алгоритма Евклида для нахождения мультипликативной инверсии. Решение уравнений с одним неизвестным, содержащих сравнение.	ОПК-3	1,5		3	3								
4	Тема 4. Матрицы вычетов. Определение матрицы вычетов. Операции над матрицами вычетов. Решение систем уравнений, содержащих сравнения.	ОПК-3	1,5		3	3								
5	Тема 5. Проверка чисел на простоту. Способы проверки на простое число. Решето Эратосфена. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма. Теорема Ферма. Теорема Эйлера.	ОПК-3	1,5		3	3								

6	Тема 6. Алгоритмы генерации простых чисел. Генераторы псевдослучайных чисел. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.	ОПК-3	1,5			3								
7	Тема 7. Разложение чисел на простые множители. Основная теорема арифметики. Приложения разложения на множители. Алгоритмы разложения на множители: метод проверки делением, метод Ферма, метод PO (Rho) Полларда.	ОПК-3	1,5		3	3								
8	Тема 8. Китайская теорема об остатках. Решение систем линейных уравнений с модулями. Примеры практических задач.	ОПК-3	1,5		3	3								
9	Тема 9. Алгебраические основы криптологии. Группы, кольца, поля, их определения и виды, полиномы над структурой.	ОПК-3	1,5			3								
10	Тема 10. Эллиптические кривые. Эллиптические кривые в вещественных числах. Эллиптические кривые в GF(p). Эллиптические кривые в $GF(2^n)$.	ОПК-3	1,5			3								
11	Тема 11. Классификация традиционных шифров. Шифры замены, шифры перестановки, поточные и блочные шифры, моноалфавитные и многоалфавитные шифры.	ОПК-7 ОПК-9	1,5			3								

12	Тема 12. Виды атак криптоанализа. Принцип Керкгоффса. Атаки грубой силы. Статистические атаки.Атака только на зашифрованный текст. Атака знания исходного текста. Атака с выборкой исходного текста. Атака с выбором зашифрованного текста. Способы противодействия атакам.	ОПК-7 ОПК-9	1,5			3								
13	Тема 13. Традиционные шифры с симметричным ключом. Шифры замены: аддитивные, мультипликативные, аффинные, автоключевой, Виженера, Плейфера, Хилла, роторный, одноразового блокнота.	ОПК-7 ОПК-9	1,5		6	3								
14	Тема 14. Криптоанализ традиционных шифров замены. Криптоанализ аддитивных шифров, автоключевого шифра, шифра Плейфера, шифра Виженера, одноразового блокнота, шифра Хилла, роторного шифра.	ОПК-7 ОПК-9	1,5			3								
15	Тема 15. Классические шифры перестановки. Бесключевой шифр, ключевые шифры перестановки столбцов, ключевые шифры перестановки строк, шифры с двойной перестановкой.	ОПК-7 ОПК-9	1,5			3								

16	Тема 16. Криптоанализ шифров перестановки. Статистические атаки на шифры перестановки. Атаки грубой силы на ключевые шифры перестановки.	ОПК-7 ОПК-9	1,5			3								
17	Тема 17. Понятие сложности алгоритма. инейная, полиномиальная и неполиномиальная сложность. Класс NP – полных задач. Способы определения сложности алгоритмов.	ОПК-7 ОПК-9	1,5			3								
18	Тема 18. Сложность криптографических алгоритмов. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.	ОПК-7 ОПК-9	1,5			3								
	Итого за 5 семестр:		27		**27**	**54**								
6 СЕМЕСТР														
19	Тема 19. Современные блочные шифры с симметричным ключом. Различия между современными и традиционными шифрами с симметричным ключом. Современные блочные шифры: шифры замены и шифры перестановки. Основные компоненты современного блочного шифра. Шифры Фейстеля и не-Фейстеля. Атаки на блочные шифры.	ОПК-7 ОПК-9	1,5	1,5	1,5	0,5								

20	Тема 20. Современные поточные шифры с симметричным ключом. Синхронные и несинхронные шифры потока. Преимущества и проблемы современных шифров потока. Криптоанализ шифров потока.	ОПК-7 ОПК-9	1,5	1,5		0,5								
21	Тема 21. Современный стандарт шифрования (DES) Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов. Двукратный и трехкратный DES. Криптоанализ шифра DES.	ОПК-7 ОПК-9	1,5	1,5	3	0,5								
22	Тема 22. Усовершенствованный стандарт шифрования (AES). Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES. Анализ AES.	ОПК-7 ОПК-9	1,5	1,5		0,5								
23	Тема 23. Российские стандарты симметричного шифрования. ГОСТ 28147-89, ГОСТ Р 34.12-2015: особенности, принципы построения, методы шифрования. Различные комбинированные методы шифрования.	ОПК-7 ОПК-9	1,5	1,5		0,5								
24	Тема 24. Алгоритмы шифрования с открытыми ключами. Концепция криптографии с открытым ключом. Криптосистема RSA.	ОПК-7 ОПК-9	1,5	1,5	1,5	0,5								
25	Тема 25. Криптоанализ RSA Стойкость RSA. Виды атак на RSA.	ОПК-7 ОПК-9	1,5	1,5	3	0,5								

26	Тема 26. Криптосистема Рабина. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистеме Рабина. Безопасность криптосистемы.	ОПК-7 ОПК-9	1,5	1,5		0,5								
27	Тема 27. Криптографическая система Эль-Гамаля. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистеме Эль-Гамаля. Безопасность криптосистемы.	ОПК-7 ОПК-9	1,5	1,5		0,5								
28	Тема 28. Криптосистемы на основе метода эллиптических кривых. Эллиптические кривые в вещественных числах. Эллиптические кривые в GF(p). Эллиптические кривые в GF(2^n). Криптография эллиптической кривой, моделирующая криптосистему Эль-Гамаля. Генерация общедоступных и частных ключей. Шифрование и дешифрование. Безопасность криптосистемы с эллиптической кривой.	ОПК-7 ОПК-9	1,5	1,5		0,5								
29	Тема 29. Аутентификация данных. Электронная цифровая подпись. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. Алгоритмы ЭЦП: RSA, Эль-Гамаля, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена.	ОПК-7 ОПК-9	1,5	1,5	1,5	0,5								

30	Тема 30. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94. 9	ОПК-7 ОПК-9	1,5	1,5		0,5								
31	Тема 31. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля. Алгоритм формирования схемы Эль-Гамаля. Алгоритм формирования цифровой подписи. Проверка подписи.	ОПК-7 ОПК-9	1,5	1,5		0,5								
32	Тема 32. Понятие о структуре и способах построения криптографических протоколов. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия".	ОПК-7 ОПК-9	1,5	1,5	1,5	0,5								
33	Тема 33 Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации.	ОПК-7 ОПК-9	1,5	1,5		0,5								

34	Тема 34. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа. Способы отражения атак.	ОПК-7 ОПК-9	1,5	1,5		1,5								
	Итого за семестр		**24**	**24**	**24**	**9**								
	ИТОГО		**51**	**24**	**51**	**63**								

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств (ФОС) по дисциплине (модулю) 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 (модуля).

7. Методические указания для обучающихся по освоению дисциплины

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

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Практические работы направлены на приобретение опыта практической работы в соответствующей предметной.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к 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. Фороузан Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id =428998.

2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/52158.— ЭБС «IPRbooks».

8.1.2. Перечень дополнительной литературы:

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/ 63800.html

2. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков; под ред. М.А. Иванова; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». - М.: МИФИ, 2012. - 400 с.: табл.,

схем. - ISBN 978-5-7262-1676-8; То же [Электронный ресурс]. - URL: //biblioclub.ru /index.php?page=book&id=231673.

3. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=

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

1. Методические рекомендации по выполнению лабораторных работ по дисциплине "Методы и средства криптографической защиты информации"

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине "Методы и средства криптографической защиты информации"

3. Методические рекомендации по подготовке к практическим занятиям по дисциплине "Методы и средства криптографической защиты информации"

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 «Методы и средства криптографической защиты информации»

2. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий.

3. http://www.iqlib.ru - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия.

4. http://www.iprbookshop.ru – ЭБС «IPRbooks».

5. http://www.biblioclub.ru - электронная библиотечная система «Университетская библиотека – online».

6. http://window.edu.ru – образовательные ресурсы ведущих вузов.

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, демонстрации презентационных мультимедийных материалов. На семинарских и практических 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	Операционная система: Microsoft Windows 8: 2013-02(3000). Бессрочная лицензия. Договор № 01-эа/13 от 25.02.2013. Окончание бесплатной поддержки – 2023-01 ИЛИ Операционная система: Microsoft Windows 10: 2016-08(20), 2017-10(67), 2018-01(18), 2018-04(6), 2018-05(6), 2019-02(7). Бессрочная лицензия. Договоры № 27-эа/16 от 02.08.2016. и № 0321100021117000009_229123 от 10.10.2017. На текущий момент окончания поддержки не анонсировано.
2	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). MicrosoftOfficeStandard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензирование Microsoft Office https://support.microsoft.com/ru-ru/lifecycle/search/16674 Дата начала жизненного цикла 09.01.2013г., набор обновлений Office 2013 Service Pack1 Дата начала жизненного цикла 25.02.2014г., Дата окончания основной фазы поддержки 10.04.2018; Дополнительная дата окончания поддержки 11.04.2023г.

3	Python IDLE.

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

Лекционные занятия	Для проведения лекционных занятий необходимо следующее материально-техническое обеспечение: аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории; компьютер, экран настенный; переносной проектор, интерактивная доска.
Лабораторные работы	Для проведения практических занятий необходимо следующее материально-техническое обеспечение: персональный компьютер; проектор; возможность выхода в сеть Интернет для поиска по образовательным сайтам и порталам; экран настенный; принтер; сканер; интерактивная доска. Комплект учебной мебели.
Практические занятия	Для проведения практических занятий необходимо следующее материально-техническое обеспечение: персональный компьютер; проектор; возможность выхода в сеть Интернет для поиска по образовательным сайтам и порталам; экран настенный; принтер; сканер; интерактивная доска. Комплект учебной мебели.
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 для поиска по образовательным сайтам и порталам

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 (Bigbluebutton, Microsoft Teams, 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.