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
«28» марта 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки **10.03.01 Информационная безопасность**
Направленность (профиль) **Безопасность компьютерных систем**
Форма обучения очная
Год начала обучения 2022
Реализуется в 5, 6 семестрах

Разработано
Доцент кафедры СУиИТ,
кандидат физ.-мат. наук,
доцент Битюцкая Н.И.

Пятигорск 2022 г.

1. Цель и задачи освоения дисциплины (модуля)

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 (модуля) 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-1опк-3** Знает необходимые математические методы для решения задач обеспечения защиты информации. **ИД-2опк-3** Умеет применять совокупность необходимых математических методов для решения задач обеспечения защиты информации. **ИД-3опк-3** Имеет навыки 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 профессио-нальной 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
ОПК-7: Способен использовать языки программирования и технологии разработки программах средств для решения задач профессиональной деятельности	**ИД-1опк-7** Знает языки программирования и системы разработки программных средств для решения профессиональных задач. **ИД-2опк-7** Способен выбирать необходимые языки програм-мирования и системы разработки программных средств для решения профессиональных задач. **ИД-3опк-7** Имеет навыки применения языков программирования и систем разработки программных средств	

	для решения профессиональных задач.	Федеральной службы безопасности Российской Федерации, Федерации службы по техническому и экспортному контролю, 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 информацион-ной безопасности объекта защиты
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	**ИД-1опк-9** Знает криптографичес-кие алгоритмы в современных программных комплексах. **ИД-2опк-9** Умеет 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.	
ПК-4: Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**ИД-1пк-4** Знает методы комплексного подхода в организации политики информационной безопасности. **ИД-2пк-4** Умеет формулировать, настраивать политики безопасности. **ИД-3пк-4** Владеет навыками формулирования и контролирования соблюдения требований политики безопасности.	

4. Объем учебной дисциплины (модуля) и формы контроля

Объем занятий:	З.е.	Астр. ч.	Из них в форме практической подготовки
Всего:	8	216	
Из них аудиторных:		126	
Лекций		51	
Лабораторных работ		37,5	
Практических занятий		37,5	
Самостоятельной работы		63	
Формы контроля:			
Экзамен	6 семестр	27	
Зачет с оценкой	5 семестр		
Зачет			

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

5.1.Тематический план дисциплины (модуля)

№	Раздел (тема) дисциплины	Реализуемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем, часов	Самостоятельная

			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	работа, часов
5 семестр							
1	Тема 1. Основные понятия и термины криптографии.	ОПК-3	1,5	1,5	1,5		3
2	Тема 2. Основы теории делимости.	ОПК-3	1,5	1,5	1,5		3
3	Тема 3. Модульная арифметика.	ОПК-3	1,5	1,5	1,5		3
4	Тема 4. Матрицы вычетов.	ОПК-3	1,5	1,5	1,5		3
5	Тема 5. Проверка чисел на простоту.	ОПК-3	1,5	1,5	1,5		3
6	Тема 6. Алгоритмы генерации простых чисел.	ОПК-3	1,5	1,5			3
7	Тема 7. Разложение чисел на простые множители.	ОПК-3	1,5	1,5	1,5		3
8	Тема 8. Китайская теорема об остатках.	ОПК-3	1,5	1,5	1,5		3
9	Тема 9. Алгебраические основы криптологии.	ОПК-3	1,5	1,5			3
10	Тема 10. Эллиптические кривые.	ОПК-3	1,5				3
11	Тема 11. Классификация традиционных шифров.	ОПК-7 ОПК-9	1,5				3
12	Тема 12. Виды атак криптоанализа.	ОПК-7 ОПК-9	1,5				3
13	Тема 13. Традиционные шифры с симметричным ключом.	ОПК-7 ОПК-9	1,5	1,5	3		3
14	Тема 14. Криптоанализ традиционных шифров замены.	ОПК-7 ОПК-9	1,5				3
15	Тема 15. Классические шифры перестановки.	ОПК-7 ОПК-9	1,5				3
16	Тема 16. Криптоанализ шифров перестановки.	ОПК-7 ОПК-9	1,5				3
17	Тема 17. Понятие сложности алгоритма.	ОПК-7 ОПК-9	1,5				3
18	Тема 18. Сложность криптографических алгоритмов.	ОПК-7 ОПК-9	1,5				3
	Итого за 5 семестр		**27**	**13,5**	**13,5**		**54**
6 семестр							
19	Тема 19. Современные блочные шифры с	ОПК-7 ОПК-9	1,5	1,5	1,5		

	симметричным ключом.						
20	Тема 20. Современные поточные шифры с симметричным ключом.	ОПК-7 ОПК-9	1,5				
21	Тема 21. Современный стандарт шифрования (DES).	ОПК-7 ОПК-9	1,5	1,5	3		
22	Тема 22. Усовершенство-ванный стандарт шифрования (AES).	ОПК-7 ОПК-9	1,5				
23	Тема 23. Российские стандарты симметричного шифрования.	ОПК-7 ОПК-9	1,5	1,5			
24	Тема 24. Алгоритмы шифрования с открытыми ключами.	ОПК-7 ОПК-9	1,5		1,5		
25	Тема 25. Криптоанализ RSA.	ОПК-7 ОПК-9	1,5	1,5	3		
26	Тема 26. Криптосистема Рабина.	ОПК-7 ОПК-9	1,5				
27	Тема 27. Криптографическая система Эль-Гамаля.	ОПК-7 ОПК-9	1,5				
28	Тема 28. Криптосистемы на основе метода эллиптических кривых.	ОПК-7 ОПК-9	1,5	1,5			
29	Тема 29. Аутентификация данных. Электронная цифровая подпись.	ОПК-7 ОПК-9	1,5	1,5			9
30	Тема 30. Стандарты ЭЦП.	ОПК-7 ОПК-9	1,5		1,5		
31	Тема 31. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.	ОПК-7 ОПК-9	1,5	1,5			
32	Тема 32. Понятие о структуре и способах построения криптогра-фических протоколов.	ПК-4	1,5				
33	Тема 33 Взаимосвязь между протоколами аутентификации и цифровой подписи.	ПК-4	1,5	1,5	1,5		
34	Тема 34. Атаки на криптографические протоколы.	ПК-4	1,5				
	Итого за 6 семестр		**24**	**24**	**24**		**9**
	Итого		**51**	**37,5**	**37,5**		**63**

5.2 Содержание лекций

№	Наименование дисциплины	Краткое содержание	Обьем часов	Из них практическая подготовка,

			часов
	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.	1,5	
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.	1,5	
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.	1,5	
4	Тема 4. Матрицы вычетов. Определение матрицы вычетов. Операции над матрицами вычетов. Решение систем уравнений, содержащих сравнения.	1,5	
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.	1,5	
6	Тема 6. Алгоритмы генерации простых чисел. Генераторы псевдослучайных чисел. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.	1,5	
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.	1,5	
8	Тема 8. Китайская теорема об остатках. Решение систем линейных уравнений с модулями. Примеры практических задач.	1,5	
9	Тема 9. Алгебраические основы криптологии. Группы, кольца, поля, их определения и виды, полиномы над структурой.	1,5	
10	Тема 10. Эллиптические кривые. Эллиптические кривые в вещественных числах. Эллиптические кривые в GF(p). Эллиптические кривые в $GF(2^n)$.	1,5	
11	Тема 11. Классификация традиционных шифров. Шифры замены, шифры перестановки, поточные и блочные шифры, моноалфавитные и многоалфавитные шифры.	1,5	
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.	1,5	
13	Тема 13. Традиционные шифры с симметричным ключом.	1,5	

	Шифры замены: аддитивные, мультипликативные, аффинные, автоключевой, Виженера, Плейфера, Хилла, роторный, одноразового блокнота.		
14	Тема 14. Криптоанализ традиционных шифров замены. Криптоанализ аддитивных шифров, автоключевого шифра, шифра Плейфера, шифра Виженера, одноразового блокнота, шифра Хилла, роторного шифра.	1,5	
15	Тема 15. Классические шифры перестановки. Бесключевой шифр, ключевые шифры перестановки столбцов, ключевые шифры перестановки строк, шифры с двойной перестановкой.	1,5	
16	Тема 16. Криптоанализ шифров перестановки. Статистические атаки на шифры перестановки. Атаки грубой силы на ключевые шифры перестановки.	1,5	
17	Тема 17. Понятие сложности алгоритма. инейная, полиномиальная и неполиномиальная сложность. Класс NP – полных задач. Способы определения сложности алгоритмов.	1,5	
18	Тема 18. Сложность криптографических алгоритмов. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.	1,5	
	Итого 5 семестр	**27**	
	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.	1,5	
20	Тема 20. Современные поточные шифры с симметричным ключом. Синхронные и несинхронные шифры потока. Преимущества и проблемы современных шифров потока. Криптоанализ шифров потока.	1,5	
21	Тема 21. Современный стандарт шифрования (DES) Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов. Двукратный и трехкратный DES. Криптоанализ шифра DES.	1,5	
22	Тема 22. Усовершенствованный стандарт шифрования (AES). Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES. Анализ AES.	1,5	
23	Тема 23. Российские стандарты симметричного шифрования. ГОСТ 28147-89, ГОСТ Р 34.12-2015: особенности, принципы построения, методы шифрования. Различные комбинированные методы шифрования.	1,5	
24	Тема 24. Алгоритмы шифрования с открытыми ключами. Концепция криптографии с открытым ключом.	1,5	
25	Тема 25. Криптоанализ RSA Стойкость RSA. Виды атак на RSA.	1,5	
26	Тема 26. Криптосистема Рабина.	1,5	

	Алгоритмы шифрования, дешифрования и генерации ключей в криптосистеме Рабина. Безопасность криптосистемы.		
27	Тема 27. Криптографическая система Эль-Гамаля. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистеме Эль-Гамаля. Безопасность криптосистемы.	1,5	
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.	1,5	
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, ФиатаШамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена.	1,5	
30	Тема 30. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94. 9	1,5	
31	Тема 31. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля. Алгоритм формирования схемы Эль-Гамаля. Алгоритм формирования цифровой подписи. Проверка подписи.	1,5	
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".	1,5	
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.	1,5	
34	Тема 34. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа. Способы отражения атак.	1,5	
	Итого 6 семестр	**24**	
	Итого	**51**	

5.3 Наименование лабораторных работ

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
	5 семестр		

1	Лабораторная работа 1. Программная реализация вычисления наибольшего общего делителя двух чисел.	1,5	
2	Лабораторная работа 2. Программная реализация расширенного алгоритма Евклида.	1,5	
3	Лабораторная работа 3. Применение расширенного алгоритма Евклида для решения уравнений сравнения, линейных диофантовых уравнений и нахождения мультипликативной инверсии.	1,5	
4	Лабораторная работа 4. Операции над матрицами вычетов.	1,5	
5-6	Лабораторная работа 5. Программная реализация генераторов простых чисел.	1,5	
7	Лабораторная работа 6. Разложение чисел на простые множители.	1,5	
8	Лабораторная работа 7. Решение систем уравнений сравнения с одной неизвестной и различными модулями с использованием китайской теоремы об остатках.	1,5	
13	Лабораторная работа 8. Программная реализация классических шифров с симметричным ключом.	3	
	Итого за 5 семестр	**13,5**	
6 семестр			
19	Лабораторная работа 9. Программная реализация основных компонентов современных шифров с симметричным ключом.	1,5	
21	Лабораторная работа 10. Программная реализация шифра DES.	3	
24	Лабораторная работа 11. Подготовка к реализации шифра RSA.	1,5	
25	Лабораторная работа 12. Программная реализация шифра RSA.	3	
29-31	Лабораторная работа 13. Программная реализация ЭЦП.	1,5	
32-33	Лабораторная работа 14. Программная реализация криптографических протоколов.	1,5	
	Итого за 6 семестр	12	
	Итого	**25,5**	

5.4 Наименование практических занятий

№ темы	Наименование работы	Обьем часов	Из них практическая подготовка, часов
	5 семестр		
2	Основы теории делимости.	1,5	
3	Модулярная арифметика.	1,5	
4	Матрицы вычетов.	1,5	
5	Проверка чисел на простоту.	1,5	
6	Алгоритмы генерации простых чисел.	1,5	

7	Разложение чисел на простые множители.	1,5	
8	Китайская теорема об остатках	1,5	
9-10	Алгебраические основы криптологии. Эллиптические кривые.	1,5	
13	Традиционные шифры с симметричным ключом.	1,5	
	Итого за 5 семестр	**13,5**	
	6 семестр		
19-20	Современные блочные и поточные шифры с симметричным ключом.	1,5	
21-22	Современные стандарты симметричного шифрования DES и AES.	1,5	
23	Российские стандарты симметричного шифрования.	1,5	
24-27	Тема 24. Алгоритмы шифрования с открытыми ключами. Криптосистемы RSA, Рабина, Эль-Гамаля.	1,5	
28	Криптосистемы на основе метода эллиптических кривых.	1,5	
29	Тема 29. Аутентификация данных. Электронная цифровая подпись.	1,5	
30-31	Тема 30. Стандарты ЭЦП.	1,5	
32-34	Криптографические протоколы.	1,5	
	Итого за 6 семестр	**12**	
	Итого	**25,5**	

5.5 Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
5 семестр					
ОПК-3, ОПК-7, ОПК-9, ПК-4	Самостоятельное изучение литературы и источников	Собеседование	16,2	1,8	18
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к лабораторным работам	Отчет письменный	16,2	1,8	18
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к практическим занятиям	Отчет письменный	16,2	1,8	18
	Итого за 5 семестр		**48,6**	**5,4**	**54**
6 семестр					
ОПК-3, ОПК-7, ОПК-9, ПК-4	Самостоятельное изучение литературы и источников	Собеседование	4,5	0,3	3
ОПК-3	Подготовка отчетов по	Отчет	4,5	0,3	3

ОПК-7, ОПК-9, ПК-4	лабораторным работам	письменный			
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к практическим занятиям	Отчет письменный	4,5	0,3	3
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к экзамену	Экзамен	24,3	2,7	27
Итого за 6 семестр			**32,4**	**3,6**	**36**
Итого			**81**	**9**	**90**

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 «Методы и средства криптографической защиты информации» 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

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

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

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

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

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

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 (модулю)

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 (модуля)

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

Минимально необходимый для реализации ООП перечень материально-технического обеспечения включает в себя лекционную мультимедийную аудиторию, компьютерный класс с выходом в сеть Internet и локальную вычислительную сеть.

Для проведения лабораторных занятий используются программы Microsoft Office, Python IDLE.

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

Лекционные занятия	Учебная аудитория с мультимедиа оборудованием	Мультимедийное оборудование: проектор, компьютер, экран настенный. Комплект учебной мебели.
Лабораторные занятия Практические занятия	Лаборатория информационных технологий и систем автоматизированного проектирования с мультимедиа оборудованием	Мультимедийное оборудование: проектор, экран настенный. Персональные компьютеры с выходом в сеть Интернет. Комплект учебной мебели.
Самостоятельная работа	Помещения для самостоятельной работы	Персональные компьютеры с выходом в сеть Интернет. Комплект учебной мебели.

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся, оснащенные 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.