Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.07 Криптографические методы защиты информации

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

01.04.01 Математика

Направленность (профиль)

01.04.01.02 Алгебра, логика и дискретная математика

Форма обучения очная

Год набора 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили

Кандидат физико-математических наук, Доцент, Жданов Олег Николаевич

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью дисциплины «Криптографические методы защиты информации» является знакомство магистрантов с математическими основами криптографии. Рассматриваются исторические и современные криптосистемы и, в особенности, их криптоанализ и лежащие в его основе математические средства.

1.2 Задачи изучения дисциплины

Задачей изучения дисциплины является изучение основных понятий и истории развития криптографии, исторических шифров и их недостатков, современных блочных шифров и способов их криптоанализа, средств асимметричной криптографии и математического аппарата, обеспечивающего их построение и криптоанализ, приложений криптоалгоритмов при построении криптографических протоколов и систем защиты информации.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-1: Способен применять в научно-исследовательской деятельности знания математических и естественных наук, основ программирования и информационных технологий	
ПК-1.1: Обладает достаточными фундаментальными теоретическими и практическими знаниями математических и естественных наук, основ программирования и информационных технологий для проведения в конкретной области профессиональной деятельности	Какие исследовательские вопросы стоят в рамках данной дисциплины Самостоятельно освоить темы дисциплины, углубляющие и детализирующие содержание лекционных и семинарских занятий Методами решения задач и проблем, входящими в рамки данной дисциплины
ПК-1.2: Решает научные задачи в соответствии с поставленной целью и в соответствии с выбранной методикой	Основные теории становления и методы изучаемой дисциплины Применять знания и методы к решению задач в научно- исследовательской деятельности Основными методами и программными продуктами для достижения поставленной цели

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е
		1
Контактная работа с преподавателем:	**1,06 (38)**	
занятия лекционного типа	0,53 (19)	
практические занятия	0,53 (19)	
Самостоятельная работа обучающихся:	**0,94 (34)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Основные понятия и история криптографии.									
	1. Основные понятия криптографии 1.1.Постановка задачи. Виды информации, подлежащей закрытию. Три метода защиты информациот несанкционированного доступа. Отличие криптографического решения от иных. Краткий исторический очерк развития криптографии. 1.2. Открытые сообщения и их характеристики. Модели и свойства информации. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. 1.3. Основные понятия криптографии. Модели шифров. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к щифрам.	2							
	2. Криптоанализ классических шифров: простой замены, перестановки, шифра Виженера.			2					

3. Основные понятия и история криптографии.							6	
2. Симметричная криптография.								
1. Основные классы шифров и их свойства. 2.1. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. 2.2 Шифры замены. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. 2.3. Поточные цифры Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	2							

2. Надёжность шифров 3.1.Теория К. Шеннона. Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Характеризация совершенных шифров с минимальным числом ключей. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости.Избыточность языка и расстояние единственности. 3.2 Имитостойкость шифров Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. 3.3 Помехоустойчивость шифров. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.	2							
3. Симметричные алгоритмы шифрования. 4.1.Принципы построения блочных шифров. 4.2. Алгоритмы DES и ГОСТ 28147-89, алгоритмы ``Магма`` и ``Кузнечик``. 4.3. Алгоритм AES. 4.4. Алгоритм IDEA. 4.5.Требования, предъявляемые к блочным симметричным шифрам. 4.6.Режимы работы блочных шифров.	2							

4. Основные способы реализации криптографических алгоритмов 5.1. Различия между программными и аппаратными реализациями. Программные реализации шифров. 5.2.Современные криптографические интерфейсы. Криптографические стандарты. 5.3. Вопросы синтеза генераторов случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный контурный метод. Мультиплексорные последовательности. Вопросы периодичности и распределения элементов в псевдослучайных последовательностях. 5.3.Методы усложнения последовательностей псевдослучайных чисел.Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнения последовательностей.	2							
5. Линейный и дифференциальный криптоанализ S-DES.			2					
6. Шифрование по алгоритму ГОСТ 28147-89.			3					
7. Симметричная криптография.							10	
3. Асимметричная криптография.								

1. Алгоритмы асимметричные 6.1.Понятие односторонней функции и односторонней функции с «лазейкой». 6.2. Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. 6.3. Шифрование на основе эллиптических кривых. 6.4.Криптосистемы на основе задачи об укладке рюкзака.Достоинства и недостатки асимметричных систем шифрования.	2							
2. Методы анализа криптографических алгоритмов. 7.1.Понятие криптоатаки. Классификация криптоатак.Методы анализа криптографических алгоритмов: перебор ключей, метод «встречи посередине», линеаризация уровней шифрования, бесключевые методы. 7.2. Особенности линейного криптоанализа. 7.3. Особенности дифференциального криптоанализа.	2							
3. Криптографические хеш-функции и электронная подпись. 8.1.Характеристики и алгоритмы выработки хэш-функций.Примеры. 8.2. Хеш-функция по стандарту РФ. 8.3.ЭЦП: определение, отличия от собственноручной подписи. 8.4. ЭЦП на основе группы точек эллиптической кривой над конечным полем.	2							
4. Шифрование по алгоритму AES.			2					
5. Шифрование по алгоритму IDEA.			2					
6. Тестирование чисел на простоту.			2					

7. Асимметричная криптография.							14	
4. Криптографические протоколы.								
1. Криптографические протоколы. 9.1. Модели криптографического протокола.Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. 9.2. Протоколы аутентификации. Парольные системы и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и цифровой подписи. 9.3. Протоколы управления ключами. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификация. Вопросы организации сетей засекреченной связи. 9.4. Протоколы с нулевым знанием.Доказательство с нулевым знанием. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым знанием на основе NP-сложных задач.	2							
2. Заключение.Проблемы и перспективы исследований в области современной криптографии. Нерешенные задачи. Итоги изучения курса.	1							
3. Криптоанализ системы шифрования RSA при неправильном выборе параметров.			3					
4. Генерация и проверка ЭЦП на основе стандарта Российской Федерации.			3					
5. Криптографические протоколы.							4	

Всего	19		19				34	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Ященко В. В. Введение в криптографию: учеб. пособие(Москва: МЦНМО-ЧеРо).
2. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования: Монография(Москва: ООО "Научно-издательский центр ИНФРА-М").
3. Шеннон К. Э., Добрушин Р. Л., Лупанов О. Б., Колмогоров А. Н. Работы по теории информации и кибернетике: [сборник](Москва: Издательство иностранной литературы).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Программные комплексы.
2. 1.Программный комплекс Classic.
3. Программный комплекс предназначен для решения задач криптоанализа шифров столбцовой перестановки, двойной перестановки, простой замены и шифра Виженера.
4. 2.Программа DES.
5. Программа предназначена для зашифрования и расшифрования по алгоритму DES.При этом показываются результаты всех раундов.Программа позволяет также изучить лавинный эффект.
6. 3.Программа Gost.exe.
7. Программа предназначена для зашифрования и расшифрования по алгоритму ГОСТ 28147-89. Пользователь может выбирать ключ и таблицы замен.
8. 4.Программный комплекс Crypto.exe включает программы:
9. 7.Целочисленный калькулятор,
10. 8.Алгоритм Евклида,
11. 9.Генератор BBS,
12. 10.Программа проверки числа на простоту,
13. 11.Программа факторизации,
14. 12.Операции с точками эллиптической кривой.
15. Программа генерации и тестирования ключа для алгоритма блочного шифрования. Реализованы тесты Чезаро и Пирсона.
16. Программные комплексы подготовлены и используются.
17.
18. Пакет Microsoft Office, ОС Windows XP/7/8/10, браузер Google Chrome/Opera/Mozilla Firefox,

19. информационные справочные системы: google.com, yandex.ru и т.д.

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Для самостоятельной работы у студентов должен быть доступ к электронному каталогу НБ СФУ.

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Для проведения занятий требуется оборудованная доской аудитория и персональные компьютеры.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья, в зависимости от нозологий, осуществляется с использованием средств обучения общего и специального назначения.