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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.05.01 Криптография

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

01.03.02 Прикладная математика и информатика

Направленность (профиль)

01.03.02.31 Математическое моделирование и вычислительная математика

Форма обучения очная

Год набора 2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

Кандидат физико-математических наук, Доцент, Ушаков Юрий Юрьевич

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью дисциплины «Криптография» является знакомство студентов 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 ставится 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.

В результате изучения дисциплины обучающийся должен уметь:

- определять модель угроз для каждой задачи, требующей защиты информации;
- выбирать необходимые для данной задачи существующие средства защиты информации;
- анализировать составные части существующих или вновь создаваемых блочных шифров на подверженность атакам на основе линейного и дифференциального криптоанализа;
- использовать теоретико-числовой и алгебраический аппарат при разработке алгоритмов защиты информации на основе асимметрической криптографии.
- использовать защищенные протоколы при реализации 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 базовые знания математических и естественных наук, основ программирования и информационных технологий при проведении исследования в конкретной области профессиональной деятельности	
ПК-1.1: Применяет теоретические и практические знания математических и естественных наук, основ программирования и информационных технологий для проведения в кон-кретной области про-фессиональной дея-тельности	Современные виды информационного воздействия и принципы, методы противодействия несанкционированному воздействию на вычислительные системы и системы передачи информации. Использовать программные и аппаратные средства персонального компьютера. Профессиональной терминологией, навыками использования типовых криптографических

	алгоритмов.

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:	**1,89 (68)**	
занятия лекционного типа	0,94 (34)	
практические занятия	0,94 (34)	
Самостоятельная работа обучающихся:	**1,11 (40)**	
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. Лекция 1. 1.1. История криптографии. 1.2. Процесс передачи информации и его участники. Модели угроз. 1.3. Шенноновская модель открытого текста	3							
	2. Лекция 2. 1.4. Формальная модель шифра. Пример шифросистемы RSA. 1.5. Формальная модель цифровой подписи. Пример цифровой подписи RSA.	3							
	3. Семинары 1-2 Темы: 1.1 – 1.5.			6					
	4. Основные понятия и история криптографии							4	
2. Симметричная криптография									

1. Лекция 3. 2.1. Шифры перестановки и простой замены, их криптоанализ. 2.2. Шифр Виженера, его криптоанализ.	2							
2. Лекция 4. 2.3. Шифр DES, значимость его компонентов с точки зрения криптоанализа. 2.4. Режимы применения блочного шифра.	2							
3. Лекция 5. 2.5. Нелинейность булевых функций. 2.6. Анализ блоков замен шифра DES на линейность.	2							
4. Лекция 6. 2.7. Алгоритм шифрования AES. 2.8. Алгоритм блочного шифрования ГОСТ 28147-89.	2							
5. Лекция 7. 2.9. Хэш-функции. 2.10. Парадокс дней рождения. Алгоритм поиска циклов в последовательности. Нахождение коллизии Хэш-функций. 2.11. Методы генерации случайных чисел.	2							
6. Семинары 3-7 Темы: 2.1 – 2.11.			10					
7. Симметричная криптография							14	
3. Асимметричная криптография								

	1. Лекция 8. 3.1. Китайская теорема об остатках. Доказательство корректности шифросистемы RSA. 3.2. Вероятностные тесты простоты чисел. 3.3. Алгоритм факторизации в поле, основанный на парадоксе дней рождения.	2							
	2. Лекция 9. 3.4. Атаки на RSA на основе подобранного шифротекста, по принципу встречи посередине, на основе временнОго анализа. 3.5. Квадратичные вычеты. Символ Лежандра-Якоби. Квадратичный закон взаимности. 3.6. Числа Кармайкла. Обоснование тестов Рабина-Миллера и Соловея-Штрассена.	2							
	3. Лекция 10. 3.7. n-1-алгоритмы генерации доказуемо простых чисел. 3.8. Задача дискретного логарифмирования в поле. 3.9. Алгоритмы нахождения мультипликативного порождающего элемента в поле. 3.10. Методы Полларда дискретного логарифмирования в поле.	2							
	4. Лекция 11. 3.11. Алгоритм Полига-Хэллмана для дискретного логарифмирования. 3.12. Алгоритм исчисления индексов для дискретного логарифмирования. 3.13. Алгоритм Диксона для факторизации составных чисел.	2							

5. Лекция 12. 3.14. Группа точек эллиптической кривой. 3.15. Проективные координаты точек эллиптической кривой.	2							
6. Лекция 13. 3.16. Представление информации точками эллиптической кривой. 3.17. Алгоритм вычисления квадратного корня в поле простого порядка.	2							
7. Лекция 14. 3.17. Теорема Хассе о порядке группы точек эллиптической кривой. 3.18. Эндоморфизм Фробениуса. Представители смежных классов в фактор-кольце полиномов от нескольких неизвестных. 3.19. Алгоритм Шуфа для вычисления порядка группы точек эллиптической кривой.	2							
8. Семинары 8-14 Темы: 3.1 – 3.19.			14					
9. Асимметричная криптография							18	
4. Криптографические протоколы								
1. Лекция 15. 4.1. Понятие и примеры криптографических протоколов. 4.2. Понятие Оракула. Примеры его использования в криптоанализе. 4.3. Пример доказуемо стойкой криптосистемы RSA-OAEP	2							

2. Лекция 16. 4.4. Модель сетевого взаимодействия. Инфраструктура открытых ключей. 4.5. Прокотол SSL.	2							
3. Семинары 15-16 Темы: 4.1 – 4.5.			4					
4. Криптографические протоколы							4	
Всего	34		34				40	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Нестеренко Ю.В., Аматов М.А. Теория чисел: учебник для вузов.; допущено УМО по классическому университетскому образованию(М.: Академия).
2. Жельников В. Криптография от папируса до компьютера: научно-популярная литература(Москва: ABF).
3. Ященко В. В. Введение в криптографию: учеб. пособие(Москва: МЦНМО-ЧеРо).

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. Пакет Microsoft Office, ОС Windows XP/7/8/10, браузер Google Chrome/Opera/Mozilla Firefox,
2. 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)

Необходима аудитория, оборудованная доской.

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