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

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заведующий кафедрой	**Заведующий кафедрой**
Кафедра алгебры и математической логики (АиМЛ_ФМиИ)	**Кафедра алгебры и математической логики (АиМЛ_ФМиИ)**
наименование кафедры	наименование кафедры
	Левчук В.М.
подпись, инициалы, фамилия	подпись, инициалы, фамилия
«____» _____ 20__г.	«____» _____ 20__г.
институт, реализующий ОП ВО	институт, реализующий дисциплину

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ КРИПТОГРАФИЯ

Дисциплина Б1.В.ДВ.05.01 Криптография

Направление подготовки / специальность: 02.03.01 Математика и компьютерные науки
Профиль 02.03.01.31 Математическое и компьютерное моделирование

Направленность (профиль):

Форма обучения: очная

Год набора: 2020

Красноярск 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования с учетом профессиональных стандартов по укрупненной группе

020000 «КОМПЬЮТЕРНЫЕ И ИНФОРМАЦИОННЫЕ НАУКИ»

Направление подготовки /специальность (профиль/специализация)

Направление 02.03.01 Математика и компьютерные науки Профиль 02.03.01.31 Математическое и компьютерное моделирование

Программу составили	Кандидат физико-математических наук, Доцент, Ушаков Юрий Юрьевич

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

ПК-1:Способен применять в научно-исследовательской деятельности базовые знания математических и естественных наук, основ программирования и информационных технологий	
ПК-1.1:Применяет теоретические и практические знания математических и естественных наук, основ программирования и информационных технологий при проведении исследований в конкретной области профессиональной деятельности	
Уровень 1	Современные виды информационного взаимодействия и принципы,

	методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
Уровень 1	Использовать программные и аппаратные средства персонального компьютера.
Уровень 1	Профессиональной терминологией, навыками использования типовых криптографических алгоритмов.

1.4 Место дисциплины (модуля) в структуре образовательной программы

При изучении дисциплины достаточно владеть основными понятиями стандартного курса алгебры: кольца классов вычетов целых чисел, конечные поля, подстановки, полная линейная группа.

Данная дисциплина может быть полезна при освоении курсов информатики, теории баз данных, интернет-технологий.

1.5 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)	Семестр
		4
Общая трудоемкость дисциплины	**3 (108)**	**3 (108)**
Контактная работа с преподавателем:	**1,89 (68)**	**1,89 (68)**
занятия лекционного типа	0,94 (34)	0,94 (34)
занятия семинарского типа		
в том числе: семинары		
практические занятия	0,94 (34)	0,94 (34)
практикумы		
лабораторные работы		
другие виды контактной работы		
в том числе: групповые консультации		
индивидуальные консультации		
иная внеаудиторная контактная работа:		
групповые занятия		
индивидуальные занятия		
Самостоятельная работа обучающихся:	**1,11 (40)**	**1,11 (40)**
изучение теоретического курса (ТО)		
расчетно-графические задания, задачи (РГЗ)		
реферат, эссе (Р)		
курсовое проектирование (КП)	Нет	Нет
курсовая работа (КР)	Нет	Нет
Промежуточная аттестация (Зачёт)		

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа (акад.час)	Занятия семинарского типа		Самостоятельная работа, (акад.час)	Формируемые компетенции
			Семинары и/или Практические занятия (акад.час)	Лабораторные работы и/или Практикумы (акад.час)		
1	2	3	4	5	6	7
1	Основные понятия и история криптографии	6	6	0	4	ПК-1.1
2	Симметричная криптография	10	10	0	14	ПК-1.1
3	Асимметричная криптография	14	14	0	18	ПК-1.1
4	Криптографические протоколы	4	4	0	4	ПК-1.1
Всего		34	34	0	40	

3.2 Занятия лекционного типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Лекция 1. 1.1. История криптографии. 1.2. Процесс передачи информации и его участники. Модели угроз. 1.3. Шенноновская модель открытого текста	3	0	0

2	1	Лекция 2. 1.4. Формальная модель шифра. Пример шифросистемы RSA. 1.5. Формальная модель цифровой подписи. Пример цифровой подписи RSA.	3	0	0
3	2	Лекция 3. 2.1. Шифры перестановки и простой замены, их криптоанализ. 2.2. Шифр Виженера, его криптоанализ.	2	0	0
4	2	Лекция 4. 2.3. Шифр DES, значимость его компонентов с точки зрения криптоанализа. 2.4. Режимы применения блочного шифра.	2	0	0
5	2	Лекция 5. 2.5. Нелинейность булевых функций. 2.6. Анализ блоков замен шифра DES на линейность.	2	0	0
6	2	Лекция 6. 2.7. Алгоритм шифрования AES. 2.8. Алгоритм блочного шифрования ГОСТ 28147-89.	2	0	0
7	2	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	0	0

8	3	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	0	0
9	3	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	0	0
10	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	0	0

11	3	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	0	0
12	3	Лекция 12. 3.14. Группа точек эллиптической кривой. 3.15. Проективные координаты точек эллиптической кривой.	2	0	0
13	3	Лекция 13. 3.16. Представление информации точками эллиптической кривой. 3.17. Алгоритм вычисления квадратного корня в поле простого порядка.	2	0	0
14	3	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	0	0

15	4	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	0	0
16	4	Лекция 16. 4.4. Модель сетевого взаимодействия. Инфраструктура открытых ключей. 4.5. Прокотол SSL.	2	0	0
Всего			34	0	0

3.3 Занятия семинарского типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Семинары 1-2 Темы: 1.1 – 1.5.	6	0	0
2	2	Семинары 3-7 Темы: 2.1 – 2.11.	10	0	0
3	3	Семинары 8-14 Темы: 3.1 – 3.19.	14	0	0
4	4	Семинары 15-16 Темы: 4.1 – 4.5.	4	0	0
Всего			34	0	0

3.4 Лабораторные занятия

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
Всего					

4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Ященко В. В.	Введение в криптографию: учеб. пособие	Москва: МЦНМО-ЧеРо, 1999

5 Фонд оценочных средств для проведения промежуточной аттестации

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Нестеренко Ю.В., Аматов М.А.	Теория чисел: учебник для вузов.; допущено УМО по классическому университетскому образованию	М.: Академия, 2008
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Жельников В.	Криптография от папируса до компьютера: научно-популярная литература	Москва: ABF, 1997
6.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство, год
Л3.1	Ященко В. В.	Введение в криптографию: учеб. пособие	Москва: МЦНМО-ЧеРо, 1999

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Э1	Клод Шеннон. Работы по теории информации и кибернетике.	http://pv.bstu.ru/crypto/shannon.pdf

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Самостоятельная работа состоит в изучении теоретического материала и решении комплектов задач.

Основные разделы: основные понятия и история криптографии, симметричная криптография, теоретико-числовые основы асимметричной криптографии, криптографические протоколы.

Темы для самостоятельного изучения выдаются лектором. Усвоение данных тем проверяется на зачете.

Комплекты задач выдаются преподавателем, ведущим практические занятия.

Задачи проверяются во время последующих практических занятий в рамках контроля самостоятельных работ.

Форма промежуточной аттестации: устный зачет.

Аттестация по дисциплине проводится по форме устного зачета. На зачет выносятся следующие задания:

- Дать определение
- Сформулировать и доказать теорему или привести и обосновать криптографический алгоритм
- Задача по одному из разделов дисциплины

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации в зависимости от нозологии:

Для лиц с нарушениями зрения:

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

9.1 Перечень необходимого программного обеспечения

9.1.1	Пакет Microsoft Office, ОС Windows XP/7/8/10, браузер Google Chrome/Opera/Mozilla Firefox,
9.1.2	информационные справочные системы: google.com, yandex.ru и т.д.

9.2 Перечень необходимых информационных справочных систем

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

10 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.