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

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заведующий кафедрой	**Заведующий кафедрой**
Кафедра прикладной математики и компьютерной безопасности (ПМКБ_ИКИТ)	**Кафедра прикладной математики и компьютерной безопасности (ПМКБ_ИКИТ)**
наименование кафедры	наименование кафедры
	А.А.Кытманов
подпись, инициалы, фамилия	подпись, инициалы, фамилия
«____» _____ 20__г.	«____» _____ 20__г.
институт, реализующий ОП ВО	институт, реализующий дисциплину

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ТЕОРИЯ ЧИСЕЛ, КОНЕЧНЫЕ ПОЛЯ И ИХ ПРИЛОЖЕНИЯ

Дисциплина Б1.В.ДВ.01.01 Теория чисел, конечные поля и их приложения

Направление подготовки / специальность

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

010000 «МАТЕМАТИКА И МЕХАНИКА»

Направление подготовки /специальность (профиль/специализация)

01.04.02 Прикладная математика и информатика, программа
01.04.02.07 Прикладные вычисления в науке и технике 2020г.

Программу составили

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью изучения дисциплины «Теория чисел, конечные поля и их приложения» является формирование у студентов знаний и представлений об основных понятиях и методах современной вычислительной теории чисел и теории конечных полей, а также их приложений к криптографии и теории кодирования.

Указанная дисциплина занимает важное место в системе подготовки специалистов в области прикладной математики. Изучаемые в дисциплине теоретические разделы имеют прикладное значение и составляют неотъемлемую часть языка современных компьютерных наук.

1.2 Задачи изучения дисциплины

Основной задачей изучения дисциплины «Теория чисел, конечные поля и их приложения» является развитие у студентов математической культуры в области современной вычислительной теории чисел, а также дискретных (конечных) алгебраических структур. Другой значимой задачей является развитие у студентов навыков по приложению современных теоретико-числовых методов в специальных дисциплинах, которые относятся к информационной и компьютерной безопасности (в частности, при реализации криптографических методов защиты информации).

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

ПК-1:Способен преподавать по программам бакалавриата, специалитета, магистратуры и ДПП, ориентированных на соответствующий уровень квалификации.	
Уровень 1	основные понятия теории конечных полей; методы факторизации многочленов над конечными полями; примеры криптосистем с открытым ключом; знать основные термины из данной предметной области на английском языке.
Уровень 1	тестировать на простоту и факторизовать целые числа; строить большие простые числа с заданными свойствами; конструировать неприводимые и примитивные многочлены над конечными полями; вычислять минимальные многочлены элементов конечного поля
Уровень 1	практическими навыками в применении алгоритмов факторизации целых чисел, алгоритмов дискретного логарифмирования

ПК-3:Способен управлять разработкой продуктов, услуг и решений на основе больших данных.	
Уровень 1	методы тестирования на простоту и методы факторизации целых чисел; теоретические основы дискретного логарифмирования
Уровень 1	правильно выбирать параметры криптосистем с открытым ключом; уметь читать литературу по данной предметной области
Уровень 1	практическими навыками в применении критериев неприводимости и алгоритмов факторизации многочленов над конечными полями;

1.4 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Теория чисел, конечные поля и их приложения» является вариативной.

Для усвоения дисциплины требуется знать основы элементарной теории чисел, высшей алгебры, линейной алгебры, теории многочленов, а также иметь представление об основных алгебраических структурах (группы, кольца, поля). Все указанные разделы присутствуют в базовых курсах алгебры и теории чисел для бакалавриата.

Изучение дисциплины расширяет спектр тех тем, которые могут быть предложены студентам для научно-исследовательской работы.

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
		3
Общая трудоемкость дисциплины	**6 (216)**	**6 (216)**
Контактная работа с преподавателем:	**2 (72)**	**2 (72)**
занятия лекционного типа		
занятия семинарского типа		
в том числе: семинары		
практические занятия	2 (72)	2 (72)
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:	**3 (108)**	**3 (108)**
изучение теоретического курса (ТО)		
расчетно-графические задания, задачи (РГЗ)		
реферат, эссе (Р)		
курсовое проектирование (КП)	Нет	Нет
курсовая работа (КР)	Нет	Нет
Промежуточная аттестация (Экзамен)	**1 (36)**	**1 (36)**

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	Тестирование чисел на простоту	0	12	0	18	ПК-1 ПК-3
2	Алгоритмы факторизация целых чисел	0	8	0	12	ПК-1 ПК-3
3	Конечные поля и многочлены над ними	0	28	0	42	ПК-1 ПК-3
4	Дискретное логарифмирование	0	8	0	12	ПК-1 ПК-3
5	Криптография с открытым ключом	0	8	0	12	ПК-1 ПК-3
6	Приложение к теории кодирования	0	8	0	12	ПК-1 ПК-3
Всего		0	72	0	108	

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
Всего					

3.3 Занятия семинарского типа

			Объем в акад.часах

			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Различные типы псевдопростых чисел	4	0	0
2	1	Детерминированные и вероятностные тесты простоты	4	0	0
3	1	Построение больших простых чисел	4	0	0
4	2	Алгоритмы факторизации целых чисел с экспоненциальной сложностью	4	0	0
5	2	Алгоритмы факторизации целых чисел с субэкспоненциальной сложностью	4	0	0
6	3	Построение конечных полей с помощью неприводимых многочленов	4	0	0
7	3	Формула обращения Мёбиуса и число неприводимых многочленов данной степени	4	0	0
8	3	Порядок многочлена над конечным полем и примитивные многочлены	4	0	0
9	3	Критерий неприводимости Батлера. Вероятностный тест на неприводимость	4	0	0
10	3	Алгоритм факторизации Берлекэмпа и его модификации	4	0	0
11	3	Вероятностный алгоритм факторизации Кантора-Цассенхауза	4	0	0
12	3	Вычисление корней многочленов в конечных полях	4	0	0
13	4	Детерминированные алгоритмы дискретного логарифмирования	4	0	0

14	4	Дискретное логарифмирование в конечных полях	4	0	0
15	5	Криптосистема RSA и ее модификации	4	0	0
16	5	Криптосистема Эль-Гамаля. Криптосистема Рабина и вероятностное шифрование	4	0	0
17	6	Циклические коды	4	0	0
18	6	Псевдослучайные последовательности	4	0	0
Всего			72	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	Осипов Н. Н., Медведева М. И.	Теория чисел: учебное пособие [для студентов специальности 01.03.04 «Прикладная математика»]	Красноярск: СФУ, 2016
Л1.2	Осипов Н. Н., Медведева М. И.	Многочлены над конечными полями: учебное пособие [для студентов специальности 01.03.04 «Прикладная математика»]	Красноярск: СФУ, 2016

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
Л1.2	Маховенко Е. Б.	Теоретико-числовые методы в криптографии: учеб. пособие для вузов по спец. "Информационная безопасность"	Москва: Гелиос АРВ, 2006
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Лидл Р., Нидеррайтер Г., Нечаев В. И.	Конечные поля: Том 1: [в 2-х томах] : перевод с английского	Москва: Мир, 1988
Л2.2	Лидл Р., Нидеррайтер Г., Нечаев В. И.	Конечные поля: Том 2: [в 2-х томах] : перевод с английского	Москва: Мир, 1988
6.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство, год
Л3.1	Осипов Н. Н., Медведева М. И.	Теория чисел: учебное пособие [для студентов специальности 01.03.04 «Прикладная математика»]	Красноярск: СФУ, 2016
Л3.2	Осипов Н. Н., Медведева М. И.	Многочлены над конечными полями: учебное пособие [для студентов специальности 01.03.04 «Прикладная математика»]	Красноярск: СФУ, 2016

8 Методические указания для обучающихся по освоению дисциплины (модуля)

В соответствии с учебным планом дисциплина «Теория чисел, конечные поля и их приложения» изучается в 3-м семестре. На ее изучение отводится 4 часа практических занятий и 6 часов самостоятельной работы в неделю.

Самостоятельная работа студентов (изучение теоретического материала, выполнение рефератов и решение задач) контролируется в форме опросов на практических занятиях и проверки рефератов.

По окончании изучения дисциплины проводится экзамен в устной форме по списку вопросов.

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

9.1 Перечень необходимого программного обеспечения

9.1.1	Система компьютерной алгебры Reduce.

9.2 Перечень необходимых информационных справочных систем

9.2.1	Электронные каталоги библиотек (СФУ, РГБ, РНБ).

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

Учебные аудитории для проведения практических занятий должны быть оборудованы техническими средствами обучения, служащими для представления учебной информации студентам (доска, ноутбук и проектор). Желательно иметь возможность подключения к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду СФУ.