Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ОД.14 Теоретико-числовые методы в криптографии»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2017

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 7 от "21" февраля 2017 г.

Заведующий кафедрой
Кафедра алгебры и дискретной математики _____ О.А. Пихтилькова
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
старший преподаватель _____ А.Н. Благовисная
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки _____ О.А. Пихтилькова
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
_____ И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

- формирование у студентов теоретических знаний, практических умений и навыков применения методов теории чисел, необходимых для решения задач в области защиты информации.

Задачи:

- изучение математических основ и базовых конструкций теории чисел, используемых при исследовании и построении современных алгоритмов, методов и моделей защиты информации;

- овладение основными математическими методами и алгоритмами теории чисел, применяемыми в решении проблем построения криптографических конструкций;

- приобретение навыков решения теоретических и практических задач защиты информации математическими методами.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.14 Фундаментальная и компьютерная алгебра*

Постреквизиты дисциплины: *Б.1.В.ОД.3 Криптографические методы защиты информации*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: *- основы теории делимости в кольце целых чисел, теории числовых сравнений и сравнений с неизвестными, теории первообразных корней и индексов;* **Уметь:** *- решать задачи теории чисел, возникающие при создании и исследовании криптографических конструкций;* **Владеть:** *- методами проверки чисел на простоту, построения больших простых чисел, дискретного логарифмирования в конечных циклических группах.*	ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области
Знать: *- формулировки классических задач теории чисел, используемых в криптографических приложениях;* **Уметь:** *- адаптировать постановки классических задач теории чисел для криптографических целей;* **Владеть:** *- навыками постановки теоретико-числовых задач криптографии.*	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики
Знать: *- формулировки утверждений и теорем разделов теории чисел, связанных с задачами защиты информации;* **Уметь:** *- доказывать утверждения и теоремы разделов теории чисел, связанных с задачами защиты информации;*	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Владеть: *- различными методами вывода основных результатов теории чисел.*	

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 академических часов).

Вид работы	Трудоемкость, академических часов	
	3 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**69,25**	**69,25**
Лекции (Л)	34	34
Практические занятия (ПЗ)	34	34
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение расчетно-графического задания (РГЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**74,75**	**74,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 3 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Элементы теории делимости	16	4	4		8
2	Сравнения и системы сравнений	72	18	18		36
3	Проверка чисел на простоту и построение больших простых чисел	20	6	4		10
4	Криптографические приложения теории чисел	36	6	8		22
	Итого:	144	34	34		76
	Всего:	144	34	34		76

4.2 Содержание разделов дисциплины

№ 1 Элементы теории делимости

Делимость целых чисел. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Расширенный алгоритм Евклида и линейное представление наибольшего общего делителя. Обобщенный алгоритм Евклида. Линейные диофантовы уравнения. Простые и составные числа. Бесконечность множества простых чисел. Основная теорема арифметики о разложении целых чисел на простые сомножители. Важнейшие функции теории чисел: [x], {x}, мультипликативные функции, функция Мёбиуса, функция Эйлера.

№ 2 Сравнения и системы сравнений

Числовые сравнения и их свойства. Полная и приведенная система вычетов, свойства. Теорема Эйлера, малая теорема Ферма. Кольцо классов вычетов, обратимые элементы, делители нуля, мультипликативная группа кольца, ее строение. Методы нахождения мультипликативных обратных элементов, основанные на расширенном алгоритме Евклида и малой теореме Ферма.

Сравнения первой степени: анализ, способы решения. Системы линейных сравнений. Китайская теорема об остатках, ее использование при упрощении вычислений.

Теория сравнений второй степени, символ Лежандра, его свойства, символ Якоби. Алгоритм Шэнкса. Квадратичные сравнения по составному модулю.

Первообразные корни и индексы. Существование первообразного корня по простому модулю; первообразные корни по модулям p и 2p; отыскание первообразных корней. Индексы по модулям p и 2p; таблицы индексов. Решение степенных сравнений.

№ 3 Проверка чисел на простоту и построение больших простых чисел

Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Свойства чисел Кармайкла. Тест Соловея-Штрассена. Тест Рабина-Миллера. Полиномиальный тест распознавания простоты. Числа Мерсенна и проверка чисел Мерсенна на простоту.

№ 4 Криптографические приложения теории чисел

Задача разделения секрета. Протокол Диффи-Хеллмана. Алгоритм RSA. Алгоритм Эль-Гамаля. ЭЦП. Криптосистема Рабина.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1, 2	1	НОД целых чисел. Алгоритм Евклида и его модификации. Линейные диофантовы уравнения.	4
3	2	Мультипликативные обратные элементы в кольцах вычетов.	2
4	2	Сравнения первой степени.	2
5	2	Системы линейных сравнений.	2
6	2	Символы Лежандра и Якоби.	2
7	2	Квадратичные сравнения по простому модулю.	2
8	2	Квадратичные сравнения по составному модулю.	2
9	2	Первообразные корни.	2
10	2	Индексы.	2
11	2	Степенные сравнения.	2
12	3	Методы проверки чисел на простоту.	2
13	3	Методы построения больших простых чисел.	2
14, 15	4	Задачи о разделении секрета.	4
16	4	Задачи теории чисел, возникающие при реализации протокола Диффи-Хеллмана, алгоритма RSA.	2
17	4	Задачи теории чисел, возникающие при реализации алгоритма Эль-Гамаля, криптосистемы Рабина.	2
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – СПб.: Лань, 2004. – 176 с.

2. Кнауб, Л.В. Теоретико-численные методы в криптографии: учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов – Красноярск: Сибирский федеральный университет, 2011. – 160 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=229582

3. Отрыванкина, Т.М. Алгоритмы компьютерной алгебры: практикум / Т. М. Отрыванкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования «Оренбург. гос. ун-т», каф. приклад. математики. – Оренбург: ОГУ, 2007. – 26 с

4. Смарт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс] /Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 511с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428998

5.2 Дополнительная литература

1. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии [Электронный ресурс] / О.Н. Василенко. – Москва: МЦНМО, 2006. – 336 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=61814

2. Глухов М.М. Введение в теоретико-числовые методы криптографии: учеб. пособие для вузов / М. М. Глухов [и др.]. – СПб. : Лань, 2011. – 400 с.

3. Курош, А. Г. Курс высшей алгебры: учеб. для вузов / А. Г. Курош. – 18-е изд., стер. – СПб.: Лань, 2011. – 432 с.

5.3 Периодические издания

1. Прикладная математика и механика: журнал. – М.: Агентство «Роспечать», 2016.

2. Вычислительные технологии: журнал. – М.: Агентство «Роспечать», 2016.

3. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017.

4. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017.

5.4 Интернет-ресурсы

1. http://cryptography.ru – сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий.

2. http://eqworld.ipmnet.ru/indexr.htm – международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).

3. https://arxiv.org/ – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии.

4. «Рассказы о теории чисел, алгебраической геометрии и гомотопической топологии» [Электронный ресурс]: онлайн-курс на платформе https://www.lektorium.tv/mooc – «Лекториум» / Разработчик курса: Санкт-Петербургский Государственный Университет (СПбГУ), режим доступа: https://www.lektorium.tv/course/22791

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Microsoft Windows

2. OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

3. Бесплатное средство просмотра файлов PDF Adobe Reader.

4. SCOPUS [Электронный ресурс]: реферативная база данных / компания Elsevier. – Режим до-

ступа: https://www.scopus.com/, в локальной сети ОГУ.

5. Springer [Электронный ресурс]: база данных научных книг, журналов, справочных материалов / компания Springer Customer Service Center GmbH. – Режим доступа: https://link.springer.com/, в локальной сети ОГУ.

6. Общероссийский математический портал Math-Net.Ru [Электронный ресурс]: профессиональная база данных для математиков – Режим доступа: http://www.mathnet.ru/index.phtml/?option_lang=rus

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.