МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра алгебры и дискретной математики

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий
_____ С.А. Герасименко
(подпись, расшифровка подписи)
"30" октября 2015 г.

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

Оренбург 2015

Рабочая программа дисциплины «*Б.1.В.ОД.14 Теоретико-числовые методы в криптографии***» /сост.**
О.А. Пихтилькова, А.Н. Благовисная – Оренбург: ОГУ, 2015

Рабочая программа предназначена студентам очной формы обучения по направлению подготовки 02.03.01 Математика и компьютерные науки

© Пихтилькова О.А., 2015
© Благовисная А.Н., 2015
© ОГУ, 2015

Содержание

1 Цели и задачи освоения дисциплины 4
2 Место дисциплины в структуре образовательной программы 4
3 Требования к результатам обучения по дисциплине 5
4 Структура и содержание дисциплины 6
4.1 Структура дисциплины 6
4.2 Содержание разделов дисциплины 7
4.3 Практические занятия (семинары) 7
5 Учебно-методическое обеспечение дисциплины 8
5.1 Основная литература 8
5.2 Дополнительная литература 8
5.3 Периодические издания 8
5.4 Интернет-ресурсы 9
5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий 9
6 Материально-техническое обеспечение дисциплины 9
Лист согласования рабочей программы дисциплины 10
Дополнения и изменения в рабочей программе дисциплины .....
Приложения:
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине .....
Методические указания для обучающихся по освоению дисциплины .....

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*

Требования к входным результатам обучения, необходимым для освоения дисциплины

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
Знать: - *содержание ключевых понятий и определений, используемых в теории и практике решения алгебраических задач;* **Уметь:** - *применять прикладное программное обеспечение для решения задач в профессиональной деятельности, науке и образовании;* **Владеть:** - *навыками пользования прикладного программного обеспечения для решения задач в профессиональной деятельности, науке и образовании.*	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности
Знать: - *принципы построения научного исследования в соответствующей области наук;* **Уметь:** - *обосновать актуальность, новизну, теоретическую и практическую значимость собственного исследования, определять методологию исследования, уметь делать выводы из проведенного исследования и определять перспективы дальнейшей работы, анализировать собранный эмпирический материал и делать достоверные выводы,*	ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
отстаивать собственную научную концепцию в дискуссии, выступать оппонентом и рецензентом по научным работам; **Владеть:** *- навыками работы с источниками научной литературе, владеть логикой научного исследования, научным стилем изложения собственной концепции.*	
Знать: *- методы теории групп, колец, полей, векторных пространств;* **Уметь:** *- сформулировать и доказать основные результаты изучаемых разделов, применять алгебраические методы;* **Владеть:** *- понятийным аппаратом алгебраической теории и прикладных задачах.*	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики
Знать: *- новые научные результаты, связанные с алгеброй;* **Уметь:** *- использовать современные методы для исследования и решения научных и практических задач; использовать новые знания и применять их в своей профессиональной деятельности;* **Владеть:** *- способностью проводить научные исследования и получать новые научные результаты.*	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата

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, теории многочленов одной переменной над конечным полем;* **Уметь:** *- решать задачи теории чисел, возникающие при создании и исследовании криптографических конструкций;* **Владеть:** *- методами проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, 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:	ПК-3 способностью строго

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- *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;* **Владеть:** - *различными методами вывода основных результатов теории чисел.*	доказать утверждение, сформулировать результат, увидеть следствия полученного результата

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 индивидуального творческого задания (ИТЗ);* *- выполнение расчетно-графического задания (РГЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**74,75** *12* *8* *22,25* *16,5* *10* *6*	**74,75** *12* *8* *22,25* *16,5* *10* *6*
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	12	3	3		6
2	Сравнения и системы сравнений	42	12	12		18
3	Проверка чисел на простоту и построение больших простых чисел	22	5	5		12
4	Многочлены над конечными полями	32	8	8		16
5	Сложность алгоритмов теории чисел	12	2	2		8
6	Криптографические приложения теории чисел	24	4	4		16
	Итого:	144	34	34		76
	Всего:	144	34	34		76

4.2 Содержание разделов дисциплины

№ 1 Элементы теории делимости

Делимость целых чисел. Простые и составные числа. Бесконечность множества простых чисел. Основная теорема арифметики о разложении целых чисел на простые сомножители. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Расширенный алгоритм Евклида и линейное представление наибольшего общего делителя. Обобщенный алгоритм Евклида. Линейные диофантовы уравнения.

№ 2 Сравнения и системы сравнений

Числовые сравнения и их свойства. Полная и приведенная система вычетов, свойства. Функция Эйлера, ее 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.

Критерий Люка. Теорема Поклингтона. Теорема Диемитко. Метод Маурера. Метод Михалеску. (n+1)-методы. Числа Мерсенна.

№ 4 Многочлены над конечными полями

Основные понятия и теоремы теории многочленов над полем. Неприводимые многочлены над конечным полем. Строение конечных полей. Нахождение НОД. Разложение многочлена на множители.

№ 5 Сложность алгоритмов теории чисел

Свойства функций оценки сложности. Сложность арифметических операций с целыми числами. Сложность операций в кольце вычетов. Использование модульной арифметики. Вычисления с многочленами. Дискретное преобразование Фурье.

№ 6 Криптографические приложения теории чисел

Задача разделения секрета. Протокол Диффи-Хеллмана. Алгоритм RSA. Алгоритм Эль-Гамаля. ЭЦП. Псевдослучайные последовательности над полем.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1, 2	1	Нахождение НОД целых чисел с помощью алгоритма Евклида и его модификаций. Решение линейных диофантовых уравнений.	3
2, 3	2	Нахождение мультипликативных обратных элементов в конечных полях и кольцах.	2
3, 4	2	Решение сравнений первой степени.	2
4, 5	2	Решение систем линейных сравнений.	2
5, 6	2	Вычисление символов Лежандра и Якоби. Решение	3

№ занятия	№ раздела	Тема	Кол-во часов
		квадратичных сравнений.	
7, 8	2	Первообразные корни и индексы. Решение степенных сравнений.	3
8, 9	3	Исследование методов проверки чисел на простоту.	2
9, 10	3	Изучение методов построения больших простых чисел.	3
11	4	Многочлены над конечными полями. Операции над многочленами над конечными полями.	2
12	4	Неприводимые многочлены над конечным полем.	2
13	4	Нахождение НОД многочленов над простым конечным полем. Интерполяция многочлена над простым конечным полем.	2
14	4	Разложение многочлена над конечным полем на множители.	2
15	5	Исследование оценок сложности алгоритмов теории чисел.	2
16, 17	6	Решение криптографических задач с помощью алгоритмов и методов теории чисел.	4
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Кнауб, Л.В. Теоретико-численные методы в криптографии: учебное пособие [Электронный ресурс] / 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

2. 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

5.2 Дополнительная литература

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

2. 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. Журнал «Дискретная математика».
2. Журнал «Дискретный анализ и исследование операций».
3. Журнал «Математические вопросы криптографии».
4. Журнал «Обозрение прикладной и промышленной математики».
5. Журнал «Прикладная дискретная математика».
6. Журнал «Фундаментальная и прикладная математика».

5.4 Интернет-ресурсы

1. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал Math-Net.Ru — это современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России)
2. http://intuit.ru/ (сайт института дистанционного обучения "ИНТУИТ")
3. http://cryptography.ru/about/ (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)

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

Для выполнения практической части ИТЗ используется любая из доступных на момент написания работ сред программирования, имеющихся в распоряжении лаборатории кафедры. Среда и язык программирования выбираются студентами самостоятельно в соответствии с их индивидуальными учебными возможностями и предпочтениями.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных и практических занятий.

Для чтения лекций при необходимости используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

К рабочей программе прилагаются:

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

ЛИСТ
согласования рабочей программы

Направление подготовки: 02.03.01 Математика и компьютерные науки
код и наименование

Профиль: Алгоритмы и приложения компьютерной математики

Дисциплина: Б.1.В.ОД.14 Теоретико-числовые методы в криптографии

Форма обучения: очная
(очная, очно-заочная, заочная)

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры
Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 2 от "26" сентября 2015 г.

Ответственный исполнитель, заведующий кафедрой
Кафедра алгебры и дискретной математики ✓ О.А. Пихтилькова
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент О.А. Пихтилькова
должность *подпись* *расшифровка подписи*
ст. преподаватель А.Н. Благовещенская
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
Т.В. Истомина Н.Н. Грицай
личная подпись *расшифровка подписи*

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

Рабочая программа зарегистрирована в ОИОТ ЦИТ
Начальник отдела информационных образовательных технологий ЦИТ
Е.В. Дырдина
личная подпись *расшифровка подписи*