

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра математических методов и моделей в экономике

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.4.1 Дополнительные разделы алгебры»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

01.03.04 Прикладная математика
(код и наименование направления подготовки)

Применение математических методов к решению инженерных и экономических задач
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа академического бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2016

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра математических методов и моделей в экономике

наименование кафедры

протокол № 8 от "1" 02 2016 г.

Заведующий кафедрой

Кафедра математических методов и моделей в экономике

наименование кафедры

подпись

расшифровка подписи

А.Г. Реннер

Исполнители:

Профессор кафедры ММиМЭ

должность

подпись

расшифровка подписи

А.Г. Реннер

Доцент кафедры ММиМЭ

должность

подпись

расшифровка подписи

О.Н. Яркова

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

01.03.04 Прикладная математика

код наименование

личная подпись

расшифровка подписи

А.Г. Реннер

Заведующий отделом комплектования научной библиотеки

личная подпись

расшифровка подписи

Н.Н. Грицай

Уполномоченный по качеству факультета

личная подпись

расшифровка подписи

Н.В. Лужнова

№ регистрации 40398

© Реннер А.Г., 2016
© Яркова О.Н., 2016
© ОГУ, 2016

1 Цели и задачи освоения дисциплины

Цели дисциплины: Формирование теоретических знаний о понятиях и методах современной прикладной алгебры и приобретение практических навыков их использования при решении прикладных задач, в том числе задач криптографической защиты информации.

Задачи:

- изучение основ теории чисел (модульная арифметика, вычеты, сравнения, корни и индексы, квадратичные сравнения и их решение);
- формирование знаний по основам высшей алгебры (моноиды, группы, кольца, поля, неприводимые многочлены, рекуррентные последовательности);
- освоение алгоритмов прямого и обратного дискретного преобразования Фурье, быстрого преобразования Фурье;
- освоение простейших криптографических систем защиты информации.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б.1.Б.11 Линейная алгебра и аналитическая геометрия, Б.1.Б.12 Дискретная математика, Б.1.Б.13 Математическая логика и теория алгоритмов, Б.1.Б.21 Программирование для электронно-вычислительных машин, Б.1.Б.22 Программные и аппаратные средства электронно-вычислительных машин, Б.1.В.ОД.4 Разработка и применение прикладного программного обеспечения, Б.1.В.ОД.5 Основы информатики*

Постреквизиты дисциплины: *Отсутствуют*

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: разделы алгебры, применяемые при реализации математических методов защиты информации Уметь: самостоятельно применять методы алгебры при решении прикладных задач, в том числе защиты информации Владеть: навыками самостоятельного применения методов алгебры при решении прикладных задач, в том числе защиты информации	ОПК-1 готовностью к самостоятельной работе
Знать: разделы алгебры; современные математические методы и современные технологии, применяемые при построении криптографических алгоритмов защиты информации Уметь: применять современные математические методы алгебры, современные прикладные программные средства и технологии программирования при реализации математических методов защиты информации Владеть: навыками применения современных математических методов алгебры, прикладных программных средств и технологий программирования при реализации математических методов защиты информации	ОПК-2 способностью использовать современные математические методы и современные прикладные программные средства и осваивать современные технологии программирования
Знать: разделы алгебры, используемые для построения и реализации криптографических алгоритмов защиты информации Уметь: применять стандартные пакеты прикладных программ для решения задач прикладной алгебры; разрабатывать, отлаживать, тестировать программные средства при реализации алгоритмов	ПК-1 способностью использовать стандартные пакеты прикладных программ для решения практических задач на

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
прикладной алгебры Владеть: навыками решения задач прикладной алгебры, используя стандартные пакеты прикладных программ; навыками разработки, отладки, тестирования программных средств при реализации алгоритмов прикладной алгебры	электронных вычислительных машинах, отлаживать, тестировать прикладное программное обеспечение
Знать: разделы алгебры, используемые для построения и реализации криптографических методов защиты информации Уметь: применять математические методы алгебры для решения прикладных задач, в том числе защиты информации Владеть навыками: формализации прикладных задач в области криптографической защиты информации; выбора оптимальных алгоритмов решения задач; анализа полученного решения; принятия решений на основе полученных результатов	ПК-10 готовностью применять математический аппарат для решения поставленных задач, способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов
Знать: разделы алгебры, используемые для построения и реализации криптографических методов защиты информации; Уметь: применять знания для управления информацией при решении задач защиты информации Владеть: навыками управления информацией при решении задач защиты информации	ПК-11 готовностью применять знания и навыки управления информацией
Знать: фундаментальные разделы алгебры, позволяющие самостоятельно изучать новые разделы фундаментальных наук Уметь: самостоятельно осваивать новые разделы фундаментальных наук на основе знаний прикладной алгебры Владеть: навыками познания новых разделов фундаментальных наук на основе знаний прикладной алгебры	ПК-12 способностью самостоятельно изучать новые разделы фундаментальных наук

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	108	108
Контактная работа:	52,25	52,25
Лекции (Л)	26	26
Практические занятия (ПЗ)	26	26
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - выполнение индивидуального творческого задания (ИТЗ); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий; - подготовка к практическим занятиям; - подготовка к контрольным работам)	55,75	55,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	диф. зач.	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Теория делимости	10	4	4		2
2	Сравнения, решение сравнений	22	6	6		10
3	Многочлены над конечными полями	22	6	6		10
4	Высокоскоростная арифметика	22	4	4		14
5	Эллиптические кривые	14	2	2		10
6	Введение в криптографические методы защиты информации	18	4	4		10
	Итого:	108	26	26		56
	Всего:	108	26	26		56

4.2 Содержание разделов дисциплины

№ 1 Теория делимости Элементы теории делимости: общий наибольший делитель, общее наименьшее кратное, непрерывные дроби и алгоритм Евклида, простые числа, алгоритм Эратосфена получения простых чисел не превосходящих N , каноническое разложение составного числа. Функция Эйлера. Сравнимые по модулю m числа.

№ 2 Сравнения, решение сравнений Сравнения, свойства сравнений, вычеты, полная система вычетов, приведенная система вычетов, теоремы Эйлера и Ферма.

Символ Лежанда, Якоби. Квадратичные вычеты.

Сравнения первой степени с одним неизвестным. Система сравнений первой степени. Китайская теорема об остатках.

Сравнения любой степени по простому и составному модулю. Сравнения второй степени.

№ 3 Многочлены над конечными полями Моноиды, группы, кольца, идеалы, поля, полиномиальные кольца над полями, полиномиальные коды, регистры сдвига. Примитивные элементы, базисы, представления конечных полей, первообразные корни, индексы и дискретные логарифмы. Рекуррентные последовательности. Характеристические функции кодовых последовательностей. Примитивные многочлены, неприводимые многочлены и их построение.

№ 4 Высокоскоростная арифметика Дискретное преобразование Фурье, быстрое преобразование Фурье. Метод Карацубы умножения чисел и многочленов. Арифметические операции в избыточной знаково-числовой системе.

№ 5 Эллиптические кривые

Понятие эллиптической кривой (ЭК). Уравнение Вейерштрасса. Порядок ЭК. Сингулярные кривые. Эллиптические кривые и их свойства. Точки эллиптической кривой. Сложение точек.

№ 6 Введение в криптографические методы защиты информации Простейшие системы шифрования Шифр замены, перестановки, Вернама, Вижинера, гаммирование. Обзор современных систем шифрования с секретным ключом: блочные и поточные шифры; шифры DES, ГОСТ. Однонаправленные функции. Асимметричные системы шифрования.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Алгоритм нахождения НОД, построение подходящих дробей	2
2	1	Алгоритм Эратосфена, каноническое разложение составного числа, функция Эйлера	2
3	2	Вычеты, полная и приведенная система вычетов. Нахождение	2

№ занятия	№ раздела	Тема	Кол-во часов
		первообразных корней. Составление таблиц индексов	
4	2	Решение сравнений, решение систем линейных сравнений	2
5	2	Вычисление символа Лежанда, Якоби. Квадратичные вычеты	
6	3	Построение рекуррентных последовательностей.	2
7	3	Характеристические функции кодовых последовательностей.	2
8	3	Примитивные многочлены, неприводимые многочлены	2
9	4	Дискретное преобразование Фурье	2
10	4	Быстрое преобразование Фурье	2
11	5	Действия с точками на эллиптической кривой	2
12	6	Шифр замены, перестановки, шифр Вернама, Вижинера	2
13	6	Поточные системы шифрования	2
		Итого:	26

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2004, 2009.
2. Новиков, Ф. А. Дискретная математика для программистов [Текст] : учеб. для вузов / Ф. А. Новиков. - СПб. : Питер, 2009 - 384 с.
3. Вычислительно сложные задачи теории чисел [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300 "Фундаментальная информатика и информационные технологии" / Е. А. Гречников [и др.]; Мос. гос. ун-т им. М. В. Ломоносова. - Москва : Изд-во Моск. ун-та, 2012. - 312 с
4. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо. - Москва : Техносфера, 2006. - 528 с.

5.2 Дополнительная литература

1. Биркгоф, Г. Современная прикладная алгебра = Modern Applied Algebra [Текст] : пер. с англ. / Г. Биркгоф, Т.К. Барти.- 2-е изд., стер. - СПб. : Лань, 2005. - 400 с.
2. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Текст]: [монография] / О. Н. Василенко. - М. : МЦНМО, 2006. - 328 с. Режим доступа: <http://www.biblioclub.ru/index.php?page=book&id=61814>

Методические материалы

1. Василего, И. П. Теория чисел в криптографии [Текст] : методические указания / И. П. Василего; М-во образования Рос. Федерации, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. приклад. математики. - Оренбург : ГОУ ОГУ, 2004. - 20 с.
2. Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Электронный ресурс] : методические указания к лабораторному практикуму / Т. Н. Шалкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Электрон. текстовые дан. (1 файл: 0.42 Мб). - Оренбург : ОГУ, 2006. - 44 с. - Загл. с тит. экрана. -Adobe Acrobat Reader 6.0
3. Сердюк, А. И. Криптография. Разработка приложений для шифрования информации [Электронный ресурс] : методические указания для студентов, обучающихся по программам высшего профессионального образования по специальности 090104.65 Комплексная защита объектов информатизации, 230101.65 Вычислительные машины, комплексы, системы и

сети, направлению подготовки 090900.62 Информационная безопасность, профиль "Комплексная защита объектов информатизации" / А. И. Сердюк, О. Н. Яркова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Электрон. текстовые дан. (1 файл: 1.62 Мб). - Оренбург : ОГУ, 2012. - 98 с.

5.3 Периодические издания

1. Информационные технологии : журнал. - М. : Агентство "Роспечать", 2016.
2. Вычислительные технологии : журнал. - М. : Агентство "Роспечать", 2016.
3. Прикладная математика и механика : журнал. - М. : Агентство "Роспечать", 2016.

5.4 Интернет-ресурсы

- <http://www.securitylab.ru/> информационный портал по ИТ безопасности
- <http://www.osp.ru/> сайт издательства «Открытые системы»
- <http://www.citforum.ru/> форум по информационным технологиям, методам защиты информации
- <http://www.itlab.unn.ru/?dir=104> Лаборатория информационные технологии
- <https://www.ams.org> – Американское математическое сообщество (статьи, журналы)
- <https://mathscinet.ams.org/mathscinet/> - публикации научных работ (математические науки)
- <http://window.edu.ru/> Единое окно доступа к образовательным ресурсам

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

Перечень лицензионного программного обеспечения

1. Операционная система **Microsoft Windows**
2. Пакет настольных приложений **Microsoft Office (Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Access)**
3. Средства для разработки и проектирования **Microsoft Visual Studio**
4. Интегрированная система решения математических, инженерно-технических и научных задач **MathCAD 14.0** (лицензия ОГУ, выделена на каф. ММиМЭ на 10 ПК)
5. ПО для решения широкого спектра научных и прикладных задач **MathWorks MATLAB R2013b + Fuzzy Logic Toolbox + Wavelet Toolbox**

Свободно-распространяемое ПО

Кроссплатформенный, свободно распространяемый офисный пакет с открытым исходным кодом **LibreOffice**

Средства для разработки прикладных программ **PascalABC.NET**

Профессиональные базы данных

1. Технорма / Документ [Электронный ресурс] : [система программных продуктов] / ООО Гло-сис-Сервис, ФБУ КВФ Интерстандарт. – Версия 1.11.36. – Электрон. дан. и прогр. – [Москва; Санкт-Петербург], [1999–2013]. – Режим доступа осуществляется в локальной сети ОГУ.
2. SCOPUS [Электронный ресурс] : реферативная база данных / компания Elsevier. – Режим доступа: <https://www.scopus.com/>, в локальной сети ОГУ.
3. 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.

Информационные справочные системы

1. Законодательство России [Электронный ресурс] : информационно-правовая система. – Режим доступа : <http://pravo.fso.gov.ru/ips/>, в локальной сети ОГУ.
2. Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. – Москва, [1992–2016]. – Режим доступа : в локальной сети ОГУ <\\fileserv1\CONSULT\cons.exe>
3. Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. - Москва, [1990–2016]. – Режим доступа <\\fileserv1\GarantClient\garant.exe> в локальной сети ОГУ.

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 практических занятий и самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.