ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

математико-механический факультет

кафедра алгебры и дискретной математики

ИОНЦ «Информационная безопасность»

Конечные поля

Программа специальной дисциплины
(Стандарт ПД.ОПД)

Екатеринбург
2008

УТВЕРЖДАЮ:
Декан математико-механического факультета

_____ М.О. Асанов

« » _____ 2008 г.

Программа дисциплины «Конечные поля» составлена в соответствии с требованиями федерального компонента к обязательному минимуму содержания и уровню подготовки дипломированного специалиста по специальности 090102 «Компьютерная безопасность» и бакалавра по направлению 010300 «Математика. Компьютерные науки»

по циклу специальных дисциплин государственного образовательного стандарта высшего профессионального образования.

Семестр: 6.

Общая трудоемкость дисциплины: 54 часа, в том числе:
лекций - 36 часов,
практических занятий - нет.

Контрольные мероприятия:
1контрольная работа.

Составитель:

Кабанов Владислав Владимирович, доктор физ.-мат. наук,
профессор кафедры и дискретной математики УрГУ

Рекомендовано к печати протоколом заседания
кафедры алгебры и дискретной математики УрГУ
от « » _____ 2008 г., № _____.

1. Цели и задачи дисциплины

Целью дисциплины «Конечные поля» является формирование у студентов знаний и представлений по основам теории конечных полей.

Основной задачей дисциплины является развитие у студентов математической культуры в области строения конечных полей, вычислений в конечных полях, нахождения неприводимых многочленов над конечными полями, вычисления минимальных многочленов элементов конечного поля.

Другой целью является развитие у студентов навыков по приложению методов теории конечных полей в других областях знания, включая компьютерные науки, подготовка студентов к применению методов теории конечных полей в различных разделах информационной безопасности и дисциплинах, используемых при изложении общепрофессиональных и специальных дисциплин, относящихся к информационной безопасности, и, в частности, при изложении криптографических методов защиты информации.

Дисциплина «Конечные поля» занимает важное место в системе подготовки специалистов в области Компьютерной безопасности и Компьютерных наук. Она используется при чтении ряда общепрофессиональных и специальных дисциплин таких, как «Теория кодирования», «Лингвистические основы информатики», «Криптографические методы защиты информации» и ряда других.

Методическая новизна предлагаемого курса состоит в том, что основы теории конечных полей излагаются систематичной форме, доступной для студентов. Ранее основы теории конечных полей излагались лишь в специальной математической литературе в форме трудно доступной для студентов. Развивается мысль о том, что приводимые разделы теории конечных полей входят в состав языка, на котором говорит современная компьютерная наука.

2. Требования к уровню освоения дисциплины

Требования к уровню освоения содержания дисциплины состоят в следующем:

- студент должен знать строение конечных полей, свободно оперировать вычислениями в конечных полях;
- уметь вычислять неприводимые многочлены над конечными полями;
- уметь находить минимальные многочлены элементов конечных полей;
- применять свойства конечных полей в различных приложениях математики, компьютерных наук и информационной безопасности.

3. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость дисциплины	54
Аудиторные занятия	36
Лекции	36
Практические занятия	-
Самостоятельная работа	18
Вид итогового контроля (зачет, экзамен)	зачет

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

№ п/п	Наименование тем	ВСЕГО (часов)	Аудиторные занятия (часов)		Самостоятельная работа
			в том числе		
			Лекции	Практические занятия	
1	Основы теории конечных полей	15	10	-	5
2	Строение конечных полей	12	8	-	4
3	Неприводимые многочлены над конечными полями	27	18	-	9
	ИТОГО:	54	36	-	18

4.2. Содержание тем дисциплины

4.2.1. Основы теории конечных полей

1. Вложения областей целостности в поля, поле частных области целостности, поля рациональных дробей.
2. Китайская теорема об остатках.
3. Конечные расширения поля, алгебраические элементы над полем, трансцендентные элементы над полем, минимальный многочлен алгебраического элемента, алгебраические и трансцендентные расширения полей, простое расширение поля.
4. Поле разложения многочлена и его существование и единственность.
5. Свойства операции взятия производного многочлена, характеризация конечных полей и их подполей, мультипликативная группа конечного поля, примитивные элементы поля, примитивные многочлены над конечным полем
6. Свойства корней неприводимых многочленов, автоморфизм Фробениуса, группа автоморфизмов конечного поля.

4.2.2. Строение конечных полей

1. Формула обращения Мебиуса (аддитивный и мультипликативный варианты).
2. Круговые поля (циклотомические поля или поля деления круга), корни из единицы над конечным полем, первообразные корни из единицы над конечным полем, круговые многочлены над конечным полем, строение круговых полей над конечным полем.
3. Три способа представления элементов конечного поля, дискретные логарифмы и антилогарифмы.

4.2.3. Неприводимые многочлены над конечными полями

1. Алгоритм Берлекемпа разложения многочлена на неприводимые множители.
2. Порядок многочлена, теорема о порядке многочлена и порядке его корней, порядок примитивных многочленов, теорема о связи примитивных многочленов и круговых многочленов.
3. Метод нахождения минимального многочлена элемента через сопряженные элементы.
4. Два метода построения примитивных многочленов данной степени над конечным полем.
5. Вычисление числа нормированных неприводимых многочленов данной степени над конечным полем.
6. Вычисление произведения всех нормированных неприводимых многочленов данной степени над конечным полем.
7. Второй метод нахождения минимального многочлена элемента.

5. Учебно-методическое обеспечение дисциплины

5.1. Основная рекомендуемая литература

1. Кабанов В.В. Конечные поля (электронное издание) – Екатеринбург: УрГУ, 2008.
2. Ван-дер-Варден Б.Л. Алгебра. – М.: Наука, 1976.
3. Ленг С. Алгебра – М.: Мир, 1968.
4. Лидл Р., Нидеррайтер Г. Конечные поля, том 1 и 2. – М.: Мир, 1988.

6. **Материально-технического обеспечения дисциплины** не требуется**.**