МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Государственное образовательное учреждение
высшего профессионального образования
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Механико-математический факультет
Кафедра алгебры и геометрии

УТВЕРЖДАЮ
Проректор по учебной работе
_____В.П. Гарькин
«_____»_____2011 г.

РАБОЧАЯ ПРОГРАММА СПЕЦИАЛЬНОГО КУРСА

Алгебраические основы теории кодирования

(блок «Общие математические и естественнонаучные дисциплины»; раздел «Федеральный компонент»; основная образовательная программа специальности 090102 Компьютерная безопасность)

Самара
2011

Рабочая программа составлена на основании Государственного образовательного стандарта высшего профессионального образования специальности 090102 Компьютерная безопасность, утвержденного 05.04.00 (номер государственной регистрации 283 ИНФ/СП) и типовой (примерной) программы дисциплины «Алгебраические основы теории кодирования», одобренной Советом УМО по образованию в области информационной безопасности.

Составитель рабочей программы: доц. Фролов И.С, доц. Попов С.Ю.
Рецензент: д.ф.-м..н., проф В.Е. Воскресенский

Рабочая программа утверждена на заседании кафедры алгебры и геометрии (протокол № 6 от «17» января 2011 г.)

Заведующий кафедрой
17 января 2011 г. _____ А.Н.Панов

СОГЛАСОВАНО
Декан
факультета
″____″ _____ 2011 г. _____ С.Я.Новиков

Начальник
методического отдела
″____″ _____ 2011 г. _____ Н.В.Соловова

ОДОБРЕНО
Председатель
методической
комиссии факультета
″____″ _____ 2011 г. _____ Е.Я.Горелова

Цели и задачи дисциплины, ее место в учебном процессе, требования к уровню освоения содержания дисциплины

1.1. Цели и задачи изучения дисциплины

Познакомить студентов с алгебраическими вопросами теории кодирования и декодирования. Познакомить с основными типами алгеброгеометрических кодов.

Задачи дисциплины

Требования к уровню подготовки студента, завершившего изучение данной дисциплины: студенты должны знать методы решения систем линейных уравнений, методы построения конечных полей, алгебру многочленов

Студенты, закончившие изучение данной дисциплины, должны:

- иметь представление:

1) о приложениях линейной алгебры и алгебры многочленов в теории кодирования
2) о теории алгебраических кривых
3) о методах построения алгеброгеометрических кодов

--знать:

1) основные определения и формулировки теорем теорем курса и умение их применять при решении прикладных проблем теории кодирования:
2) знание постановки задачи теории кодирования,
3) знание принципов декодирования блочных кодов и вероятностного обоснования оптимальности декодирования посредством ближайшего кодового слова,
4) знание основных методик кодирования.

- уметь:

1) вычислять размерность линейного кода, составлять матрицу кода и его проверочную матрицу, вычислять кодовое расстояние
2) применять конструкции алгебраической геометрии с целью построения помехоустойчивых линейных кодов

1.2. Связь с предшествующими дисциплинами

Этот курс является естественным продолжением курсов алгебры и теории чисел. Курс показывает как основные положения алгебры и теории чисел прилагаются в теории кодирования

1.3. Связь с последующими дисциплинами

Курс поможет студентам в написании курсовых и дипломных работ.

2. Содержание дисциплины

2.1. Объем дисциплины в виде учебной работы (в часах)

ОЧНАЯ ФОРМА ОБУЧЕНИЯ, 9-й семестр, экзамен

Объем дисциплины и виды учебной работы (час)

Виды занятий	Всего часов
Лекции	50
Самостоятельная работа	40
Вид итогового контроля	экзамен

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

№	Раздел дисциплины	Количество часов
		Лекции
1.	Основные структуры алгебры и основы алгебраической геометрии	10
2.	Блочные коды, исправляющие ошибки	12
3.	БЧХ-коды, циклические коды	8
4.	Линейные коды и системы точек	10
5.	Алгеброгеометрические коды	10

3.2.Содержание разделов дисциплины

Раздел 1. Основные структуры алгебры и основы алгебраической геометрии. Повторение основных сведений из курса алгебры, касающихся групп, колец, конечных полей. Аффинные и проективные пространства над конечным полем. Аффинные и проективные алгебраические многообразия. Алгебраические кривые. Дифференциальный критерий гладкости кривой. Поле рациональных функций на проективной неприводимой кривой. Группа дивизоров на кривой. Главные дивизоры. Теорема о степени главного дивизора на проективной кривой. Эллиптические кривые: определение, вывод уравнения, групповой закон. Пространство дивизора, его размерность.

Раздел 2. Блочные коды, исправляющие ошибки. Постановка задачи теории кодирования: математическая модель канала с помехами, функция кодирования, функция ошибок и декодирование. Алфавит. Блочные коды. Метрика Хэмминга и расстояние между сообщениями. Понятие минимального кодового расстояния. Принципы декодирования, вероятностное обоснование принципа максимального правдоподобия при декодировании. Критерии обнаружения и исправления ошибок при блочном кодировании.

Совершенные коды, граница Хэмминга (необходимое условие совершенности кода). Совершенные коды Хэмминга. Групповые коды и схема оптимального декодирования. Наименьшее кодовое расстояние и минимальный вес ненулевого кодового слова при групповом кодировании. Линейные коды, матричное кодирование, кодирующие матрицы и их характеризация. Полиномиальные коды. Кодирующие матрицы полиномиального кода. Особенности характеристик полиномиальных кодов с кодирующим многочленом с достаточно большой экспонентой.

Раздел 3. БЧХ-коды, циклические коды. Конструкция кодов Боуза-Чоудхури-Хоквингема как полиномиальных кодов с заранее заданной нижней границей для минимального кодового расстояния. Число контрольных символов для двоичного БЧХ-кода. Циклические коды, их полиномиальность. Особенности декодирования циклических кодов. Модели декодеров, построенные на основе системы вспомогательных функций. Пример: декодер двоичного совершенного кода Голея. Построение циклических кодов посредством выбора корней кодирующего многочлена, примеры: циклические совершенные коды Хэмминга.

Раздел 4. Линейные коды и системы точек. Определение $[m,n,d]_q$-системы точек в n-мерном аффинном пространстве над конечным полем GF(q). Теорема о взаимно-однозначном соответствии между $[m,n,d]_q$-системами и линейными $[m,n,d]_q$-кодами. Алгоритм вычисления минимального кодового расстояния линейного кода. Граница Синглтона и коды с максимально достижимым кодовым расстоянием (МДР-коды). Описание двоичных МДР-кодов. Оценка параметров q-ичного МДР-кода, пример: коды Рида-Соломона.

Раздел 5. Алгеброгеометрические коды. Основные конструкции алгебро-геометрических кодов: L-конструкция, Ω-конструкция, P-конструкция. Количество точек на кривых над конечным полем. Максимальные кривые, примеры: максимальные эллиптические кривые. Вычисление пространства одноточечных дивизоров. Построение одноточечных кодов $(C,X,D)_L$ на максимальных эллиптических кривых над полями из 16 и 27 элементов.

4. Литература

4.1. Основная литература

1. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. *Алгеброгеометрические коды. Основные понятия.* М.: МЦНМО, 2003.
2. Биркгоф Г., Барти Т., *Современная прикладная алгебра*. Изд.2, стереот. 2005.

4.2. Дополнительная литература

1. Кассами Т., Токура Н., Ивадари Е., Инагаки Я. *Теория кодирования*. М.: Мир, 1978.
2. Питерсон У., Уэлдон Э. *Коды, исправляющие ошибки.* М.: Мир, 1976.