ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

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

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Конечные поля

Методические указания

Автор: профессор кафедры алгебры
и дискретной математики
В.В. Кабанов

Екатеринбург
2008

Методические указания
по изучению дисциплины «Конечные поля»

Дисциплина «Конечные поля» является специальной дисциплиной, на основе которой излагаются ряд других дисциплин специальности 090102 «Компьютерная безопасность» и направления 010300 «Математика. Компьютерные науки». Данная дисциплина читается в 6 семестре. Изначально предполагается использование предварительных сведений по общей алгебре и дискретной математике, излагаемых на первом курсе. Изучаемый материал достаточно абстрактен. Поэтому предполагается определенный уровень математической культуры студентов, которым они должны были овладеть на младших курсах.

Содержание дисциплины изложено на основе государственного образовательного стандарта, но в авторской интерпретации. Основные объекты теории конечных полей и их свойства излагаются с подробными примерами. Дается обоснование того факта, что теория конечных полей входит в универсальный язык, на котором говорит современная компьютерная наука.

Основной задачей дисциплины является развитие у студентов математической культуры в области строения конечных полей и вычислений в них, ознакомление со свойствами неприводимых и примитивных многочленов над конечными полями, ознакомление с алгоритмами, решающими ряд задач для неприводимых многочленов над конечными полями.

Некоторые разделы курса вызовут трудности у студентов, поскольку придется столкнуться с достаточно абстрактными понятиями. В первую очередь это относится к строению конечных полей и вычислениям в них. Именно по данной причине и было написано учебное пособие «Конечные поля». В этом пособии предпринята попытка привести элементарное изложение основ теории конечных полей с сохранением уровня математической строгости, соответствующей традициям математических факультетов классических университетов. В пособии «минимизированы» доказательства всех приводимых теорем с целью достижения прозрачности доказательств.

Большую часть учебного материала курса можно обнаружить в замечательной монографии Лидла и Нидеррайтера. Однако эта монография написана для специалистов и не рассчитана на студентов. Наше пособие в доступной форме излагает необходимый материал, делая его понятным для студентов.