АННОТАЦИЯ

на методическое пособие «Специальные функции» для студентов 2 курса специальности «Безопасность информационных и коммуникационных сетей»

автора Курганского А.Н.

В методическом пособии собран лекционный материал односеместрового курса «Специальные функции», который читается студентам 2 курса физико-технического факультета специальности безопасность информационных и коммуникационных сетей.

Курс лекций «Специальные функции» является базовым для курса лекций по криптографии. Пособие содержит современные теоретические сведения и алгоритмы теории чисел и абстрактной алгебры и состоит из четырех глав, разбитых на разделы и подразделы. Первая глава содержит элементы теории чисел, связанные с модулярной арифметикой и классами вычетов. Первый раздел главы знакомит с соответствующими понятиями. В последующих разделах представлены алгоритмы, используемые в учебном варианте алгоритма шифрования RSA. Вторая глава посвящена элементам абстрактной группы. Первый и второй раздел главы знакомят с понятиями теории конечных групп, колец и полей. Два следующих раздела посвящены кольцам и полям многочленов от одной и нескольких переменных. Следующий раздел знакомит с элементами алгебраической геометрии и теории эллиптических кривых над конечными полями. Далее идет общее описание групп на эллиптических кривых и в заключительных разделах главы приводятся подробные примеры групп на эллиптических кривых над полем характеристики 2 и 3. В третье главе продолжено изложение элементов теории чисел. В ней даны китайская теорема об остатках, понятия символов Лежандра и Якоби, алгоритмы проверки числа на простоту, алгоритмы решения степенных и показательных уравнений в конечных числовых полях и группах. В заключительной главе приведены примеры контрольных работ по темам всего курса. В дополнительных разделах собраны необходимые таблицы, списки обозначений и сокращений, а также предметный указатель.