АННОТАЦИЯ

на методическое пособие «Математические основы защиты информации» для студентов направления подготовки 09.03.01 «Информатика и вычислительная техника» квалификационного уровня бакалавр

автора Курганского А.Н.

В методическом пособии собран лекционный материал семестрового курса по учебной дисциплине «Защита информации» для студентов физико-технического факультета направления подготовки «Информатика и вычислительная техника».

Курс лекций «Математические основы защиты информации» является базовым для учебной дисциплины «Технические средства защиты информации». Пособие содержит современные теоретические сведения и алгоритмы из теории чисел и абстрактной алгебры, а также описание ряда современных криптографических алгоритмов и протоколов на их основе. Пособие состоит из четырех глав, разбитых на разделы и подразделы. Первая глава содержит элементы теории чисел по тематике модулярной арифметики и классов вычетов. Первый раздел главы знакомит с соответствующими понятиями. В последующих разделах представлены все вспомогательные алгоритмы, используемые в алгоритме шифрования RSA. Вторая глава посвящена элементам теории абстрактных групп. Первый и второй раздел главы знакомят с понятиями теории конечных групп, колец и полей. Два последующих 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 третьей 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. Пятая глава посвящена интерактивным доказательствам и доказательствам с нулевым разглашением – современным направлениям развития криптографических протоколов. Шестая глава посвящена элементам теории информации Шеннона: понятиям энтропии и избыточности языка, формальным моделям блочных шифров и анализу классических шифров. 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.

Материал курса закладывает основы для изучения учебной дисциплины «Технические средства защиты информации». Считаю, что представление материала и выбранный автором объем является достаточным для студентов данного направления. Материал подан в аккуратном и ясном стиле изложения с достаточным числом иллюстрирующих таблиц, рисунков, упражнений и контрольных вопросов.

Считаю, что данное методическое пособие является необходимым и полезным для учебного процесса, и рекомендую ее для издания.

Доктор технических наук, профессор,

зав. кафедрой физики неравновесных

процессов, метрологии

и экологии им. И. Л. Повха В.В. Белоусов