Министерство образования Российской Федерации
Ярославский государственный университет им. П.Г. Демидова
Кафедра компьютерных сетей

Математические методы защиты информации

Часть 3

Методические указания

Рекомендовано
Научно-методическим советом для университета для студентов, обучающихся по направлению
Прикладная математика и информатика

Ярославль
ЯрГУ
2013

УДК 004.056:51(072)
ББК В13я73
М34

Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2013 года

Рецензент
кафедра компьютерных сетей ЯрГУ

Составитель **М. В. Краснов**

М34 **Математические методы защиты информации. Ч. 3** : методические указания / сост. М. В. Краснов; Яросл. гос. ун-т им. П. Г. Демидова. – Ярославль : ЯрГУ, 2013. – 48 с.

Основное использование вычислительной техники связано с хранением информации. Естественно, возникает задача защиты информации от несанкционированного использования. В работе сформулированы основные идеи создания поточных алгоритмов. Наиболее известные из них подробно описаны. Рассмотрена также проблема формирования хеш-значения, которая возникает при криптографических методах защиты информации. Указания могут быть использованы как справочный материал при выполнении домашних заданий, курсовых работ и при подготовке к экзаменам.

Предназначены для студентов, обучающихся по направлению 010400.62 Прикладная математика и информатика (дисциплина «Математические методы защиты информации», цикл Б3), очной формы обучения.

УДК 004.056:51(072)
ББК В13я73

ŋqdqүеɏ bƎ dеqƎbүзе d еɑɑбɑɏ ɟqdqҮqүè

Оглавление