

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 студен-  
тов, 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**

**Математические методы защиты информации. Ч. 3 :**  
М34 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

© ЯрГУ, 2013

## Оглавление

ВВЕДЕНИЕ .....	3
ПОТОЧНЫЕ ШИФРЫ .....	5
Генераторы псевдослучайных последовательностей .....	6
Конгруэнтные генераторы .....	7
Регистр сдвига с линейной обратной связью (LFSR) .....	8
Аддитивные генераторы .....	16
Генераторы, построенные с использованием односторонних функций .....	17
Генераторы, построенные с использованием блочных шифров .....	21
Генераторы, построенные с использованием блоков стохастического преобразования .....	22
Примеры поточных шифров .....	25
Шифр RC4 .....	25
Шифр A5 .....	27
Шифр WAKE .....	29
Шифр Fish .....	30
SEAL .....	31
Хеш-функция .....	35
Хеш-функция MD5 .....	38
Хеш-функция SHA-1 .....	41
ЗАДАЧИ .....	44
ЛИТЕРАТУРА .....	46