

Министерство образования и науки Российской Федерации
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Т.А. ГУЛЬТЯЕВА

ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ И КРИПТОГРАФИИ

Утверждено Редакционно-издательским советом университета
в качестве конспекта лекций

НОВОСИБИРСК
2010

УДК 004.056.55(075.8)
Г 944

Рецензенты:

канд. техн. наук, доц. кафедры программных систем
и баз данных *Н.Л. Долозов,*

канд. техн. наук, доц. кафедры защиты информации *В.Е. Хиценко*

Работа подготовлена на кафедре программных систем и баз данных
для студентов III курса ФПМИ по специальностям
«Прикладная математика и информатика» (010500),
«Математическое обеспечение и администрирование
информационных систем» (010503),
«Прикладная информатика в менеджменте» (080801)

Гульятеева Т.А.

Г 944 Основы теории информации и криптографии : конспект лекций / Т.А. Гульятеева. – Новосибирск : Изд-во НГТУ, 2010. – 88 с.

ISBN 978-5-7782-1425-5

Конспект лекций посвящен основам теории информации и криптографии и охватывает широкий круг вопросов, позволяющих студентам получить базовые знания по курсу.

Он также может быть полезен для инженеров и сотрудников, осваивающих базовые знания основ теории информации и криптографии.

УДК 004.056.55(075.8)

ISBN 978-5-7782-1425-5

© Гульятеева Т.А., 2010
© Новосибирский государственный
технический университет, 2010

ОГЛАВЛЕНИЕ

Тема № 1. ОСНОВНЫЕ АСПЕКТЫ ТЕОРИИ ИНФОРМАЦИИ	3
1.1. Введение в теорию информации. Задачи, решаемые в рамках теории информации	3
1.2. Вероятностно-статистические модели сообщений и их свойства	4
1.2.1. Источники дискретных сообщений и их вероятностные модели	4
1.2.2. Собственная информация	6
1.2.3. Взаимная информация	8
1.2.4. Энтропия	12
1.2.5. Условная энтропия	15
1.2.6. Избыточность	18
Тема № 2. ОСНОВНЫЕ ПРИНЦИПЫ КОДИРОВАНИЯ	22
2.1. Введение в теорию кодирования	22
2.2. Основы экономного кодирования	23
2.2.1. Сжатие без потерь информации	23
2.2.2. Сжатие с потерями информации	23
2.2.3. Кодеры, основанные на системе сжатия без потерь информации	24
2.2.4. Основные методы побуквенного кодирования	25
2.2.4.1. Код Хаффмана	26
2.2.4.2. Код Шеннона	28
2.2.4.3. Код Шеннона–Фано	30
2.2.4.4. Код Гильбера–Мура	31
2.3. Помехоустойчивое кодирование	33
2.3.1. Коды с обнаружением ошибок	35
2.3.2. Коды с исправлением ошибок	36
2.3.2.1. Линейные блочные коды	36
2.3.2.2. Коды Хэмминга	38
2.3.2.3. Циклические коды	40
Тема № 3. ОСНОВЫ КРИПТОГРАФИИ	43
3.1. Терминология и основные понятия криптологии	43
3.1.1. Основные аспекты криптографии	43
3.1.2. Основные аспекты криптоанализа	46

3.2. Шенноновские модели криптографии.....	48
3.3. Теоретико-информационные оценки стойкости симметричных криптосистем.....	50
Тема № 4. МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ.....	55
4.1. Псевдослучайные последовательности.....	55
4.1.1. Равномерно распределенная случайная последовательность.....	56
4.1.2. Алгоритмы генерации псевдослучайных последовательностей.....	57
4.2. Теория чисел.....	58
4.2.1. Простые числа.....	58
4.2.2. Тестирование чисел на простоту и построение больших простых чисел.....	59
4.2.3. Теория сравнения.....	60
4.2.3.1. Арифметика вычетов.....	60
4.2.3.2. Функция Эйлера.....	63
4.2.3.3. Сравнение первой степени.....	67
4.2.3.3.1. Решение сравнения первой степени с использованием алгоритма Евклида.....	68
4.2.3.3.2. Решение сравнения первой степени с использованием расширенного алгоритма Евклида.....	71
4.2.3.3.3. Решение сравнения способом Эйлера.....	73
4.2.3.4. Первообразные корни.....	73
4.2.3.5. Дискретные логарифмы в конечном поле.....	75
4.2.4. Примеры систем шифрования, основанные на проблемах теории чисел.....	76
4.2.4.1. Система шифрования RSA.....	76
4.2.4.2. Система шифрования Диффи–Хеллмана.....	78
4.2.5. Разложение на множители (факторизация).....	79
4.2.6. Вычисление в поле Галуа.....	80
Библиографический список.....	84