

В.М.Белов, С.Н.Новиков, О.И.Солонская

ТЕОРИЯ ИНФОРМАЦИИ

Курс лекций

*Допущено Сибирским региональным отделением
УМО по образованию в области информационной
безопасности в качестве учебного пособия для студентов,
обучающихся специальности
090302 – «Информационная безопасность
телекоммуникационных систем»*

Москва
Горячая линия - Телеком
2012

УДК 621.391 (075.8)

ББК 32.811

Б78

Белов В. М., Новиков С. Н., Солонская О. И.

Б78 Теория информации. Курс лекций. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2012. – 143 с.: ил.
ISBN 978-5-9912-0237-4.

Рассмотрены в доступной форме основные положения теории информации. Материалы систематизированы по следующим ключевым разделам: определение информационных потерь в каналах связи с помехами, построение оптимальных кодов, обнаружение и исправление ошибок при использовании различных методов передачи и обработки информации, представление кодов в памяти ЭВМ в сжатом виде и в виде разнообразных структур.

Для студентов специальности 090302 – «Информационная безопасность телекоммуникационных систем». Может быть полезно студентам других инфокоммуникационных и радиотехнических специальностей, аспирантам и специалистам.

ББК 32.811

Адрес издательства в Интернет www.techbook.ru

**Белов Виктор Матвеевич, Новиков Сергей Николаевич,
Солонская Оксана Игоревна**

Теория информации. Курс лекций.

Учебное пособие для вузов

Обложка художника В. Г. Ситникова

Подписано в печать 19.02.2012. Формат 60×88/16. Уч. изд. л. 9,14. Тираж 500 экз. (1-й завод 100 экз.)

ISBN 978-5-9912-0237-4

© В. М. Белов, С. Н. Новиков,
О. И. Солонская, 2012

© Издательство «Горячая линия–Телеком», 2012

Содержание

Предисловие	6
1. Введение в теорию информации	7
1.1. Краткая историческая справка о развитии систем передачи информации (систем связи) и теории информации (теории связи)	8
1.1.1. Краткая история развития систем связи	8
1.1.2. О понятии «информация». Краткая история развития теории информации	10
1.1.2.1. О понятии «информация»	10
1.1.2.2. Краткая историческая справка о развитии теории информации	11
1.2. Информационные метрики	13
1.2.1. Структурные меры информации	13
1.2.1.1. Геометрическая мера	13
1.2.1.2. Комбинаторная мера	14
1.2.1.3. Аддитивная мера	16
1.2.2. Статистическая мера	16
1.2.3. Семантическая мера	17
2. Энтропия вероятностной схемы	18
2.1. Энтропия, как мера степени неопределенности физической системы	18
2.2. Единицы измерения энтропии	20
2.3. Основные свойства энтропии простой физической системы	21
2.4. Энтропия и математическое ожидание	23
2.5. Условная энтропия и энтропия объединения	24
Контрольные вопросы к главам 1 и 2	29
3. Основные теоремы Шеннона о характеристизации источников информации	31
3.1. Количество информации в дискретном сообщении. Дискретные источники сообщений без памяти и с памятью. Избыточность дискретного источника сообщений	31
3.2. Первая теорема Шеннона	35
3.2.1. Прямая и обратная теоремы Шеннона для канала связи без шума. Первый способ доказательства прямой теоремы Шеннона	35
3.2.2. Второй способ доказательства прямой теоремы Шеннона для канала связи без шума. Метод Фано. Оптимальные коды	40
3.2.3. Практическое применение первой теоремы Шеннона	44

3.3. Вторая теорема Шеннона и ее следствия	45
3.3.1. Прямая теорема Шеннона для дискретного постоянного канала с шумом	45
3.3.2. Обратная теорема Шеннона для дискретного постоянного канала с шумом	47
3.3.3. Следствие из второй теоремы Шеннона	49
3.4. Статистический анализ случайных последовательностей. Энтропийные и информационные характеристики случайных последовательностей.	52
Контрольные вопросы к главе 3	53
4. Статистические модели каналов связи	55
4.1. Математические модели каналов связи	55
4.1.1. Схема передачи информации. Классификация каналов связи	55
4.1.2. Непрерывные каналы связи	58
4.1.3. Дискретные каналы связи	60
4.2. Влияние шумов на пропускную способность дискретного канала связи	62
4.3. Пропускная способность систем передачи информации	63
5. Оптимальное кодирование	67
5.1. Префиксные коды	67
5.2. Неравенство Крафта	75
5.3. Информационная избыточность. Границы для средней длины кодов	79
Контрольные вопросы к главам 4 и 5	82
6. Обнаружение и исправление ошибок в сообщениях. Понятие об идее коррекции ошибок	84
7. Линейное кодирование	88
7.1. Свойства помехозащищающих кодов	88
7.1.1. Помехоустойчивые коды и их применение	88
7.1.2. Основные параметры помехоустойчивых кодов	89
7.1.3. Граничные соотношения между параметрами помехоустойчивых кодов	89
7.1.4. Классификация помехоустойчивых кодов	90
7.2. Линейные коды. Параметры и свойства	92
7.3. Код Хэмминга	98
Контрольные вопросы к главам 6 и 7	100
8. Циклические коды	101
8.1. Определение и свойства двоичных циклических кодов	101
8.2. Систематические циклические коды	105
8.3. Обнаружение пакетов ошибок	108

9. Построение и декодирование конкретных циклических кодов	110
9.1. Коды, исправляющие одиночную ошибку, кодовое расстояние $d_0 = 3$	110
9.2. Коды, обнаруживающие трехкратные ошибки, $d_0 = 4$	112
9.3. Циклические коды, исправляющие две и большее количество ошибок, $d_0 \geq 5$	113
10. Обнаружение и исправление ошибок при передаче и обработке информации на стандартной аппаратуре.	116
11. Сжатие информации	121
Контрольные вопросы к главам 8, 9, 10, 11.	126
12. Структурное кодирование.	128
Контрольные вопросы к главе 12	139
Примерные вопросы к экзамену по дисциплине «Теория информации»	140
Библиография	142

Предисловие

Дисциплина «Теория информации» определена в государственном образовательном стандарте высшего профессионального образования специальности 090302 «Информационная безопасность телекоммуникационных систем» как федеральный компонент общих математических и естественнонаучных дисциплин.

Теория информации тесно связана с другими дисциплинами, изучаемыми студентами. Она предполагает знания таких дисциплин как «Математический анализ», «Алгебра», «Теория вероятностей и математическая статистика», является базой для дисциплин «Теория радиотехнических сигналов» и «Криптографические методы защиты информации».

Предлагаемое учебное пособие по «Теории информации» отвечает требованиям большинства разделов программы одноименного курса, читаемых студентам, обучающимся по специальности 090302 «Информационная безопасность телекоммуникационных систем».

Цель учебного пособия — помочь освоить основные положения теории информации и кодирования, научить определять информационные потери в каналах связи с помехами, строить оптимальные коды, обнаруживать и исправлять ошибки при различных методах передачи и обработки информации, представлять коды в памяти ЭВМ в сжатом виде и в виде разнообразных структур.

Материал учебного пособия разбит на 12 тем. В каждой теме предложен необходимый минимум теоретических сведений.

Авторы выражают глубокую благодарность коллегам, работающим в области защиты информации, А. Б. Архиповой, Е. Н. Пивкину, О. В. Воробьевой за неоценимую помощь в подготовке материалов для данного пособия.