

УДК 621.391
ББК 32.811
К 73

Рецензенты:

профессор Военно-воздушной инженерной академии им. Н.Е. Жуковского,
доктор технических наук, профессор **Величкин А. И.**, г. Москва;
начальник кафедры Ростовского военного института ракетных войск, доктор
технических наук, профессор **Габриэльян Д. Д.**, г. Ростов-на-Дону;
председатель правления ЗАО "Институт информационных технологий", заведующий
кафедрой "Безопасность информационных технологий" Харьковского национального
университета радиоэлектроники, доктор технических наук, профессор **Горбенко И. Д.**,
г. Харьков.

*Монография подготовлена и издана в рамках
национального проекта «Образование»
по «Программе развития федерального государственного образовательного учреждения
«Южный федеральный университет» на 2007–2010 гг.»*

Котенко В.В., Румянцев К.Е.

К 73 Теория информации и защита телекоммуникаций: монография / В. В. Котенко,
К. Е. Румянцев. – Ростов н/Д: Изд-во ЮФУ, 2009. – 369 с.: ил. 49.
ISBN 978-5-9275-0670-5

Содержание монографии составляют результаты исследований в направлении развития фундаментальных основ теории информации с позиций обеспечения информационной безопасности. Основу изложения материала составляет конкретизация модифицированной концепции теории информации, которая развивается на стратегии кодирования источников и кодирования для каналов, принципы информационного анализа источников и каналов, методы эффективного и помехоустойчивого кодирования, теоретические основы защиты информации при кодировании источников, принципы информационного анализа методов защиты информации источников, информационный подход к оценке качества связи и защиты информации. Приводятся оригинальные подходы к решению широкого круга задач обработки передачи и защиты информации, теоретически подкрепленные теоремами, следствиями и их доказательствами. Рассмотрение ведется с согласованных единых позиций, в едином стиле, что не вызовет разночтения в понимании отдельных сложных вопросов. Особое внимание уделено тенденциям развития комплексных подходов к обработке, передаче и защите информации, что особенно актуально в условиях интенсивного развития информационно-телекоммуникационных технологий.

Книга предназначена для научных работников и инженеров, занимающихся разработкой и исследованием защищенных телекоммуникационных систем. Может быть полезна студентам, магистрантам и аспирантам при освоении вопросов информационной защиты телекоммуникаций.

ISBN 978-5-9275-0670-5

УДК 621.391
ББК 32.811

© ТТИ ЮФУ, 2009
© В.В. Котенко, К.Е. Румянцев, 2009
© Южный федеральный
университет, 2009

ОГЛАВЛЕНИЕ

Предисловие.....	3
Введение.....	5
ГЛАВА 1. ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ.....	10
1.1. Состояние и проблемы современной теории информации.....	10
1.2. Принципы теоретического построения. Система аксиом и исходных определений.....	13
1.3. Концепция теории информации.....	25
1.4. Количественная оценка информации.....	28
1.4.1. <i>Количество информации</i>	28
1.4.2. <i>Среднее количество информации и энтропия</i>	32
1.5. Средняя взаимная информация для дискретных ансамблей.....	38
1.5.1. <i>Взаимная информация и условная собственная информация</i> ..	38
1.5.2. <i>Средняя взаимная информация и условная энтропия</i>	41
1.5.3. <i>Средняя условная взаимная информация</i>	44
1.5.4. <i>Свойства средней взаимной информации</i>	45
1.6. Средняя взаимная информация для непрерывных ансамблей.....	47
ГЛАВА 2. ИСТОЧНИКИ ИНФОРМАЦИИ.....	51
2.1. Представление источников информации.....	51
2.1.1. <i>Непрерывные источники</i>	51
2.1.2. <i>Дискретные источники</i>	53
2.2. Энтропия дискретных источников.....	55
2.2.1. <i>Дискретные источники без памяти</i>	55
2.2.2. <i>Дискретные стационарные источники</i>	58
2.2.3. <i>Эргодические стационарные источники</i>	60
2.2.4. <i>Марковские источники</i>	64

2.3. Энтропия непрерывных источников.....	71
2.4. Избыточность источников информации.....	74
ГЛАВА 3. КОДИРОВАНИЕ ДИСКРЕТНЫХ ИСТОЧНИКОВ.....	78
3.1. Стратегия кодирования дискретных источников.....	78
3.2. Теоремы кодирования для дискретных источников без памяти...	81
3.2.1. Коды с фиксированной длиной.....	81
3.2.2. Неравномерные коды.....	86
3.3. Теоремы кодирования для дискретных источников с памятью....	93
3.3.1. Стационарные источники.....	93
3.3.2. Эргодические источники.....	95
3.3.3. Марковские источники.....	95
3.4. Стоимость и избыточность кодирования. Теорема Шеннона для кодирования источников.....	96
3.5. Стратегия защиты информации при кодировании дискретных источников.....	99
ГЛАВА 4. ЭФФЕКТИВНОЕ КОДИРОВАНИЕ. МЕТОДЫ СЖАТИЯ ИНФОРМАЦИИ ПРИ КОДИРОВАНИИ ДИСКРЕТНЫХ ИСТОЧНИКОВ.....	116
4.1. Побуквенное кодирование.....	116
4.1.1. Префиксное кодирование.....	117
4.1.2. Оптимальное кодирование.....	121
4.2. Блочное кодирование.....	126
4.3. Неблочное кодирование.....	127
4.3.1. Метод Хоака.....	132
4.3.2. Методы арифметического кодирования.....	134
4.4. Универсальное кодирование.....	140
4.4.1. Методы интервального кодирования.....	141
4.4.2. Словарные методы кодирования. Методы Лемпела-Зива.....	142

ГЛАВА 5. КОДИРОВАНИЕ НЕПРЕРЫВНЫХ ИСТОЧНИКОВ.....	148
5.1. Цифровое представление непрерывных сообщений.....	148
5.1.1. Дискретизация. Теорема дискретизации.....	150
5.1.2. Квантование.....	151
5.1.3. Кодирование.....	152
5.1.4. Особенности цифрового представления.....	153
5.2. Информационные характеристики точности цифрового представления. Эпсилон-энтропия.....	155
5.2.1. Проблемы передачи непрерывной информации с оценкой ошибок дискретизации по времени и по амплитуде.....	155
5.2.2. Оценка ошибок дискретизации по амплитуде. Эпсилон-энтропия квантования.....	157
5.2.3. Эпсилон-энтропия цифрового представления аудиоинформации.....	160
5.2.4. Эпсилон-энтропия цифрового представления видеоинформации.....	163
5.3. Стратегия кодирования непрерывных источников.....	166
5.4. Информационные пределы избыточности. Теорема кодирования для непрерывных источников.....	169
5.5. Стратегия защиты информации при кодировании непрерывных источников.....	176
ГЛАВА 6. МЕТОДЫ СЖАТИЯ ИНФОРМАЦИИ ПРИ КОДИРОВАНИИ НЕПРЕРЫВНЫХ ИСТОЧНИКОВ.....	186
6.1. Принципы сжатия информации при кодировании непрерывных источников.....	186
6.2. Информационное квантование.....	190
6.3. Дифференциальная импульсно-кодовая модуляция.....	192
6.4. Дискретные wavelet-преобразования.....	195
6.5. Дискретные косинусные преобразования.....	204
6.6. Фрактальное кодирование.....	208

ГЛАВА 7. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПЕРЕДАЧИ ИНФОРМАЦИИ.	213
7.1. Схема и общая математическая модель передачи информации....	213
7.2. Принципы кодирования для канала.....	217
7.3. Общая математическая модель каналов передачи информации...	226
7.4. Представление кодов в виде многочленов.....	227
7.4.1. Группы и подгруппы.....	228
7.4.2. Поля и многочлены.....	229
7.4.3. Методика построения кодов. Алгоритм Евклида.....	231
7.5. Представление кодов в виде матриц.....	233
7.6. Минимальное кодовое расстояние.....	237
ГЛАВА 8. КОДИРОВАНИЕ ДЛЯ ДИСКРЕТНЫХ КАНАЛОВ.....	241
8.1. Дискретные каналы.....	241
8.2. Пропускная способность и скорость передачи.....	243
8.3. Влияние помех на передачу информации.....	247
8.4. Правила декодирования.....	252
8.5. Прямая и обратная теоремы кодирования Шеннона.....	256
8.6. Кодирование для дискретных каналов при передаче информации непрерывных источников.....	260
8.7. Стратегия кодирования для каналов. Общая методика помехоустойчивого кодирования.....	262
ГЛАВА 9. МЕТОДЫ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ.....	266
9.1. Общая характеристика методов помехоустойчивого кодирования.....	266
9.2. Линейные коды.....	268
9.3. Коды Хэмминга.....	271
9.4. Циклические коды.....	276
9.5. Коды Боуза-Чоудхури-Хоквингема.....	283

9.6. Псевдоциклические коды.....	285
9.7. Кодовые последовательности максимальной длины.....	288
9.8. Коды с постоянным весом.....	292
ГЛАВА 10. КОДИРОВАНИЕ ДЛЯ НЕПРЕРЫВНЫХ КАНАЛОВ.....	294
10.1. Взаимная информация для непрерывных каналов.....	294
10.2. Пропускная способность непрерывных каналов с аддитивным гауссовским шумом и ограничениями на полосу частот и по мощности.....	297
10.3. Эффективность помехоустойчивых кодов при кодировании для непрерывных каналов.....	301
ГЛАВА 11. ИНФОРМАЦИОННЫЙ ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИЙ.....	305
11.1. Возможности информационного подхода к оценке качества телекоммуникаций.....	305
11.2. Информационная оценка качества связи.....	314
11.2.1. Информационные пределы избыточности при передаче дискретной информации.....	314
11.2.2. Информационные пределы избыточности при передаче речевой информации.....	319
11.3. Информационная оценка эффективности защиты телекоммуникаций.....	320
11.3.1. Оценка эффективности и стойкости шифрования.....	320
11.3.2. Оценка эффективности аналогового скремблирования.....	322
11.3.3. Оценка эффективности цифрового скремблирования.....	332
Список принятых сокращений.....	338
Предметный указатель.....	340
Библиографический список.....	358