

# Содержание

<b>Наука об информации и качество образования</b> .....	9
<b>Предисловие</b> .....	24
<b>Глава 1. Введение</b> .....	27
1.1. Темы для анализа .....	28
1.2. Уроки информации .....	30
<b>Часть I. ЭНТРОПИЯ: Основания информации</b>	
<b>Глава 2. Определение информации</b> .....	34
2.1. Мера информации .....	35
2.2. Определение энтропии .....	37
2.3. Источники информации .....	39
2.4. Комбинации источников .....	40
2.5. Биты в качестве меры .....	42
2.6. О Клоде Э. Шенноне .....	43
2.7. Упражнения .....	44
2.8. Библиография .....	46
<b>Глава 3. Коды</b> .....	47
3.1. Проблема кодирования .....	47
3.2. Средняя длина кода и энтропия .....	54
3.3. Первая теорема Шеннона .....	57
3.4. Упражнения .....	59
3.5. Библиография .....	60
<b>Глава 4. Сжатие</b> .....	61
4.1. Кодирование по алгоритму Хаффмена .....	61
4.2. Межсимвольная зависимость .....	66
4.3. Кодирование Лемпеля – Зива .....	71
4.4. Другие формы сжатия информации .....	76
4.5. Упражнения .....	79
4.6. Библиография .....	81
<b>Глава 5. Каналы</b> .....	83
5.1. Дискретный канал .....	83
5.2. Условная и общая энтропия .....	85
5.3. Переключение канала .....	88
5.4. Взаимная информация .....	90
5.5. Пропускная способность канала .....	93
5.6. Вторая теорема Шеннона .....	94
5.7. Упражнения .....	96
5.8. Библиография .....	98
<b>Глава 6. Коды с исправлением ошибок</b> .....	99
6.1. Простейшие понятия кода .....	100
6.2. Расстояние Хемминга .....	102

6.3. Коды Хемминга .....	105
6.4. Линейные коды .....	107
6.5. Низкоплотностные коды проверки четности .....	108
6.6. Чередование .....	109
6.7. Сверточные коды .....	110
6.8. Турбокоды .....	112
6.9. Применение .....	113
6.10. Упражнения .....	115
6.11. Библиография .....	117
<b>Выводы по части I</b> .....	<b>119</b>

## Часть II. ЭКОНОМИКА: Стратегия стоимости

<b>Глава 7. Рынки</b> .....	<b>122</b>
7.1. Спрос .....	123
7.2. Производители .....	126
7.3. Общественный эффект .....	128
7.4. Конкуренция .....	130
7.5. Оптимальность формирования предельной себестоимости .....	131
7.6. Линейные кривые спроса .....	132
7.7. Авторские права и монополия .....	133
7.8. Другие методы ценообразования .....	136
7.9. Олигополия .....	138
7.10. Упражнения .....	141
7.11. Библиография .....	143
<b>Глава 8. Схемы ценообразования</b> .....	<b>144</b>
8.1. Дискриминация .....	144
8.2. Варианты .....	146
8.3. Пакетирование .....	148
8.4. Разделение .....	154
8.5. Упражнения .....	157
8.6. Библиография .....	159
<b>Глава 9. Стоимость</b> .....	<b>161</b>
9.1. Условная информация .....	162
9.2. Информативность и обобщенная энтропия .....	164
9.3. Решения .....	166
9.4. Структура стоимости .....	167
9.5. Функции полезности .....	170
9.6. Информативность и принятие решения .....	172
9.7. Упражнения .....	172
9.8. Библиография .....	173
<b>Глава 10. Взаимодействие</b> .....	<b>175</b>
10.1. Общеизвестная информация .....	176
10.2. Договориться о том, что существуют разногласия? .....	179
10.3. Информация и решения .....	182
10.4. Формальный анализ .....	183

10.5. Закон Меткалфа .....	186
10.6. Сетевая экономика .....	188
10.7. Упражнения .....	192
10.8. Библиография .....	194
<b>Выводы по части II .....</b>	<b>195</b>

### **Часть III. КРИПТОЗАЩИТА: Безопасность посредством математики**

<b>Глава 11. Шифры .....</b>	<b>198</b>
11.1. Определения .....	199
11.2. Примеры шифров .....	199
11.3. Анализ частотности .....	202
11.4. Криптограммы .....	202
11.5. Шифр Виженера .....	204
11.6. Шифр Плейфэра .....	208
11.7. Гомофонические коды .....	209
11.8. Шифр колеса Джефферсона .....	210
11.9. Машина «Энигма» .....	211
11.10. Одноразовый блокнот .....	215
11.11. Упражнения .....	216
11.12. Библиография .....	218
<b>Глава 12. Теория криптографии .....</b>	<b>219</b>
12.1. Идеальная безопасность .....	219
12.2. Отношения энтропии .....	221
12.3. Использование одноразового блокнота .....	227
12.4. Системы DES и AES .....	229
12.5. Упражнения .....	230
12.6. Библиография .....	232
<b>Глава 13. Криптография с открытым ключом .....</b>	<b>233</b>
13.1. Основная дилемма .....	233
13.2. Односторонние функции .....	234
13.3. Дискретные логарифмы .....	235
13.4. Обмен ключом Диффи – Хеллмана .....	236
13.5. Модульная математика .....	239
13.6. Альтернативное решение головоломки .....	241
13.7. Криптосистема RSA .....	242
13.8. Возведение в квадрат и умножение .....	245
13.9. Нахождение простых чисел .....	246
13.10. Эффективность .....	247
13.11. Будущее .....	248
<i>Приложение. Расширенный алгоритм Евклида .....</i>	<i>249</i>
13.12. Упражнения .....	250
13.13. Библиография .....	252
<b>Глава 14. Протоколы безопасности .....</b>	<b>254</b>
14.1. Цифровые подписи .....	254
14.2. Слепые подписи .....	257

14.3. Цифровые деньги .....	259
14.4. Идентификация .....	260
14.5. Доказательство нулевого знания .....	262
14.6. Смарткарты (интеллектуальные карты) .....	265
14.7. Упражнения .....	268
14.8. Библиография .....	269
<b>Выводы по части III .....</b>	<b>271</b>

#### Часть IV. ИЗВЛЕЧЕНИЕ информации из данных

<b>Глава 15. Структуры данных .....</b>	<b>274</b>
15.1. Списки .....	274
15.2. Деревья .....	278
15.3. Прослеживание деревьев .....	280
15.4. Двоичные деревья поиска (ДДП) .....	282
15.5. Частично упорядоченные деревья .....	285
15.6. Поиски .....	288
15.7. Основные алгоритмы сортировки .....	289
15.8. Быстрая сортировка .....	292
15.9. Пирамидальная сортировка .....	294
15.10. Слияния .....	295
15.11. Упражнения .....	296
15.12. Библиография .....	297
<b>Глава 16. Системы базы данных .....</b>	<b>299</b>
16.1. Реляционная структура .....	299
16.2. Ключи .....	302
16.3. Операции .....	304
16.4. Функциональные зависимости .....	306
16.5. Нормализация .....	307
16.6. Соединения и произведения .....	313
16.7. Языки базы данных .....	315
16.8. Упражнения .....	316
16.9. Библиография .....	318
<b>Глава 17. Информационный поиск .....</b>	<b>319</b>
17.1. Инвертированные файлы .....	320
17.2. Стратегии индексирования .....	322
17.3. Сжатие инвертированных файлов .....	326
17.4. Запросы .....	329
17.5. Методы ранжирования .....	330
17.6. Сетевое ранжирование .....	332
17.7. Упражнения .....	335
17.8. Библиография .....	335
<b>Глава 18. Добывание информации .....</b>	<b>337</b>
18.1. Обзор приемов .....	337
18.2. Анализ рыночной корзины .....	339
18.3. Аппроксимация по методу минимальных квадратов .....	343

18.4. Классификационные деревья .....	346
18.5. Методы Байеса .....	351
18.6. Машины опорного вектора .....	356
18.7. Другие методы .....	360
18.8. Упражнения .....	361
18.9. Библиография .....	362
<b>Выводы по части IV .....</b>	<b>363</b>

## Часть V. ИЗЛУЧЕНИЯ: Овладение частотой

<b>Глава 19. Понятия частоты .....</b>	<b>366</b>
19.1. Телеграф .....	368
19.2. Когда точки становятся тире .....	370
19.3. Ряды Фурье .....	373
19.4. Преобразование Фурье .....	374
19.5. Томас Эдисон и телеграф .....	377
19.6. Белл и телефон .....	377
19.7. Уроки по частоте .....	381
19.8. Упражнения .....	382
19.9. Библиография .....	385
<b>Глава 20. Радиоволны .....</b>	<b>386</b>
20.1. Частоты – почему? .....	386
20.2. Резонанс .....	390
20.3. Рождение радио .....	390
20.4. Радио Маркони .....	391
20.5. Ширина искровой полосы .....	394
20.6. Проблемы .....	396
20.7. Генерирование непрерывных волн .....	396
20.8. Триодная вакуумная лампа .....	398
20.9. Модуляционная математика .....	400
20.10. Принцип гетеродина .....	403
20.11. Частотная модуляция .....	404
20.12. Упражнения .....	406
20.13. Библиография .....	409
<b>Глава 21. Выборки и пропускная способность канала .....</b>	<b>410</b>
21.1. Энтропия .....	410
21.2. Пропускная способность гауссового канала .....	413
21.3. Теорема выборки .....	415
21.4. Обобщенная теорема выборки .....	418
21.5. Тепловой шум .....	420
21.6. Пропускная способность канала с ограниченной полосой пропускания ..	421
21.7. Расширенный спектр .....	422
21.8. Метод расширения .....	425
21.9. Системы множественного доступа .....	426
21.10. Упражнения .....	429
21.11. Библиография .....	431

<b>Глава 22. Сети</b> .....	432
22.1. Процессы Пуассона .....	433
22.2. Фреймы (кадры) .....	434
22.3. Система ALOHA .....	435
22.4. Регистрация несущей частоты .....	437
22.5. Алгоритмы маршрутизации .....	439
22.6. Алгоритм Беллмана – Форда .....	440
22.7. Маршрутизация вектора расстояния .....	441
22.8. Алгоритм Дейкстра .....	442
22.9. Другие вопросы .....	444
22.10. Упражнения .....	444
22.11. Библиография .....	445
<b>Выводы по части V</b> .....	446