

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ	23
Структура книги	25
Благодарности	26
ГЛАВА 1. СИГНАЛЫ И СПЕКТРЫ	29
1.1. Обработка сигналов в цифровой связи	30
1.1.1. Почему “цифровая”	30
1.1.2. Типичная блочная диаграмма и основные преобразования	32
1.1.3. Основная терминология области цифровой связи	39
1.1.4. Цифровые и аналоговые критерии производительности	41
1.2. Классификация сигналов	41
1.2.1. Детерминированные и случайные сигналы	41
1.2.2. Периодические и непериодические сигналы	42
1.2.3. Аналоговые и дискретные сигналы	42
1.2.4. Сигналы, выраженные через энергию или мощность	42
1.2.5. Единичная импульсная функция	44
1.3. Спектральная плотность	44
1.3.1. Спектральная плотность энергии	44
1.3.2. Спектральная плотность мощности	45
1.4. Автокорреляция	47
1.4.1. Автокорреляция энергетического сигнала	47
1.4.2. Автокорреляция периодического сигнала	48
1.5. Случайные сигналы	48
1.5.1. Случайные переменные	48
1.5.2. Случайные процессы	50
1.5.3. Усреднение по времени и эргодичность	53
1.5.4. Спектральная плотность мощности и автокорреляция случайного процесса	54
1.5.5. Шум в системах связи	58
1.6. Передача сигнала через линейные системы	61
1.6.1. Импульсная характеристика	62
1.6.2. Частотная передаточная функция	63
1.6.3. Передача без искажений	64
1.6.4. Сигналы, каналы, спектры	70
1.7. Ширина полосы при передаче цифровых данных	71
1.7.1. Узкополосные и широкополосные сигналы	71
1.7.2. Дилемма при определении ширины полосы	74
1.8. Резюме	77
Литература	77
Задачи	78
Вопросы для самопроверки	81

ГЛАВА 2. ФОРМАТИРОВАНИЕ И УЗКОПОЛОСНАЯ МОДУЛЯЦИЯ	83
2.1. Узкополосные системы	84
2.2. Форматирование текстовой информации (знаковое кодирование)	87
2.3. Сообщения, знаки и символы	87
2.3.1. Пример сообщений, знаков и символов	90
2.4. Форматирование аналоговой информации	91
2.4.1. Теорема о дискретном представлении	91
2.4.2. Наложение	97
2.4.3. Зачем нужна выборка с запасом	101
2.4.4. Сопряжение сигнала с цифровой системой	103
2.5. Источники искажения	104
2.5.1. Влияние дискретизации и квантования	104
2.5.2. Воздействие канала	105
2.5.3. Отношение сигнал/шум для квантованных импульсов	106
2.6. Импульсно-кодовая модуляция	107
2.7. Квантование с постоянным и переменным шагом	109
2.7.1. Статистика амплитуд при передаче речи	109
2.7.2. Неравномерное квантование	111
2.7.3. Характеристики компандирования	111
2.8. Узкополосная передача	113
2.8.1. Представление двоичных цифр в форме сигналов	113
2.8.2. Типы сигналов РСМ	113
2.8.3. Спектральные параметры сигналов РСМ	117
2.8.4. Число бит на слово РСМ и число бит на символ	118
2.8.5. <i>M</i> -арные импульсно-модулированные сигналы	119
2.9. Корреляционное кодирование	122
2.9.1. Двубинарная передача сигналов	122
2.9.2. Двубинарное декодирование	123
2.9.3. Предварительное кодирование	124
2.9.4. Эквивалентная двубинарная передаточная функция	125
2.9.5. Сравнение бинарного и двубинарного методов передачи сигналов	126
2.9.6. Полибинарная передача сигналов	127
2.10. Резюме	127
Литература	128
Задачи	128
Вопросы для самопроверки	131
ГЛАВА 3. УЗКОПОЛОСНАЯ ДЕМОДУЛЯЦИЯ/ОБНАРУЖЕНИЕ	133
3.1. Сигналы и шум	134
3.1.1. Рост вероятности ошибки в системах связи	134
3.1.2. Демодуляция и обнаружение	135
3.1.3. Векторное представление сигналов и шума	138
3.1.4. Важнейший параметр систем цифровой связи — отношение сигнал/шум	146
Содержание	7

3.1.5. Почему отношение E_b/N_0 — это естественный критерий качества	147
3.2. Обнаружение двоичных сигналов в гауссовом шуме	148
3.2.1. Критерий максимального правдоподобия приема сигналов	148
3.2.2. Согласованный фильтр	151
3.2.3. Реализация корреляции в согласованном фильтре	153
3.2.4. Оптимизация вероятности ошибки	155
3.2.5. Вероятность возникновения ошибки при двоичной передаче сигналов	159
3.3. Межсимвольная интерференция	164
3.3.1. Формирование импульсов с целью снижения ISI	167
3.3.2. Факторы роста вероятности ошибки	171
3.3.3. Демодуляция/обнаружение сформированных импульсов	174
3.4. Выравнивание	177
3.4.1. Характеристики канала	177
3.4.2. Глазковая диаграмма	179
3.4.3. Типы эквалайзеров	180
3.4.4. Заданное и адаптивное выравнивание	187
3.4.5. Частота обновления фильтра	189
3.5. Резюме	189
Литература	190
Задачи	190
Вопросы для самопроверки	193

ГЛАВА 4. ПОЛОСОВАЯ МОДУЛЯЦИЯ И ДЕМОДУЛЯЦИЯ

	195
4.1. Зачем нужна модуляция	196
4.2. Методы цифровой полосовой модуляции	196
4.2.1. Векторное представление синусоиды	199
4.2.2. Фазовая манипуляция	201
4.2.3. Частотная манипуляция	202
4.2.4. Амплитудная манипуляция	203
4.2.5. Амплитудно-фазовая манипуляция	203
4.2.6. Амплитуда сигнала	203
4.3. Обнаружение сигнала в гауссовом шуме	204
4.3.1. Области решений	204
4.3.2. Корреляционный приемник	205
4.4. Когерентное обнаружение	210
4.4.1. Когерентное обнаружение сигналов PSK	210
4.4.2. Цифровой согласованный фильтр	211
4.4.3. Когерентное обнаружение сигналов MPSK	215
4.4.4. Когерентное обнаружение сигналов FSK	218
4.5. Некогерентное обнаружение	221
4.5.1. Обнаружение сигналов в дифференциальной модуляции PSK	221
4.5.2. Пример бинарной модуляции DPSK	223
4.5.3. Некогерентное обнаружение сигналов FSK	225
4.5.4. Расстояние между тонами для некогерентной ортогональной передачи сигналов FSK	227

4.6. Комплексная огибающая	231
4.6.1. Квадратурная реализация модулятора	231
4.6.2. Пример модулятора D8PSK	232
4.6.3. Пример демодулятора D8PSK	234
4.7. Вероятность ошибки в бинарных системах	236
4.7.1. Вероятность появления ошибочного бита при когерентном обнаружении сигнала BPSK	236
4.7.2. Вероятность появления ошибочного бита при когерентном обнаружении сигнала в дифференциальной модуляции BPSK	238
4.7.3. Вероятность появления ошибочного бита при когерентном обнаружении сигнала в бинарной ортогональной модуляции FSK	239
4.7.4. Вероятность появления ошибочного бита при некогерентном обнаружении сигнала в бинарной ортогональной модуляции FSK	240
4.7.5. Вероятность появления ошибочного бита для бинарной модуляции DPSK	243
4.7.6. Вероятность ошибки для различных модуляций	245
4.8. M -арная передача сигналов и производительность	246
4.8.1. Идеальная достоверность передачи	246
4.8.2. M -арная передача сигналов	246
4.8.3. Векторное представление сигналов MPSK	248
4.8.4. Схемы BPSK и QPSK имеют одинаковые вероятности ошибки	250
4.8.5. Векторное представление сигналов MFSK	251
4.9. Вероятность символьной ошибки для M -арных систем ($M > 2$)	256
4.9.1. Вероятность символьной ошибки для модуляции MPSK	256
4.9.2. Вероятность символьной ошибки для модуляции MFSK	257
4.9.3. Зависимость вероятности битовой ошибки от вероятности символьной ошибки для ортогональных сигналов	258
4.9.4. Зависимость вероятности битовой ошибки от вероятности символьной ошибки для многофазных сигналов	260
4.9.5. Влияние межсимвольной интерференции	261
4.10. Резюме	262
Литература	262
Задачи	263
Вопросы для самопроверки	266
ГЛАВА 5. АНАЛИЗ КАНАЛА СВЯЗИ	269
5.1. Что такое бюджет канала связи	270
5.2. Канал	270
5.2.1. Понятие открытого пространства	271
5.2.2. Снижение достоверности передачи	271
5.2.3. Источники возникновения шумов и ослабления сигнала	272
5.3. Мощность принятого сигнала и шума	277
5.3.1. Дистанционное уравнение	277
5.3.2. Мощность принятого сигнала как функция частоты	280
5.3.3. Потери в тракте зависят от частоты	282
5.3.4. Мощность теплового шума	283
5.4. Анализ бюджета канала связи	285

5.4.1. Два важных значения E_b/N_0	287
5.4.2. Бюджет канала обычно вычисляется в децибелах	289
5.4.3. Какой нужен резерв	290
5.4.4. Доступность канала	292
5.5. Коэффициент шума, шумовая температура системы	297
5.5.1. Коэффициент шума	297
5.5.2. Шумовая температура	299
5.5.3. Потери в линии связи	300
5.5.4. Суммарный шум-фактор и общая шумовая температура	302
5.5.5. Эффективная температура системы	303
5.5.6. Шумовая температура неба	308
5.6. Пример анализа канала связи	312
5.6.1. Элементы бюджета канала	313
5.6.2. Добротность приемника	315
5.6.3. Принятая изотропная мощность	315
5.7. Спутниковые ретрансляторы	316
5.7.1. Нерегенеративные ретрансляторы	316
5.7.2. Нелинейное усиление ретрансляторов	322
5.8. Системные компромиссы	323
5.9. Резюме	324
Литература	324
Задачи	325
Вопросы для самопроверки	330
ГЛАВА 6. КАНАЛЬНОЕ КОДИРОВАНИЕ: ЧАСТЬ 1	331
6.1. Кодирование сигнала и структурированные последовательности	332
6.1.1. Антиподные и ортогональные сигналы	332
6.1.2. M -арная передача сигналов	335
6.1.3. Кодирование сигнала	335
6.1.4. Примеры системы кодирования сигналов	339
6.2. Типы защиты от ошибок	341
6.2.1. Связность оконечных устройств	341
6.2.2. Автоматический запрос повторной передачи	342
6.3. Структурированные последовательности	344
6.3.1. Модели каналов	344
6.3.2. Степень кодирования и избыточность	346
6.3.3. Коды с контролем четности	347
6.3.4. Зачем используется кодирование с коррекцией ошибок	350
6.4. Линейные блочные коды	354
6.4.1. Векторные пространства	355
6.4.2. Векторные подпространства	355
6.4.3. Пример линейного блочного кода $(6, 3)$	357
6.4.4. Матрица генератора	357
6.4.5. Систематические линейные блочные коды	359
6.4.6. Проверочная матрица	360
6.4.7. Контроль с помощью синдромов	361
6.4.8. Исправление ошибок	362

6.4.9. Реализация декодера	366
6.5. Возможность обнаружения и исправления ошибок	368
6.5.1. Весовой коэффициент двоичных векторов и расстояние между ними	368
6.5.2. Минимальное расстояние для линейного кода	368
6.5.3. Обнаружение и исправление ошибок	369
6.5.4. Визуализация пространства b -кортежей	372
6.5.5. Коррекция со стиранием ошибок	374
6.6. Полезность нормальной матрицы	375
6.6.1. Оценка возможностей кода	375
6.6.2. Пример кода (n, k)	377
6.6.3. Разработка кода $(8, 2)$	377
6.6.4. Соотношение между обнаружением и исправлением ошибок	378
6.6.5. Взгляд на код сквозь нормальную матрицу	381
6.7. Циклические коды	382
6.7.1. Алгебраическая структура циклических кодов	383
6.7.2. Свойства двоичного циклического кода	384
6.7.3. Кодирование в систематической форме	385
6.7.4. Логическая схема для реализации полиномиального деления	386
6.7.5. Систематическое кодирование с $(n - k)$ -разрядным регистром сдвига	388
6.7.6. Обнаружение ошибок с помощью $(n - k)$ -разрядного регистра сдвига	390
6.8. Известные блочные коды	391
6.8.1. Коды Хэмминга	391
6.8.2. Расширенный код Голея	394
6.8.3. Коды БХЧ	395
6.9. Резюме	399
Литература	399
Задачи	400
Вопросы	404
ГЛАВА 7. КАНАЛЬНОЕ КОДИРОВАНИЕ: ЧАСТЬ 2	405
7.1. Сверточное кодирование	406
7.2. Представление сверточного кодера	408
7.2.1. Представление связи	408
7.2.2. Представление состояния и диаграмма состояний	412
7.2.3. Древоподобные диаграммы	415
7.2.4. Решетчатая диаграмма	415
7.3. Формулировка задачи сверточного кодирования	418
7.3.1. Декодирование по методу максимального правдоподобия	418
7.3.2. Модели каналов: мягкое или жесткое принятие решений	420
7.3.3. Алгоритм сверточного декодирования Витерби	424
7.3.4. Пример сверточного декодирования Витерби	425
7.3.5. Реализация декодера	429
7.3.6. Память путей и синхронизация	430
7.4. Свойства сверточных кодов	432
7.4.1. Пространственные характеристики сверточных кодов	432
7.4.2. Систематические и несистематические сверточные коды	436
7.4.3. Накопление катастрофических ошибок в сверточных кодах	436

7.4.4. Границы рабочих характеристик сверточных кодов	438
7.4.5. Эффективность кодирования	439
7.4.6. Наиболее известные сверточные коды	440
7.4.7. Компромиссы сверточного кодирования	442
7.4.8. Мягкое декодирование по алгоритму Витерби	443
7.5. Другие алгоритмы сверточного декодирования	445
7.5.1. Последовательное декодирование	445
7.5.2. Сравнение декодирования по алгоритму Витерби с последовательным декодированием и их ограничения	448
7.5.3. Декодирование с обратной связью	450
7.6. Резюме	452
Литература	452
Задачи	453
Вопросы для самопроверки	457
ГЛАВА 8. КАНАЛЬНОЕ КОДИРОВАНИЕ: ЧАСТЬ 3	459
8.1. Коды Рида-Соломона	460
8.1.1. Вероятность появления ошибок для кодов Рида-Соломона	461
8.1.2. Почему коды Рида-Соломона эффективны при борьбе с импульсными помехами	463
8.1.3. Рабочие характеристики кода Рида-Соломона как функция размера, избыточности и степени кодирования	464
8.1.4. Конечные поля	467
8.1.5. Кодирование Рида-Соломона	472
8.1.6. Декодирование Рида-Соломона	476
8.2. Коды с чередованием и каскадные коды	483
8.2.1. Блочное чередование	486
8.2.2. Сверточное чередование	488
8.2.3. Каскадные коды	489
8.3. Кодирование и чередование в системах цифровой записи информации на компакт-дисках	491
8.3.1. Кодирование по схеме CIRC	493
8.3.2. Декодирование по схеме CIRC	495
8.3.3. Интерполяция и подавление	497
8.4. Турбокоды	498
8.4.1. Понятия турбокодирования	498
8.4.2. Алгебра логарифма правдоподобия	502
8.4.3. Пример композиционного кода	503
8.4.4. Кодирование с помощью рекурсивного систематического кода	510
8.4.5. Декодер с обратной связью	515
8.4.6. Алгоритм MAP	519
8.4.7. Пример декодирования по алгоритму MAP	527
8.5. Резюме	531
Приложение 8А. Сложение логарифмических отношений правдоподобий	532
Литература	533
Задачи	534
Вопросы для самопроверки	541

ГЛАВА 9. КОМПРОМИССЫ ПРИ ИСПОЛЬЗОВАНИИ МОДУЛЯЦИИ И КОДИРОВАНИЯ	543
9.1. Цели разработчика систем связи	544
9.2. Характеристика вероятности появления ошибки	544
9.3. Минимальная ширина полосы пропускания по Найквисту	545
9.4. Теорема Шеннона-Хартли о пропускной способности канала	548
9.4.1. Предел Шеннона	550
9.4.2. Энтропия	551
9.4.3. Неоднозначность и эффективная скорость передачи информации	553
9.5. Плоскость “полоса-эффективность”	556
9.5.1. Эффективность использования полосы при выборе схем MPSK и MFSK	557
9.5.2. Аналогия между графиками эффективности использования полосы частот и вероятности появления ошибки	558
9.6. Компромиссы при использовании модуляции и кодирования	559
9.7. Определение, разработка и оценка систем цифровой связи	560
9.7.1. <i>M</i> -арная передача сигналов	561
9.7.2. Системы ограниченной полосы пропускания	562
9.7.3. Системы ограниченной мощности	563
9.7.4. Требования к передаче сигналов MPSK и MFSK	564
9.7.5. Система ограниченной полосы пропускания без кодирования	565
9.7.6. Система ограниченной мощности без кодирования	567
9.7.7. Система ограниченной мощности и полосы пропускания с кодированием	568
9.8. Модуляция с эффективным использованием полосы частот	577
9.8.1. Передача сигналов с модуляцией QPSK и OQPSK	577
9.8.2. Манипуляция с минимальным сдвигом	581
9.8.3. Квадратурная амплитудная модуляция	585
9.9. Модуляция и кодирование в каналах ограниченной полосы	588
9.9.1. Коммерческие модемы	588
9.9.2. Границы совокупности сигналов	589
9.9.3. Совокупности сигналов высших размерностей	592
9.9.4. Решетчатые структуры высокой плотности	594
9.9.5. Комбинированная эффективность: отображение на <i>N</i> -мерную сферу и плотная решетка	595
9.10. Решетчатое кодирование	595
9.10.1. Истоки решетчатого кодирования	597
9.10.2. Кодирование TCM	598
9.10.3. Декодирование TCM	601
9.10.4. Другие решетчатые коды	604
9.10.5. Пример решетчатого кодирования	607
9.10.6. Многомерное решетчатое кодирование	611
9.11. Резюме	611
Литература	612
Задачи	614
Вопросы	617

ГЛАВА 10. СИНХРОНИЗАЦИЯ	619
10.1. Вступление	620
10.1.1. Виды синхронизации	620
10.1.2. Плата за преимущества	621
10.1.3. Подход и предположения	623
10.2. Синхронизация приемника	623
10.2.1. Частотная и фазовая синхронизация	623
10.2.2. Символьная синхронизация — модуляции дискретных символов	645
10.2.3. Синхронизация при модуляциях без разрыва фазы	652
10.2.4. Кадровая синхронизация	659
10.3. Сетевая синхронизация	663
10.3.1. Открытая синхронизация передатчиков	664
10.3.2. Закрытая синхронизация передатчиков	667
10.4. Резюме	670
Литература	671
Задачи	672
Вопросы для самопроверки	674
ГЛАВА 11. УПЛОТНЕНИЕ И МНОЖЕСТВЕННЫЙ ДОСТУП	675
11.1. Распределение ресурса связи	676
11.1.1. Уплотнение/множественный доступ с частотным разделением	678
11.1.2. Уплотнение/множественный доступ с временным разделением	683
11.1.3. Распределение ресурса связи по каналам	686
11.1.4. Сравнение производительности FDMA и TDMA	687
11.1.5. Множественный доступ с кодовым разделением	690
11.1.6. Множественный доступ с поляризационным и пространственным разделением	692
11.2. Системы связи множественного доступа и архитектура	694
11.2.1. Информационный поток в системах множественного доступа	694
11.2.2. Множественный доступ с предоставлением каналов по требованию	696
11.3. Алгоритмы доступа	697
11.3.1. ALOHA	697
11.3.2. ALOHA с выделением временных интервалов	699
11.3.3. Алгоритм ALOHA с использованием резервирования	701
11.3.4. Сравнение производительности систем S-ALOHA и R-ALOHA	701
11.3.5. Методы опроса	704
11.4. Методы множественного доступа, используемые INTELSAT	706
11.4.1. Режимы работы FDM/FM/FDMA и MCPC	706
11.4.2. MCPC-режимы доступа к спутнику INTELSAT	708
11.4.3. Работа алгоритма SPADE	709
11.4.4. Использование TDMA в системах INTELSAT	714
11.4.5. Использование схемы TDMA со спутниковой коммутацией на спутнике INTELSAT	721
11.5. Методы множественного доступа в локальных сетях	724

11.5.1. Сети CSMA/CD	724
11.5.2. Сети Token Ring	726
11.5.3. Сравнение производительности сетей CSMA/CD и Token Ring	727
11.6. Резюме	728
Литература	729
Задачи	730
Вопросы для самопроверки	732

ГЛАВА 12. МЕТОДЫ РАСШИРЕННОГО СПЕКТРА 733

12.1. Расширенный спектр	734
12.1.1. Преимущества систем связи расширенного спектра	734
12.1.2. Методы расширения спектра	738
12.1.3. Моделирование подавления интерференции с помощью расширения спектра методом прямой последовательности	740
12.1.4. Историческая справка	741
12.2. Псевдослучайные последовательности	742
12.2.1. Свойства случайной последовательности	742
12.2.2. Последовательности, генерируемые регистром сдвига	743
12.2.3. Автокорреляционная функция псевдослучайного сигнала	744
12.3. Системы расширения спектра методом прямой последовательности	745
12.3.1. Пример схемы прямой последовательности	747
12.3.2. Коэффициент расширения спектра и производительность	748
12.4. Системы со скачкообразной перестройкой частоты	752
12.4.1. Пример использования скачкообразной перестройки частоты	753
12.4.2. Устойчивость	754
12.4.3. Одновременное использование скачкообразной перестройки частоты и разнесения сигнала	756
12.4.4. Быстрая и медленная перестройка частоты	757
12.4.5. Демодулятор FFH/MFSK	758
12.4.6. Коэффициент расширения спектра сигнала	759
12.5. Синхронизация	759
12.5.1. Первоначальная синхронизация	760
12.5.2. Сопровождение	765
12.6. Учет влияния преднамеренных помех	767
12.6.1. “Состязание” с помехами	767
12.6.2. Подавление сигнала широкополосным шумом	773
12.6.3. Подавление сигнала узкополосным шумом	774
12.6.4. Подавление сигнала разнотонными помехами	776
12.6.5. Подавление сигнала импульсными помехами	778
12.6.6. Создание ретрансляционных помех	780
12.6.7. Система BLADES	781
12.7. Использование систем связи расширенного спектра в коммерческих целях	782
12.7.1. Множественный доступ с кодовым разделением	782
12.7.2. Каналы с многолучевым распространением	784
12.7.3. Стандартизация систем связи расширенного спектра	786
12.7.4. Сравнительные характеристики систем DS и FH	787
12.8. Сотовые системы связи	789

12.8.1. CDMA/DS	790
12.8.2. Сравнительный анализ аналоговой частотной модуляции, TDMA и CDMA	793
12.8.3. Системы, ограниченные интерференцией и пространственными факторами	795
12.8.4. Цифровые сотовые системы связи CDMA стандарта IS-95	797
12.9. Резюме	811
Литература	811
Задачи	813
Вопросы	818
ГЛАВА 13. КОДИРОВАНИЕ ИСТОЧНИКА	821
13.1. Источники	822
13.1.1. Дискретные источники	822
13.1.2. Источники волновых сигналов	826
13.2. Квантование амплитуды	828
13.2.1. Шум квантования	831
13.2.2. Равномерное квантование	834
13.2.3. Насыщение	838
13.2.4. Добавление псевдослучайного шума	841
13.2.5. Неравномерное квантование	843
13.3. Дифференциальная импульсно-кодовая модуляция	852
13.3.1. Одноотводное предсказание	855
13.3.2. <i>N</i> -отводное предсказание	857
13.3.3. Дельта-модуляция	859
13.3.4. Сигма-дельта-модуляция	859
13.3.5. Сигма-дельта-аналого-цифровой преобразователь	865
13.3.6. Сигма-дельта-цифро-аналоговый преобразователь	865
13.4. Адаптивное предсказание	867
13.4.1. Прямая адаптация	867
13.4.2. Синтетическое/аналитическое кодирование	868
13.5. Блочное кодирование	870
13.5.1. Векторное квантование	871
13.6. Преобразующее кодирование	873
13.6.1. Квантование для преобразующего кодирования	874
13.6.2. Многополосное кодирование	874
13.7. Кодирование источника для цифровых данных	876
13.7.1. Свойства кодов	877
13.7.2. Код Хаффмана	879
13.7.3. Групповые коды	882
13.8. Примеры кодирования источника	887
13.8.1. Аудиосжатие	887
13.8.2. Сжатие изображения	892
13.9. Резюме	900
Литература	901
Задачи	902
Вопросы для самопроверки	905

ГЛАВА 14. ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ	907
14.1. Модели, цели и ранние системы шифрования	908
14.1.1. Модель процесса шифрования и дешифрования	908
14.1.2. Задачи системы шифрования	909
14.1.3. Классические угрозы	910
14.1.4. Классические шифры	911
14.2. Секретность системы шифрования	913
14.2.1. Совершенная секретность	913
14.2.2. Энтропия и неопределенность	916
14.2.3. Интенсивность и избыточность языка	917
14.2.4. Расстояние единственности и идеальная секретность	918
14.3. Практическая защищенность	920
14.3.1. Смешение и диффузия	921
14.3.2. Подстановка	921
14.3.3. Перестановка	922
14.3.4. Продукционный шифр	923
14.3.5. Стандарт шифрования данных	925
14.4. Поточное шифрование	931
14.4.1. Пример генерирования ключа с использованием линейного регистра сдвига с обратной связью	932
14.4.2. Слабые места линейных регистров сдвига с обратной связью	933
14.4.3. Синхронные и самосинхронизирующиеся системы поточного шифрования	935
14.5. Криптосистемы с открытыми ключами	936
14.5.1. Проверка подлинности подписи с использованием криптосистемы с открытым ключом	937
14.5.2. Односторонняя функция с “лазейкой”	938
14.5.3. Схема RSA	938
14.5.4. Задача о рюкзаке	941
14.5.5. Криптосистема с открытым ключом, основанная на “лазейке” в рюкзаке	942
14.6. Pretty Good Privacy	944
14.6.1. “Тройной” DES, CAST и IDEA	947
14.6.2. Алгоритмы Диффи-Хэллмана (вариант Элгемала) и RSA	950
14.6.3. Шифрование сообщения в системе PGP	952
14.6.4. Аутентификация с помощью PGP и создание подписи	953
14.7. Резюме	956
Литература	956
Задачи	957
Вопросы для самопроверки	958
ГЛАВА 15. КАНАЛЫ С ЗАМИРАНИЯМИ	961
15.1. Сложности связи по каналу с замираниями	962
15.2. Описание распространения радиоволн в мобильной связи	963
15.2.1. Крупномасштабное замирание	967
15.2.2. Мелкомасштабное замирание	970

15.3. Расширение сигнала во времени	976
15.3.1. Расширение сигнала во времени, рассматриваемое в области задержки	976
15.3.2. Расширение сигнала во времени, рассматриваемое в частотной области	978
15.3.3. Примеры амплитудного и частотно-селективного замирания	981
15.4. Нестационарное поведение канала вследствие движения	983
15.4.1. Нестационарное поведение канала, рассматриваемое во временной области	983
15.4.2. Нестационарное поведение канала, рассматриваемое в области доплеровского сдвига	986
15.4.3. Релеевский канал с медленным и амплитудным замиранием	993
15.5. Борьба с ухудшением характеристик, вызванным эффектами замирания	995
15.5.1. Борьба с частотно-селективными искажениями	997
15.5.2. Борьба с искажениями, вызванными быстрым замиранием	999
15.5.3. Борьба с уменьшением SNR	1000
15.5.4. Методы разнесения	1001
15.5.5. Типы модуляции для каналов с замираниями	1004
15.5.6. Роль чередования	1005
15.6. Краткий обзор ключевых параметров, характеризующих каналы с замираниями	1008
15.6.1. Искажения вследствие быстрого замирания: случай 1	1009
15.6.2. Искажения вследствие частотно-селективного замирания: случай 2	1010
15.6.3. Искажения вследствие быстрого и частотно-селективного замирания: случай 3	1010
15.7. Приложения: борьба с эффектами частотно-селективного замирания	1013
15.7.1. Применение эквалайзера Витерби в системе GSM	1013
15.7.2. Приемник Рейка в системах с расширением спектра методом прямой последовательности	1016
15.8. Резюме	1018
Литература	1018
Задачи	1020
Вопросы	1026
ПРИЛОЖЕНИЕ А. ОБЗОР АНАЛИЗА ФУРЬЕ	1029
А.1. Сигналы, спектры и линейные системы	1029
А.2. Применение методов Фурье к анализу линейных систем	1029
А.2.1. Разложение в ряд Фурье	1031
А.2.2. Спектр последовательности импульсов	1035
А.2.3. Представление в виде интеграла Фурье	1037
А.3. Свойства преобразования Фурье	1038
А.3.1. Сдвиг во времени	1038
А.3.2. Сдвиг по частоте	1038
А.4. Полезные функции	1039
А.4.1. Дельта-функция	1039
А.4.2. Спектр синусоиды	1040
А.5. Свертка	1040

A.5.1. Графическая иллюстрация свертки	1044
A.5.2. Свертка по времени	1045
A.5.3. Свертка по частоте	1045
A.5.4. Свертка функции с единичным импульсом	1046
A.5.5. Применение свертки при демодуляции	1046
A.6. Таблицы Фурье-образов и свойств преобразования Фурье	1048
Литература	1050

ПРИЛОЖЕНИЕ Б. ОСНОВЫ ТЕОРИИ ПРИНЯТИЯ СТАТИСТИЧЕСКИХ РЕШЕНИЙ

Б.1. Теорема Байеса	1051
Б.1.1. Дискретная форма теоремы Байеса	1052
Б.1.2. Теорема Байеса в смешанной форме	1054
Б.2. Теория принятия решений	1056
Б.2.1. Элементы задачи теории принятия решений	1056
Б.2.2. Проверка методом отношения правдоподобий и критерий максимума апостериорной вероятности	1056
Б.2.3. Критерий максимального правдоподобия	1057
Б.3. Пример обнаружения сигнала	1058
Б.3.1. Двоичное решение по принципу максимального правдоподобия	1058
Б.3.2. Вероятность битовой ошибки	1059
Литература	1061

ПРИЛОЖЕНИЕ В. ОТКЛИК КОРРЕЛЯТОРОВ НА БЕЛЫЙ ШУМ

ПРИЛОЖЕНИЕ Г. ПОЛЕЗНЫЕ СООТНОШЕНИЯ

ПРИЛОЖЕНИЕ Д. S-ОБЛАСТЬ, Z-ОБЛАСТЬ И ЦИФРОВАЯ ФИЛЬТРАЦИЯ

Д.1. Преобразование Лапласа	1068
Д.1.1. Стандартное преобразование Лапласа	1069
Д.1.2. Свойства преобразования Лапласа	1069
Д.1.3. Использование преобразования Лапласа	1070
Д.1.4. Передаточная функция	1071
Д.1.5. Фильтрация нижних частот в RC-цепи	1072
Д.1.6. Полюсы и нули	1072
Д.1.7. Устойчивость линейных систем	1072
Д.2. z-преобразование	1073
Д.2.1. Вычисление z -преобразования	1074
Д.2.2. Обратное z -преобразование	1075
Д.3. Цифровая фильтрация	1076
Д.3.1. Передаточная функция цифрового фильтра	1077
Д.3.2. Устойчивость однополюсного фильтра	1077
Д.3.3. Устойчивость произвольного фильтра	1078

Д.3.4. Диаграмма полюсов-нулей и единичная окружность	1079
Д.3.5. Дискретное преобразование Фурье импульсной характеристики цифрового фильтра	1080
Д.4. Фильтры с конечной импульсной характеристикой	1081
Д.4.1. Структура фильтра с конечной импульсной характеристикой	1082
Д.4.2. Дифференциатор с конечной импульсной характеристикой	1082
Д.5. Фильтры с бесконечной импульсной характеристикой	1084
Д.5.1. Оператор левосторонней разности	1084
Д.5.2. Использование билинейного преобразования для создания фильтров с бесконечной импульсной характеристикой	1085
Д.5.3. Интегратор с бесконечной импульсной характеристикой	1085
Литература	1086
ПРИЛОЖЕНИЕ Е. ПЕРЕЧЕНЬ СИМВОЛОВ	1087
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ	1093