

ОГЛАВЛЕНИЕ

Предисловие к третьему изданию	13
Список используемых сокращений	15
Глава 1. ВВЕДЕНИЕ	20
1.1. Системы автоматической идентификации	21
1.1.1. Системы с использованием штриховых кодов	22
1.1.2. Системы оптического распознавания текста	23
1.1.3. Биометрические системы	23
1.1.3.1. Идентификация по голосу	23
1.1.3.2. Идентификация по отпечаткам пальцев (дактилоскопия)	24
1.1.4. Чип-карты (Smart-cards)	24
1.1.4.1. Карты памяти	25
1.1.4.2. Микропроцессорные карты	25
1.1.5. RFID-системы	26
1.2. Сравнение различных систем идентификации	26
1.3. Основные компоненты RFID-систем	28
Глава 2. ОСНОВНЫЕ ОСОБЕННОСТИ RFID-СИСТЕМ	30
2.1. Основные характеристики систем радиочастотной идентификации	30
2.2. Основные конструкции транспондеров	33
2.2.1. Транспондеры, выполненные в форме монеты или диска	33
2.2.2. Корпус из стекла	34
2.2.3. Пластмассовый корпус	35
2.2.4. Идентификация инструмента и газовых баллонов	35
2.2.5. Ключ или брелок	37
2.2.6. Часы	37
2.2.7. Конструкция ID-1, бесконтактные чип-карты	38
2.2.8. Этикетки (Smart Label)	39
2.2.9. Антенна на кристалле	40
2.2.10. Другие конструкции	41
2.3. Рабочая частота, дальность действия и принцип взаимодействия	41
2.4. Обработка данных транспондером	43
2.5. Критерии, которыми следует руководствоваться при выборе RFID-системы	45
2.5.1. Рабочая частота	45
2.5.2. Дальность действия	46
2.5.3. Требования к безопасности данных	47
2.5.4. Объем памяти	48
Глава 3. ОСНОВНЫЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ	49
3.1. Однобитные транспондеры	50
3.1.1. Используемая радиочастота	50
3.1.2. Микроволновые системы	54
3.1.3. Делитель частоты	56
3.1.4. Системы электромагнитного типа	57

3.1.5. Акустомагнитные системы	59
3.2. Дуплексные и полудуплексные системы	61
3.2.1. Системы с индуктивной связью.	63
3.2.1.1. Передача энергии пассивному транспондеру.	63
3.2.1.2. Передача данных от транспондера к считывающему устройству	66
3.2.2. Связь с помощью электромагнитного рассеяния	69
3.2.2.1. Энергоснабжение транспондера.	69
3.2.2.2. Передача данных от транспондера к считывающему устройству	71
3.2.3. Системы Close-coupling.	72
3.2.3.1. Источник питания транспондера	72
3.2.3.2. Передача данных от транспондера к считывающему устройству	74
3.2.4. Передача данных от считывающего устройства к транспондеру	74
3.2.5. Электрическая связь	75
3.2.5.1. Передача энергии пассивному транспондеру.	75
3.2.5.2. Передача данных от транспондера к считывающему устройству	77
3.3. Последовательные методы.	77
3.3.1. Системы с индуктивной связью.	77
3.3.1.1. Передача энергии транспондеру.	77
3.3.1.2. Сравнение дуплексных/полудуплексных и последовательных систем	78
3.3.1.3. Передача данных от транспондера к считывающему устройству	80
3.3.2. Транспондеры, использующие поверхностные акустические волны	81
Глава 4. ФИЗИЧЕСКИЕ ОСНОВЫ RFID-СИСТЕМ	85
4.1. Магнитное поле	86
4.1.1. Напряженность магнитного поля H	86
4.1.1.1. Распределение напряженности магнитного поля $H(x)$ для индуктивного витка	87
4.1.1.2. Оптимальный диаметр антенны	90
4.1.2. Магнитный поток и плотность магнитного потока	91
4.1.3. Индуктивность L	92
4.1.3.1. Индуктивность витка катушки	93
4.1.4. Взаимная индуктивность M	93
4.1.5. Коэффициент связи k	95
4.1.6. Закон электромагнитной индукции (закон Фарадея)	96
4.1.7. Резонанс.	99
4.1.8. Примеры практического использования транспондеров	103
4.1.8.1. Напряжение питания транспондера.	103
4.1.8.2. Стабилизация напряжения питания	104
4.1.9. Минимальная напряженность магнитного поля H_{\min} , при которой транспондер еще способен работать	106
4.1.9.1. Энергетическая дальность действия транспондера	108
4.1.9.2. Зона считывания ридера.	110
4.1.10. Система ридер — транспондер	112
4.1.10.1. Трансформированный импеданс транспондера Z'_T	114
4.1.10.2. Параметры, которые влияют на Z'_T	117
4.1.10.3. Модуляция нагрузкой.	124
4.1.11. Измерение параметров системы	131
4.1.11.1. Измерение коэффициента связи k	131
4.1.11.2. Измерение резонансной частоты транспондера	132
4.1.12. Материалы с магнитными свойствами	134
4.1.12.1. Материалы с магнитными свойствами и ферриты	134

4.1.12.2. Ферритовые антенны для низкочастотных транспондеров	136
4.1.12.3. Ферритовое экранирование при наличии металлических объектов.	136
4.1.12.4. Установка транспондеров в металл.	137
4.2. Электромагнитные волны	140
4.2.1. Возникновение электромагнитных волн	140
4.2.1.1. Переход от ближней к дальней зоне для индуктивного витка.	141
4.2.2. Плотность излучения S	143
4.2.3. Волновое сопротивление и напряженность поля E	143
4.2.4. Поляризация электромагнитных волн	144
4.2.4.1. Отражение электромагнитных волн.	145
4.2.5. Антенны	148
4.2.5.1. Коэффициент усиления и направленность.	148
4.2.5.2. EIRP и ERP.	150
4.2.5.3. Входной импеданс	150
4.2.5.4. Эффективная площадь и эффективное сечение рассеяния	151
4.2.5.5. Эффективная длина	154
4.2.5.6. Дипольная антенна	154
4.2.5.7. Антенна типа «волновой канал»	156
4.2.5.8. Плоская, или микрополосковая, антенна.	157
4.2.5.9. Щелевые антенны	160
4.2.6. Практическое применение транспондеров с щелевыми антеннами	160
4.2.6.1. Эквивалентная схема транспондера.	161
4.2.6.2. Питание пассивного транспондера	162
4.2.6.3. Питание активного транспондера	170
4.2.6.4. Отражение и затухание	170
4.2.6.5. Чувствительность срабатывания транспондера	172
4.2.6.6. Модуляция эффективного сечения рассеяния.	172
4.2.6.7. Дальность считывания	175
4.3. Поверхностные акустические волны	178
4.3.1. Возникновение поверхностных акустических волн	178
4.3.2. Отражение поверхностных акустических волн	181
4.3.3. Функциональная схема транспондера на ПАВ	181
4.3.4. Сенсорный эффект.	184
4.3.4.1. Отражательная линия задержки	186
4.3.4.2. Резонансные датчики	187
4.3.4.3. Импедансные датчики	189
4.3.5. Коммутируемые датчики.	189
Глава 5. ДИАПАЗОНЫ ЧАСТОТ И ПРАВИЛА, РЕГЛАМЕНТИРУЮЩИЕ	
ИСПОЛЬЗОВАНИЕ РАДИОЧАСТОТ	190
5.1. Используемые частотные диапазоны.	190
5.1.1. Диапазон частот 9...135 кГц.	191
5.1.2. Диапазон частот 6.78 МГц.	193
5.1.3. Диапазон частот 13.56 МГц.	194
5.1.4. Диапазон частот 27.125 МГц.	194
5.1.5. Диапазон частот 40.680 МГц.	194
5.1.6. Диапазон частот 433.920 МГц.	195
5.1.7. Диапазон частот 869.0 МГц.	195
5.1.8. Диапазон частот 915.0 МГц.	195
5.1.9. Диапазон частот 2.45 ГГц.	196
5.1.10. Диапазон частот 5.8 ГГц.	196
5.1.11. Диапазон частот 24.125 ГГц.	196

5.1.12. Выбор рабочей частоты для RFID-системы с индуктивной связью	196
5.2. Действующие в Европе правила, регламентирующие использование радиочастот	199
5.2.1. Стандарт CEPT/ERC REC 70-03	199
5.2.1.1. Приложение 1. SRD-устройства общего назначения	201
5.2.1.2. Приложение 4. Применение на железнодорожном транспорте	202
5.2.1.3. Приложение 5. Устройства для автомобильного транспорта и телематические устройства для отслеживания дорожного движения	202
5.2.1.4. Приложение 9. Индуктивные устройства	202
5.2.1.5. Приложение 11. Устройства радиочастотной идентификации	203
5.2.1.6. Частотный диапазон 868 МГц	203
5.2.2. Стандарт EN 300330: 9 кГц...25 МГц	204
5.2.2.1. Мощность несущей — предельные значения для передатчиков, использующих <i>H</i> -поле	205
5.2.2.2. Паразитное излучение	206
5.2.3. Стандарты EN 300220-1, EN 300220-2	207
5.2.4. Стандарт EN 300440	208
5.3. Национальные правила, действующие в странах Европы	209
5.3.1. Федеративная Республика Германия.	209
5.4. Национальное законодательство в других странах	211
5.4.1. США	211
5.4.2. Взгляд в будущее: США — Япония — Европа	213
Глава 6. СПОСОБЫ КОДИРОВАНИЯ И МОДУЛЯЦИИ	214
6.1. Кодирование в основной полосе частот	215
6.2. Способы цифровой модуляции.	218
6.2.1. Амплитудная манипуляция (ASK).	219
6.2.2. Модуляция 2-FSK	221
6.2.3. Модуляция 2-PSK.	222
6.2.4. Модуляция с использованием поднесущей	223
Глава 7. ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ	225
7.1. Использование контрольной суммы	225
7.1.1. Проверка четности	225
7.1.2. Метод LRC.	226
7.1.3. Метод CRC.	227
7.2. Методы множественного доступа — предупреждение коллизий	231
7.2.1. Пространственное разделение каналов (SDMA)	233
7.2.2. Частотное разделение каналов (FDMA).	235
7.2.3. Временное разделение каналов (TDMA)	236
7.2.4. Примеры практической реализации методов предупреждения коллизий	238
7.2.4.1. Метод ALOHA	238
7.2.4.2. Метод Slotted-ALOHA	241
7.2.4.3. Алгоритмы двоичного поиска	245
Глава 8. БЕЗОПАСНОСТЬ ДАННЫХ	254
8.1. Двусторонняя симметричная аутентификация	255
8.2. Аутентификация с производным ключом.	256
8.3. Шифрование при передаче данных	257
8.3.1. Последовательное шифрование.	259

Глава 9. НОРМАТИВНЫЕ ДОКУМЕНТЫ	262
9.1. Идентификация животных	262
9.1.1. ISO 11784 — Структура кода	263
9.1.2. ISO 11785 — Техническая концепция	263
9.1.2.1. Требования	264
9.1.2.2. Дуплексные и полудуплексные системы	266
9.1.2.3. Последовательные системы	266
9.1.3. ISO 14223 — Транспондеры с расширенными функциями	267
9.1.3.1. Часть 1 — Радиочастотный интерфейс	267
9.1.3.2. Часть 2 — Структура кодов и команд	270
9.2. Бесконтактные чип-карты	272
9.2.1. ISO 10536 — Чип-карты Close-coupling	273
9.2.1.1. Часть 1 — Физические характеристики	273
9.2.1.2. Часть 2 — Размер и положение зон, которые обеспечивают электромагнитное взаимодействие	273
9.2.1.3. Часть 3 — Электронные сигналы и процедура перезагрузки	274
9.2.1.4. Часть 4 — Ответ на сигнал сброса и протокол передачи	275
9.2.2. ISO 14443 — Чип-карты Proximity-coupling	276
9.2.2.1. Часть 1 — Физические характеристики	276
9.2.2.2. Часть 2 — Радиочастотный интерфейс	276
9.2.2.3. Часть 3 — Инициализация и предотвращение коллизий	281
9.2.2.4. Часть 4 — Протокол передачи	289
9.2.3. ISO 15693 — Чип-карты Vicinity-coupling	294
9.2.3.1. Часть 1 — Физические характеристики	294
9.2.3.2. Часть 2 — Радиочастотный интерфейс и инициализация	295
9.2.4. ISO 10373 — Методы испытаний чип-карт	299
9.2.4.1. Часть 4 — Методы испытаний чип-карт, относящихся к категории Close-coupling	300
9.2.4.2. Часть 6 — Методы испытаний чип-карт, относящихся к категории Proximity	301
9.2.4.3. Часть 7 — Методы испытаний чип-карт, относящихся к категории Vicinity-coupling	304
9.3. DIN/ISO 69873 — Носители данных для инструмента и зажимных устройств	305
9.4. ISO 10374 — Идентификация контейнеров	305
9.5. VDI 4470 — Системы охраны товаров	306
9.5.1. Часть 1 — Правила приемки RFID-системы на основе контрольных ворот	306
9.5.1.1. Определение доли ложных срабатываний	307
9.5.1.2. Определение коэффициента обнаружения	307
9.5.1.3. Формы документов, которые устанавливаются в стандарте VDI 4470	308
9.5.2. Часть 2 — Правила приемки деактивирующего устройства	308
9.6. Логистика и управление товарными запасами	309
9.6.1. Серия стандартов ISO 18000	309
9.6.2. Инициатива GTAG	310
9.6.2.1. Транспортный уровень GTAG	312
9.6.2.2. Коммуникационный уровень и уровень приложений GTAG	313
Глава 10. АРХИТЕКТУРА ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ . . .	314
10.1. Транспондер, который обеспечивает функции хранения данных	315
10.1.1. Высокочастотный интерфейс	315
10.1.1.1. Пример схемы — модуляция нагрузкой с использованием поднесущей . . .	316

10.1.1.2. Типовая схема — высокочастотный интерфейс для транспондера, соответствующего ISO 14443	317
10.1.2. Схема адресации и обеспечения защиты данных	320
10.1.2.1. Конечный автомат	321
10.1.3. Организация памяти	322
10.1.3.1. Транспондер Read-only	322
10.1.3.2. Транспондеры, которые позволяют записывать данные	324
10.1.3.3. Транспондеры, которые поддерживают криптографические функции	324
10.1.3.4. Сегментация памяти	327
10.1.3.5. Директории приложений MIFARE®	330
10.1.3.6. Двухпортовая EEPROM-память	333
10.2. Микропроцессоры	336
10.2.1. Карты с двумя интерфейсами	338
10.2.1.1. Карты MIFARE-plus	340
10.2.1.2. Современная концепция карт с двумя интерфейсами	341
10.3. Технологии микросхем памяти	344
10.3.1. RAM-память	344
10.3.2. EEPROM-память	345
10.3.3. FRAM-память	346
10.3.4. Сравнение возможностей двух типов памяти: FRAM и EEPROM	348
10.4. Измерение физических величин	349
10.4.1. Транспондер с функциями датчика	349
10.4.2. Проведение измерений с помощью микроволнового транспондера	351
10.4.3. Сенсорный эффект для транспондеров на поверхностных акустических волнах	352
Глава 11. СЧИТЫВАЮЩИЕ УСТРОЙСТВА	355
11.1. Поток данных в приложении	355
11.2. Компоненты, из которых состоит считывающее устройство	356
11.2.1. Высокочастотный интерфейс	358
11.2.1.1. Система с индуктивной связью, FDX/HDX	358
11.2.1.2. Микроволновая система полудуплексного типа	359
11.2.1.3. Транспондеры последовательного типа	361
11.2.1.4. Микроволновая система с использованием ПАВ-транспондера	362
11.2.2. Схема управления	363
11.3. Конструкция недорогого считывающего устройства на основе микросхемы U2270B	364
11.4. Подключение антенны для системы с индуктивной связью	367
11.4.1. Непосредственное подключение антенны с согласованием по току	367
11.4.2. Подключение с помощью коаксиального кабеля	370
11.4.3. Влияние добротности	373
11.5. Формы исполнения считывающих устройств	374
11.5.1. OEM-ридеры	374
11.5.2. Считывающие устройства для промышленного применения	375
11.5.3. Портативные считывающие устройства	376
Глава 12. ПРОИЗВОДСТВО ТРАНСПОНДЕРОВ И БЕСКОНТАКТНЫХ ЧИП-КАРТ	377
12.1. Стекланные и пластиковые транспондеры	377
12.1.1. Изготовление модуля	378
12.1.2. Полуфабрикаты для производства транспондеров	379
12.1.3. Корпусирование	380

12.2. Бесконтактные чип-карты	381
12.2.1. Изготовление катушки	382
12.2.1.1. Метод намотки	382
12.2.1.2. Метод встраивания	382
12.2.1.3. Метод трафаретной печати	384
12.2.1.4. Метод травления	385
12.2.2. Методы соединения	386
12.2.3. Ламинирование	387
Глава 13. ПРИМЕРЫ ПРИМЕНЕНИЯ	389
13.1. Бесконтактные чип-карты	389
13.2. Общественный транспорт	391
13.2.1. Предпосылки	392
13.2.2. Требования	392
13.2.2.1. Время осуществления транзакции	393
13.2.2.2. Устойчивость к различным погодным условиям, долговечность, удобство в использовании	393
13.2.3. Преимущества при использовании RFID-систем	393
13.2.4. Модели тарифов для электронной системы оплаты	395
13.2.5. Рыночный потенциал	396
13.2.6. Примеры проектов	397
13.2.6.1. Южная Корея — Сеул	397
13.2.6.2. Германия — Лунебург, Ольденбург	399
13.2.6.3. Проекты Евросоюза — ICARE и CALYPSO	400
13.3. Системы продажи билетов	404
13.3.1. Карта Miles & More авиакомпании Lufthansa	404
13.3.2. Продажа билетов на горнолыжных трассах	406
13.4. Контроль доступа	408
13.4.1. Системы on-line	408
13.4.2. Системы off-line	409
13.4.3. Транспондер	411
13.5. Транспортные системы	412
13.5.1. Система Eurobalise S21	412
13.5.2. Международные контейнерные перевозки	415
13.6. Системы идентификации животных	416
13.6.1. Слежение за крупным рогатым скотом	416
13.6.2. Почтовые голуби: гонка за наградами	422
13.7. Электронные иммобилайзеры	424
13.7.1. Принцип действия иммобилайзера	425
13.7.2. Краткие истории успеха	427
13.7.3. Перспективы на будущее	428
13.8. Идентификация контейнеров	429
13.8.1. Газовые баллоны и химические контейнеры	429
13.8.2. Сбор и утилизация отходов	432
13.9. Спортивное оборудование	434
13.10. Промышленная автоматизация	436
13.10.1. Идентификация инструментов	436
13.10.2. Промышленное производство	439
13.10.2.1. Централизованное управление	440
13.10.2.2. Децентрализованное управление	441
13.10.2.3. Преимущества, которые обеспечивает применение RFID-систем	442

13.10.2.4. Выбор оптимальной RFID-системы	443
13.10.2.5. Примеры проектов	444
13.11. Медицинские приложения	448
Глава 14. ПРИЛОЖЕНИЯ	450
14.1. Адреса для контактов, ассоциации и специализированные издания	450
14.1.1. Промышленные ассоциации	450
14.1.2. Специализированные издания	452
14.1.3. Ссылки на RFID в Интернете	454
14.2. Стандарты и рекомендации, которые имеют отношение к RFID.	455
14.2.1. Адреса, по которым можно получить стандарты и рекомендации.	460
14.3. Список литературы	461
14.4. Печатные платы	471
14.4.1. Карта для тестирования согласно стандарту ISO 14443	471
14.4.2. Катушка генератора поля	476
Предметный указатель	479

ПРЕДИСЛОВИЕ К ТРЕТЬЕМУ ИЗДАНИЮ

Данная книга рассчитана на самую широкую аудиторию. В первую очередь она предназначена для студентов и инженеров, которые впервые сталкиваются с RFID-технологиями. Им адресованы те главы, где рассказывается о принципах работы, а также излагаются основы RFID-технологий с физической точки зрения и с точки зрения теории передачи данных. Однако эта книга также рассчитана и на специалистов-практиков, которые хотели бы получить исчерпывающее и концентрированное описание различных технологий радиочастотной идентификации, изучить правовые вопросы, связанные с их использованием, а также ознакомиться с возможностями практического применения таких устройств.

Существует большое количество литературы, посвященной отдельным разделам RFID-технологий, однако найти и объединить все эти материалы в одно полное руководство — достаточно трудная задача, которая требует много времени, о чем свидетельствует работа над каждым новым изданием данной книги. Настоящая книга призвана ликвидировать этот пробел и послужить полным и исчерпывающим руководством в области систем радиочастотной идентификации. Доказательством высокого спроса на техническую литературу, посвященную рассматриваемой теме, является то, что предыдущие издания книги были переведены на английский, японский и китайский языки¹⁾.

Еще одна особенность данной книги — большое количество рисунков и схем, с помощью которых мы попытались дать как можно более наглядное описание RFID-технологий. При этом основное внимание было уделено физическим основам функционирования систем радиочастотной идентификации, соответствующий материал составляет самую большую главу в данной книге. Также особое внимание было уделено вопросам практического применения; по этой причине одной из наиболее объемных глав книги является глава 13 «Примеры практического применения».

Настоящее издание дает лишь основное представление о современных методах радиочастотной идентификации и не ставит перед собой задачу угнаться за развивающимися с невероятной скоростью RFID-технологиями. Невозможно описать все появившиеся за последнее время устройства, стандарты и методы их

¹⁾ Дополнительную информацию о немецкоязычном издании данной книги, а также о выполненных переводах на другие языки вы сможете найти на сайте <http://RFID-handbook.com>.

реализации. Автор благодарен всем, кто предоставил в его распоряжение подобную информацию, особенно тем, кто работает непосредственно в промышленной области. Однако в первую очередь задачей автора было дать ясное представление об основополагающих принципах работы устройств радиочастотной идентификации, на базе которых читателю будет легче воспринять новую информацию и составить представление о состоянии дел в этой отрасли.

К сожалению, в третьем издании мы вынуждены были опустить обзор рынка компонентов, так как с ростом количества фирм — производителей транспондеров это становится все более обременительным занятием. Вместе с тем в книге появился новый раздел, в котором подробно описываются главные физические принципы, лежащие в основе высокочастотных и микроволновых систем (раздел 4.2 «Электромагнитные волны»). Именно такие системы все увереннее завоевывают в Европе диапазон частот 868 МГц. Также была расширена весьма важная глава о стандартизации (глава 9), которая представляет особый интерес в связи с быстрым прогрессом в отрасли.

И наконец, следует поблагодарить те компании, которые предоставили в распоряжение автора многочисленные технические данные, статьи, рисунки и фотографии. Все это оказало автору неоценимую помощь в работе над книгой.

Мюнхен, лето 2002 года

Клаус Финкенцеллер

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

- ACM (Access Configuration Matrix)** — матрица конфигурирования доступа
- ABS (AcrylnitrilButadienStyrol)** — АБС-смола, сополимер акрилонитрила бутадиена и стирола
- AFC (Automatic Fare Collection)** — системы автоматического сбора платы за проезд на транспорте
- AFI (Application Family Identifier, ISO 14443-3)** — идентификатор семейства приложений
- AI (Application Identifier)** — идентификатор приложения
- AM (Amplitude Modulation)** — амплитудная модуляция
- APDU (Application Data Unit)** — блок данных приложения
- ASIC (Application Specific Integrated Circuit)** — специализированная интегральная микросхема
- ASK (Amplitude Shift Keying)** — амплитудная манипуляция
- ATR (Answer to Reset)** — ответ на сигнал сброса
- ATQ (Answer to Request)** — ответ на запрос (ATQA, ATQB — см. стандарт ISO 14443-3)
- AVI (Automatic Vehicle Identification)** — автоматическая идентификация транспорта (ж/д)
- BAPT (Bundesamt fur Post und Telekommunikation)** — Федеральное управление почты и телекоммуникаций
- Bd (Baud)** — скорость передачи данных, выраженная как бит/с или бод
- BGT (Block Guard Time)** — защитный интервал для блока данных
- BMBF (BundesMinisterium fur Bildung und Forschung)** — Федеральное министерство образования и научно-исследовательских разработок (ранее носило название BMFT)
- BP (BandPass (filter))** — полосовой фильтр
- C (Capacity)** — емкость конденсатора, конденсатор
- CCITT (Comitee Consultatif International Telegrafique et Telephonique)** — Международный консультативный комитет по телеграфной и телефонной связи
- CEN (Comitee Europeen de Normalisation)** — Европейский комитет по стандартизации

CEPT (Conference Europeenne des Postes et Telecommunications) — Европейская конференция по почтовой и телеграфной связи

CICC (Closed-Coupling Integrated Circuit Chip Card) — содержащая микросхему чип-карта с сильной связью

CIU (Contactless Interface Unit) — модуль бесконтактного интерфейса (модуль приемника/передатчика для бесконтактного интерфейса микропроцессора)

CLK (CLOCK) — тактовый сигнал

CRC (Cyclic Redundancy Checksum) — контрольная сумма циклического избыточного кода

dBm — мера мощности в логарифмическом масштабе относительно высокочастотного излучения с мощностью 1 мВт (0 дБм = 1 мВт, 30 дБм = 1 Вт)

DBP (Differential Bi-Phase encoding) — дифференциальное бифазное (двухфазное) кодирование

DIN (Deutsche IndustrieNorm) — Промышленный стандарт Германии

EAN (European Article Number) — Европейский товарный код (штрих-код на товарах и продовольственных продуктах)

EAS (Electronic Article Surveillance) — электронное наблюдение за предметами (электронные устройства защиты от краж)

EC (Electronic Cash) — электронный чек или электронный кошелек

ECC (European Communications Committee) — Европейский комитет по связи

EDI (Electronic Document Interchange) — электронный документооборот

EEPROM (Electronic Erasable and Programmable Read Only Memory) — электрически стираемое и программируемое ПЗУ

EMC (ElectroMagnetic Compatibility) — электромагнитная совместимость

EOF (End of Frame) — конец кадра

ERC (European Radiocommunications Committee) — Европейский комитет по радиосвязи

ERM (Electromagnetic Compatibility and Radio Spectrum Matters) — вопросы электромагнитной совместимости и радиочастотного спектра

ERO (European Radiocommunications Organization) — Европейская организация по радиосвязи

ERP (Equivalent Radiated Power) — эквивалентная излучаемая мощность

ETCS (European Train Control System) — Европейская система управления движением поездов

ETS (European Telecommunication Standard) — Европейский стандарт по связи

ETSI (European Telecommunication Standards Institute) — Европейский институт по стандартизации в области связи

EVC (European Vital Computer) — Европейский компьютер для выполнения ответственных функций

EVU (Energieversorgungsunternehmen) — энергоснабжающее предприятие

FCC (Federal Commission of Communication) — Федеральная комиссия по связи

FDX (Full-Duplex) — дуплексный режим (передачи данных)

FHSS (Frequency Hopping Spread Spectrum) — широкополосный сигнал со скачкообразной перестройкой частоты

FM (Frequency Modulation) — частотная модуляция

FRAM (Ferroelectric Random Access Memory) — ферроэлектрическое оперативное запоминающее устройство

FSK (Frequency Shift Keying) — частотная манипуляция

GSM (Global System for Mobile communication) — глобальная система мобильной связи (прежнее название: Groupe Special Mobile)

GTAG (Global-TAG) — глобальная метка (инициатива в области RFID, предложенная EAN и UCC)

I²C — шина передачи данных Inter-IC-Bus

HDX (Half-Duplex) — полудуплексный режим передачи данных

HF (High Frequency) — высокая частота (3...30 МГц)

ICC (Integrated Chip Card) — интегрированная чип-карта

ID — идентификация, идентификатор

ISM (Industrial Scientific Medical) — диапазон частот, отведенный для промышленных, научных и медицинских систем

ISO (International Standardization Organization) — Международная организация по стандартизации

L — индуктивность катушки

L (Loop) — петля, шлейф

LAN (Local Area Network) — локальная вычислительная сеть

LF (Low Frequency) — низкая частота (30...300 кГц)

LPD (Low Power Device) — радиоустройство, которое предназначено для передачи голоса или данных на расстояние, не превышающее нескольких сот метров

LRC (Longitudinal Redundancy Check) — продольный контроль; метод проверки на четность, при котором проверяется весь блок данных

LSB (Least Significant Bit) — младший значащий бит

MAD (MIFARE® Application Directory) — директория приложений MIFARE®

MSB (Most Significant Bit) — старший значащий бит

NAD (Node Address) — адрес узла

nomL (Nicht-offentlicher mobiler Landfunk) — закрытая мобильная радиосвязь (для использования в такси, на транспортных предприятиях, в промышленности и т.д.)

NRZ (Non Return to Zero Encoding) — кодирование без возврата к нулю

NTC (Negative Temperature Coefficient) — отрицательный температурный коэффициент (температурной зависимости сопротивления)

NVB (Number of Valid Bits) — количество значащих битов (стандарт ISO 14443-3)

- OCR (Optical Character Recognition)** — оптическое распознавание текста
- OEM (Original Equipment Manufacturer)** — фирма — производитель комплектного оборудования
- OFW (OberflächenWellen)** — поверхностные акустические волны (ПАВ)
- OPNV (Offentliche Personen NahVerkehr)** — общественный пассажирский транспорт
- OTP (One Time Programmable)** — однократно программируемая память
- PC (Personal Computer)** — персональный компьютер
- PCD (Proximity Card Device)** — бесконтактное считывающее устройство категории Proximity (см. стандарт ISO 14443)
- PICC (Proximity Integrated Chip Card)** — интегрированная бесконтактная чип-карта Proximity (см. стандарт ISO 14443)
- PKI (Public Key Infrastructure)** — инфраструктура сертификации открытых ключей (шифрования)
- PMU (Power Management Unit)** — блок управления электропитанием
- PP (Plastic Package)** — пластиковый корпус
- PPS (PolyPhenylenSulfid)** — полифенилсульфид
- PSK (Phase Shift Keying)** — фазовая манипуляция
- PUPI (Pseudo Unique PICC Identifier)** — псевдоуникальный идентификатор PICC-карты (см. стандарт ISO 14443-3)
- PVC (PolyVinylChlorid)** — ПВХ, поливинилхлорид
- R&TTE (Radio and Telecommunication Terminal Equipment)** — оконечное радио- и телекоммуникационное оборудование (Директива по радиочастотному оборудованию и терминальному телекоммуникационному оборудованию, 1995/5/EC)
- RADAR (Radio Detecting And Ranging)** — радар
- RAM (Random Access Memory)** — ОЗУ, оперативная память с произвольным доступом
- RCS (Radar Cross Section)** — эффективное сечение рассеяния, эффективная площадь рассеяния
- REQ (REQuest)** — запрос
- RFID (Radio Frequency IDentification)** — радиочастотная идентификация
- RFU (Reserved for Future Use)** — зарезервировано для использования в будущем
- RTI (Returnable Trade Items)** — торговое оборудование, подлежащее возврату или пригодное для повторного использования
- RTIS (Road Transport Information System)** — транспортная информационная система
- RTTT (Road Transport & Traffic Telematics)** — телематические устройства транспортных систем и систем наблюдения за дорожным движением
- RWD (Read Write Device)** — устройство, для которого разрешены как чтение, так и запись данных
- SAM (Security Authentication Module)** — модуль обеспечения безопасности данных, который осуществляет аутентификацию

- SCL (Serial CLock)** — тактовый сигнал последовательного интерфейса (шина I2C)
- SDA (Serial Data Address)** — линия ввода/вывода данных и адреса (шина I2C)
- SEQ (Sequentielles System)** — последовательные системы
- SMD (Surface Mount Devices)** — компоненты для поверхностного монтажа
- SNR (Serial Number)** — серийный номер
- SOF (Start of Frame)** — начало кадра
- SRAM (Static Random Access Memory)** — статическая оперативная память
- SRD (Short Range Devices)** — радиоустройства, которые предназначены для передачи голоса или данных на малые расстояния, обычно не превышающие нескольких сот метров
- TR** — технические условия
- UART (Universal Asynchronous Receiver Transmitter)** — универсальный асинхронный приемопередатчик
- UCC (Universal Code Council)** — Совет по единому коду (американский стандарт, который определяет использование штрих-кодов для товаров и продовольственных продуктов)
- UHF (Ultra High Frequency)** — СВЧ, сверхвысокая частота (300 МГц...3 ГГц)
- UPC (Universal Product Code)** — универсальный товарный код
- VCD (Vicinity Card Device)** — бесконтактное считывающее устройство категории Vicinity (см. стандарт ISO 15693)
- VDE (Verein Deutscher Elektrotechniker)** — общество немецких электриков
- VICC (Vicinity Integrated Contactless Chip Card)** — интегрированная бесконтактная чип-карта Vicinity (см. стандарт ISO 15693)
- VSWR (Voltage Standing Wave Ratio)** — коэффициент стоячей волны по напряжению
- XOR (eXclusive-OR)** — логическая операция Исключающее ИЛИ
- ZV (Zulassungsvorschritt)** — процесс приемки в эксплуатацию
- HITAG®, i-Code®, MIFARE®** — зарегистрированные товарные знаки компании Philips electronics N.V.
- LEGIC®** — зарегистрированный товарный знак компании KABA Security Locking Systems AG
- MICROLOGIC®** — зарегистрированный товарный знак компании Idesco
- TagIt®, TIRIS®** — зарегистрированные товарные знаки компании Texas Instruments
- TROVAN®** — зарегистрированный товарный знак компании AEG ID-Systeme

В последнее время в таких сферах деятельности, как оптовая торговля и логистика товаров, розничная торговля, производство или системы управления распределением и учетом материалов, все большее распространение получают системы автоматической идентификации (Auto-ID). Основным назначением подобных систем является сохранение и передача информации о людях, домашних животных, товарах и других объектах.

Первыми в этой области были этикетки со штрих-кодами, появление которых вызвало настоящую революцию. Однако сегодня их возможности не удовлетворяют требованиям, предъявляемым к подобным системам. Даже низкая стоимость не может компенсировать такие недостатки этих этикеток, как небольшой объем хранимой информации и отсутствие возможности записи новых данных.

Одно из решений указанных проблем состоит в использовании полупроводниковой микросхемы в качестве носителя информации. Из всех подобных электронных носителей данных наибольшей известностью пользуется чип-карта, например телефонная или банковская. Однако и у таких карт имеется слабое место — наличие механических контактов, что существенно ограничивает область их применения. Более удобным оказывается способ передачи данных между носителем и считывающим устройством, при котором не требуется непосредственного контакта между этими устройствами. В идеальном случае устройство считывания должно также являться для электронного носителя информации и источником питания (передавая необходимую для работы энергию), причем тоже без непосредственного контакта. Системы, в которых передача данных и энергии осуществляется без какого-либо механического контакта между устройствами, получили название *бесконтактных*, или *радиочастотных систем идентификации* — сокращенно *RFID-системы* (Radio Frequency IDentification).

О растущем значении этого рынка свидетельствует также увеличение числа компаний, активно занимающихся производством и продажей RFID-систем. Если в 2000 году объем продаж систем радиочастотной идентификации составлял 900 млн долларов, то в 2005 году этот рынок вырос до 2 650 млн долларов [vcd]. Согласно этим данным (см. **Рис. 1.1**) рынок систем радиочастотной идентификации относится к наиболее быстро развивающимся, наряду с мобильной связью и портативными компьютерами.

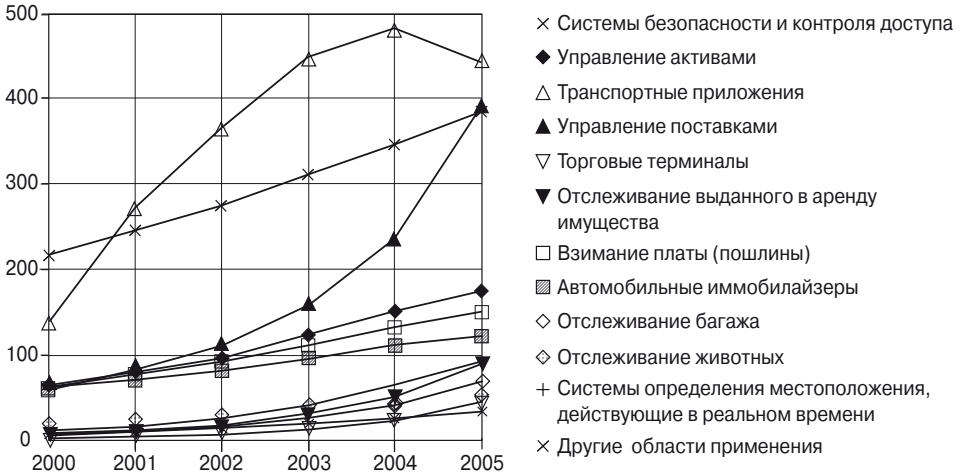


Рис. 1.1. Оценка развития мирового производства RFID-систем в период 2000...2005 гг. в миллионах долларов и области применения RFID-систем.

За последние годы сегмент систем радиочастотной идентификации оформился во вполне самостоятельную область, которую трудно отнести к какому-либо классическому разделу электроники, поскольку здесь переплелись воедино высокочастотные технологии и проблемы электромагнитной совместимости (ЭМС), полупроводниковые технологии, технологии защиты данных, криптография, телекоммуникации, производственные и другие самые различные технологии.

В качестве введения в эту область электроники рассмотрим основные системы автоматической идентификации (Auto-ID), а также используемые в их составе или связанные с ними системы радиочастотной идентификации (RFID).

1.1. Системы автоматической идентификации

Основные системы автоматической идентификации приведены на Рис. 1.2.

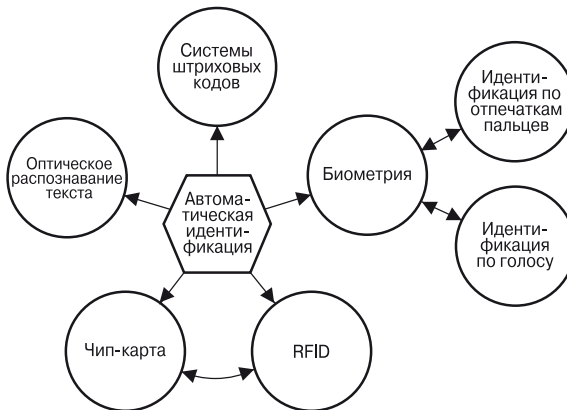


Рис. 1.2. Основные системы автоматической идентификации.

1.1.1. Системы с использованием штриховых кодов

Технология *штрихового кодирования* появилась почти 20 лет назад и была первой системой автоматической идентификации. По оценкам экспертов, объем рынка подобных систем в начале 90-х годов составлял около трех миллиардов немецких марок, и это только в пределах Западной Европы [virnich].

Обычный штрих-код — это двоичный код, который отображается в виде упорядоченных параллельных линий (англ. — bar), разделенных пробелами. Подобная структура представляет собой набор цифр или знаков, при этом полосы и пробелы (промежутки) между ними могут иметь различную ширину. Считывание данных производится с помощью лазера — здесь используется различие коэффициентов отражения от белых разделительных пространств и от темных линий штрихового кода [ident 1]. Несмотря на одинаковые физические принципы, существует значительное различие в структуре современных штрих-кодов и штрих-кодов, которые использовались десять лет назад.

Наиболее распространенной среди систем кодирования с использованием штрих-кодов (причем с большим отрывом) является система кодирования EAN (European Article Number), которая появилась в 1976 году и была специально предназначена для торговли продовольственными товарами. Коды EAN были созданы на основе разработанных в США кодов UPS (Universal Product Code), которые были введены в действие в 1973 году. На сегодняшний момент кодировка UPC является разновидностью кода EAN и, следовательно, полностью совместима с европейской кодировкой [virnich]. Код EAN состоит из 13 цифр: кода страны, общедоказательного номера предприятия, установленного производителем кода товара, а также контрольной цифры PZ (см. Рис. 1.3).

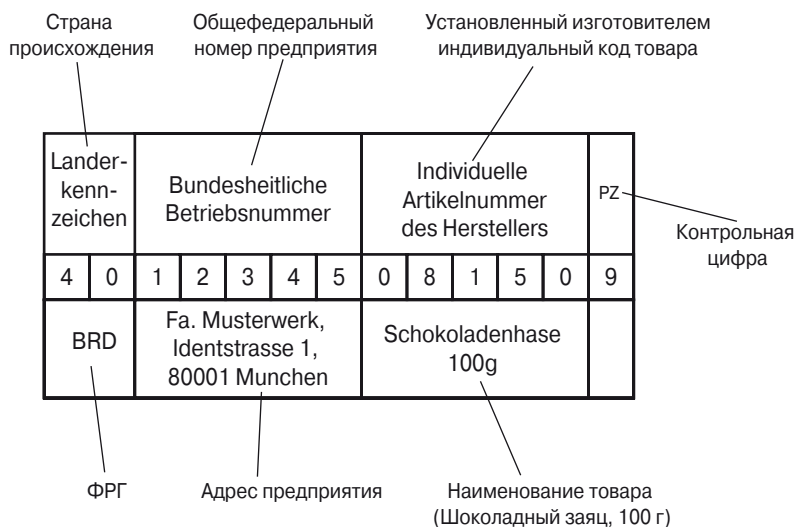


Рис. 1.3. Пример штрих-кода в системе EAN (European Article Number).

Системы штрихового кодирования, получившие распространение в других отраслях, приведены в Табл. 1.1.

Таблица 1.1. Популярные системы штрихового кодирования и области их применения

Система	Типичные области применения
Code Codabar	Медицинские приложения, приложения, где существуют высокие требования к безопасности
Code 2/5 interleaved	Автомобильная промышленность, товарные склады, паллеты, морские контейнеры, тяжелая промышленность
Code 39	Перерабатывающая промышленность, логистика, университеты и библиотеки

1.1.2. Системы оптического распознавания текста

Первые *системы оптического распознавания текста* (Optical Character Recognition — OCR) появились еще в начале 60-х годов. Однако для них требовалась разработка и использование для написания текста специальных типов шрифтов, которые не только были бы понятны человеку, но и могли автоматически считываться машинами. Главным преимуществом систем OCR является высокая плотность информации, а также то, что при необходимости (или в целях контроля) данные могут быть просто считаны без использования каких-либо систем кодирования [virnich]. Эти системы получили наибольшее распространение в области производства и управления, в сфере обслуживания и в банковской отрасли — при обработке чеков¹⁾. Широкому распространению систем оптического распознавания мешает более высокая по сравнению с другими системами автоматической идентификации цена, а также сложность считывающего оборудования.

1.1.3. Биометрические системы

Биометрика — согласно словарю иностранных слов — это наука, основанная на описании и измерении характеристик тела живых существ. В применении к системам автоматической идентификации под биометрическими понимают те системы и методы, которые основаны на использовании каких-либо уникальных качеств человеческого организма. На практике чаще всего используются отпечатки пальцев, отпечаток руки, идентификация по голосу или же по главному дну (реже по радужной оболочке глаза).

1.1.3.1. Идентификация по голосу

Для идентификации человека по голосу в последнее время было разработано большое количество систем, работающих по следующему принципу: голос записывается с помощью микрофона, данные с которого передаются в компьютер. Преобразованный в цифровую форму речевой сигнал затем обрабатывается программой идентификации.

Задача подобных систем состоит в сравнении голоса человека с образцом, хранящимся в базе данных. В случае положительного результата система может выполнять какие-либо дополнительные действия, например подать команду «Открыть дверь».

¹⁾ В самой нижней строке чека находятся персональные данные (имя и фамилия, номер банковского счета), которые напечатаны шрифтом, понятным для системы оптического распознавания.

1.1.3.2. Идентификация по отпечаткам пальцев (дактилоскопия)

Дактилоскопия, или идентификация по отпечаткам пальцев, уже более сотни лет используется в криминалистике для поиска правонарушителей. Здесь идентификация объекта осуществляется по папиллярному рисунку кончиков или подушечек пальцев, которые могут быть получены не только непосредственно с самих пальцев, но и с тех предметов, к которым прикасался этот человек.

В системах идентификации по отпечаткам пальцев, которые чаще всего используются в системах контроля доступа, необходимо приложить подушечку пальца к специальному считывающему устройству. Система преобразует считанное изображение в набор цифровых данных и пытается найти аналогичный образец в базе данных. Современные системы идентификации такого типа осуществляют сканирование и идентификацию менее чем за половину секунды. Для того чтобы усилить защиту от несанкционированного проникновения, в некоторых системах используются дополнительные методы, позволяющие определить, принадлежит ли этот палец живому человеку [schmidhäusler].

1.1.4. Чип-карты (Smart-cards)

Под *чип-картами* понимают устройства электронного хранения информации, которые дополнительно имеют встроенный микроконтроллер (микропроцессорные карты) и которые — для удобства обращения — размещаются в пластиковой карточке, размерами напоминающей банковскую карту. Первые такие карты появились в 1984 году и использовались для оплаты телефонных переговоров. При этом чип-карта вставляется в специальное считывающее устройство, и ее контакты электрически соединяются с контактами считывающего устройства (ридера).

После установления электрического контакта считывающее устройство обеспечивает питание для чип-карты и передает сигналы синхронизации. Для передачи данных используется последовательный интерфейс (I/O Port — порт ввода/вывода), передача данных по которому может осуществляться в двух направлениях. В зависимости от устройства карты различают *карты памяти* и микропроцессорные карты.

Одним из важнейших преимуществ чип-карт является то, что они способны защитить хранящиеся в них данные от несанкционированного считывания и модификации. Использование чип-карт позволило значительно упростить, ускорить и удешевить множество операций, связанных с передачей информации или с денежными операциями. В 1992 году в мире было выпущено 200 миллионов чип-карт (из них 20% — в Германии!), в 1995 году — уже 600 миллионов, из них 500 миллионов карт памяти и 100 миллионов микропроцессорных карт. Таким образом, этот рынок превратился в один из наиболее быстрорастущих сегментов рынка электронных устройств.

Важнейшим недостатком чип-карт является уязвимость их контактов — материал подвержен износу, загрязнению, коррозии. Если считывающее устройство интенсивно используется, то оно будет часто выходить из строя и на его обслуживание будут расходоваться значительные средства. Кроме того, если устрой-

ства для считывания чип-карт (например, телефонные автоматы) расположены в открытых местах, то их достаточно сложно защитить от вандализма.

1.1.4.1. Карты памяти

В *картах памяти* доступ к внутренней памяти (чаще всего EEPROM) осуществляется с помощью последовательной логики (State Machine — конечный автомат). Кроме того, с помощью этой логики могут быть реализованы простейшие алгоритмы защиты данных (см. **Рис. 1.4**), например поточное шифрование (Streamcipher). Функциональность такой карты ограничена, как правило, какой-то узкой областью, и благодаря высокой степени специализации и отсутствию гибкости и универсальности эти карты очень дешевы. Подобные карты находят применение там, где основное значение имеют низкая цена и большие объемы, например в области медицинского страхования в системе государственных больничных касс [lemme].

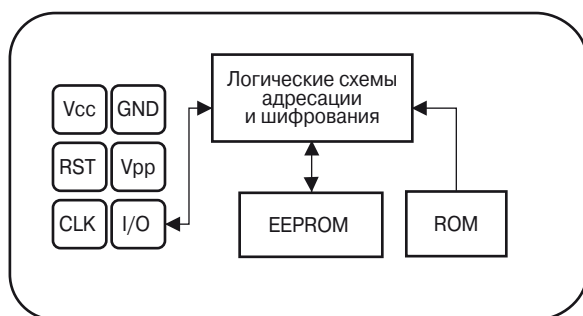


Рис. 1.4. Архитектура чип-карты, в которой реализована схема защиты данных (RST — сигнал сброса, V_{pp} — напряжение программирования EEPROM, I/O — сигналы ввода/вывода).

1.1.4.2. Микропроцессорные карты

Как следует из их названия, *микропроцессорные карты* содержат микропроцессор, который взаимодействует с микросхемами памяти различных типов (ROM, RAM, EEPROM).

В памяти ROM хранится управляющая программа микропроцессора, которая прошивается в эту память в процессе производства карты. Содержание программы идентично для всех карт данной серии и не может быть изменено.

В памяти EEPROM хранятся специфичные для конкретного приложения данные, а также код дополнительных программ. Запись или чтение из этой области памяти производится микропроцессором под управлением операционной системы.

Память RAM необходима для временного (промежуточного) хранения данных, используемых в ходе выполнения программы микропроцессором. Все данные, которые хранятся в этой области памяти, при выключении питания будут утеряны.

Преимуществом микропроцессоров является их высокая гибкость: операционная система современных чип-карт позволяет интегрировать на одной карточке несколько приложений. Коды таких приложений могут записываться в EEPROM в процессе производства чип-карты и при необходимости вызываются операционной системой микропроцессора (см. **Рис. 1.5**).

Наибольшее распространение микропроцессорные карты получили в чувствительных к безопасности приложениях, например чип-карты для мобильных телефонов стандарта GSM или же новые платежные ЕС-карты (ЕС — Electronic Cash). Микропроцессорные карты позволяют добавлять новые программы или вносить изменения в существующие, благодаря чему они легко адаптируются к новым требованиям.

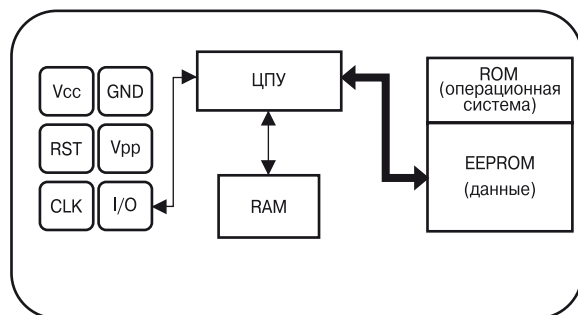


Рис. 1.5. Типичная архитектура микропроцессорной карты.

1.1.5. RFID-системы

Системы радиочастотной идентификации (RFID) тесно связаны с описанными выше чип-картами. Здесь также носителем данных является электронное устройство — транспондер. Однако подача питания и обмен данными производятся без какого-либо непосредственного контакта — с помощью электромагнитного поля. Основой данной технологии являются методы, получившие широкое распространение в радарных и радиосистемах. Собственно, сокращение RFID образовано от названия Radio-Frequency-Identification (радиочастотная идентификация).

За последнее время благодаря своим очевидным преимуществам перед другими системами автоматической идентификации системы RFID завоевывают все большую долю рынка. Например, они все чаще применяются в виде бесконтактных чип-карт для оплаты проезда в общественном транспорте.

1.2. Сравнение различных систем идентификации

В **Табл. 1.2** приведены преимущества и недостатки систем радиочастотной идентификации по сравнению с системами других типов. Анализируя данную таблицу, можно убедиться в тесном родстве RFID и чип-карт, при этом системы радиочастотной идентификации свободны от многих недостатков последних,

так как здесь не требуется непосредственного контакта со считывающим устройством. В связи с этим уменьшается опасность вандализма, загрязнения, а также нет необходимости тратить время на то, чтобы вставить карту в разъем считывающего устройства.

Таблица 1.2. Сравнение различных систем идентификации

Параметр	Система на основе штрих-кодов	OCR-система	Система распознавания речи	Биометрическая система	Чип-карта	RFID-система
Объем хранимых данных, байт	1...100	1...100	—	—	16...64К	16...64К
Плотность данных	Низкая	Низкая	Высокая	Высокая	Очень высокая	Очень высокая
Читаемость данных для устройства	Хорошая	Хорошая	Связана с высокими затратами	Связана с высокими затратами	Хорошая	Хорошая
Читаемость данных для человека	Относительная	Легко	Легко	Тяжело	Невозможно	Невозможно
Влияние загрязнений или влаги	Очень сильное	Очень сильное	—	—	Возможно (контакты)	Не влияет
Влияние препятствий (оптических)	Полная неработоспособность	Полная неработоспособность	—	Возможно	—	Не влияет
Ограничение на положение и направление	Небольшое	Небольшое	—	—	Определяется конструкцией разъема	Нет
Влияние износа и амортизации	Относительное	Относительное	—	—	Контакты	Не влияет
Стоимость изготовления электроники	Очень низкая	Средняя	Очень высокая	Очень высокая	Низкая	Средняя
Эксплуатационные расходы (например, печать на принтере)	Низкие	Низкие	Отсутствуют	Отсутствуют	Средние (контакты)	Отсутствуют
Возможность несанкционированного копирования или изменения	Легко	Легко	Возможно (фонограмма) ¹⁾	Невозможно	Невозможно	Невозможно
Скорость считывания данных (включая подготовку носителя данных)	Низкая, ~ 4 с	Низкая, ~ 3 с	Очень низкая, > 5 с	Очень низкая, > 5 с	Низкая, ~ 4 с	Очень высокая, ~ 0.5 с