RFID-технологии

Справочное пособие

Klaus Finkenzeller

RFID-Handbuch

Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten

3., aktualisierte und erweiterte Auflage

HANSER

Клаус Финкенцеллер

RFID-технологии

Справочное пособие

Перевод с немецкого

Москва
Издательский дом «Додэка-XXI»
2010

УДК 621.396.6(035)
ББК 32.844я22
Ф59

Финкенцеллер, Клаус

Ф59 RFID-технологии. Справочное пособие / К. Финкенцеллер; пер. с нем. Сойунханова Н.М. — М. : Додэка-XXI, 2010. — 496 с.: ил. — Доп. тит. л. нем. — ISBN 978-5-94120-232-4.

Данный справочник представляет собой исчерпывающий обзор систем RFID (систем радиочастотной идентификации), который ориентирован, главным образом, на практические вопросы их применения. Системы RFID находят применение в самых разнообразных областях, например в системах контроля допуска на предприятия или в гостиничные номера, в качестве электронных иммобилайзеров или же как средства предотвращения краж в супермаркетах. Основой подобных систем являются электронные носители данных, не обладающие собственным источником питания (транспондеры). Информация с такого носителя считывается бесконтактным способом.

В книге описываются физические принципы работы систем радиочастотной идентификации, содержится информация по действующим в этой области стандартам и основным областям практического применения RFID-систем. Представлены также материалы, касающиеся физических принципов функционирования СВЧ и микроволновых систем, которые приобретают все большее значение в связи с открытием соответствующих частотных диапазонов.

Для иллюстрации достаточно сложных понятий используются многочисленные рисунки. Приводятся примеры, которые поясняют вопросы, связанные с практическим применением систем радиочастотной идентификации. В приложении содержится контактная информация, а также обзор стандартов и рекомендаций, приводятся ссылки на литературу и на источники информации в Интернете.

Предназначена для разработчиков систем радиочастотной идентификации, инженеров, студентов, а также будет полезна менеджерам, занимающимся вопросами применения устройств RFID.

УДК 621.396.6(035)
ББК 32.844я22

ISBN 978-5-94120-232-4 (рус.)
ISBN 3-446-22071-2 (нем.)

ОГЛАВЛЕНИЕ

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 языки[1)].

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 Erasible 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)

I^2C — 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 (OberflachenWellen) — 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 (PolyVinilChlorid) — 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 (eXlusive-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

ГЛАВА 1

ВВЕДЕНИЕ

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.

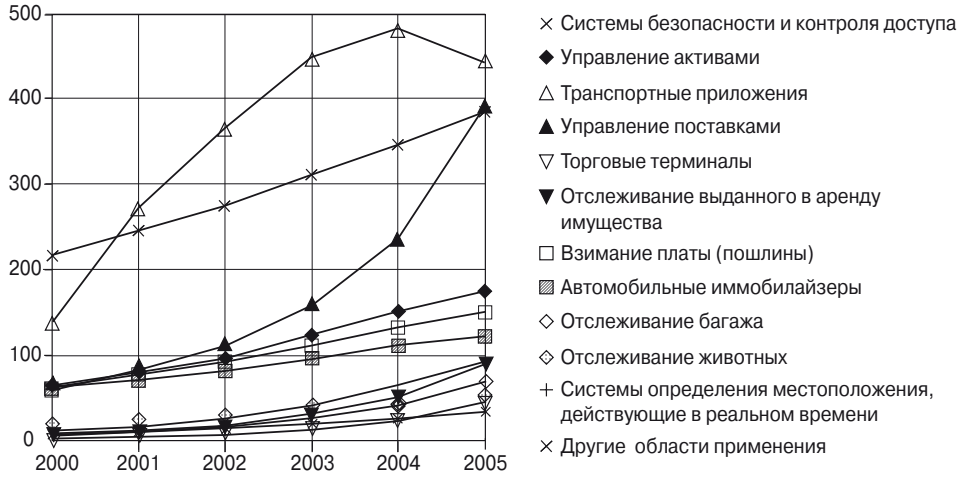


Рис. 1.1. Оценка развития мирового производства RFID-систем в период 2000...2005 гг. в миллионах долларов и области применения RFID-систем.

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**.

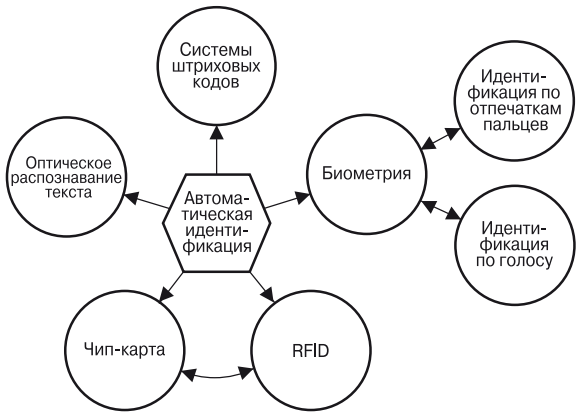


Рис. 1.2. Основные системы автоматической идентификации.

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, общефедерального номера предприятия, установленного производителем кода товара, а также контрольной цифры PZ (см. **Рис. 1.3**).

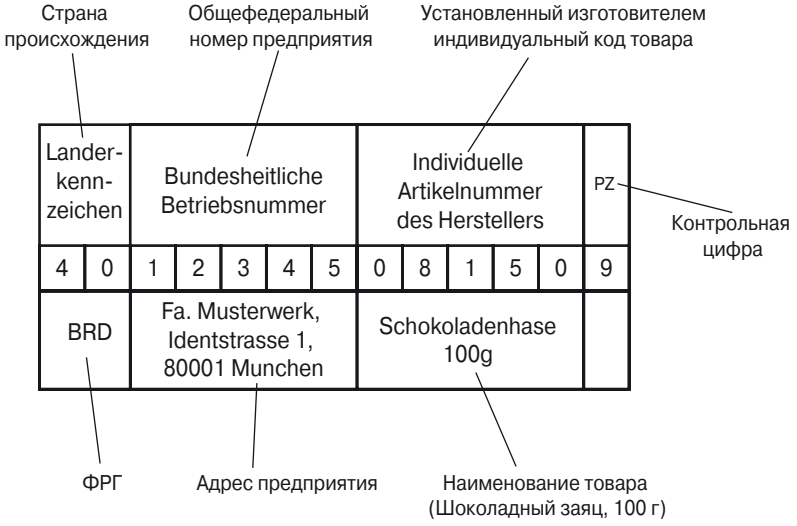


Рис. 1.3. Пример штрих-кода в системе EAN (European Article Number).

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 чеков[1]. 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 биметрическими 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 глазному 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].

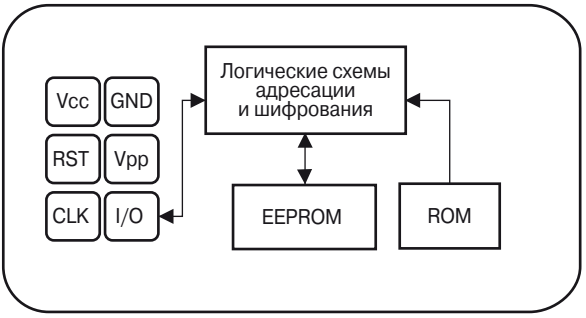


Рис. 1.4. Архитектура чип-карты, в которой реализована схема защиты данных (RST — сигнал сброса, V_{PP} — напряжение програмирования EEPROM, I/O — сигналы ввода/вывода).

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 EC-карты (EC — Electronic Cash). Микропроцессорные карты позволяют добавлять новые программы или вносить изменения в существующие, благодаря чему они легко адаптируются к новым требованиям.

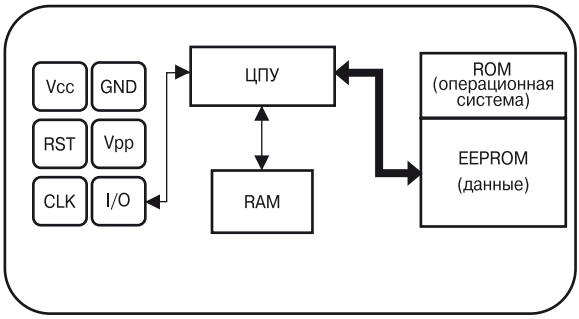


Рис. 1.5. Типичная архитектура микропроцессорной карты.

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 бóльшую 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...64K	16...64K
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

Таблица 1.2. **Сравнение различных систем идентификации** *(продолжение)*

Параметр	Система на основе штрих-кодов	OCR-система	Система распознавания речи	Биометрическая система	Чип-карта	RFID-система
Максимально допустимое удаление носителя данных от считывающего устройства	0...50 см	Менее 1 см (сканер)	0...50 см	Непосредственный контакт[2)]	Непосредственный контакт	0...5 м

Примечания:

1. Для систем распознавания речи можно снизить успех использования фонограммы (replay), если пользователю при проведении идентификации дать прочитать текст, который генерируется случайным образом.

2. Это относится к системам идентификации на основе отпечатков пальцев; если идентификация проводится по радужной оболочке глаза, то непосредственный контакт отсутствует.

1.3. Основные компоненты RFID-систем

Система радиочастотной идентификации состоит из двух основных компонентов (**Рис. 1.6**):

- *Транспондер*, закрепляемый на объекте, который должен пройти процедуру идентификации.
- *Считывающее устройство*, или ридер[1)], которое в зависимости от приложения может не только считывать, но и записывать данные.

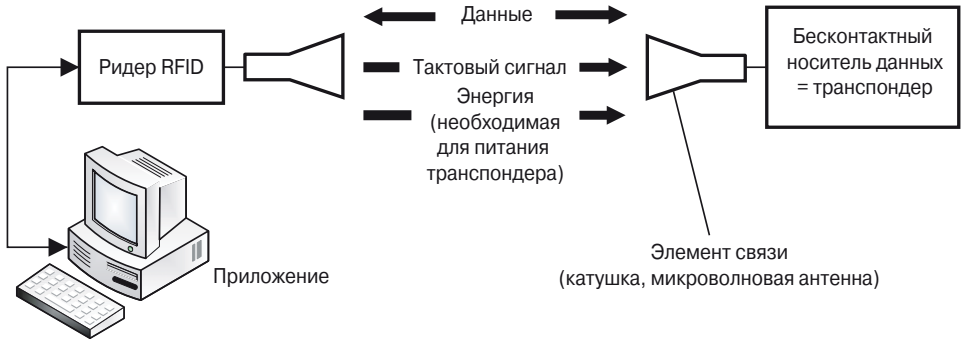


Рис. 1.6. Основные компоненты системы радиочастотной идентификации: слева — считывающее устройство, справа — транспондер.

Считывающее устройство (**Рис 1.7**) содержит высокочастотный модуль (приемопередающее устройство), контроллер и элемент связи с транспондером. Кроме того, многие считывающие устройства также имеют дополнительный интерфейс

[1)] В данной книге мы будем использовать именно название «считывающее устройство/ридер». При этом сам термин не говорит о направлении считывания данных, так как считывающее устройство может как считывать, так и передавать данные транспондеру.

Рис. 1.7. Считывающее устройство и бесконтактная чип-карта (фото: Philips Semiconductors Gratkorn, A-Gratkorn)

(RS-232, RS-485 и т.п.), который служит для передачи данных другим компонентам системы (персональному компьютеру или системе автоматизированного управления).

Транспондер (**Рис 1.8**) является *носителем данных* в системе RFID и состоит из *элемента связи* и специализированной микросхемы. За пределами зоны действия считывающего устройства транспондер не проявляет никакой активности, поскольку не содержит собственного источника питания. Однако при перемещении в зону действия системы радиочастотной идентификации транспондер активизируется, получая необходимую энергию с помощью элемента связи, который также отвечает за передачу сигналов синхронизации и данных.

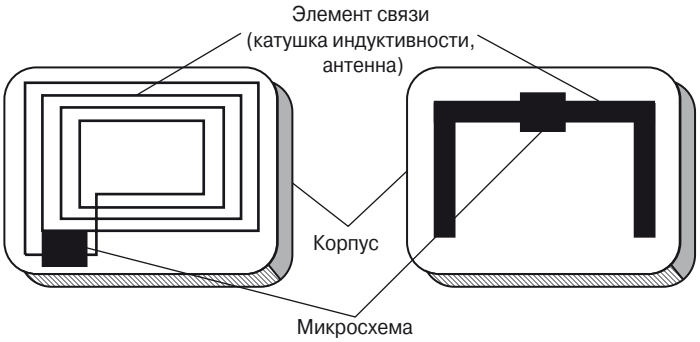


Рис. 1.8. Принципиальная схема транспондера, цифрового носителя данных в системе RFID. Слева — транспондер с индуктивной связью, показана катушка антенны; справа — микроволновый транспондер с антенной-диполем.

ГЛАВА 2

ОСНОВНЫЕ ОСОБЕННОСТИ RFID-СИСТЕМ

2.1. Основные характеристики систем радиочастотной идентификации

На сегодняшний день существует огромное количество различных систем радиочастотной идентификации от большого числа компаний — производителей. Для того чтобы дать ясное представление о присутствующих на рынке системах, необходимо для начала определить ключевые характеристики и создать стройную классификацию современных RFID-систем (см. **Рис. 2.1**).

В первую очередь системы радиочастотной идентификации можно разделить по принципу их работы: *дуплексные* (Full DupleX — FDX) и *полудуплексные* (Half DupleX — HDX), кроме этого существуют и *последовательные* системы (SEQuential — SEQ).

При дуплексном и полудуплексном методе транспондер передает ответные данные при включенном высокочастотном поле ридера. Когда сигнал от транспондера достигает антенны считывающего устройства, он значительно ослаблен по сравнению с сигналом, который передает считывающее устройство. Для того чтобы считывающее устройство могло выделить полученный сигнал на фоне передаваемого им сигнала, в транспондере используются специальные способы передачи сигнала: модуляция нагрузкой (load modulation), модуляция нагрузкой с использованием поднесущей, а также передача данных на частоте гармоник (или субгармоник) основной частоты считывающего устройства.

При *последовательном* методе передачи (SEQ) считывающее устройство в определенное время прекращает передачу сигнала на основной частоте. Эти временные промежутки распознаются транспондером, который использует их для передачи данных считывающему устройству. Основным недостатком такого способа является то, что в этот момент транспондер не получает извне энергии, и поэтому приходится использовать дополнительные конденсаторы или батареи, которые заранее запасают энергию и обеспечивают питание, когда транспондер передает сигнал считывающему устройству.

Объем данных, передаваемый от транспондера к считывающему устройству, может изменяться от нескольких байтов до нескольких килобайтов. Однако существует и исключение — так называемые однобитные транспондеры (1-bit transponder); такой транспондер действительно передает только один бит данных,

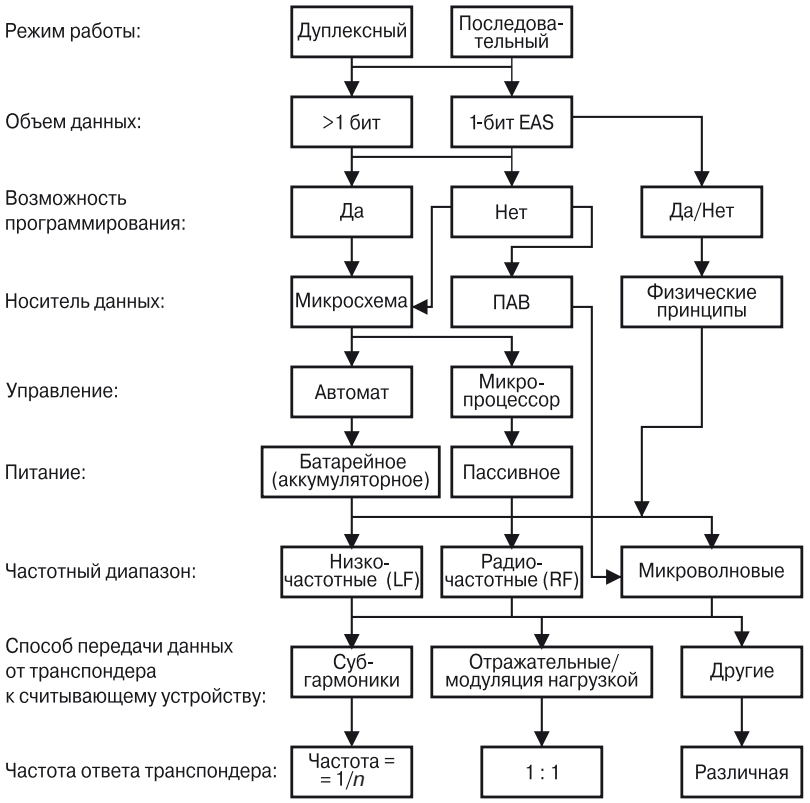


Рис. 2.1. Основные характеристики RFID-систем [isd].

и этого вполне достаточно для того, чтобы считывающее устройство сигнализировало об одном из двух состояний: «транспондер находится в зоне действия» или «транспондер вышел из зоны действия». Возможностей таких транспондеров вполне хватает для многих простых систем охраны или сигнализации, а так как для создания подобных однобитных транспондеров нет необходимости использовать какие-либо электронные компоненты, то их стоимость может составлять доли пфеннига. По этой причине транспондеры данного типа в огромных количествах используются в EAS-системах для контроля и предотвращения краж товаров в больших магазинах и супермаркетах. При попытке тайно вынести товар транспондер подает сигнал «нахожусь в поле действия считывающего устройства», и соответствующее сообщение передается охране. При оплате покупки транспондер извлекается или деактивируется на кассе.

Следующей важной характеристикой транспондера является наличие цифрового идентификатора. В наиболее простом случае цифровой идентификатор (чаще всего это просто серийный номер транспондера) прошивается в устройство при его производстве и в дальнейшем не может быть изменен. Но существуют и такие типы транспондеров, которые позволяют считывающему устройству не только считывать, но и изменять цифровой идентификатор транспондера. Для хранения данных в основном используются три метода. В системах RFID с индуктивной

связью для хранения чаще всего используется память EEPROM (Electrically Erasable Programmable Read-Only Memory), которая обеспечивает до 100 000 циклов записи данных. Ранее также использовалась и память FRAM (Ferromagnetic Random Access Memory), которая в сравнении с EEPROM имеет более низкое энергопотребление (приблизительно в 100 раз), а также меньшее время записи — приблизительно в 1000 раз. Однако широкому распространению памяти FRAM мешают технологические проблемы, возникающие при ее производстве.

В микроволновых системах RFID для хранения данных также может использоваться и память SRAM (Static Random Access Memory), которая имеет чрезвычайно быстрый цикл записи и чтения данных. Однако эта память не является энергонезависимой, и для предотвращения потери данных необходимо использовать непрерываемый источник питания.

В программируемых системах для управления циклами чтения и записи данных, а также для определения прав на чтение или запись данных используется «внутренняя логика» носителя данных. Обычно она реализуется с помощью конечных автоматов (подробнее см. в главе 10 «Архитектура электронных носителей информации»). С помощью конечных автоматов можно реализовывать самые сложные процессы, однако их недостатком является невысокая гибкость, так как при изменении протокола необходимо заменять саму электронную микросхему. Это означает, что при разработке новых версий транспондера вам придется вновь разрабатывать и микросхему, что связано с достаточно высокими затратами.

Применение микропроцессоров позволяет избавиться от подобных ограничений. Основная исполняемая программа или операционная система, которая осуществляет управление используемыми в приложении данными, может быть записана в процессе изготовления микропроцессора в самой микросхеме. При этом вы имеете возможность свободно вносить изменения и дополнения в логику работы программы, а также модифицировать ее для нужд различных приложений. Когда говорят о бесконтактных чип-картах, то для тех носителей данных, которые обеспечивают возможность записи информации и основаны на конечных автоматах, часто используют название «Карты памяти», чтобы отличить их от микропроцессорных карт.

Следует также упомянуть и о тех транспондерах, где для хранения данных используются различные физические эффекты, — сюда относятся транспондеры на ПАВ (поверхностных акустических волнах) без возможности записи. К таким устройствам также относятся 1-битные транспондеры, которые бóльшую часть времени находятся в пассивном состоянии (логический 0), но достаточно редко могут переходить и в активное состояние (логическая 1).

Важнейшей характеристикой транспондера является способ подачи питания. Различают *пассивные* транспондеры, которые не имеют собственного источника питания и всю необходимую энергию получают от считывающего устройства (используя электрическое или магнитное поле). В отличие от них *активные* транспондеры имеют собственный источник питания (батарейку), который полностью обеспечивает питание электронных компонентов или же запасает переданную энергию для кратковременной поддержки работы устройства.

Следующей важной характеристикой является *рабочая частота* излучения транспондера, которая в свою очередь определяет его дальность действия. При этом под рабочей частотой RFID-системы понимают частоту, которую считы-

вающее устройство использует для передачи данных; частота, на которой отвечает транспондер, здесь никак не учитывается. В большинстве случаев частота передачи данных транспондером не отличается от частоты, которую использует считывающее устройство (модуляция нагрузкой, отражение). Однако часто мощность передаваемого транспондером излучения может быть на несколько порядков ниже, чем мощность излучения, передаваемого считывающим устройством.

Обычно используются три частотных диапазона: низкочастотный — LF (Low Frequency, 30...300 кГц), высокочастотный и радиочастотный — HF/RF (High frequency/Radio frequency, 3...30 МГц), диапазон сверхвысоких частот — UHF (Ultra High Frequency, 300 МГц...3 ГГц), а также диапазон миллиметровых волн (свыше 3 ГГц). Существует и дополнительное разделение RFID-систем по дальности их действия: ближнего действия (close coupling, 0...1 см), средней дальности действия (remote-coupling, 0...1 м) и дальнего действия (более одного метра).

Существует и классификация по способам передачи данных в направлении от транспондера к считывающему устройству. Здесь выделяют три группы: первая — использующая отражение, или рассеяние (частота отраженного, или рассеянного, сигнала при этом равна частоте, на которой ведет передачу считывающее устройство, соотношение частот — 1:1). Вторая — это модуляция нагрузкой (транспондер воздействует на поле, которое излучает считывающее устройство, соотношение частот — 1:1), и третья — использование транспондером субгармоник (соотношение частот — $1/N$) или использование поверхностных волн (N раз).

2.2. Основные конструкции транспондеров

2.2.1. Транспондеры, выполненные в форме монеты или диска

Наиболее часто транспондеры производятся в форме диска (или монетки), корпус которого изготавливается литьем под давлением из ABS-пластика и имеет диаметр от нескольких миллиметров до десяти сантиметров (см. **Рис. 2.2**). В сере-

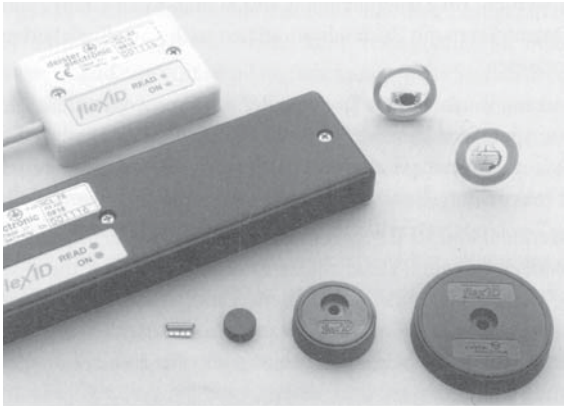


Рис. 2.2. Различные формы транспондеров (фото: Desiter Electronic, Барзингхаузен). Справа — антенна и чип, которые будут встроены в корпус. Слева — антенны считывающих устройств различной формы.

дине диска, как правило, имеется отверстие для крепления с помощью винта. Наряду с ABS-пластиком может использоваться полистирол или даже эпоксидная смола. Эти материалы способны обеспечить транспондеру более широкий диапазон рабочих температур.

2.2.2. Корпус из стекла

Для идентификации зверей и домашних животных были разработаны специальные транспондеры в корпусе из стекла, которые вводятся под кожу животных (подробнее о них рассказывается в главе 13 «Примеры применения»).

В продолговатой стеклянной трубке размером от 12 до 32 мм расположена печатная плата, на которой смонтированы электронная микросхема и развязывающий конденсатор, сглаживающий колебания напряжения питания. Антенна транспондера выполнена из провода диаметром всего 0.03 мм и намотана на один ферритовый сердечник. Для большей механической прочности все эти компоненты заключены в достаточно мягкую внешнюю оболочку (см. **Рис. 2.3** и **Рис. 2.4**).

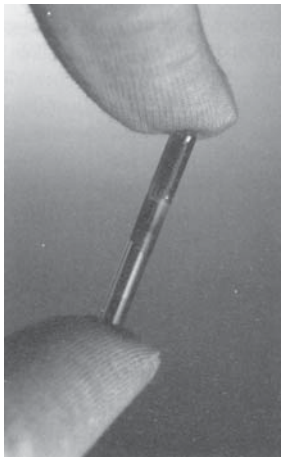


Рис. 2.3. Увеличенная фотография транспондера в 32-миллиметровом стеклянном корпусе, который используется для идентификации животных или же может встраиваться в другие конструкции (фото: Texas Instruments, Фрайзинг).

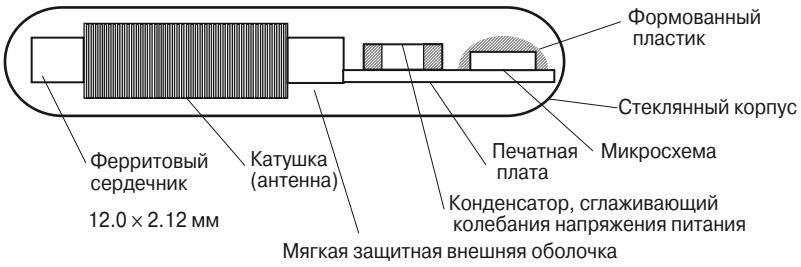


Рис. 2.4. Механическая конструкция транспондера со стеклянным корпусом.

2.2.3. Пластмассовый корпус

Пластмассовый корпус (**Рис. 2.5**) (Plastic Package — PP) был разработан для транспондеров, предназначенных для работы в системах, где предъявляются высокие требования по механической прочности. Такой корпус также легко встраивается в другие системы, например в охранные системы автомобильной сигнализации.

Рис. 2.5. Транспондер в пластмассовом корпусе (фото: Philips Semiconductors, Гамбург).

Транспондер, корпус которого изготовлен из пластика (специальный состав, из которого изготавливаются корпуса микросхем) в виде параллелепипеда со скошенным углом, содержит те же компоненты (см. **Рис. 2.6**), что и описанный чуть ранее транспондер в стеклянном корпусе, однако благодаря более длинной катушке он имеет больший радиус действия. Другими преимуществами являются возможность использования электронных компонентов с бóльшим размером корпуса, а также более высокая устойчивость к механическим нагрузкам, что, например является обязательным требованием для применения в автомобильной отрасли. Кроме этого, PP-транспондеры удовлетворяют и другим стандартам качества, например легко проходят испытания на термоциклирование или на падение с высоты [bruhnke].

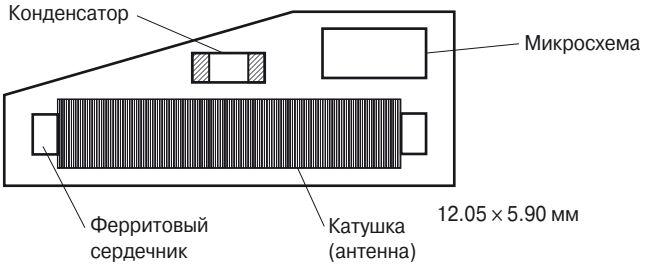


Рис. 2.6. Механическая конструкция транспондера в пластмассовом корпусе, толщина корпуса составляет приблизительно 3 мм.

2.2.4. Идентификация инструмента и газовых баллонов

Для того чтобы устанавливать транспондеры с индуктивной связью в объекты с металлическим корпусом, были разработаны специальные конструкции. В них

катушка антенны транспондера наматывалась на сегментный ферритовый сердечник, после чего микросхема транспондера монтировалась на обратной стороне такого сердечника и соединялась контактами с катушкой. Для того чтобы придать транспондеру механическую прочность, а также устойчивость к вибрациям и необходимую термостойкость, микросхема транспондера вместе с сегментным ферритовым сердечником и эпоксидным закрепителем помещается в полуцилиндр, изготовленный из PPS (полифенилсульфид) [link].

Если транспондер предназначен для установки в затяжные болты (**Рис. 2.7**) или хвостовики с целью идентификации рабочего инструмента, то его внешние размеры и способы крепления должны соответствовать нормам, установленным в стандарте DIN/ISO 69873. Для идентификации газовых баллонов могут использоваться и другие конструкции (см. **Рис. 2.8**).

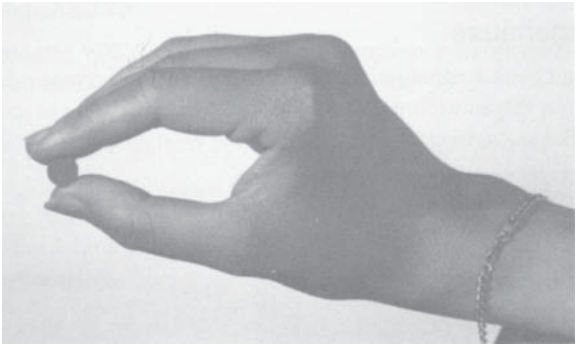


Рис. 2.7. Транспондер в корпусе, соответствующем требованиям DIN/ISO 69873 и предназначенный для установки в затяжной болт ЧПУ типа CNC (фото: Leitz GmbH & Co, Оберкохен).

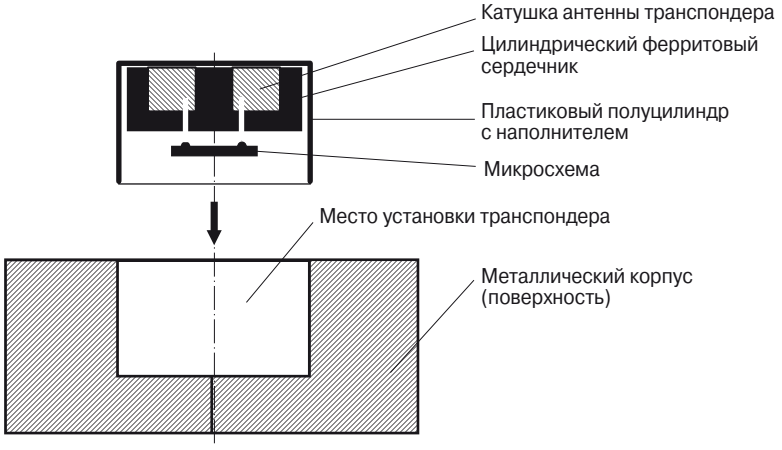


Рис. 2.8. Механическая конструкция транспондера, предназначенного для установки в металлический корпус. Катушка антенны транспондера наматывается на U-образный ферритовый сердечник, а затем помещается в пластиковый полуцилиндр. При установке открытая часть U-образного сердечника должна смотреть наружу.

2.2.5. Ключ или брелок

Транспондеры часто встраивают в механические ключи для дверей или шлагбаумов в тех системах, где важна высокая безопасность. Для этого чаще всего используют транспондеры в корпусе, который заливается пластиком или вводится в головку ключа.

Для доступа в офисные или рабочие помещения, кроме того, часто используют транспондеры, выполненные в виде брелков (**Рис. 2.9**).

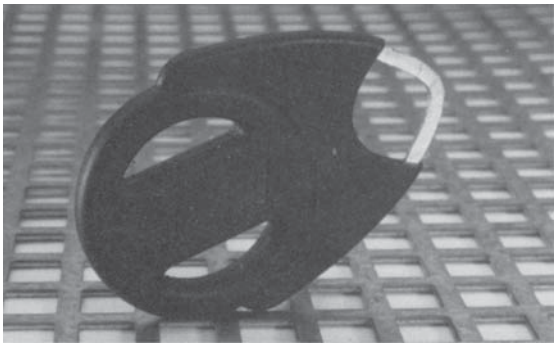


Рис. 2.9. Транспондер в виде брелка часто используется в системах доступа.

2.2.6. Часы

Такая конструкция (**Рис. 2.10**) была впервые применена в начале 90-х годов австрийской фирмой Ski-Data и поначалу использовалась в качестве пропуска на горнолыжные трассы. В течение некоторого времени подобные транспондеры получили широкое распространение, и прежде всего в системах контроля доступа. Внутри таких часов находится тонкая печатная плата, на поверхности которой расположены дорожки, образующие рамочную антенну с небольшим

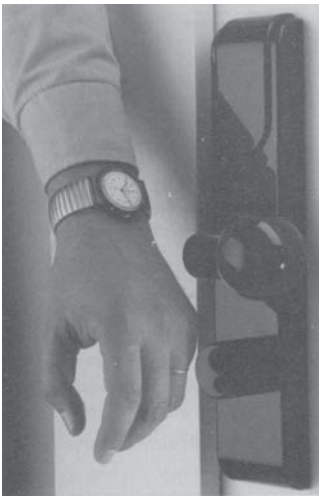


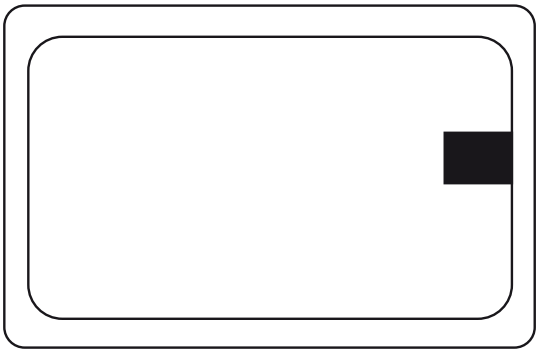
Рис. 2.10. Часы со встроенным транспондером используются как бесконтактное средство идентификации в системах контроля доступа (фото: Junghans Uhren GmbH, Шрамберг)

числом витков. Для того чтобы обеспечить наибольшую дальность действия, необходимо использовать антенну как можно большей площади, поэтому она занимает почти весь объем внутри корпуса часов.

2.2.7. Конструкция ID-1, бесконтактные чип-карты

Конструкция ID-1 (**Рис. 2.11**) хорошо знакома нам по кредитным и телефонным картам (85.72 × 54.03 × 0.76 мм ± допуск); эти небольшие пластиковые карточки находят все большее применение и как транспондеры в виде бесконтактных чип-карт. Преимущество такой формы для использования в RFID-системах с индуктивной связью заключается в большой площади катушки, благодаря чему данные транспондеры могут иметь большую дальность действия.

Бесконтактные чип-карты (**Рис. 2.12**) изготавливают ламинированием транспондера между четырьмя слоями ПВХ-пленки. Отдельные слои при высоком давлении и температуре свыше +100°C спекаются в единую конструкцию (подробно о технологиях производства бесконтактных чип-карт рассказывается в главе 12 «Производство транспондеров и бесконтактных чип-карт»).



Вид спереди

Рис. 2.11. Конструкция бесконтактной чип-карты: состоит из каркаса с модулем транспондера и антенной.

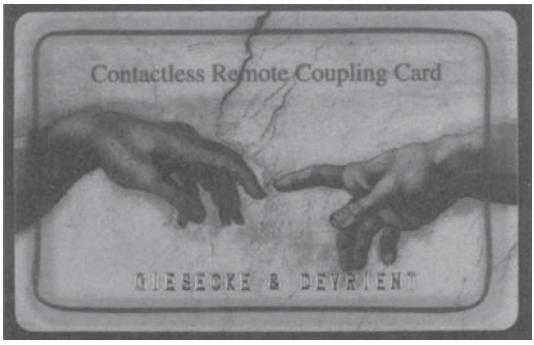


Рис. 2.12. Полупрозрачная бесконтактная чип-карта. Вдоль краев карты отчетливо видна антенна транспондера (фото: Giesecke & Devrient, Мюнхен).

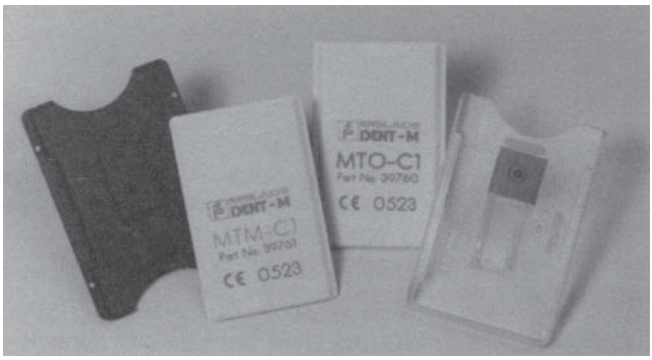


Рис. 2.13. Микроволновый транспондер в пластмассовом корпусе в виде полуцилиндра (фото: Pepperl & Fuchs, Маннхайм).

Бесконтактные чип-карты в формате ID-1 очень привлекательны для размещения рекламы, поэтому на них часто, как и на телефонных картах, можно увидеть красочные рекламные изображения.

Однако не всегда удается уложиться в толщину 0.8 мм, которая установлена согласно ISO 7819 для карт формата ID-1. В первую очередь большая толщина необходима микроволновым транспондерам (**Рис. 2.13**), так как такие транспондеры чаще всего располагаются между двумя оболочками из ПВХ или запрессовываются в корпус из ABS-пластика.

2.2.8. Этикетки (Smart Label)

Конструкция Smart Label (см. **Рис. 2.14** и **Рис. 2.15**) имеет толщину, приблизительно равную толщине листа бумаги. Здесь антенна транспондера изготавливается по технологии *трафаретной печати* или методом *травления* и может размещаться на пластиковом листе толщиной всего 0.1 мм. Далее этот лист пластика ламинируется слоем бумаги, а на обратной стороне наносится слой клея.

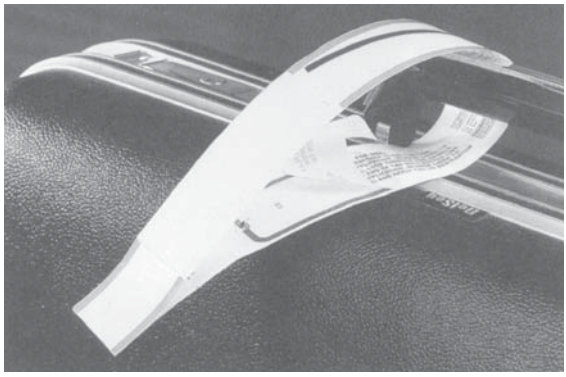


Рис. 2.14. Транспондер Smart Label является достаточно тонким и гибким, так как он должен наклеиваться как самоклеящаяся этикетка на багаж при авиаперевозках (фото: i-code Transponder, Philips Semiconductors, A-Gratcorn).

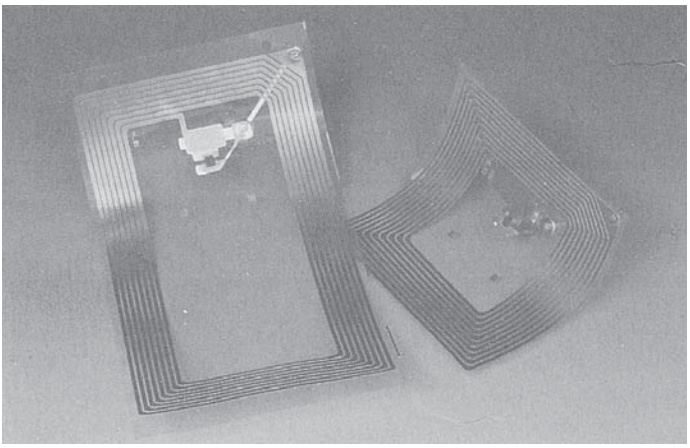


Рис. 2.15. Smart Label состоит из тонких листов пластика или бумаги, между которыми находится катушка и микросхема транспондера (фото: Tag-It Transponder, Texas Instruments, Фрайзинг).

В качестве упаковки для таких транспондеров используют рулон бумаги, после этого транспондер может применяться в качестве *самоклеящейся этикетки*, которая является достаточно тонкой и гибкой, чтобы наклеиваться на багаж, пакеты или другие предметы подобного рода самой различной формы. На поверхность этикетки легко наносится дополнительная графическая информация с помощью принтера, в том числе и штрих-код товара.

2.2.9. Антенна на кристалле

Во всех приведенных выше примерах схема транспондера содержит отдельную катушку, которая служит в качестве антенны транспондера, и микросхему (гибридная технология). Катушка транспондера соединяется с контактами микросхемы традиционно принятыми в электронике способами.

С целью дальнейшей миниатюризации транспондеров антенна транспондера была интегрирована в саму микросхему (coil-on-chip). Это стало возможно благодаря использованию специальных процессов микрогальванизации, которые широко применяются при производстве микросхем по КМОП-технологиям. Катушка в виде плоской спирали наносится на поверхность подложки полупроводниковой микросхемы, ее соединение с расположенным ниже кристаллом осуществляется через отверстия в пассивирующем слое [jurisch-95, jurisch-98]. Ширина проводников при этом составляет от 5 до 10 мкм, толщина — от 15 до 30 мкм. Для того чтобы обеспечить необходимую механическую прочность, затем проводится окончательная пассивация с помощью полиамида.

При использовании данной технологии размер кремниевой пластины и всего транспондера составляет приблизительно 3 × 3 мм. Для большего удобства транспондер часто заключается в пластмассовый корпус, и благодаря таким размерам (6 × 1.5 мм) транспондеры coil-on-chip являются самыми миниатюрными из всех современных типов RFID-транспондеров (см. **Рис. 2.16**).

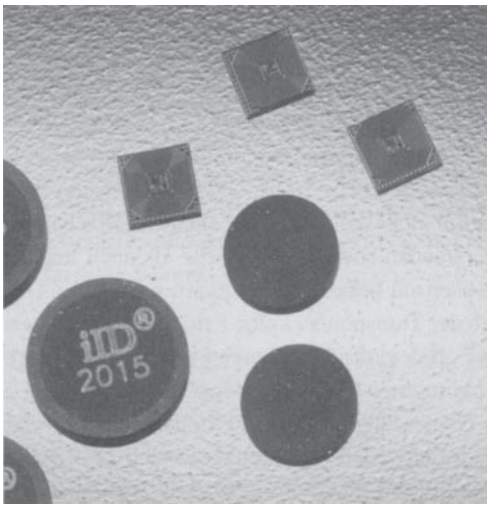


Рис. 2.16. Технология coil-on-chip (антенна на кристалле) позволяет создавать транспондеры самых миниатюрных размеров (фото: Micro Sensys, Эрфурт).

2.2.10. Другие конструкции

Кроме описанных выше наиболее распространенных конструкций транспондеров, для отдельных областей применения разработано и выпускается большое количество специальных конструкций. В качестве примера можно привести транспондеры Brieftaubentransponder (транспондер «Почтовый голубь») или Champion-Chip, которые специально предназначены для измерения времени в спортивных состязаниях. При необходимости транспондер можно изготовить в исполнении, которое максимально соответствует запросам клиента. Наиболее технологичными для подобных целей являются транспондеры в стеклянном или пластмассовом корпусе.

2.3. Рабочая частота, дальность действия и принцип взаимодействия

Важнейшими отличительными характеристиками для классификации RFID-систем являются рабочая частота считывающего устройства, способ физического взаимодействия и дальность действия системы. Системы радиочастотной идентификации могут работать в диапазоне от 135 кГц до 5.8 ГГц, то есть использовать диапазон от длинных волн до микроволн. По способу физического взаимодействия различают взаимодействие с помощью *электрического*, *магнитного* или *электромагнитного* поля. Следующий важнейший параметр — дальность действия — может изменяться от нескольких миллиметров до 15 м и более.

Системы радиочастотной идентификации с небольшой дальностью действия получили название Close-coupling; обычно их дальность действия составляет около 1 см. При этом транспондер для проведения идентификации либо помеща-

ется внутрь считывающего устройства, либо точно позиционируется на определенном месте на поверхности считывающего устройства. Взаимодействие в системах Close-coupling может осуществляться как с помощью электрического, так и с помощью магнитного поля. Теоретически такие устройства способны работать в диапазоне частот до 30 МГц, так как транспондеры подобного типа не зависят от мощности излучения. В таких системах можно передавать транспондеру достаточно большую энергию, что позволяет использовать не только микропроцессоры со сверхнизким потреблением, но и микропроцессоры общего назначения. Системы Close-coupling главным образом используются там, где очень высоки требования к безопасности и где не требуется большая дальность действия. Например, это могут быть системы допуска в помещения или бесконтактные чип-карты для электронных платежей. Сегодня для таких систем почти всегда используются бесконтактные чип-карты в формате ID-1 (ISO 10536), однако пока системы Close-coupling не смогли завоевать заметной доли на рынке.

Для RFID-систем с дальностью чтения и записи данных до 1 м используется название *Remote-coupling*. Подавляющее большинство подобных систем используют *индуктивное* (*магнитное*) взаимодействие, поэтому их также иногда называют *индуктивными радиоустройствами*. Однако существует и небольшое количество систем с *емкостным* (*электрическим*) взаимодействием [bistatix]. Сегодня почти 90% всех коммерческих систем радиочастотной идентификации относятся к системам с индуктивным взаимодействием, и на рынке присутствуют самые разнообразные решения для такого рода систем. Для наиболее распространенных областей применения, таких как бесконтактные чип-карты, системы идентификации домашних животных или промышленная автоматизация, уже разработан ряд нормативов, которые стандартизируют технические параметры транспондера и считывающего устройства. К их числу относятся стандарты на системы Proximity-coupling (ISO 11443, бесконтактные чип-карты) и Vicinity-coupling (ISO 15693, этикетки Smart Label и бесконтактные чип-карты). В качестве рабочих частот здесь используются частоты ниже 135 кГц или же диапазон 13.56 МГц, для некоторых специальных приложений (см. подраздел 13.5.1 «Система Eurobalise S21») также используется частота 27.125 МГц.

Системы радиочастотной идентификации, дальность действия которых значительно превышает 1 м, получили название Long-range. Все подобные системы работают в микроволновом диапазоне или же в диапазоне СВЧ (UHF). Подавляющее большинство таких систем используют принцип обратного рассеяния (backscatter). Кроме того, в диапазоне микроволнового излучения также находят применение транспондеры на поверхностных акустических волнах. Все указанные системы в диапазоне UHF используют частоты 868 МГц (Европа) и 915 МГц (США), а в микроволновом диапазоне — 2.5 ГГц и 5 8 ГГц. В таких системах пассивные транспондеры (которые не имеют собственного источника питания) сегодня могут обеспечивать дальность действия до 3 м[1)], а активные отражательные (backscatter) транспондеры (которые имеют встроенную батарейку) — до 15 м и даже более. При этом собственный источник питания активного транспондера не используется для передачи данных, он только обепечивает питание микро-

[1)] Сейчас известны системы с дальностью действия до 7...10 м. — *Примеч. ред.*

схемы и гарантирует сохранение данных. Для передачи данных между транспондером и считывающим устройством используется энергия электромагнитного излучения, передаваемого считывающим устройством.

Для того чтобы избежать путаницы в классификации систем RFID, в дальнейшем, говоря о физических свойствах таких систем, мы будем использовать только понятия «системы с индуктивным или емкостным типом взаимодействия» и «микроволновые или отражательные системы».

2.4. Обработка данных транспондером

Если попытаться классифицировать имеющиеся на сегодня RFID-системы по возможностям транспондеров в части обработки информации, а также по объему памяти транспондера, то мы получим широкий спектр различных вариантов, среди которых будут как простые (Low-end), так и сложные (High-end) системы (см. **Рис. 2.17**).

К *простым системам* относятся системы EAS (Elektronische Artikelsicherings Systeme — электронные системы предупреждения краж товаров, см. раздел 3.1 «Однобитные транспондеры»). Транспондеры этого типа используют в своей работе законы физики и способны лишь сообщать о своем нахождении в зоне действия считывающего устройства системы обнаружения.

К этому же классу относятся *транспондеры Read-only*, которые хотя и оснащены полупроводниковой микросхемой, но все-таки относятся к простым системам. Дело в том, что такой транспондер может хранить только строго фиксированный на+бор данных; обычно это несколько байтов, которые несут информацию об *уникальном серийном номере* (unique number) транспондера. Когда транспондер подобного типа попадает в область действия считывающего устройства, он начинает передавать собственный серийный номер, причем передача данных всегда осуществляется в одном направлении — от транспондера к считывающему устройству.

При практическом применении таких систем необходимо понимать, что в поле действия считывающего устройства одновременно не могут находиться несколько транспондеров, поскольку это приводит к коллизии при передаче данных, и считывающее устройство не сможет корректно обработать поступающую информацию. Однако, несмотря на подобные ограничения, транспондеры Read-only отлично подходят для многих применений, к тому же благодаря своей ограниченной функциональности такие транспондеры просты в изготовлении, что обеспечивает малое энергопотребление и низкую стоимость производства.

Системы Read-only могут работать во всех диапазонах частот, предназначенных для систем радиочастотной идентификации. Благодаря небольшому энергопотреблению микросхемы транспондера и малому объему передаваемых данных дальность действия таких систем, как правило, весьма велика. Системы Read-only находят применение там, где не требуется передавать большие объемы данных или где просто требуется заменить традиционные системы штрихового кодирования, — это управление потоками товаров, идентификация палет, контейнеров, газовых баллонов (ISO 18000), а также идентификация домашних животных (ISO 11785).

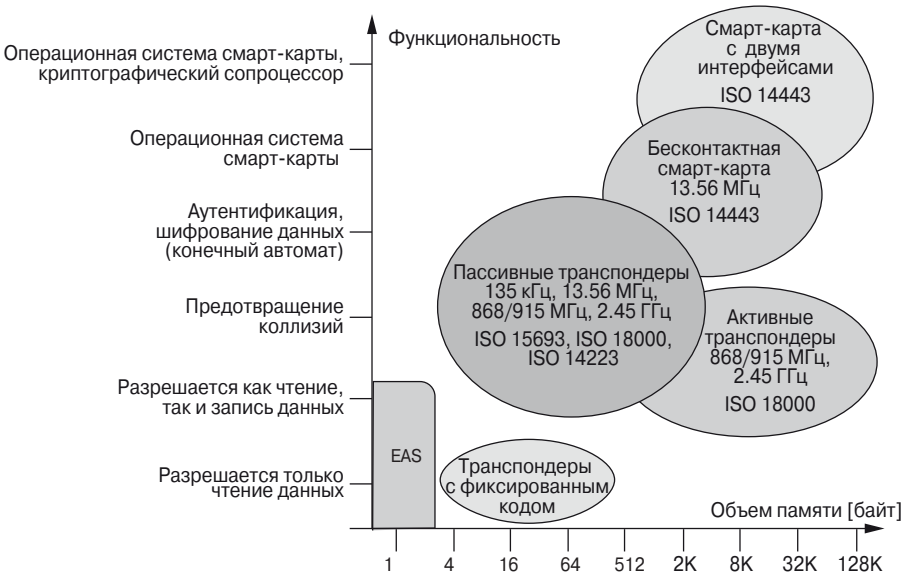


Рис. 2.17. Системы RFID различаются по своей функциональности: можно выделить системы простые (Low-end) и сложные (High-end).

К устройствам среднего уровня в такой классификации относятся те системы, которые позволяют записывать данные в память транспондера, и этот сегмент отличается наибольшим разнообразием используемых систем. Емкость памяти может изменяться от нескольких байтов до более чем 100 Кбайт памяти типа EEPROM (пассивные транспондеры) или SRAM (для транспондеров с собственной батарейкой, то есть для активных транспондеров). Такие транспондеры имеют встроенную схему, которая декодирует достаточно простые команды, полученные от считывающего устройства, и управляет как процессом передачи данных, так и процессом записи данных в собственную память. Как правило, подобные транспондеры реализуют определенный механизм *предотвращения коллизий* (антиколлизий, от англ. anticollision); благодаря этому несколько транспондеров, одновременно находящихся вблизи считывающего устройства, уже не создают взаимных помех и могут выборочно опрашиваться считывающим устройством (см. раздел 7.2 «Методы множественного доступа — предупреждение коллизий»).

В этих системах часто применяются и криптографические методы — процедура *аутентификации* между транспондером и считывающим устройством, а также шифрование при передаче данных (см. главу 8 «Безопасность данных»). Подобные системы могут использовать любую частоту из диапазона, доступного для систем радиочастотной идентификации.

Сегмент сложных систем (High-end) занимают бесконтактные чип-карты с микропроцессором и чип-карты с собственной операционной системой (smart-card OS). Использование микропроцессоров позволяет реализовать достаточно сложные алгоритмы аутентификации и шифрования передаваемых данных, которые нельзя реализовать с помощью фиксированной схемы на жесткой логике.

К числу наиболее функциональных устройств в сегменте High-end относятся современные чип-карты с двумя интерфейсами (см. подраздел 10.2.1 «Карты с двумя интерфейсами»), которые обладают встроенным криптографическим *сопроцессором*. Применение такого сопроцессора значительно сокращает время, необходимое для кодирования данных, что позволяет использовать бесконтактные чип-карты в тех приложениях, где важна высокая надежность шифрования при передаче данных, например в электронных системах биржевой торговли или же в системах оплаты проезда (ticketing) на пассажирском транспорте.

Подавляющее большинство систем класса High-end использует частоту 13.56 МГц, а протокол передачи данных между транспондером и считывающим устройством соответствует стандарту ISO 14443.

2.5. Критерии, которыми следует руководствоваться при выборе RFID-системы

В последнее время системы радиочастотной идентификации быстро развиваются, одним из свидетельств этого является расширение использования бесконтактных чип-карт в качестве электронных билетов для общественного пассажирского транспорта. Хотя 5 лет назад подобное было трудно себе даже представить, сегодня по всему миру уже используются миллионы таких бесконтактных билетов. Также быстро расширялось и применение бесконтактных систем идентификации.

Разработчики RFID-систем лучше всех почувствовали оживление рынка, и сегодня на рынке предлагаются самые разнообразные системы, технические характеристики которых оптимизированы для самых различных областей применения — *электронные проездные билеты*, *идентификация домашних животных*, *промышленная автоматика*, системы контроля доступа. Все эти системы могут перекрываться между собой по своим техническим характеристикам, что затрудняет их классификацию и выбор наиболее подходящей RFID-системы. Ситуация осложняется еще и тем, что, за исключением небольшого количества применений (идентификация домашних животных и чип-карты Close-coupling), стандарты для используемых RFID-систем пока не разработаны.

Составить четкую картину всех предлагаемых на сегодняшний день систем радиочастотной идентификации достаточно сложно даже для специалиста в данной области. Поэтому можно представить, с какими трудностями вы столкнетесь при выборе RFID-системы, соответствующей вашим требованиям.

Дадим краткие рекомендации, какими критериями следует руководствоваться при выборе системы радиочастотной идентификации.

2.5.1. Рабочая частота

Системы радиочастотной идентификации с рабочей частотой от 30 кГц до приблизительно 30 МГц относятся к системам с индуктивной связью. В отличие от них микроволновые системы, работающие в диапазоне 2.45 ГГц или 5.5 ГГц, используют для взаимодействия электромагнитное поле.

При частоте 100 кГц *коэффициент поглощения* водой или непроводящими веществами приблизительно в 100 000 раз ниже, чем на частоте 1 ГГц. Можно сказать, что на низких радиочастотах поглощение или затухание сигнала практически незаметно, поэтому такие системы используются в основном там, где необходимо значительное проникновение в глубь объекта [schyrmann-94]. В качестве примера можно привести болюс (от англ. bolus — таблетка, капсула), который внутри содержит транспондер и помещается в преджелудок (рубец) крупного рогатого скота. Для чтения данных с транспондера здесь используется частота ниже 135 кГц.

По сравнению с системами с индуктивной связью микроволновые системы имеют значительно бóльшую дальность действия — обычно от 2 до 15 м. Однако в отличие от устройств с индуктивной связью микроволновым системам необходим дополнительный автономный источник питания. Обычно мощности, получаемой от считывающего устройства, недостаточно для нормальной работы транспондера.

Еще одним важным качеством является устойчивость к электромагнитным помехам, которые возникают при сварке или создаются мощными электродвигателями. Индуктивные транспондеры здесь существенно проигрывают микроволновым системам. Например, именно микроволновые системы господствуют на производственных линиях и лакировальных установках в автомобильной промышленности. Этому также способствует большой объем памяти (до 32 Кбайт) и способность работать при высоких температурах (до +250°C) [Bachthaler].

2.5.2. Дальность действия

Дальность действия, которая необходима для конкретного приложения, определяется несколькими факторами:

- Точность позиционирования транспондера.
- Минимальное расстояние между транспондерами при их практическом применении.
- Скорость, с которой транспондер перемещается в поле действия считывающего устройства.

Рассмотрим в качестве примера систему оплаты проезда в общественном пассажирском транспорте. Здесь скорость позиционирования достаточно мала — транспондер перемещается к считывающему устройству рукой человека. Минимальное допустимое расстояние между транспондерами соответствует расстоянию между двумя пассажирами, которые стоят в очереди на посадку в автобус. Оптимальная дальность действия системы в таком случае составляет 5...10 см, бóльшая дальность привела бы только к дополнительным сложностям, так как в зоне действия считывающего устройства одновременно могло бы находиться большее количество транспондеров. В этом случае сложнее было бы установить однозначное соответствие между билетом и пассажиром.

На сборочной линии автомобильного предприятия часто одновременно могут находиться разные модели автомобилей с совершенно различными габаритами. Поэтому трудно определить, каково будет расстояние между расположенным в автомобиле транспондером и считывающим устройством [Bachthalter]. В этом

случае при выборе дальности чтения/записи RFID-системы необходимо учитывать максимально возможное расстояние. При определении расстояния между транспондерами следует исходить из того, что в поле действия считывающего устройства всегда должен находиться только один транспондер. Здесь микроволновые системы благодаря *направленности диаграммы излучения* имеют заметное преимущество перед ненаправленным, изотропным излучением систем с индуктивной связью (**Рис. 2.18**).

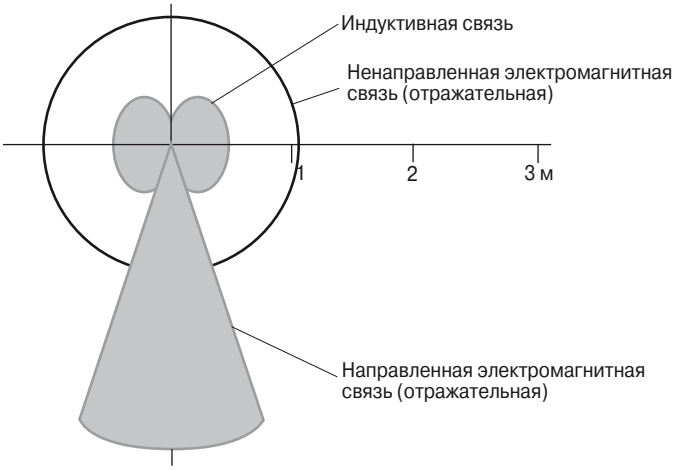


Рис. 2.18. Сравнение рабочих областей для различных систем радиочастотной идентификации.

Скорость перемещения транспондера относительно считывающего устройства (вместе с максимальной дальностью, на которой возможно чтение/запись данных с транспондера) определяет длительность пребывания транспондера в области действия считывающего устройства. Например, если стоит задача идентификации проезжающих мимо считывающего устройства автомобилей, то при максимальной скорости движения автомобиля дальность действия RFID-системы должна быть такой, чтобы времени, в течение которого автомобиль находится в зоне действия системы, было достаточно для передачи всех необходимых данных.

2.5.3. Требования к безопасности данных

Необходимо быть очень внимательным при определении требований к безопасности данных в RFID-системе, включая аутентификацию и шифрование данных, иначе вы можете столкнуться с неожиданностями на стадии реализации системы. Для этого необходимо сначала определить, какой интерес система представляет для потенциального взломщика, то есть какую выгоду он может получить от несанкционированного доступа к деньгам или другим ценным ресурсам. С этой точки зрения мы будем подразделять все приложения на две группы:

- Первая — промышленные или закрытые приложения.
- Вторая — открытые, публичные системы с возможностью доступа к денежным средствам и другим ценным ресурсам.

Приведем два примера подобных систем.

Типичный пример системы первого типа (промышленная или закрытая) — сборочная линия на автомобильном заводе. В этом случае доступ к RFID-системе имеет ограниченное число сотрудников компании и возможен полный контроль над личностями потенциальных взломщиков. Однако злонамеренное изменение или фальсификация хранящихся в транспондере данных может вызвать значительные убытки и нарушить обычный ритм работы предприятия, даже если злоумышленник и не получит при этом никакой личной выгоды. Вероятность такого вмешательства в работу RFID-системы невелика, и поэтому можно использовать недорогие системы класса Low-end без какой-либо поддержки функций безопасности данных.

В качестве второго примера рассмотрим систему электронных билетов для общественного пассажирского транспорта. В этой системе носитель данных в виде бесконтактной чип-карты может быть приобретен практически каждым, так что круг потенциальных злоумышленников заранее определить просто невозможно. Успешный взлом системы идентификации может нанести транспортной компании значительный ущерб, ведь злоумышленники могут организовать продажу поддельных билетов. Кроме прямых финансовых потерь, это может ухудшить и имидж компании. Для таких приложений необходимо использовать транспондеры сегмента High-end, которые поддерживают аутентификацию и шифрование передаваемых данных. Для приложений с наивысшими требованиями к безопасности информации, таких как банковские приложения или электронные платежные средства, необходимо использовать только транспондеры со встроенными микропроцессорами.

2.5.4. Объем памяти

Основной характеристикой электронной начинки транспондера является *объем памяти*, используемой для хранения данных. В приложениях, где важна низкая стоимость системы, применяются транспондеры Read-only, которые не позволяют изменять записанную в них информацию, — здесь вы можете только идентифицировать объект, все остальные данные могут быть получены, например, из центральной базы данных, где хранится подробная информация об объекте. Если же требуется записывать данные на транспондер в процессе работы системы, то вам необходим транспондер с памятью типа EEPROM или RAM.

Память типа EEPROM чаще применяется в системах с индуктивной связью, обычно такая память имеет объем от 16 байт до 8 Кбайт[1)].

Для использования памяти SRAM необходимо постоянно обеспечивать питание для микросхемы памяти, иначе данные будут утеряны. Такая память применяется в микроволновых системах, ее объем обычно составляет от 256 байт до 64 Кбайт.

[1)] Сегодня уже есть чип-карты с емкостью EEPROM более 64 Кбайт. — *Примеч. ред.*

ГЛАВА 3

ОСНОВНЫЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ

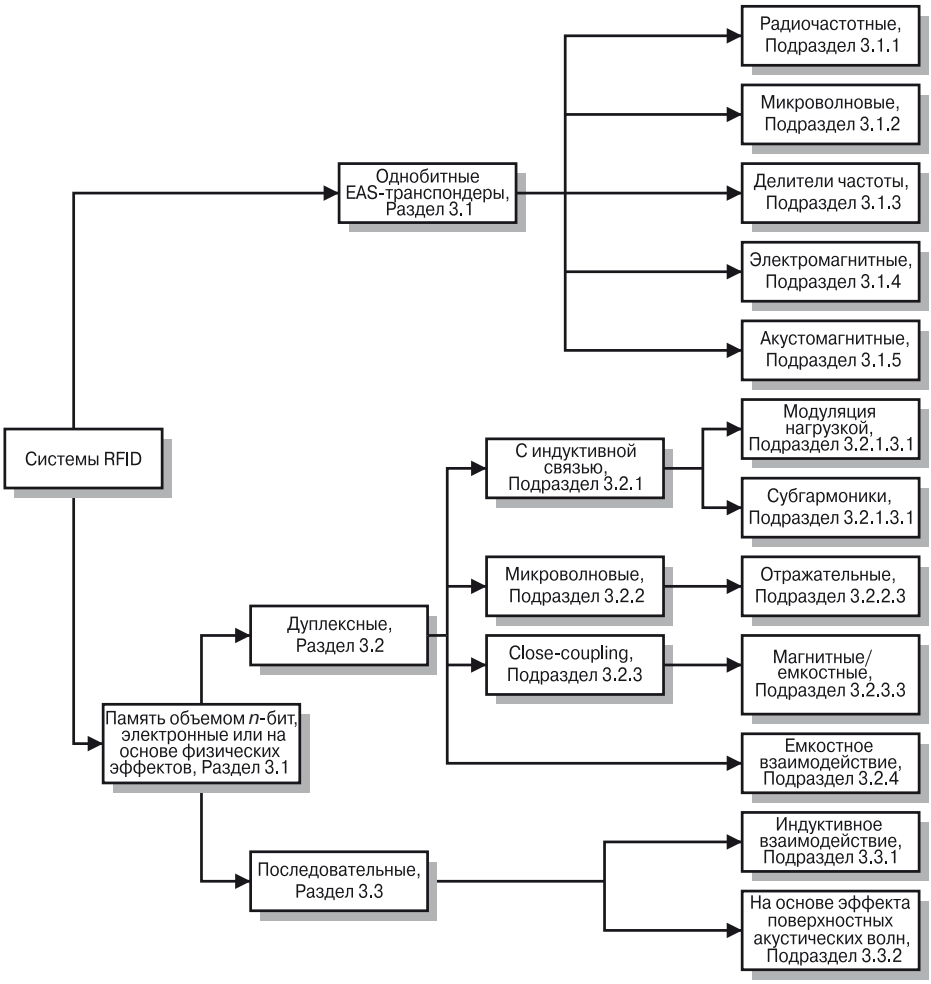


Рис. 3.1. Классификация систем радиочастотной идентификации по принципу функционирования с указанием соответствующих разделов книги.

В данной главе речь идет об основных принципах взаимодействия транспондера и считывающего устройства, включая способ передачи энергии и способ передачи данных между транспондером и считывающим устройством (см. **Рис. 3.1**). Физические принципы систем радиочастотной идентификации, а также математические модели RFID-систем с индуктивной связью и систем типа backscatter будут обсуждаться в главе 4 «Физические основы RFID-систем».

3.1. Однобитные транспондеры

Основной единицей представления информации является один бит, и он может принимать только два значения: 0 или 1. В применении к системам RFID, в которых используются так называемые *однобитные транспондеры* (1-bit transponder), это означает, что возможны только два состояния: «транспондер находится в зоне действия системы» или «транспондер находится за пределами зоны действия системы». Несмотря на это, подобные транспондеры нашли чрезвычайно широкое применение — в основном в системах защиты от краж (EAS).

Такая система слежения за товарами состоит из следующих компонентов: антенна считывающего устройства или детектора, элемент обеспечения безопасности или специальная этикетка, возможно также использование специального *деактиватора*, который прекращает работу транспондера после оплаты товара. В современных системах деактивация транспондера производится при регистрации кода оплаты в кассе магазина, некоторые системы также имеют в своем составе и *активатор*, благодаря которому транспондер может быть активирован вновь [gillert]. Основной характеристикой подобных систем является *коэффициент обнаружения* транспондеров в зависимости от расстояния до считывающего устройства (обычно рассматривается при максимально допустимом расстоянии между транспондером и антенной детектора).

Методика приемки и проверки установленных систем безопасности такого типа описывается в стандарте VDI 4470 «Системы контроля товаров — Рекомендации приемки клиентом шлюзовых систем». В этом документе содержатся все определения и методы испытаний, которые позволяют определить скорость детектирования и выявить причины возникновения ложной тревоги. Эти нормативы могут использоваться предприятиями розничной торговли в качестве основы для заключения договора с поставщиком или же при проверке возможностей установленной системы. Для производителей подобных систем контроля эти документы могут служить руководством и инструментом контроля при разработке и оптимизации интегрированных решений в области систем безопасности [согласно VDI 4470].

3.1.1. Используемая радиочастота

Радиочастотные устройства используют в качестве чувствительного элемента колебательный *LC*-контур, который настроен на резонансную частоту f_R. Ранее для этого использовались катушка индуктивности из лакированного медного провода и припаянный к ней конденсатор в пластмассовом корпусе (*жесткая*

этикетка). Сегодня все чаще используются наклеиваемые ярлыки, в которых катушка наносится на металлическую фольгу. Для того чтобы уменьшить затухание и обеспечить высокую добротность колебательного контура, толщина алюминиевых проводящих дорожек, проложенных по прочной *полиэтиленовой пленке* толщиной 25 мкм, должна составлять не менее 50 мкм [jorn]. Для изготовления пластин конденсатора используется фольгированная пленка толщиной 20 мкм.

Считывающее устройство (детектор) излучает переменное магнитное поле с частотой в диапазоне от 1 до 15 МГц (см. **Рис. 3.2**). Когда колебательный *LC*-контур оказывается под воздействием электромагнитного поля, в катушке индуктивности, согласно закону взаимной индукции, возникает ток с частотой, равной частоте магнитного поля. Если частота колебаний внешнего переменного магнитного поля f_G равна резонансной частоте колебательного контура, то в *LC*-контуре возникают резонансные колебания.

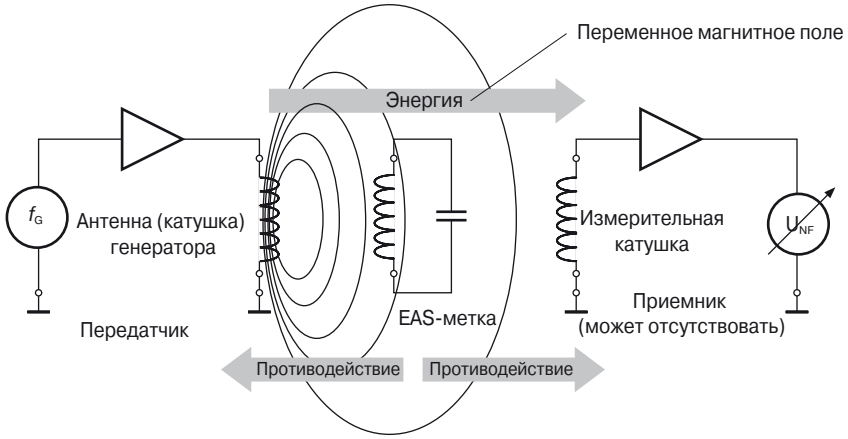


Рис. 3.2. Принцип действия радиочастотного EAS-транспондера.

Возникающий в колебательном контуре ток пытается противодействовать вызвавшей его причине, то есть пытается уменьшить внешнее переменное магнитное поле (см. подраздел 4.1.10.1 «Трансформированный импеданс транспондера Z'_T»). Это приводит к небольшому падению напряжения на антенне передатчика и, соответственно, к снижению измеренной интенсивности магнитного поля. Данный эффект можно заметить по падению индуцированного напряжения в специальной измерительной катушке, таким образом можно отследить появление резонансного контура в магнитном поле детектора.

Относительная величина такого изменения зависит от расстояния между двумя катушками (расстояние между катушкой генератора и катушкой транспондера, расстояние между катушкой транспондера и измерительной катушкой), а также от добротности Q возбуждаемого внешним полем резонансного контура, который располагается в транспондере.

Обычно относительное изменение напряжения на катушке генератора, которая служит антенной, очень мало́ и его очень трудно измерить. Однако для надежного распознавания транспондера желательно получить как можно более отчетли-

вый сигнал. Для этого применяют определенное ухищрение: частота переменного магнитного поля не является постоянной, она «плавает». Генерируемая частота изменяется в диапазоне между двумя граничными частотами (см. **Рис. 3.3**), часто для таких систем используется диапазон частот 8.2 МГц ±10% [jorn].

В тот момент, когда такая плавающая частота совпадает с резонансной частотой колебательного контура транспондера, возникает резонанс, который приводит к заметному падению напряжения как на катушке генератора, так и на измерительной катушке. Преимуществом данного метода является и то, что нет необходимости точно настраивать резонансную частоту колебательного контура транспондера, достаточно теперь лишь обеспечить, чтобы она попадала в сканируемый диапазон частот.

Так как после оплаты товара в кассе этикетка обычно не удаляется, то необходимо дать ей команду, что она больше не должна отвечать на запросы детектора. Кассир просто подносит купленные товары к специальному устройству — деактиватору, который создает достаточно сильное магнитное поле, приводящее к разрушению пленочного конденсатора транспондера. Для этого в конденсаторах намеренно создаются области, в которых может возникнуть короткое замыкание — так называемые dimples (места с меньшим расстоянием между обкладками конденсатора, в которых происходит пробой конденсатора и, как следствие, короткое замыкание). После подобного пробоя конденсатор уже невозможно восстановить. Это приводит к смещению резонансной частоты контура и как результат — к отсутствию реакции транспондера на воздействие внешнего электромагнитного поля.

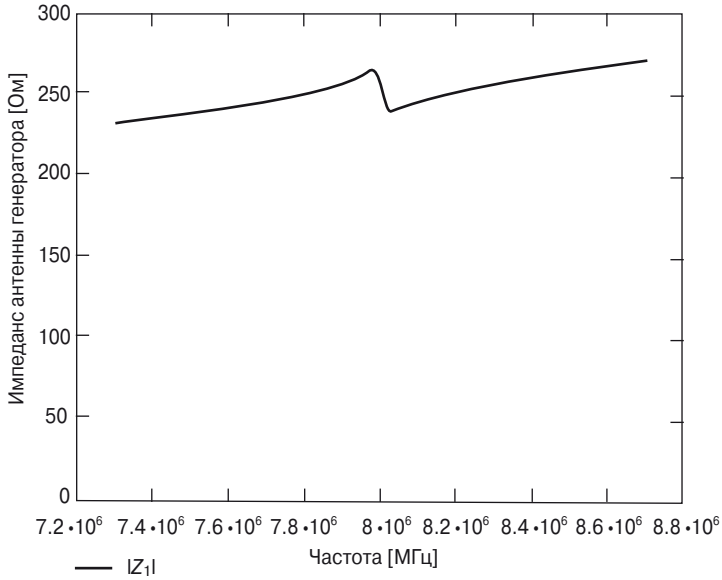


Рис. 3.3. Изменение импеданса антенны (катушки) генератора на резонансной частоте антенны транспондера ($Q = 90$, $k = 1\%$). Частота f_G излучаемого антенной генератора переменного магнитного поля непрерывно изменяется в диапазоне между двумя граничными частотами. Радиочастотная этикетка имеет резонансную частоту f_R, и на этой частоте отчетливо заметно изменение импеданса.

Для создания переменного магнитного поля достаточной интенсивности в зоне действия системы безопасности, обычно используются *рамочные антенны* большой площади. Эти рамочные антенны встраиваются в колонны шлюзовой системы на входе в помещение. Классическая конструкция, знакомая нам по любому крупному супермаркету, представлена на **Рис. 3.4**. Использование радиочастотного метода позволяет создавать ворота шириной до 2 м. Однако доля обнаруживаемых предметов относительно невысока и составляет 70% [gillert]. Это объясняется достаточно сильным влиянием определенных материалов. В первую очередь к таким материалам относятся металлы (например, консервные банки), которые оказывают влияние на резонансную частоту этикеток, а также на степень взаимодействия с катушкой детектора, что уменьшает вероятность обнаружения товара. Для того чтобы при указанной ширине прохода добиться нужной вероятности обнаружения, необходимо использовать этикетки размером 50 × 50 мм.

Рис. 3.4. Слева — типичная рамочная антенна для RF-систем (высота 1.20...1.60 м); справа — различные типы этикеток.

Другой важной особенностью, которую необходимо учитывать при проектировании радиочастотных систем, являются свойства различных товаров (например, катушки с кабелем), которые могут иметь резонансную частоту в пределах частоты сканирования 8.2 МГц ±10%, что может вызывать ложное срабатывание системы безопасности.

Типичные характеристики RF-систем приведены в **Табл. 3.1**, а частотные диапазоны, в которых работают различные RF-системы сигнализации, — в **Табл. 3.2**.

Таблица 3.1. **Типичные характеристики RF-систем [VDI 4471]**

Параметр	Значение
Коэффициент добротности, Q, средства защиты	> 60...80
Минимальная напряженность магнитного поля, H_D, необходимая для деактивирования транспондера	1.5 А/м
Максимальная напряженность поля области детектирования	0.9 А/м

Таблица 3.2. **Частотные диапазоны, которые используются различными радиочастотными системами сигнализации [plotzke]**

	Система 1	**Система 2**	**Система 3**	**Система 4**
Частота, МГц	1.6...2.18	7.44...8.73	7.30...8.70	7.40...8.60
Частота, с которой изменяется рабочая частота системы, Гц	141	141	85	85

3.1.2. Микроволновые системы

В EAS-системах, работающих в диапазоне микроволнового излучения, используется свойство компонентов с нелинейной характеристикой (например, диодов) создавать в процессе своей работы *гармоники*. Под гармоникой синусоидального напряжения A с заданной частотой f_A мы понимаем синусоидальное напряжение B, у которого частота f_B получается умножением частоты f_A на произвольное целое число. Таким образом, гармониками для частоты f_A являются частоты $2f_A$, $3f_A$, $4f_A$ и т.д. Сигнал, частота которого получается умножением исходной частоты на N, в радиотехнике носит название N-й гармоники (N-й гармонической составляющей), при этом сама исходная частота является основной волной или первой гармоникой.

Каждый нелинейный элемент создает гармоники основной частоты, однако такие нелинейные элементы потребляют энергию, и лишь небольшая часть этой энергии преобразуется в энергию колебания гармоник. При благоприятных условиях увеличение частоты с f до $n \times f$ осуществляется с коэффициентом полезного действия $\eta = 1/n^2$. Однако если для умножения частоты используется нелинейный накопитель энергии, то в идеальном случае преобразование может осуществляться без потерь [flackner].

Для преобразования частоты в качестве нелинейного накопителя энергии оптимальными компонентами являются *варикапы* (параметрические диоды). Число и амплитуда возникающих гармоник определяются *профилем распределения легирующей примеси* и соответственно крутизной характеристики варикапа. Мерой крутизны (характеристическая кривая зависимости емкость — напряжение) является показатель экспоненты n (или также γ), который для простых диффузионных диодов равен 0.33 (например, для BA110), для легированных диодов — 0.5 и для варикапов — около 0.75 (например, BB141) [itt75].

Легированные варикапы имеют квадратичную зависимость емкость — напряжение и используются для удвоения исходной частоты. С помощью диффузионных варикапов можно получить гармоники более высокого порядка [fleckner].

Конструкция 1-битных транспондеров, которые используют гармоники основной частоты, чрезвычайно проста: варикап включается в цепь антенны-диполя, настроенной на частоту поля, излучаемого считывающим устройством (**Рис. 3.5**). Например, если основная частота равна 2.45 ГГц, то длина диполя должна составлять 6 см. Для основной частоты используются значения 915 МГц (вне пределов Европы), 2.45 ГГц и 5.6 ГГц. Когда транспондер попадает в зону действия излучения антенны, через диод начинает протекать ток. В результате образуются гармоники высокой частоты, которые излучаются в пространство; особенно заметным

является излучение с частотой в 2 или 3 раза выше основной частоты, его можно получить с помощью варикапа подходящего типа.

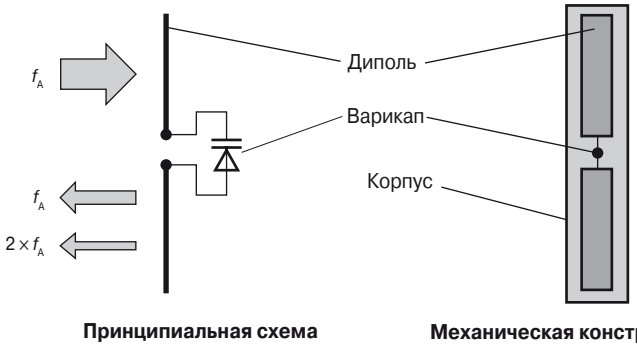


Рис. 3.5. Принципиальная схема и типичная конструкция микроволновых этикеток.

Транспондеры данного типа помещаются в пластмассовый корпус (жесткие этикетки) и используются в основном для защиты текстильных товаров, после прохождения кассы эти транспондеры удаляются и могут использоваться вновь.

На **Рис. 3.6** показан такой транспондер, который попадает в зону действия микроволнового передатчика, работающего на частоте 2.45 ГГц. Благодаря диоду возникает и излучается вторая гармоника с частотой 4.90 ГГц, которая обнаруживается приемником, настроенным именно на эту частоту. Возникновение сигнала на данной частоте рассматривается как повод для подачи сигнала тревоги.

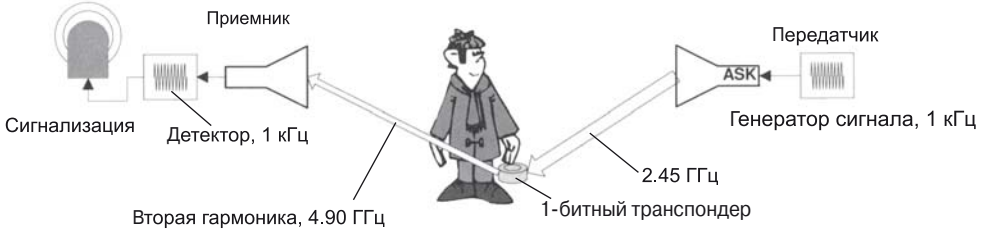


Рис. 3.6. Микроволновая этикетка-транспондер в зоне действия детектора.

Если основная частота модулируется по амплитуде или частоте (ASK- или FSK-модуляция), то эта модуляция будет присутствовать и во всех созданных транспондером гармониках. Данное свойство может использоваться для выделения «полезного» сигнала на фоне помех, что позволяет исключить случайное возникновение сигнала тревоги. В приведенном выше примере мы можем модулировать амплитуду генерируемого высокочастотного излучения сигналом с частотой 1 кГц (100%-ная ASK-модуляция). Это приводит к тому, что излучаемая транспондером вторая гармоника также будет модулирована сигналом ASK с частотой 1 кГц. В приемнике считывающего устройства излучение на частоте второй гармоники демодулируется, и мы получаем сигнал с частотой 1 кГц. Благодаря этому мы можем распознать случайные сигналы на частоте 4.90 ГГц, так как они, как правило, не содержат сигнал с подобной модуляцией.

3.1.3. Делитель частоты

Данная технология используется в диапазоне длинных волн на частотах 100...135.5 кГц. В этом случае (см. **Рис. 3.7**) транспондер состоит из полупроводниковой микросхемы и колебательного контура, который представляет собой катушку из лакированного медного провода, намотанного на сердечник. С помощью конденсатора добиваются, чтобы резонансная частота контура совпадала с рабочей частотой EAS-системы. Такие транспондеры изготавливаются в пластмассовом корпусе и после оформления покупки удаляются с отслеживаемого товара.

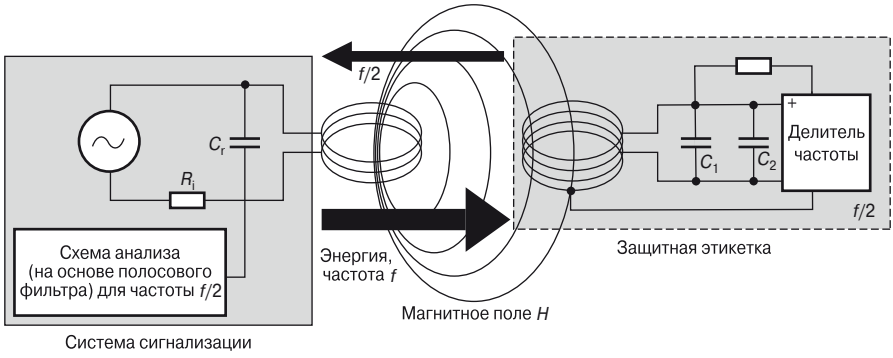


Рис. 3.7. Транспондер, работающий по принципу деления частоты: справа — транспондер (защитная этикетка), слева — детектор (считывающее устройство).

Микросхема транспондера получает питание от магнитного поля, излучаемого детектором (см. подраздел 3.2.1.1 «Передача энергии пассивному транспондеру»). Полученная от колебательного контура частота делится на два с помощью микросхемы транспондера. Затем полученный сигнал, частота которого вдвое меньше, чем рабочая, передается через отвод в катушке в колебательный контур.

Для того чтобы повысить вероятность обнаружения транспондера, магнитное поле модулируется низкочастотным сигналом (ASK-модуляция), при этом низкочастотный сигнал, подобно приведенному выше способу с использованием гармоник, сохраняется и в излучаемом транспондером сигнале с частотой *f*/2. Это помогает отличить помехи от «полезного» сигнала и позволяет почти полностью исключить вероятность возникновения ложного срабатывания.

В качестве антенн детекторов в таких системах используются рамочные антенны, которые мы уже обсуждали выше в разделе, посвященном RF-системам.

Типичные параметры рассматриваемой системы приведены в **Табл. 3.3**.

Таблица 3.3. **Типичные параметры системы с делением частоты [plotzke]**

Параметр	Значение
Частота	130 кГц
Тип модуляции	100% ASK
Частота модуляции/сигнал модуляции	12.5 или 25 Гц, прямоугольный сигнал, скважность 50%

3.1.4. Системы электромагнитного типа

Системы электромагнитного типа используют сильное магнитное поле в диапазоне низких частот — от 10 Гц до 20 кГц. Транспондер содержит металлические полоски из магнитомягкого аморфного металла, у которого кривая гистерезиса имеет достаточно крутой наклон (см. подраздел 4.1.12). В сильном переменном магнитном поле эти металлические полоски намагничиваются и переходят в состояние магнитного насыщения. Благодаря сильной нелинейной зависимости плотности магнитной индукции B от напряженности внешнего магнитного поля H вблизи точки насыщения (см. **Рис. 4.50**), а также скачкообразному изменению B вблизи перехода напряженности внешнего магнитного поля через 0 возникают гармоники основной частоты переменного внешнего магнитного поля, которые принимаются детектором и свидетельствуют о присутствии транспондера.

Дальнейшая оптимизация электромагнитного способа заключается в том, что к основному сигналу добавляются гармоники с более высокой частотой. Благодаря высокой нелинейности кривой гистерезиса для металлических полосок возникают дополнительные гармоники с частотой, равной сумме и разности частот входящих сигналов. Например, если основная рабочая частота равна f_H = 20 Гц и добавлены дополнительные сигналы с частотами $f_1 = 3.5$ и $f_2 = 5.3$ кГц, то в результате мы получим следующие сигналы:

$$f_1 + f_2 = f_{1+2} = 8.80 \text{ кГц}$$
$$f_1 - f_2 = f_{1-2} = 1.80 \text{ кГц}$$
$$f_H + f_1 = f_{H+1} = 3.52 \text{ кГц и т.д.}$$

При этом детектор реагирует не только на гармоники основной частоты, но также и на сигналы, полученные в результате сложения и вычитания частот дополнительных сигналов.

Транспондеры в основном имеют форму самоклеящихся этикеток в виде полосок длиной от нескольких сантиметров до 20 см (см. **Рис. 3.8** и **Рис. 3.9**).

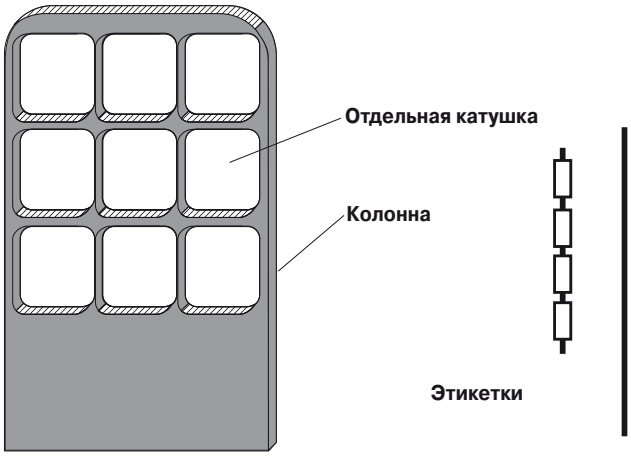


Рис. 3.8. Слева — типичная конструкция антенны для системы сигнализации (высота приблизительно 1.40 м); справа — возможные конструкции этикеток.

Благодаря низкой частоте излучаемого детектором поля электромагнитные системы особенно подходят для товаров, изготовленных из металла. Недостатком таких систем является высокая требовательность к ориентации этикетки относительно антенны считывающего устройства: для надежного обнаружения этикетки линии внешнего магнитного поля должны проходить через полосы аморфного металла вертикально.

Рис. 3.9. Применение электромагнитных этикеток (фото: Schreiner Codedruck, Мюнхен).

Для деактивации этикетки экранируются слоем магнитотвердого металла или же частично закрываются пластинами из магнитотвердого материала. При прохождении через кассу транспондер деактивируется с помощью сильного постоянного магнита, который ориентирован вдоль металлических полосок [plotzke]. Под его воздействием пластины из магнитотвердого материала намагничиваются. При этом полосы из магнитотвердого металла спроектированы таким образом, что создаваемое ими благодаря остаточному магнетизму поле позволяет удерживать металлические полоски, изготовленные из аморфного материала, в состоянии насыщения (подробнее см. подраздел 4.1.12 «Материалы с магнитными свойствами»). Благодаря этому переменное магнитное поле, которое излучается устройством безопасности, уже не будет оказывать на транспондер никакого воздействия.

После снятия магнитного поля этикетки можно использовать вновь, причем процесс деактивации и активации этикетки можно проводить с любой желаемой частотой, предельное количество таких циклов также не ограничено. В связи с этим поначалу основной областью применения электромагнитных систем контроля были частные платные библиотеки, однако затем благодаря своим небольшим размерам (полоски могут иметь длину до 32 мм) и низкой цене подобные этикетки нашли применение и в розничной торговле продуктами питания.

Чтобы создать поле с интенсивностью, достаточной для размагничивания полосок из пермаллоя, обычно такие системы состоят из двух катушек, которые устанавливаются в расположенных по бокам от охраняемого прохода колоннах

(**Рис. 3.10**). В каждой колонне находится система катушек (обычно от 9 до 12 штук), создающих такое магнитное поле, которое в центре имеет довольно небольшую интенсивность и существенно бóльшую — по краям [plotzke]. В современных системах подобного типа ширина прохода может составлять до 1.50 м, при этом вероятность детектирования — 70% [gillert].

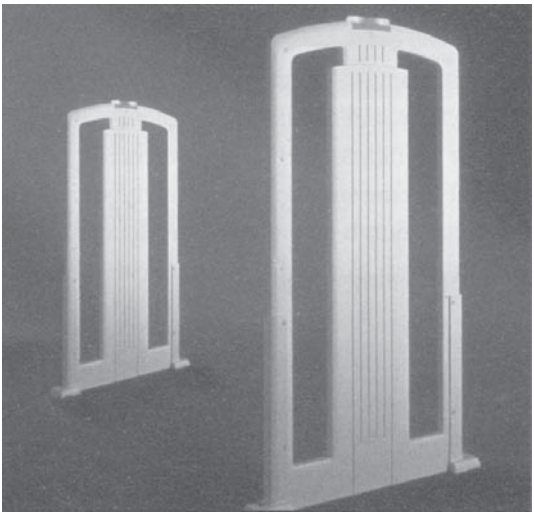


Рис. 3.10. Пример используемой на практике антенны для системы слежения за товарами (фото: METO EAS-System, Esselte Meto, Хиршборн).

Типичные параметры системы электромагнитного типа приведены в **Табл. 3.4**.

Таблица 3.4. **Типичные параметры системы электромагнитного типа [plotzke]**

Параметр	Значение
Частота	70 Гц
Возможные комбинированные частоты для различных систем	12 Гц, 215 Гц, 3.3 кГц, 5 кГц
Напряженность поля H_{eff} в зоне детектирования	25...120 А/м
Минимальная напряженность поля, необходимая для деактивирования	16 000 А/м

3.1.5. Акустомагнитные системы

Системы безопасности акустомагнитного типа представляют собой пластиковые кубики небольшого размера: около 40 мм в длину, от 8 до 14 мм в ширину, в зависимости от исполнения, и всего около миллиметра в высоту. Каждый такой кубик содержит две металлические полоски, изготовленные из магнитотвердого металла, которые жестко закреплены внутри этого пластикового кубика. Кроме того, имеется полоска аморфного металла, которая располагается таким образом, чтобы она могла свободно совершать механические колебания [zechbauer].

Ферромагнитные материалы, такие как никель, железо и т.п., под действием напряженности магнитного поля H изменяют свою длину (на очень незначительную величину) — этот эффект носит название *магнитострикции* и связан с малым изменением расстояния между атомами вещества при его намагничивании. В переменном магнитном поле полоски, изготовленные из магнитострикционного материала, начинают колебаться в продольном направлении с частотой внешнего переменного магнитного поля. Если частота магнитного поля совпадает с (акустической) резонансной частотой металлической полоски, то амплитуда колебаний значительно увеличивается. Этот эффект особенно четко проявляется в аморфных материалах.

Важно также то, что эффект магнитострикции является обратимым — это означает, что при механических колебаниях магнитострикционного материала возникает магнитное поле. Современные *акустомагнитные системы* устроены таким образом, что частота создаваемого магнитного поля точно совпадает с резонансной частотой встроенных в транспондер металлических полосок. Под воздействием внешнего переменного магнитного поля металлическая полоска начинает совершать механические колебания, и когда магнитное поле через некоторое время выключается, то металлическая полоска еще некоторое время продолжает колебаться подобно камертону. При этом она создает собственное магнитное поле, которое может быть обнаружено детектором (**Рис. 3.11**).

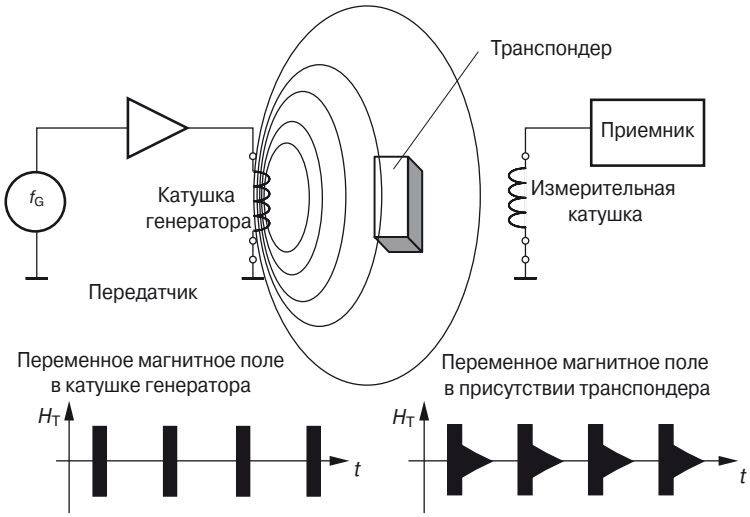


Рис. 3.11. Акустомагнитные системы состоят из передающего устройства и детектора (приемника). Когда транспондер оказывается в зоне действия поля, создаваемого катушкой генератора, то под действием модулированных импульсов от катушки генератора транспондер начинает колебаться подобно камертону. Создаваемое транспондером (акустическое) излучение может быть обнаружено специальным детектирующим устройством.

Одним из главных преимуществ таких систем является то, что в момент приема сигнала от транспондера магнитное поле выключается, благодаря этому можно создавать детекторы с высокой чувствительностью.

Типичные параметры акустомагнитных систем приведены в **Табл. 3.5**.

Таблица 3.5. **Типичные параметры акустомагнитных систем [VDI4471]**

Параметр	Значение
Резонансная частота f_0	58 кГц
Точность установки частоты	±0.52%
Добротность Q	> 150
Минимальная напряженность H_A, которая необходима для активации	> 16 000 А/м
Длительность сигнала (ON) при передаче сигнала	2 мс
Пауза при передаче сигнала (OFF)	20 мс
Время затухания остаточных колебаний в транспондере	5 мс

В активированном состоянии транспондеры акустомагнитных систем намагничиваются, а так как упомянутые ранее полосы из магнитотвердого металла обладают высокой остаточной намагниченностью, то их можно рассматривать как постоянный магнит. Для того чтобы деактивировать транспондер, необходимо размагнитить металлические полосы из магнитотвердого материала. Это приводит к рассогласованию резонансной частоты аморфной металлической полоски, и она больше не будет возбуждаться под воздействием поля, создаваемого устройством безопасности. Для размагничивания полосы из магнитотвердого материала необходимо использовать переменное магнитное поле достаточной интенсивности, причем интенсивность должна медленно уменьшаться с течением времени. Поэтому все попытки обмануть систему при помощи манипулирования постоянными магнитами, которые злоумышленник может принести с собой, обречены на неудачу.

3.2. Дуплексные и полудуплексные системы

В отличие от предыдущего раздела, где мы рассматривали однобитные транспондеры, которые используют какие-либо простые физические эффекты (механические колебания, генерация гармоник с помощью варикапов или нелинейность кривой гистерезиса в металлах), в настоящем и последующих разделах мы будем рассматривать транспондеры, в которых для хранения данных используются полупроводниковые микросхемы. Такие транспондеры могут хранить данные объемом до нескольких килобайтов. При операциях чтения и записи данных необходимо передавать информацию между транспондером и считывающим устройством. По способу передачи данных различают два основных типа систем: дуплексные и полудуплексные, о которых и пойдет речь в данном разделе. Существуют также последовательные системы, которым посвящен следующий раздел.

Если в системе передача данных от транспондера к считывающему устройству не может осуществляться одновременно с передачей данных в обратном направлении (эти процессы разнесены во времени), то такая система носит название *полудуплексной* (Half DupleX — HDX). При частотах ниже 30 МГц в подобных системах наиболее часто применяются методы модуляции нагрузкой (с использованием или без использования поднесущей), которые достаточно легко реализовать с точки зрения схемотехники. С этим методом тесно связан широко известный по технологии радаров метод отражения, который используется на частотах

свыше 100 МГц. Метод модуляции нагрузкой и метод отражения непосредственно влияют на созданное считывающим устройством электромагнитное поле и по этой причине относятся к гармоническим методам.

Если же передача данных от транспондера к считывающему устройству может производиться одновременно с передачей данных в обратном направлении, то такая система называется *дуплексной* (Full DupleX — FDX). В подобных системах передача данных транспондером производится на *субгармониках* основной частоты, на которой ведется передача данных считывающим устройством, или же для передачи данных может использоваться совершенно независимая частота.

Общей особенностью этих двух систем является то, что передача энергии от считывающего устройства к транспондеру производится непрерывно и независимо от передачи данных. В противоположность им в системах с последовательной передачей (SEQ) передача энергии транспондеру производится в течение ограниченного промежутка времени (импульсные системы). Передача данных от транспондера к считывающему устройству в таких системах осуществляется в паузах между периодами передачи энергии (**Рис. 3.12**).

К сожалению, сегодня в литературе по RFID-системам не существует единой классификации для систем такого типа. Система может причисляться к дуплексным или полудуплексным в соответствии с неясными и размытыми критериями, например импульсные системы часто обозначают как полудуплексные. При этом одновременно все системы, которые не относятся к категории импульсных, ошибочно причисляются к дуплексным системам. В данной книге предпринята попытка избежать подобной путаницы, поэтому импульсные системы выделены в совершенно особый класс. Это сделано для того, чтобы отделить их от систем других типов, и в отличие от принятого в обычной литературе подхода данным системам присвоено обозначение SEQ (последовательные системы).

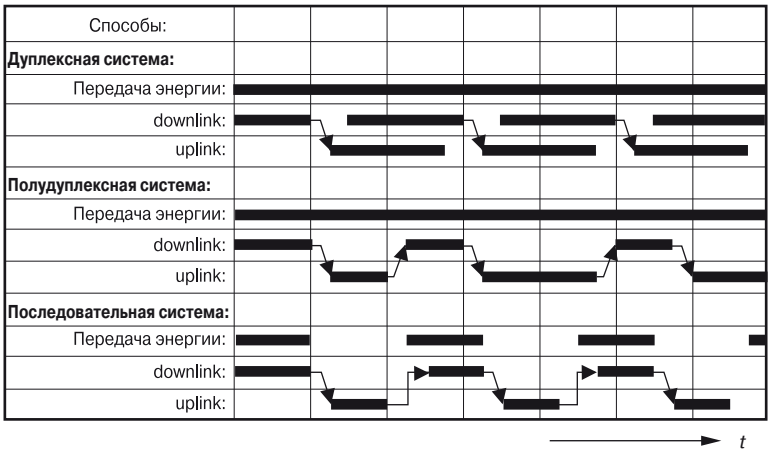


Рис. 3.12. Временная диаграмма передачи данных и энергии для дуплексных, полудуплексных и последовательных систем. Передача данных от считывающего устройства транспондеру обозначена как downlink, передача данных от транспондера к считывающему устройству — как uplink.

3.2.1. Системы с индуктивной связью

3.2.1.1. Передача энергии пассивному транспондеру

Транспондер с индуктивной связью состоит из электронного устройства хранения данных, которое чаще всего является единственной микросхемой в транспондере, и катушки, которая также служит в качестве антенны и занимает достаточно большую площадь.

Транспондеры с индуктивной связью почти все без исключения относятся к *пассивным* транспондерам. Это означает, что всю необходимую для функционирования микросхемы энергию транспондер получает извне, от считывающего устройства. Антенна считывающего устройства создает достаточно сильное электромагнитное поле высокой частоты, которое проникает через внутреннюю и внешнюю поверхность катушки. Так как длина волны электромагнитного излучения в диапазоне рабочих частот (при частоте менее 135 кГц длина волны примерно равна 2400 м, при частоте 13.56 МГц — 22.1 м) намного превышает расстояние между антенной считывающего устройства и транспондером, то на таких расстояниях излучаемое считывающим устройством электромагнитное поле с точки зрения воздействия на антенну транспондера может рассматриваться как переменное магнитное поле (подробнее см. подраздел 4.2.1.1).

Незначительная часть электромагнитного излучения, создаваемого считывающим устройством, проникает через катушку-антенну транспондера, которая располагается на некотором удалении от считывающего устройства, и индуцирует в ней напряжение U_i. Это переменное напряжение преобразуется в постоянное и используется для питания микросхемы, в которой хранятся данные. Параллельно катушке считывающего устройства включен конденсатор C_r, емкость которого выбрана таким образом, что с учетом индуктивности катушки образуется колебательный контур с резонансной частотой, равной рабочей частоте считывающего устройства. В условиях резонанса через катушку считывающего устройства текут токи большой величины, которые создают поле достаточно высокой интенсивности, позволяющее передавать энергию, достаточную для питания удаленного транспондера (**Рис. 3.13**).

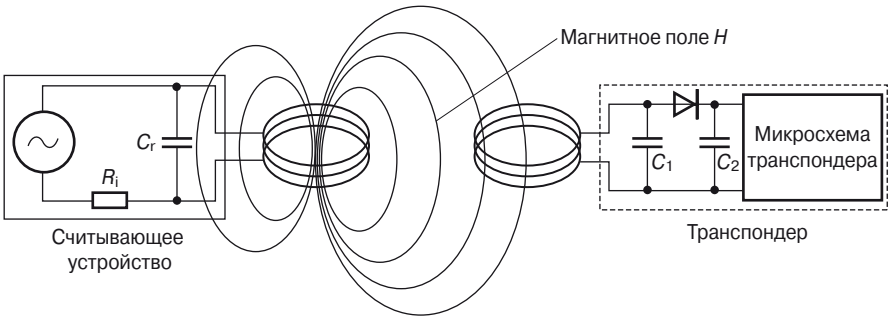


Рис. 3.13. Транспондер с индуктивной связью получает всю необходимую для работы энергию от считывающего устройства, которое излучает магнитное поле достаточно высокой интенсивности.

Антенна-катушка транспондера вместе с конденсатором C_1 также образует резонансный контур, который настроен на частоту излучения, передаваемого считывающим устройством. В условиях резонанса напряжение U на катушке транспондера достигает своего максимального значения.

На **Рис. 3.14** показаны различные формы транспондеров с индуктивной связью, а на **Рис. 3.15** — считывающее устройство.

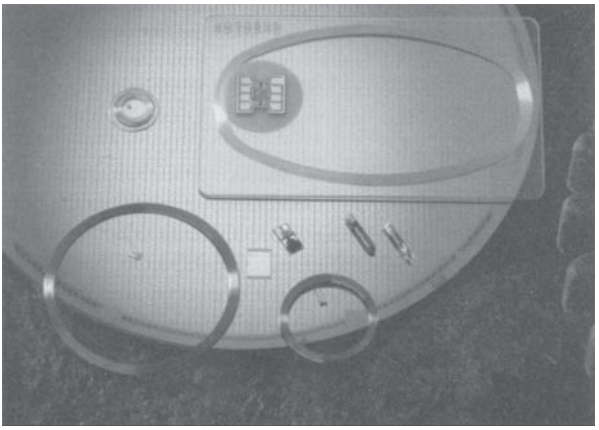


Рис. 3.14. Различные формы транспондеров с индуктивной связью. На фотографии показаны полуфабрикаты: транспондеры, еще не помещенные в пластиковый корпус (фото: AmaTech GmbH, KG, Пфронтен).

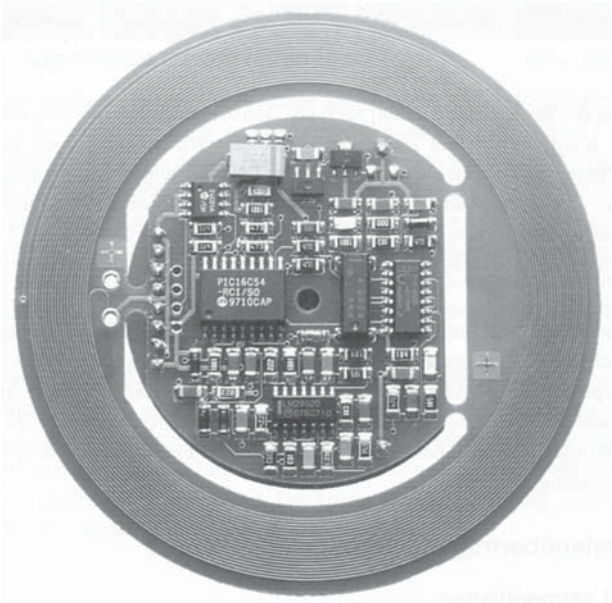


Рис. 3.15. Считывающее устройство для работы с транспондерами, использующими индуктивную связь в диапазоне частот до 135 кГц; на снимке видна интегрированная антенна (фото: easy-key System, micron, Халльбергмоос).

Сравнение энергопотребления различных специализированных микросхем, используемых в RFID-системах, приведено в **Табл. 3.6**.

Таблица 3.6. **Сравнение энергопотребления различных специализированных микросхем, используемых в RFID-системах [ATMEL].** Минимальное напряжение питания всех микросхем составляет 1.8 В, максимально допустимое напряжение — 10 В

	Память [байт]	Расстояние чтения/записи	Ток потребления	Частота	Применение
ASIC#1	6	15 см	10 мкА	120 кГц	Идентификация животных
ASIC#2	32	13 см	600 мкА	120 кГц	Отслеживание товаров, проверка прав доступа
ASIC#3	256	2 см	6 мкА	128 кГц	Общественный транспорт
ASIC#4	256	0.5 см	< 1 мА	4 МГц*	Отслеживание товаров, общественный транспорт
ASIC#5	256	< 2 см	~ 1 мА	4/13.56 МГц	Отслеживание товаров
ASIC#6	256	100 см	500 мкА	125 кГц	Проверка доступа
ASIC#7	2048	0.3 см	< 10 мА	4.91 МГц*	Бесконтактные чип-карты
ASIC#8	1024	10 см	~ 1 мА	13.56 МГц	Общественный транспорт
ASIC#9	8	100 см	< 1 мА	125 кГц	Отслеживание товаров
ASIC#10	128	100 см	< 1 мА	125 кГц	Проверка доступа
* Системы Close-coupling.					

Конструкция двух катушек позволяет рассматривать их как трансформатор (*трансформаторная связь*), с учетом, что в данном случае между двумя обмотками трансформатора существует очень слабая связь. В таком трансформаторе (состоящем из катушек-антенн считывающего устройства и транспондера) коэффициент полезного действия при передаче мощности определяется рабочей частотой системы f, числом витков n катушки транспондера, площадью A катушки транспондера, углом, под которым расположены катушки относительно друг друга, а также расстоянием между ними.

С увеличением рабочей частоты системы снижается необходимая индуктивность, а значит, и количество витков n катушки транспондера (при 135 кГц обычно необходимо от 100 до 1000 витков, при 13.56 МГц уже достаточно всего лишь 3...10 витков). Так как индуцируемое в транспондере напряжение прямо пропорционально рабочей частоте f (см. подраздел 4.1.7 «Резонанс»), то уменьшение числа витков катушки при увеличении частоты практически не сказывается на КПД при передаче энергии от считывающего устройства к транспондеру.

3.2.1.2. Передача данных от транспондера к считывающему устройству

3.2.1.2.1. Модуляция нагрузкой

Как говорилось выше, в системах с индуктивной связью возникает трансформаторная связь между первичной обмоткой (катушкой) считывающего устройства и вторичной обмоткой (катушкой) транспондера. Это означает, что пока расстояние между двумя катушками не превышает 0.16λ, транспондер остается в *ближней зоне* передающей антенны (более подробно о ближней и дальней зоне см. подраздел 4.2.1.1).

Когда на резонансный транспондер (собственная частота колебательного контура которого равна рабочей частоте считывающего устройства) воздействует излучаемое считывающим устройством переменное магнитное поле, он начинает получать энергию. Действие транспондера на антенну считывающего устройства может быть описано с помощью *трансформированного импеданса* Z_T, возникающего в цепи катушки-антенны. Когда в цепи антенны транспондера включается и отключается сопротивление нагрузки, это приводит к изменению импеданса Z_T и, следовательно, к изменению напряжения на антенне считывающего устройства (см. подраздел 4.1.10.3 «Модуляция нагрузкой»). Это можно представить как модуляцию с амплитудой U_L на антенне считывающего устройства, которая осуществляется с помощью удаленного транспондера. Включением и отключением сопротивления нагрузки в цепи транспондера управляет поток передаваемых данных, и таким образом данные могут быть переданы считывающему устройству. Указанный способ передачи данных в направлении от транспондера к считывающему устройству получил название «модуляция нагрузкой» (load modulation).

Для расшифровки полученных подобным образом сигналов возникающее на антенне считывающего устройства напряжение сначала детектируется — так осуществляется демодуляция принятых сигналов с амплитудной модуляцией. Пример использования специально предназначенной для этих целей микросхемы обсуждается в разделе 11.3 «Конструкция недорогого считывающего устройства на основе микросхемы U2270B».

3.2.1.2.2. Модуляция нагрузкой с использованием поднесущей

Связь между антенной считывающего устройства и антенной транспондера достаточно мала. Таким образом, получаемый от транспондера полезный сигнал вызывает на антенне считывающего устройства колебания напряжения, которые имеют значительно меньшую величину по сравнению с колебаниями напряжения, излучаемого считывающим устройством для передачи данных и энергии транспондеру. На практике в системах с рабочей частотой 13.56 МГц колебания напряжения на передающей антенне считывающего устройства составляют приблизительно 100 В (в состоянии резонанса!), в то время как полезный сигнал вызывает колебания напряжения с амплитудой 10 мВ, то есть соотношение полезного сигнала к «помехе» составляет 80 дБ. Для обнаружения такого сигнала необходимы специальные схемотехнические решения, поэтому при амплитудной модуляции напряжения на антенне предпочитают использовать поднесущие.

А именно: включение и выключение нагрузки в цепи транспондера осуществляется с очень высокой тактовой частотой f_H, благодаря этому в спектре сигнала возникают две линии на расстоянии $\pm f_H$ от рабочей частоты, на которой излучает антенна считывающего устройства. Эти линии (частоты) в радиотехнике называются *поднесущими* (subcarrier), и их довольно легко обнаружить (при этом должно выполняться условие $f_H < f_{READER}$). Передача данных осуществляется с помощью ASK-, FSK- или PSK-модуляции поднесущих с тактовой частотой потока передаваемых данных.

Реализация схемы модуляции нагрузкой с использованием полевого транзистора показана на **Рис. 3.16**.

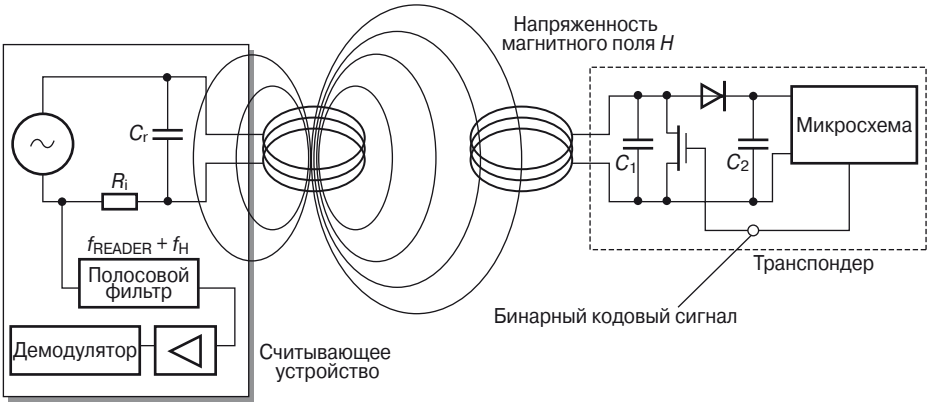


Рис. 3.16. Реализация схемы модуляции нагрузкой с использованием сопротивления сток—исток полевого (FET — МОП) транзистора, который управляется микросхемой транспондера. Показан также считыватель, который осуществляет детектирование поднесущей частоты.

Итак, при модуляции нагрузкой с использованием поднесущих в антенне считывающего устройства возникают две боковые полосы модулированного сигнала, удаленные от рабочей частоты f_{READER} на частоту поднесущих (**Рис. 3.17**).

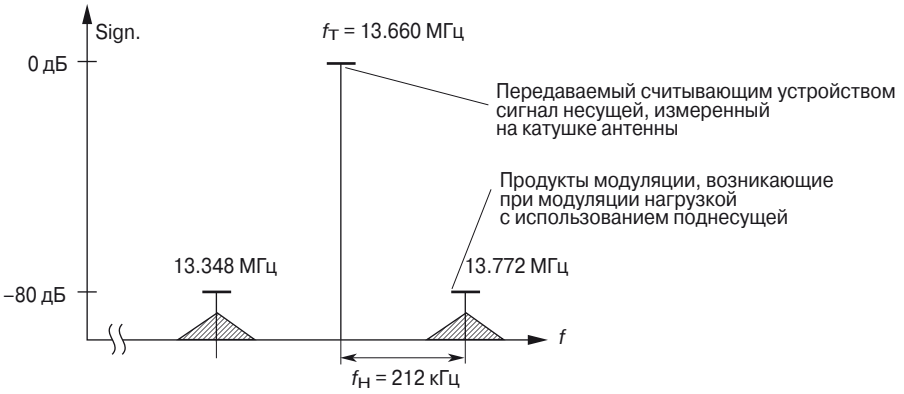


Рис. 3.17. При модуляции нагрузкой с использованием поднесущей образуются две вспомогательные полосы на расстоянии f_H от частоты, на которой осуществляет передачу считывающее устройство. Информация передается в двух боковых полосах и сохраняется с помощью модуляции поднесущих частот.

После этого возникающие боковые полосы пропускаются через полосовые фильтры (Band Pass filter — BP) с центральной частотой $f_{READER} \pm f_H$, что позволяет выделить их на фоне более мощного сигнала излучения антенны. Затем сигналы поднесущих усиливаются, и можно достаточно легко провести их демодуляцию.

Для передачи информации с помощью поднесущих необходима довольно большая полоса пропускания, поэтому данный способ используется только для достаточно высоких частот, например в диапазоне ISM на частотах 6.78, 13.56 и 27.125 МГц (подробнее см. в главе 5 «Диапазоны частот и правила, регламентирующие использование радиочастот»).

3.2.1.2.3. Пример схемы — модуляция нагрузкой с использованием поднесущей

Пример схемотехнического решения для транспондера, в котором применяется метод модуляции нагрузкой с использованием поднесущей, показан на **Рис. 3.18**. Рабочая частота системы составляет 13.56 МГц, частота поднесущей — 212 кГц.

Переменное магнитное поле, излучаемое считывающим устройством, создает в катушке L_1 антенны напряжение, которое выпрямляется с помощью диодного моста ($D_1 ... D_4$) и используется в качестве напряжения питания схемы. Параллельно включен ограничитель (стабилитрон ZD 5V6), который ограничивает повышение напряжения питания при приближении транспондера к антенне считывающего устройства.

Благодаря предварительному сопротивлению R_1 часть высокочастотного излучения (13.56 МГц) попадает на вход тактового сигнала (CLK) микросхемы (IC_1) и служит для транспондера источником тактовых импульсов для формирования внутреннего синхросигнала. С помощью делителя на 2^6 (= 64) на выходе Q7 мы получаем тактовый сигнал частотой 212 кГц, который будет использоваться для формирования поднесущей. Поток синхроимпульсов управляется последовательным потоком данных (DATA) и затем подается на ключ (T_1). При этом сопротивление нагрузки (R_2) подключается и отключается с частотой, равной частоте поднесущей.

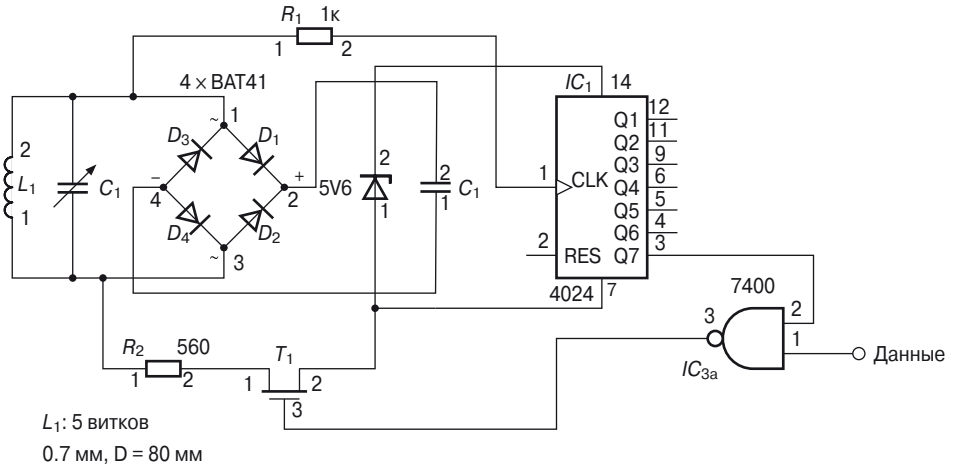


Рис. 3.18. Схема транспондера с индуктивной связью, в которой применяется модуляция нагрузкой с использованием поднесущей.

В показанную выше схему можно добавить конденсатор C_1 и создать резонансный контур с частотой 13.56 МГц. Таким способом можно значительно увеличить дальность действия этой «минималистской» схемы.

3.2.1.2.4. Субгармонические способы

Под субгармониками синусоидального напряжения A с заданной частотой f_A понимают синусоидальные колебания B, частота колебания которых f_B получается делением частоты f_A на целые числа: $f_A/2, f_A/3, f_A/4, ...$

Когда для передачи данных используются субгармоники, основным способом является получение (путем деления) из переданного транспондеру электромагнитного излучения с рабочей частотой системы f_A второй частоты f_B, которая обычно в 2 раза меньше (**Рис. 3.19**). Выходной сигнал делителя с частотой f_B теперь может модулироваться потоком данных, далее этот сигнал с помощью выходного драйвера подается на антенну транспондера.

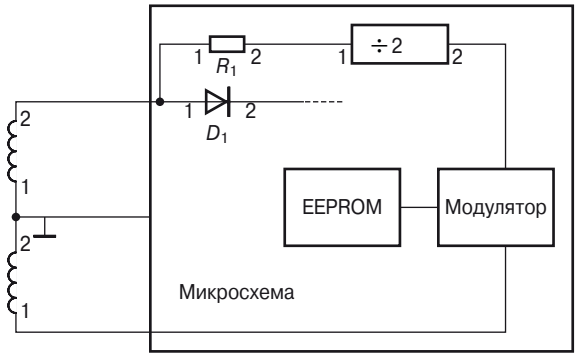


Рис. 3.19. Принципиальная схема транспондера, который для ответа на запрос считывающего устройства использует субгармоники рабочей частоты системы. Полученный от считывателя сигнал делится на два, модулируется передаваемыми данными и подается через ответвление в катушку транспондера.

Наиболее часто в субгармонических системах используется рабочая частота 128 кГц, следовательно, частота, на которой отвечает транспондер, составляет 64 кГц.

Антенна транспондера представляет собой катушку с выполненным в середине ответвителем. На один из концов катушки подается напряжение питания, на второй — передаваемый транспондером ответный сигнал.

3.2.2. Связь с помощью электромагнитного рассеяния

3.2.2.1. Энергоснабжение транспондера

RFID-системы, в которых расстояние между считывающим устройством и транспондером значительно превышает 1 м, получили название *систем дальнего действия* (long-range system). Для этих систем обычно используются следующие диапазоны частот: сверхвысокие частоты — 868 МГц (Европа) и 915 МГц (США),

а также микроволновые частоты — 2.5 и 5.8 ГГц. Благодаря меньшей длине волны в таких системах можно использовать значительно более компактные антенны, которые имеют более высокий коэффициент полезного действия по сравнению с антеннами, рассчитанными на частоту 30 МГц.

Для того чтобы оценить количество получаемой транспондером энергии, воспользуемся следующей формулой:

$$a_F = -147.6 + 20\log(r) + 20\log(f) - 10\log(G_T) - 10\log(G_R), \quad (3.1)$$

где r — расстояние между транспондером и считывающим устройством, a_F — коэффициент затухания в свободном пространстве, G_T и G_R — коэффициенты усиления транспондера и считывающего устройства соответственно, f — рабочая частота электромагнитного излучения считывающего устройства.

Коэффициент затухания в свободном пространстве служит для описания соотношения между количеством энергии, которое излучается в виде радиоволн считывающим устройством, и количеством энергии, которое принимает транспондер.

Благодаря современным технологиям производства полупроводниковых компонентов энергопотребление микросхем транспондеров не превышает 5 мкВт [friedrich], коэффициент полезного действия интегрального выпрямителя (преобразователя переменного напряжения в постоянное) для сигналов UHF- и микроволнового диапазона сегодня составляет 5...25% [tanneberger]. Если принять КПД равным 10%, то для того, чтобы обеспечить питание микросхемы транспондера, мощность на выходе антенны транспондера должна быть не ниже P_e = 50 мкВт. Это означает, что если мощность излучения считывающего устройства равна P_S = 0.5 Вт EIRP, то коэффициент затухания должен составлять не менее 40 дБ (т.е. P_S/P_e) — только в этом случае антенна транспондера получит излучение, достаточное для питания устройства. Как показано в **Табл. 3.7**, для рабочей частоты 868 МГц это означает дальность чуть более 3 м, а для частоты 2.45 ГГц — немногим более 1 м. Если электронные компоненты транспондера имеют более высокое потребление, то дальность действия будет пропорционально уменьшаться.

***Таблица 3.7.* Затухание в свободном пространстве a_F при различных частотах и расстояниях.** Коэффициент усиления для антенны транспондера равен 1.64 (диполь), коэффициент усиления для антенны считывающего устройства равен 1 (изотропный излучатель)

Расстояние r [м]	Затухание в свободном пространстве a_F [дБ]		
	868 МГц	915 МГц	2.45 МГц
0.3	18.6	19.0	27.6
1	29.0	29.5	38.0
3	38.6	39.0	47.6
10	49.0	49.5	58.0

Для того чтобы увеличить дальность действия (до 15 м) или использовать при том же рабочем расстоянии микросхемы с более высоким потреблением энергии, в отражательных транспондерах (backscatter) часто используется батарейное питание (**Рис. 3.20**). В целях экономии в таких устройствах обычно реализуются режимы пониженного энергопотребления — power down или stand-by. Когда транспондер

покидает пределы зоны действия считывающего устройства, автоматически включается режим пониженного энергопотребления power down, в этом случае максимальный ток потребления составляет лишь несколько микроампер. Когда транспондер вновь попадает в поле достаточно высокой интенсивности, микросхема активируется и переходит в нормальный рабочий режим. Однако энергия встроенной батарейки никогда не используется для передачи данных между транспондером и считывающим устройством — она предназначена исключительно для питания микросхемы. Передача данных осуществляется за счет энергии, полученной путем преобразовании энергии электромагнитного излучения, поступающего от считывающего устройства.

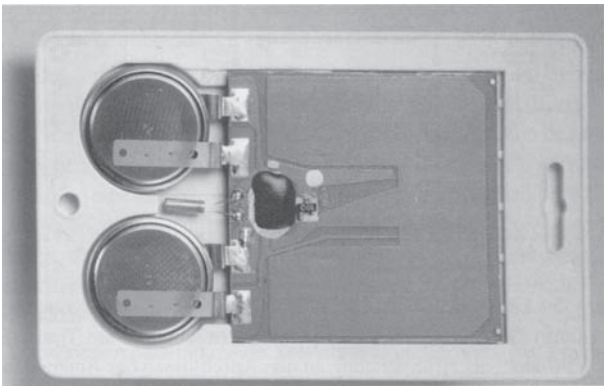


Рис. 3.20. Активный транспондер, предназначенный для работы в диапазоне 2.45 ГГц. Питание для микросхемы хранения данных обеспечивается с помощью двух литиевых батареек. Также на рисунке можно разглядеть микроволновую антенну транспондера — это поверхность в форме символа *U* на печатной плате (фото: Pepperl & Fuchs, Маннхайм).

3.2.2.2. Передача данных от транспондера к считывающему устройству

3.2.2.2.1. Модулирование эффективного сечения рассеяния

Из теории *радаров* известно, что если физические размеры какого-либо объекта превышают половину длины волны падающего на него электромагнитного излучения, то электромагнитное излучение будет отражаться от этого объекта. Для количественного выражения меры отражения вводится понятие *эффективной площади,* или *сечения, рассеяния*. Эффективное сечение рассеяния резко увеличивается, когда объект вступает в резонанс с падающим на него электромагнитным излучением, что имеет место, например, для настроенной на эту частоту антенны.

Итак, считывающее устройство создает электромагнитное излучение мощностью P_1, однако вследствие ослабления сигнала по мере увеличения расстояния от считывающего устройства только небольшая часть данного излучения достигает антенны транспондера. Под воздействием этого излучения на выводах антенны транспондера возникают высокочастотные колебания с мощностью P_1' (**Рис. 3.21**). Выпрямленное на диодах D_1 и D_2 напряжение служит сигналом

для выхода из режима с низким энергопотреблением (power down). В качестве диодов здесь используются диоды Шоттки (low-barrier), которые имеют чрезвычайно низкое пороговое напряжение. На небольших расстояниях от считывающего устройства преобразованное излучение можно использовать и в качестве источника энергии.

Часть излучения с мощностью P_1 отражается антенной и распространяется в обратном направлении, мощность отраженного излучения мы обозначим как P_2. Изменяя подключенную к антенне нагрузку, можно изменять *коэффициент отражения антенны* (т.е. эффективное сечение рассеяния). Для того чтобы передать информацию считывающему устройству, поток передаваемых данных подключает и отключает дополнительное сопротивление нагрузки R_L, которое подсоединено параллельно выходу антенны. В результате отраженное излучение с мощностью P_2 модулируется по амплитуде (modulated backscatter — *модулированное эффективное сечение рассеяния*).

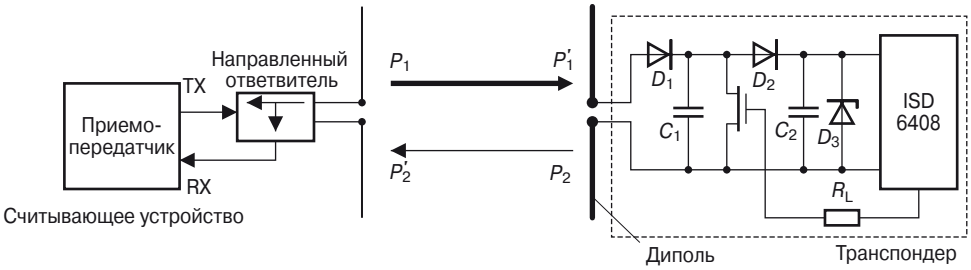


Рис. 3.21. Принцип действия отражательного транспондера. Модуляция импеданса осуществляется путем подачи сигнала на транзистор [isd].

Модулированное по амплитуде излучение с мощностью P_2 отражается от транспондера, но в результате пространственного ослабления излучение, которое достигает считывающего устройства, значительно ослабляется. Затем отраженный сигнал попадает на разъем считывающего устройства, двигаясь уже в обратном направлении, и через *направленный ответвитель* этот сигнал поступает на вход приемника считывающего устройства. Направленный ответвитель позволяет уменьшить влияние сигнала передатчика, который по своей интенсивности на порядки превосходит интенсивность сигнала, отраженного транспондером.

Соотношение мощности излучаемого и принимаемого сигнала P_1/P_2 может быть рассчитано с помощью уравнения радиолокации (см. подраздел 4.2.5.4 «Эффективная площадь и эффективное сечение рассеяния»).

3.2.3. Системы Close-coupling

3.2.3.1. Источник питания транспондера

Системы Close-coupling предназначены для работы на расстоянии от 0.1 до максимум 1 см и в основном используются в приложениях touch & go, т.е., например, там, где для прохода на охраняемую территорию необходимо поднести транспондер к указанному участку на поверхности считывающего устройства.

В таких системах транспондер часто вставляется или кладется на считыватель (**Рис. 3.22**), по этой причине катушку транспондера помещают в центре воздушного зазора сердечника, выполненного в виде кольца или в виде буквы *U*. Функционально катушки транспондера и считывающего устройства являются катушками трансформатора, при этом первичной обмоткой является катушка считывающего устройства, а катушка транспондера — вторичной. Высокочастотные колебания в первичной обмотке посредством магнитного поля, распространяющегося через сердечник и воздушный зазор, возбуждают высокочастотные колебания во вторичной обмотке трансформатора. Колебания в первичной и во вторичной катушке трансформатора имеют одну и ту же частоту. С помощью выпрямителя высокочастотное переменное напряжение преобразуется в постоянное, которое затем используется как напряжение питания микросхемы транспондера.

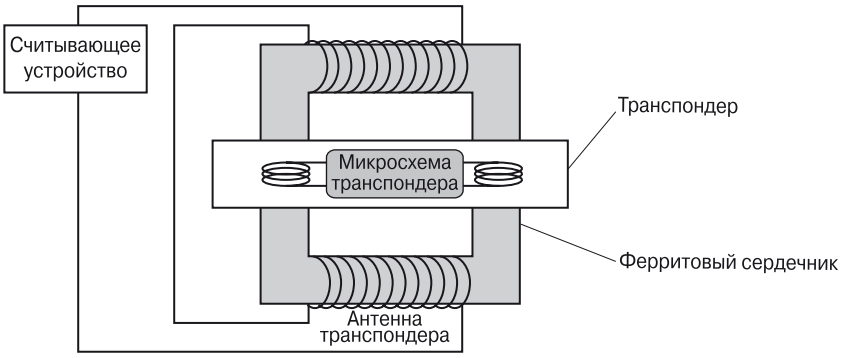


Рис. 3.22. В системах Close-coupling транспондер вставляется в разъем считывающего устройства, который окружен магнитными катушками связи.

Величина напряжения *U*, индуцируемого во вторичной обмотке, пропорциональна частоте *f* тока возбуждения, текущего в первичной обмотке. Таким образом, для более эффективной передачи энергии от ридера к транспондеру необходимо использовать как можно более высокую частоту; на практике используют частоту в диапазоне от 1 до 10 МГц. Для того чтобы уменьшить потери энергии в сердечнике, в качестве материала для сердечника выбирают ферриты, причем при выборе материала учитывают рабочую частоту трансформатора.

Так как эффективность передачи энергии в системах Close-coupling существенно выше по сравнению с индуктивными или микроволновыми системами, то в данных системах часто используют микросхемы со сравнительно высоким энергопотреблением. Например, это микропроцессоры с потреблением порядка нескольких десятков милливатт [sickert]. Почти все коммерческие системы Close-coupling на основе чип-карт содержат такие высокопроизводительные микропроцессоры.

Механические и электрические параметры бесконтактных чип-карт, относящихся к типу Close-coupling, описываются в специальном стандарте — ISO 10536. Если в системе используются другие конструкции транспондеров, то на них не налагается никаких ограничений.

3.2.3.2. Передача данных от транспондера к считывающему устройству

3.2.3.2.1. Магнитная связь

В системах Close-coupling при использовании *магнитной связи* для передачи данных от транспондера к считывающему устройству также широко применяется модуляция нагрузкой с использованием поднесущей. Если в системе Close-coupling используются чип-карты, то частота и тип модуляции поднесущей определяются стандартом ISO 10536.

3.2.3.2.2. Емкостная связь

Так как в системах Close-coupling расстояние между считывающим устройством и транспондером сравнительно невелико, то для передачи данных может использоваться и *емкостная связь*. Для этого создается плоский конденсатор, состоящий из изолированных друг от друга пластин. Когда транспондер устанавливается в считывающее устройство, эти пластины располагаются строго параллельно друг другу (**Рис. 3.23**).

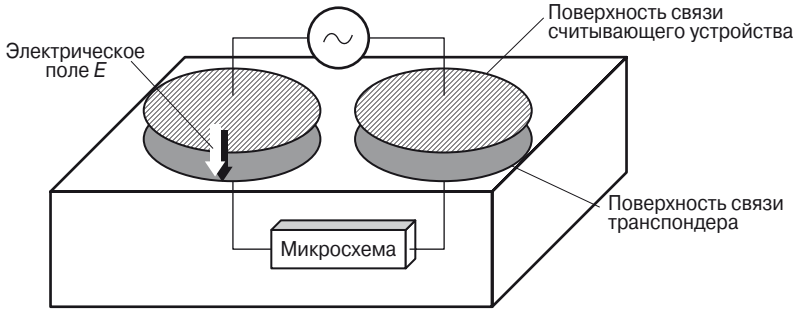


Рис. 3.23. Емкостная связь в системах Close-coupling осуществляется с помощью двух металлических пластин, которые располагаются параллельно друг другу на небольшом расстоянии.

Указанный способ также используется для передачи данных с чип-карт в системах Close-coupling. Механические и электрические свойства таких чип-карт описываются в стандарте ISO 10536.

3.2.4. Передача данных от считывающего устройства к транспондеру

Для передачи данных от ридера к транспондеру как в дуплексных, так и в полудуплексных системах могут применяться все существующие методы цифровой модуляции, независимо от рабочей частоты и от типа связи, который используется в данной системе. Существуют три основных типа модуляции:

- ASK: Amplitude Shift Keying — амплитудная манипуляция;
- FSK: Frequency Shift Keying — частотная манипуляция;
- PSK: Phase Shift Keying — фазовая манипуляция.

Благодаря простоте своей реализации, в большинстве систем радиочастотной идентификации используется первый метод — амплитудная манипуляция, ASK.

3.2.5. Электрическая связь

3.2.5.1. Передача энергии пассивному транспондеру

При *электрической* (емкостной) связи считывающее устройство создает высокочастотное поле достаточно высокой напряженности, при этом антенна считывающего устройства представляет собой проводящую электричество поверхность довольно большой площади — электрод, который на практике обычно изготавливается из металлической фольги (**Рис. 3.24**). Если на такой электрод подается высокочастотное напряжение достаточно большой величины, то между электродом и потенциалом земли (ground) возникает высокочастотное электрическое поле. Величина напряжения составляет от нескольких сот до нескольких тысяч вольт, для создания такого напряжения в считывающем устройстве используется резонансный контур. Резонансный контур состоит из катушки индуктивностью L_1, включенного параллельно ей конденсатора емкостью C_1, а также эффективной емкости $C_{R\text{-}GND}$, которая представляет действительную емкость между электродом считывающего устройства и землей. Резонансная частота этой цепи соответствует рабочей частоте считывающего устройства.

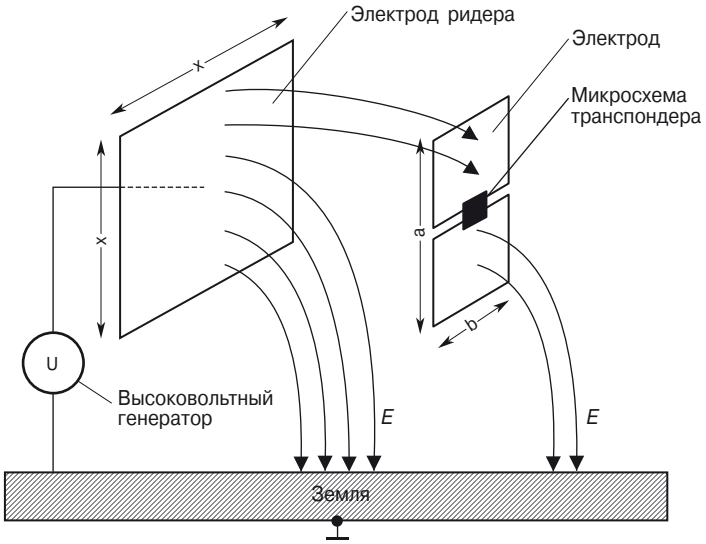


Рис. 3.24. Система с электрической связью использует для передачи энергии и данных электростатическое поле.

Антенна транспондера представляет собой две проводящие поверхности (электроды), которые лежат в одной плоскости. Когда транспондер оказывается в электрическом поле считывающего устройства, между его двумя электродами возникает электрическое напряжение, которое используется в качестве источника питания транспондера.

Зависимость напряжения на электродах, необходимого для чтения данных с транспондера, от размеров электродов приведена на **Рис. 3.25**.

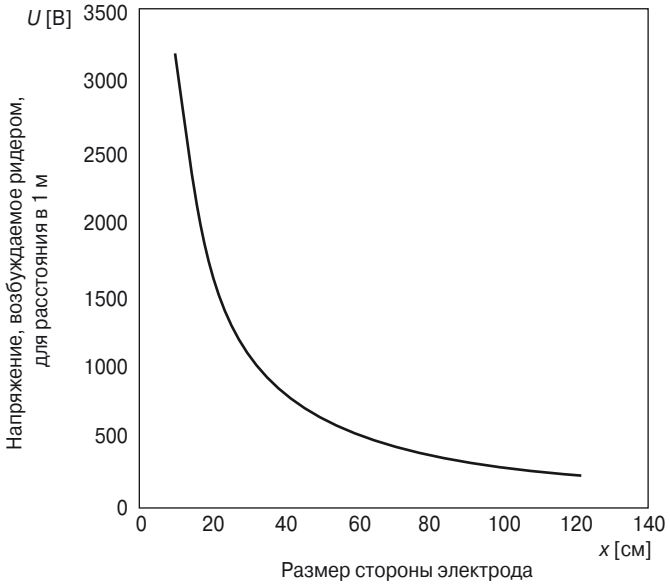


Рис. 3.25. Напряжение на электродах, необходимое для чтения данных с транспондера. Размер электродов a × b = 4.5 × 7 см (соответствует размерам чип-карты), расстояние — 1 м, частота — 125 кГц.

Как между транспондером и передающей антенной ($C_{R\text{-}T}$), так и между антенной транспондера и потенциалом земли ($C_{T\text{-}GND}$) существует эффективная емкость. Эквивалентная схема для системы с электрической связью может быть упрощенно представлена в виде *делителя напряжения*, который состоит из элементов $C_{R\text{-}T}$, R_L (собственное сопротивление транспондера) и $C_{T\text{-}GND}$ (см. **Рис. 3.26**). Если коснуться рукой электрода транспондера, то увеличивается емкость $C_{T\text{-}GND}$, что также увеличивает и *дальность действия* считывающего устройства.

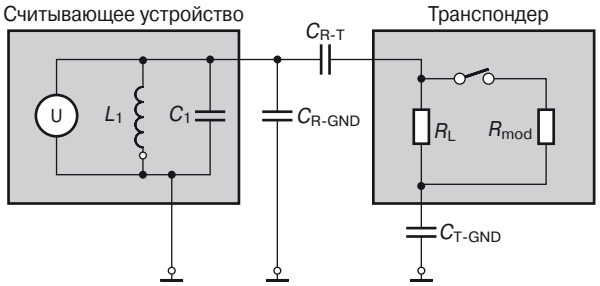


Рис. 3.26. Эквивалентная схема RFID-системы с электрической связью.

Ток, текущий по поверхности электродов, имеет очень небольшую величину. В связи с этим к материалу, из которого изготавливаются электроды, не предъявляется никаких особых требований с точки зрения электрической проводи-

мости — наряду с обычной *металлической фольгой* часто поверхность электродов просто покрывают электропроводящей краской (например, *серебряной проводящей пастой*) или же наносят *слой графита* [bistatix].

3.2.5.2. Передача данных от транспондера к считывающему устройству

Когда транспондер с электрической связью попадает в зону действия считывающего устройства, то можно представить, что входное сопротивление транспондера R_L оказывается включенным последовательно с эффективной емкостью $C_{R\text{-}T}$, которая входит в состав колебательного контура считывающего устройства (**Рис. 3.26**). Это немного ухудшает добротность контура. Подключая и отключая сопротивление модуляции R_{mod}, мы изменяем характеристику затухания колебательного контура транспондера. За счет подключения и отключения сопротивления R_{mod} в цепь транспондера происходит амплитудная модуляция напряжения, присутствующего на L_1 и C_1, при этом модуляция осуществляется с помощью удаленного транспондера. Если включением и отключением сопротивления модуляции R_{mod} управляет поток передаваемых данных, то таким образом производится передача информации от транспондера к считывающему устройству. Мы будем называть этот способ модуляции *модуляцией нагрузкой* (load modulation).

3.3. Последовательные методы

Последовательные системы (SEQ) — это системы радиочастотной идентификации, в которых передача данных и энергии от считывающего устройства к транспондеру и передача данных от транспондера к считывающему устройству разделены во времени и не могут осуществляться одновременно.

Мы уже рассказывали в разделе 3.2 «Дуплексные и полудуплексные системы» о различиях между SEQ-системами и системами других типов.

3.3.1. Системы с индуктивной связью

3.3.1.1. Передача энергии транспондеру

Последовательные системы с индуктивной связью почти все без исключения работают в частотном диапазоне ниже 135 кГц. В таких системах между катушкой считывающего устройства и катушкой транспондера существует трансформаторная связь. Под действием передаваемого считывающим устройством переменного электромагнитного поля на катушке транспондера возникает переменное напряжение, которое выпрямляется и используется для питания микросхемы транспондера.

Для достижения высокой эффективности передачи энергии необходимо обеспечить точное совпадение рабочей частоты считывающего устройства и резонансной частоты транспондера, а также высокую добротность катушки транспондера. Для точной подстройки резонансной частоты колебательного контура транспондера обычно устанавливают *подстроечный конденсатор*.

В отличие от дуплексной и полудуплексных систем, в последовательных системах передатчик считывающего устройства работает в течение достаточно короткого времени. Переданная считывающим устройством энергия используется для того, чтобы зарядить конденсатор транспондера, который служит в качестве аккумулятора энергии. Микросхема транспондера в процессе заряда конденсатора находится в режиме Standby или другом режиме с пониженным энергопотреблением, благодаря этому вся полученная энергия расходуется на заряд конденсатора. По истечении заданного промежутка времени передатчик считывающего устройства прекращает передачу.

Запасенная в конденсаторе энергия используется для передачи данных от транспондера к считывающему устройству. Исходя из необходимого для данной микросхемы напряжения питания и тока потребления, можно определить минимально допустимую емкость конденсатора (см. пояснения в **Табл. 3.8**):

$$C = Q/U = I \times t/(V_{max} - V_{min}). \quad (3.2)$$

Таблица 3.8. **Пояснения к формуле (3.2)**

$V_{max} - V_{min}$	Граничные значения напряжения питания, за эти границы выходить не следует
I	Ток потребления в рабочем режиме микросхемы
t	Время, необходимое для передачи данных от транспондера к считывающему устройству

В качестве примера рассмотрим следующие значения: I = 5 мкА, t = 20 мс, V_{max} = 4.5 В и V_{min} = 3.5 В. Отсюда получаем значение емкости конденсатора C = 100 нФ [schurmann-93].

3.3.1.2. Сравнение дуплексных/полудуплексных и последовательных систем

Различия между системами радиочастотной идентификации дуплексного/полудуплексного типа (FDX/HDX) и системами последовательного типа (SEQ) приведены на **Рис. 3.27**.

В дуплексных системах передача данных и энергии от считывающего устройства к транспондеру может осуществляться одновременно с передачей данных в обратном направлении, а это означает, что микросхема транспондера должна постоянно находиться в рабочем состоянии.

Для того чтобы использовать полученную от считывающего устройства энергию оптимальным образом, необходимо обеспечить *согласование по мощности* между антенной транспондера, которая является источником тока, и микросхемой транспондера, которая является потребителем тока. Однако при точном согласовании по мощности для микросхемы будет доступна только половина напряжения источника питания (от напряжения на катушке при отсутствии нагрузки). Для того чтобы повысить доступное рабочее напряжение, необходимо увеличить импеданс (т.е. сопротивление нагрузки) микросхемы, однако одновременно это означает, что следует уменьшать потребляемую микросхемой мощность.

При разработке дуплексной системы идентификации необходимо также определить нужный компромисс между согласованием по мощности (максимальная мощность потребления P_{chip} достигается при $U_{chip} = 1/2U_Q$) и *согласованием по напряжению* (минимальная мощность потребления P_{chip} при максимальном напряжении питания $U_{chip} = U_Q$).

Совершенно иначе дело обстоит в случае последовательных систем: при осуществлении процесса заряда микросхема находится в «спящем» или другом режиме с пониженным потреблением, таким образом в этот момент микросхема практически не расходует энергию.

Конденсатор, в котором запасается энергия для питания системы, в момент начала заряда является полностью разряженным и, таким образом, представляет для источника напряжения весьма небольшую нагрузку (см. **Рис. 3.27**, момент начала заряда). В этот момент в конденсатор течет наиболее высокий ток, при этом напряжение на конденсаторе близко к нулю (*согласование по току*). В процессе заряда текущий через конденсатор зарядный ток постепенно снижается согласно графику экспоненциальной функции и при полном заряде обращается в ноль. Состояние, в котором конденсатор полностью заряжен, соответствует согласованию по напряжению с катушкой транспондера.

В отличие от систем FDX/HDX в данном случае обеспечиваются следующие преимущества при питании микросхемы:

- Для питания микросхемы может использоваться полный диапазон напряжения, возникающего на катушке транспондера. Таким образом, по сравнению с дуплексными и полудуплексными системами можно получить в 2 раза большее напряжение питания.
- В данном случае можно легко рассчитать имеющуюся в распоряжении транспондера энергию — она определяется емкостью конденсатора и временем, в течение которого осуществляется передача энергии. Теоретически (!) эти две величины могут быть установлены сколь угодно большими. В дуплексных/полудуплексных системах максимальное потребление микросхемы определяется условием согласования по мощности (т.е. геометрией катушки и напряженностью поля H).

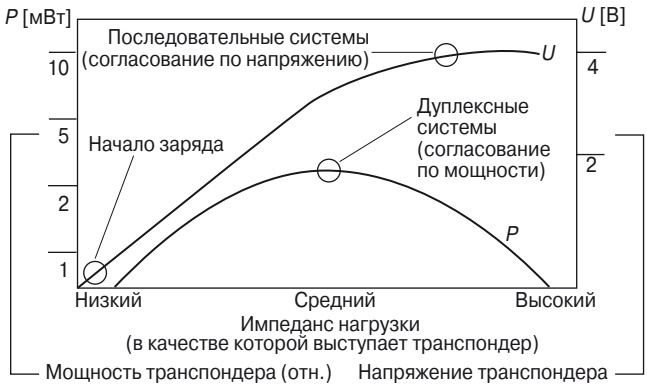


Рис. 3.27. Сравнение индуцируемого на транспондере напряжения для систем FDX/HDX и SEQ.

3.3.1.3. Передача данных от транспондера к считывающему устройству

Полный цикл считывания данных с транспондера в случае последовательных систем состоит из двух различных фаз: первая — фаза заряда конденсатора, вторая — собственно считывание данных.

Блок-диаграмма транспондера последовательной системы с индуктивной связью приведена на **Рис. 3.28**, а график изменения напряжения на конденсаторе транспондера в зависимости от времени — на **Рис. 3.29**.

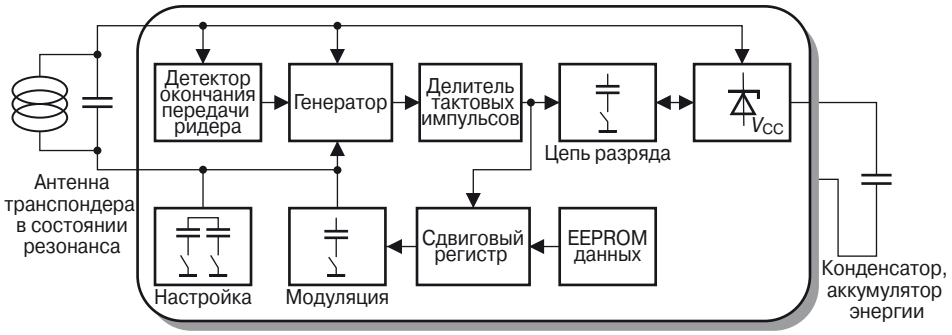


Рис. 3.28. Блок-диаграмма транспондера, входящего в состав системы TIRIS корпорации Texas Instruments (последовательная система с индуктивной связью).

Момент окончания фазы заряда детектируется с помощью детектора, который обнаруживает окончание передачи от считывающего устройства (end-of-burst detector). Этот детектор отслеживает уровень напряжения на катушке транспондера и таким образом может обнаруживать окончание процесса заряда. При обнаружении окончания процесса заряда запускается генератор (источник тактовых импульсов) микросхемы, в котором в качестве элемента колебательного контура используется катушка транспондера. При этом катушка транспондера создает довольно слабое переменное магнитное поле, которое тем не менее может быть обнаружено считывающим устройством. По сравнению с дуплексными/полудуплексными системами это обеспечивает улучшение отношения сигнал/шум примерно на 20 дБ, что позволяет увеличить дальность действия последовательных систем.

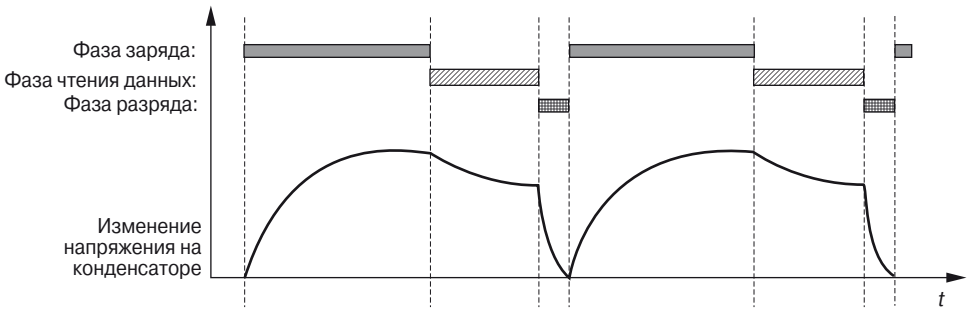


Рис. 3.29. График изменения напряжения на конденсаторе транспондера в зависимости от времени для SEQ-транспондера с индуктивной связью.

Частота, на которой передает данные транспондер, равна резонансной частоте катушки транспондера, которая в процессе своего изготовления настраивается на рабочую частоту считывающего устройства.

Для того чтобы процесс модуляции создаваемого транспондером высокочастотного сигнала происходил без потери энергии, потоком передаваемых данных производится параллельное подключение к резонансному контуру дополнительного модулирующего конденсатора. Благодаря такому переключению на частоту, отличную от резонасной, осуществляется так называемая 2-FSK-модуляция.

После окончания передачи данных транспондер переходит в режим разряда конденсатора, при котором необходимо полностью разрядить конденсатор. Это требуется для надежной перезагрузки при подаче питания (Power-On-Reset — POR), которое производится в начале следующего цикла считывания данных с транспондера.

3.3.2. Транспондеры, использующие поверхностные акустические волны

Компоненты на *поверхностных акустических волнах* (ПАВ) основываются на *пьезоэлектрическом* эффекте[1)], а также на эффекте распространения поверхностных волн (акустических) с достаточно низкой скоростью. Транспондеры, в которых используются ПАВ, в основном работают в микроволновом диапазоне, обычно в диапазоне ISM (Industrial, Scientific, Medical) на частоте 2.45 ГГц.

На пьезоэлектрическую подложку наносится структура планарных электродов, которые образуют *встречно-штыревые преобразователи* (Interdigital) и отражатели (Reflectors). Как правило, в качестве материала для подложки используется *ниобат лития* или же *танталат лития*. Для создания структуры электродов применяется метод фотолитографии, который широко используется в микроэлектронике при производстве интегральных микросхем.

Принципиальная схема транспондера, основанного на эффекте поверхностных волн, представлена на **Рис. 3.30**.

На одном конце ПАВ-транспондера находится сложная структура электродов — встречно-штыревой преобразователь, к общей шине которого подключается *дипольная антенна*, настроенная на рабочую частоту системы. Основной задачей встречно-штыревого преобразователя является преобразование электрических сигналов в поверхностные акустические волны. Если на общую шину подать импульсный электрический сигнал, то благодаря пьезоакустическому эффекту на поверхности подложки между электродами создаются механические напряжения, которые вызывают распространяющиеся в обоих направлениях поверхностные волны (волны Рэлея). Для материалов, которые наиболее часто используются в качестве подложек, рабочая скорость распространения лежит в диапазоне от 3000 до 4000 м/с. Когда поверхностная акустическая волна дости-

---

[1)] В том случае, если кристалл упруго деформируется в определенном направлении, образуются поверхностные заряды, а следовательно, и напряжение (применение — пьезозажигалки). Верно и обратное: если приложить к кристаллу поверхностные заряды, то это приведет к образованию в кристалле эластичных деформаций (применение — пьезозуммер).

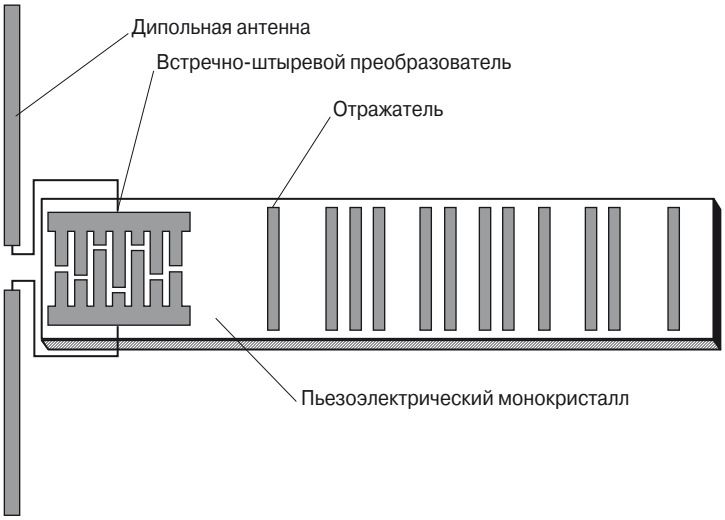


Рис. 3.30. Принципиальная схема транспондера, в котором используется эффект поверхностных акустических волн. На пьезоэлектрический кристалл наносится структура из встречно-штыревых преобразователей и отражателей.

гает встречно-штыревого преобразователя, то благодаря обратному пьезоакустическому эффекту на общей шине возникают электрические сигналы.

На протяжении оставшейся длины транспондера располагаются отдельные электроды. Края этих электродов являются *отражающими полосами*, которые отражают небольшую часть распространяющейся поверхностной волны. Отражающие полосы обычно изготавливаются из алюминия, однако иногда они создаются с помощью протравленных канавок [meinke].

Созданный считывающим устройством высокочастотный *импульс опроса* принимается дипольной антенной транспондера и подается на встречно-штыревой преобразователь, где преобразуется в поверхностную акустическую волну, которая распространяется по подложке в продольном направлении. От каждой из расположенных на подложке отражающих полос часть распространяющейся поверхностно-акустической волны отражается, а оставшаяся часть распространяется до конца подложки, где поглощается.

Часть излучения отражается обратно в направлении к встречно-штыревому преобразователю, где оно преобразуется в последовательность высокочастотных импульсов и передается в окружающее пространство с помощью дипольной антенны. После этого переданная транспондером последовательность сигналов принимается считывающим устройством, при этом количество принятых импульсов соответствует количеству отражающих полос, нанесенных на подложку. Кроме этого, временной промежуток между принятыми считывающим устройством импульсами точно соответствует пространственному расстоянию между отражающими полосами на подложке. Благодаря этому, нанеся на подложку отражающие полосы в определенной последовательности, можно закодировать определенную последовательность битов, которая будет передаваться считывающему устройству.

В связи с тем что скорость распространения поверхностных волн сравнительно невысока, ответный сигнал передается лишь по истечении приблизительно 1.5 мс после момента передачи считывающим устройством первого импульса. Однако это существенно упрощает задачу построения схемы приема ответной последовательности импульсов.

Электромагнитные волны, отраженные от металлических предметов, которые окружают считывающее устройство, распространяются со скоростью света обратно к считывающему устройству. Если транспондер расположен, например, на расстоянии 100 м от считывающего устройства, то отраженный сигнал поступит приблизительно через 0.6 мс (время распространения в прямом и обратном направлении, при этом сигнал может ослабляться более чем на 160 дБ). Таким образом, когда приблизительно через 1.5 мс от транспондера начинает поступать полезный сигнал, все отраженные от окружающих предметов сигналы уже практически полностью затухают, поэтому они не оказывают никакого влияния на прием полезного сигнала от транспондера [dziggel].

Транспондер на ПАВ показан на **Рис. 3.31**.

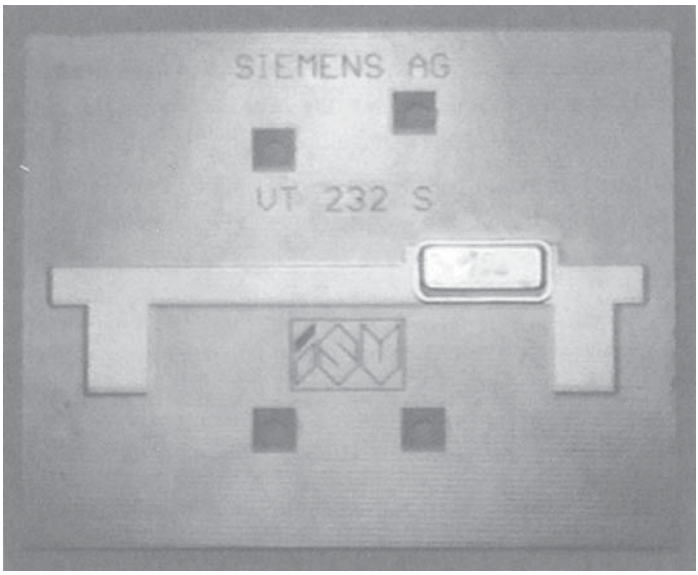


Рис. 3.31. Транспондер на ПАВ (поверхностных акустических волнах), рассчитанный на частоту 2.45 ГГц и использующий микрополосковую антенну. Пьезоэлектрический кристалл расположен в отдельном металлическом корпусе, который защищает его от внешних воздействий (фото: Siemens AG, ZT KM, Мюнхен).

Максимальный объем сохраняемых данных и максимальная скорость передачи данных для транспондера на поверхностно-акустических волнах определяются размером подложки и минимальным расстоянием между отражающими полосами, которое может быть реализовано при их нанесении на подложку. На практике обычно используют данные объемом от 16 до 32 бит и скорость передачи данных 500 Кбит/с [sofis].

Дальность действия систем на основе поверхностных акустических волн в основном определяется мощностью передаваемых считывающим устройством тестовых импульсов, и ее можно оценить с помощью упоминавшегося ранее уравнения из теории радаров (см. подраздел 4.3.3 «Функциональная схема транспондера на ПАВ»). Если использовать мощность, разрешенную для ISM-диапазона (2.45 ГГц), то вполне реально добиться дальности в один или два метра.