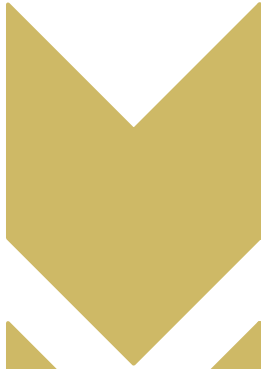


# Технология RFID

# Этапы идентификации:

---



Blank rounded rectangular box for the first step of the identification process.



Blank rounded rectangular box for the second step of the identification process.



Blank rounded rectangular box for the third step of the identification process.



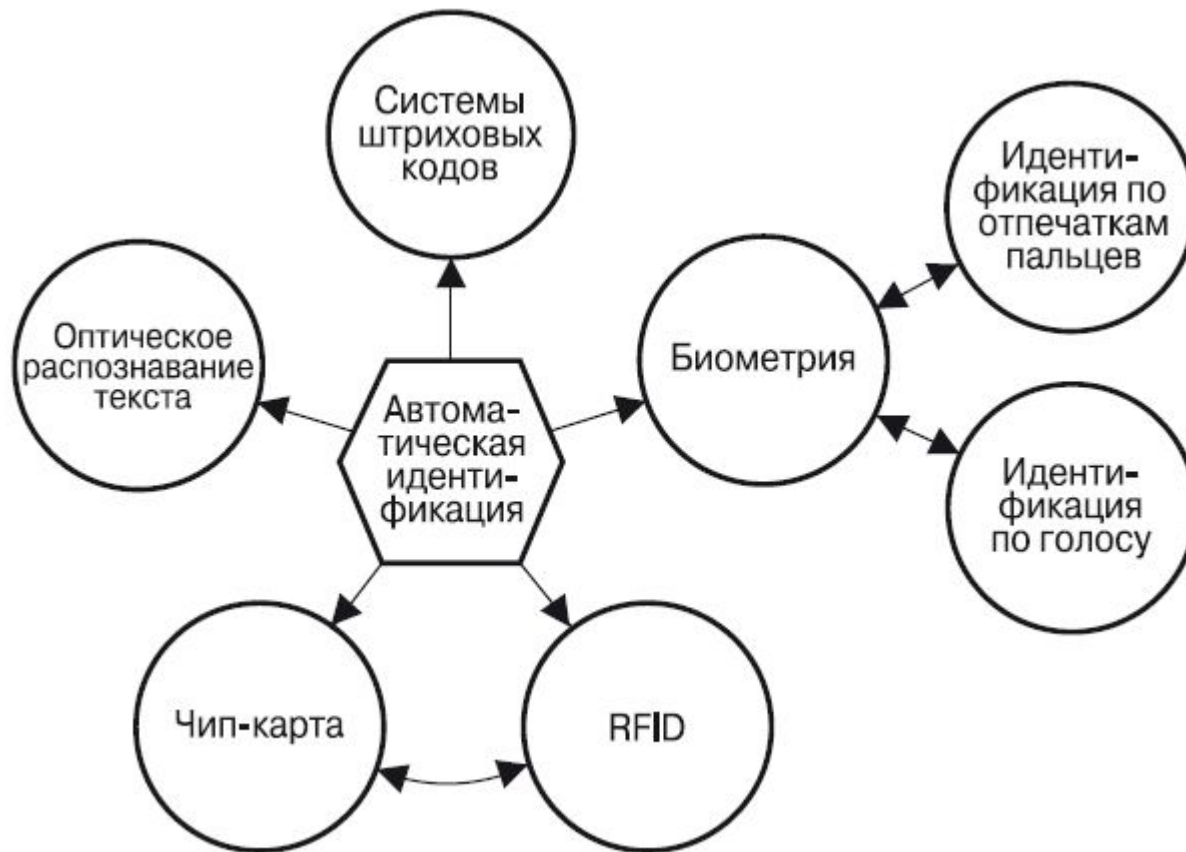
Д  
И  
К  
-  
Ш  
Е  
-  
Ф  
-  
А  
К  
-  
К  
-  
Д  
-  
И  
-  
Ф  
-  
И  
-  
Ф

# Категории аутентификации:



# Основные системы автоматической идентификации

---



# Линейный штриховой

код

---



# Пример штрих-кода в системе EAN

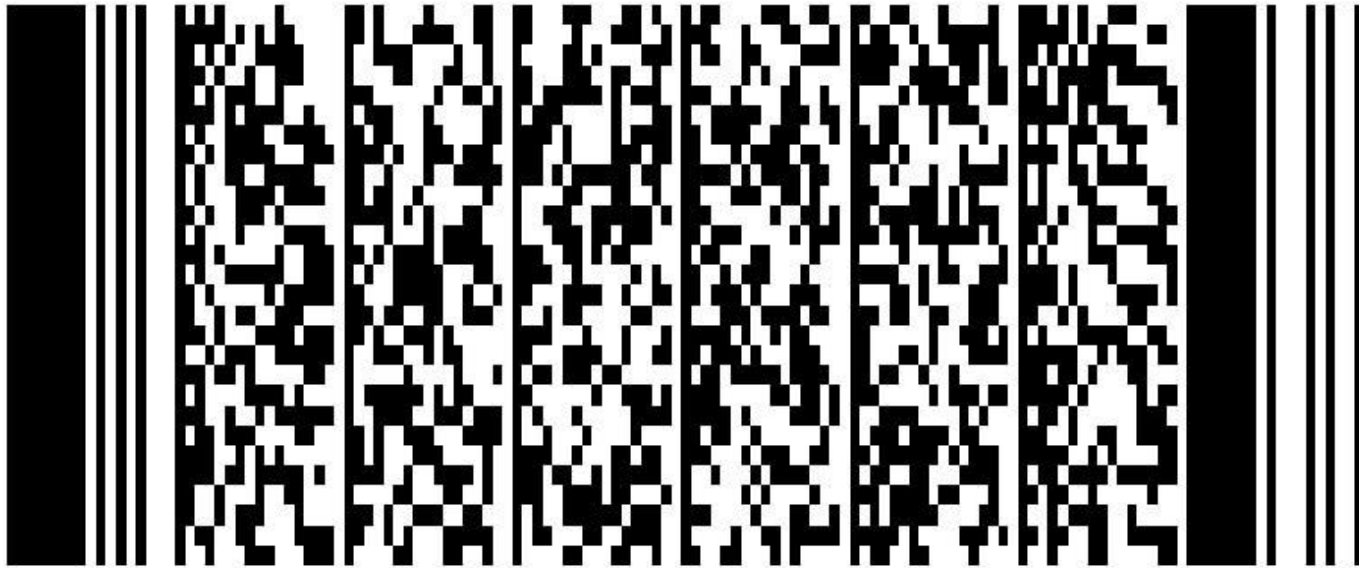
Страна происхождения		Общезональный номер предприятия					Установленный изготовителем индивидуальный код товара					
Landerkennzeichen		Bundesweite Betriebsnummer					Individuelle Artikelnummer des Herstellers					PZ
4	0	1	2	3	4	5	0	8	1	5	0	9
BRD		Fa. Musterwerk, Identstrasse 1, 80001 Munchen					Schokoladenhase 100g					
ФРГ		Адрес предприятия					Наименование товара					Контрольная цифра



# Двухмерный штриховой

код:

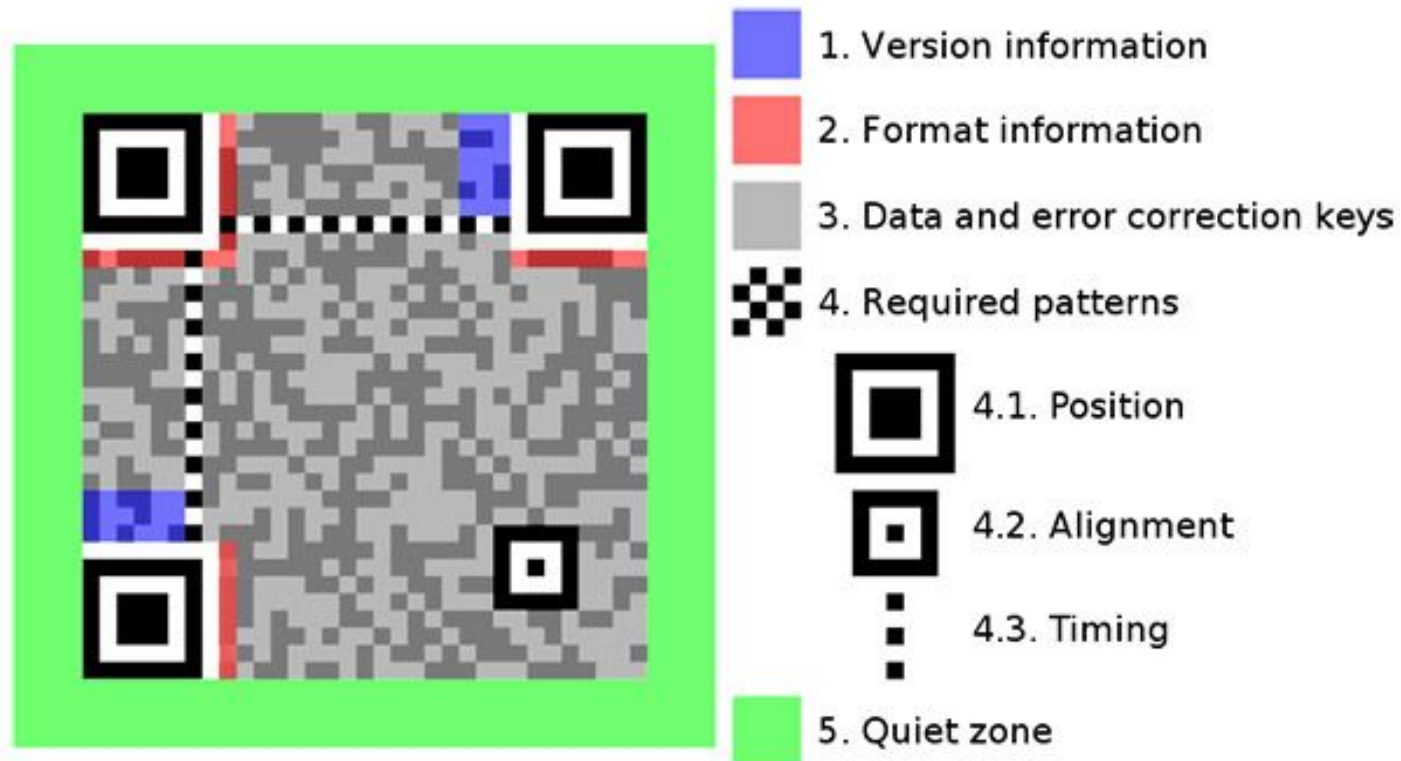
многоступенчатый (stacked code)



# Двухмерный штриховой

КОД:

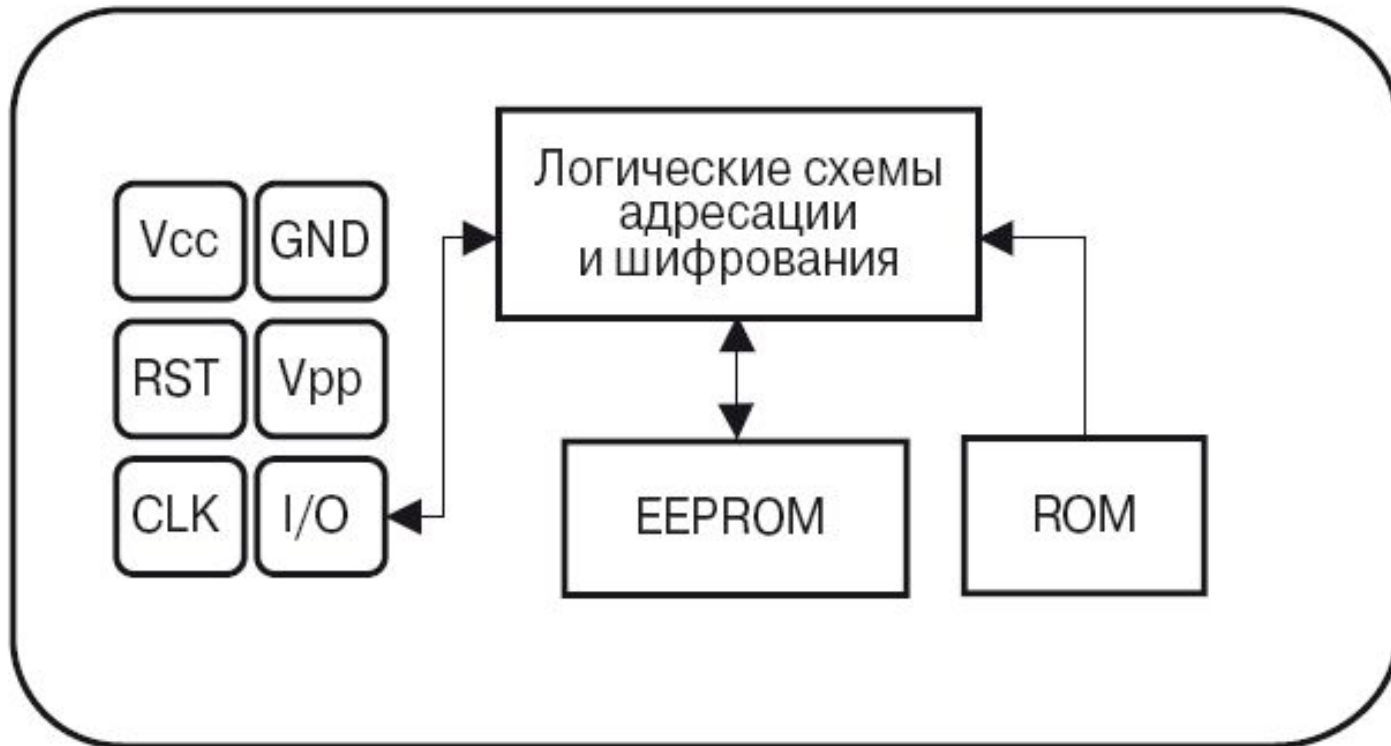
матричный (matrix code)





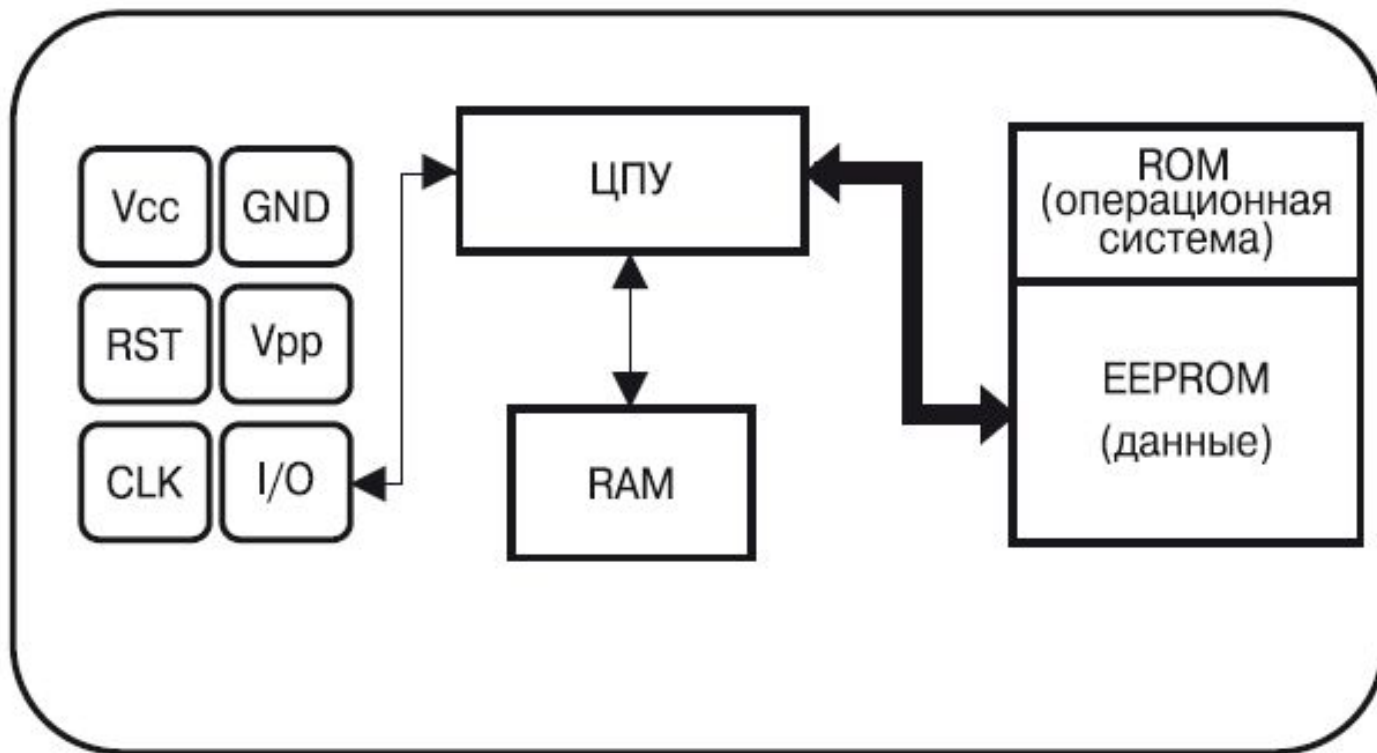
# Архитектура чип-карты

---



# Архитектура микропроцессорной карты

---



# СИСТЕМ

Параметр	BC	OCR	VoiceR	BS	CC	RFID
Объём данных байт	1...100	1...100	--	--	16...64К	16...64К
Плотность данных	Низкая	Низкая	Высокая	Высокая	Очень высокая	Очень высокая
Читаемость для устройства	Хорошая	Хорошая	Высокозатратная	Высокозатратная	Хорошая	Хорошая
Читаемость для человека	Относительная	Легко	Легко	Тяжело	Невозможно	Невозможно
Внешние влияния	Очень сильное	Очень сильное	--	--	Возможно (контакты)	Не влияет
Влияние препятствий	Полная неработоспособность	Полная неработоспособность	--	Возможно	--	Не влияет
Ограничение на положение и направление	Небольшое	Небольшое	--	--	Определяется конструкцией разъёма	Нет
Возможность несанкционированного доступа	Легко	Легко	Возможно (фонограмма)	Невозможно	Невозможно	Невозможно
Скорость считывания	Низкая ~ 4с	Низкая ~ 3с	Очень низкая > 5с	Очень низкая > 5с	Низкая ~ 4с	Очень высокая ~ 0.5с
Максимальное удаление	0...50 см	Менее 1 см (сканер)	0...50 см	Непосредственный контакт	Непосредственный контакт	0...5 м

# Преимущества RFID:

---

- Работа с любыми группами товаров
  - Считывание бесконтактным способом
  - Данные могут дополняться
  - Большой объём данных
  - Большая скорость записи
  - Секретность данных
  - Долговечность
  - Защищённость от окружающей среды
- 



# Недостатки RFID:

---

- Невозможность размещения под электрическими и электропроводными поверхностями
  - Взаимные коллизии
  - Подверженность помехам от электромагнитных полей
  - Стоимость изготовления
  - Влияние на здоровье человека ??
- 



# Сферы применения:

---

- - Access control
  - - Baggage identification
  - - Automotive immobilization
  - - Document tracking
  - - Vehicle identification
  - - Logistic/supply chain
  - - Wireless commerce
  - - Product authentication
  - - Ticketing
- 



# Компоненты RFID

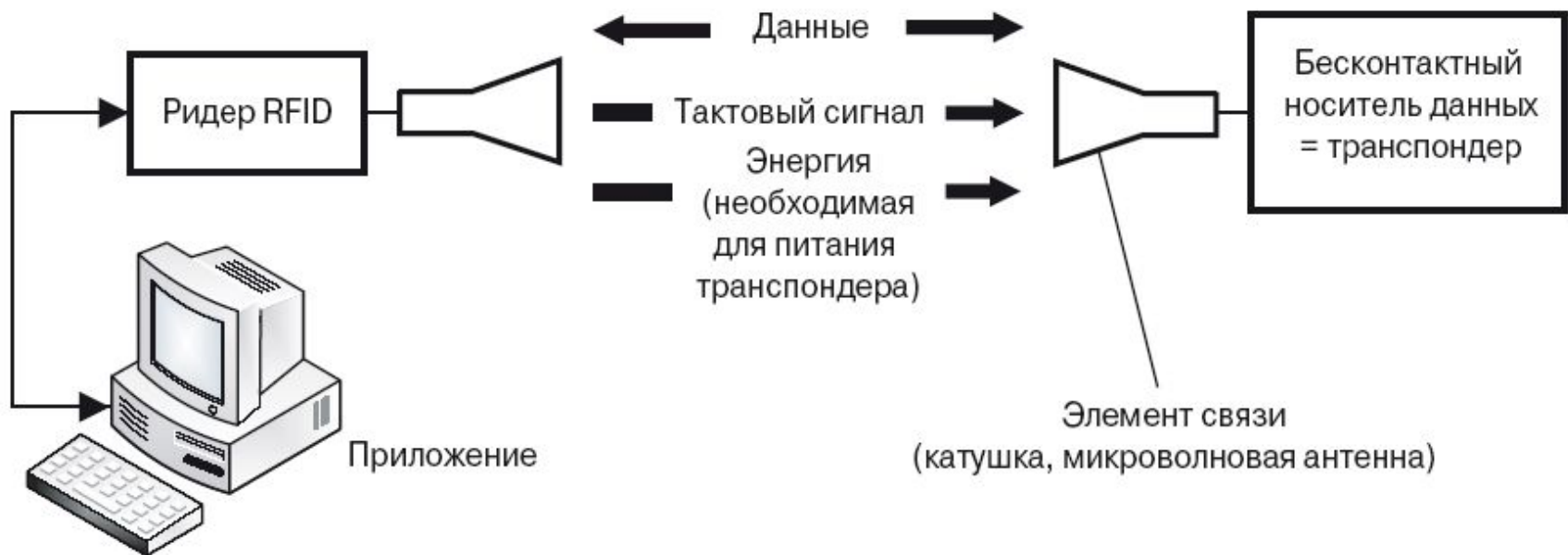
---

- Считывающее устройство (ридер)
- Антенна
- Радиочастотная метка



# Основные компоненты RFID

---





# Классификация RFID:

---

- По принципу работы
  - По объёму передаваемых данных
  - По наличию шифрования
  - По типу носителя данных
  - По типу управления
  - По наличию питания
  - По частотному диапазону
  - По способу записи данных
  - По способу передачи данных (ответ транспондера)
- 
- ▣ По сложности обработки

# Принцип работы:

---

## Full Duplex – FDX

• дуплексные системы

## Half Duplex – HDX

• полудуплексные системы

## Sequential - SEQ

• последовательные системы

---



# Наличие шифрования:

---



У  
Н  
И  
К  
а  
Л  
И  
Ф  
Р  
И  
Р  
О  
В  
А  
Н  
И  
Е  
Н  
И  
Д  
Е  
Н  
Т  
И  
Ф  
И  
К  
а

# Хранение данных:

---

## **EEPROM**

Electrically Erasable Programmable  
Read-Only Memory

## **SRAM**

Static Random Access Memory

## **ПАВ**



# Классификация RFID:

---

- По принципу работы ✓
  - По объёму передаваемых данных ✓
  - По наличию шифрования ✓
  - По типу носителя данных ✓
  - По типу управления
  - По наличию питания
  - По частотному диапазону
  - По способу записи данных
  - По способу передачи данных (ответ транспондера)
- 
- ▣ По сложности обработки

# Частотный диапазон:

---

**LF**

•30...300 Hz

**HF/RF**

•3...30 MHz

**UHF**

•0,3...3GHz

---



# Способы записи:

---

**Read only**

**WORM**

write once read many

**R/W**

read/write

---



# Передача данных:

---

- Отражение/рассеяние
- Модуляционная нагрузка
- Субгармоники
- Поверхностные волны





# Обработка информации:

---

- Low-end systems
- Mid-end systems
- High-end systems



# Характеристики RFID

## СИСТЕМЫ:

---

### Физическое взаимодействие:

- электрическое
- магнитное

### РАСЧЕТ РАБОЧЕЙ ДАЛЬНОСТИ

### Рабочая дальность

- Close-coupling
- Remote-coupling
- Long-range



# Критерии выбора RFID СИСТЕМЫ:

---

- Рабочая частота
- Дальность действия
- Требования к безопасности
- Объём памяти



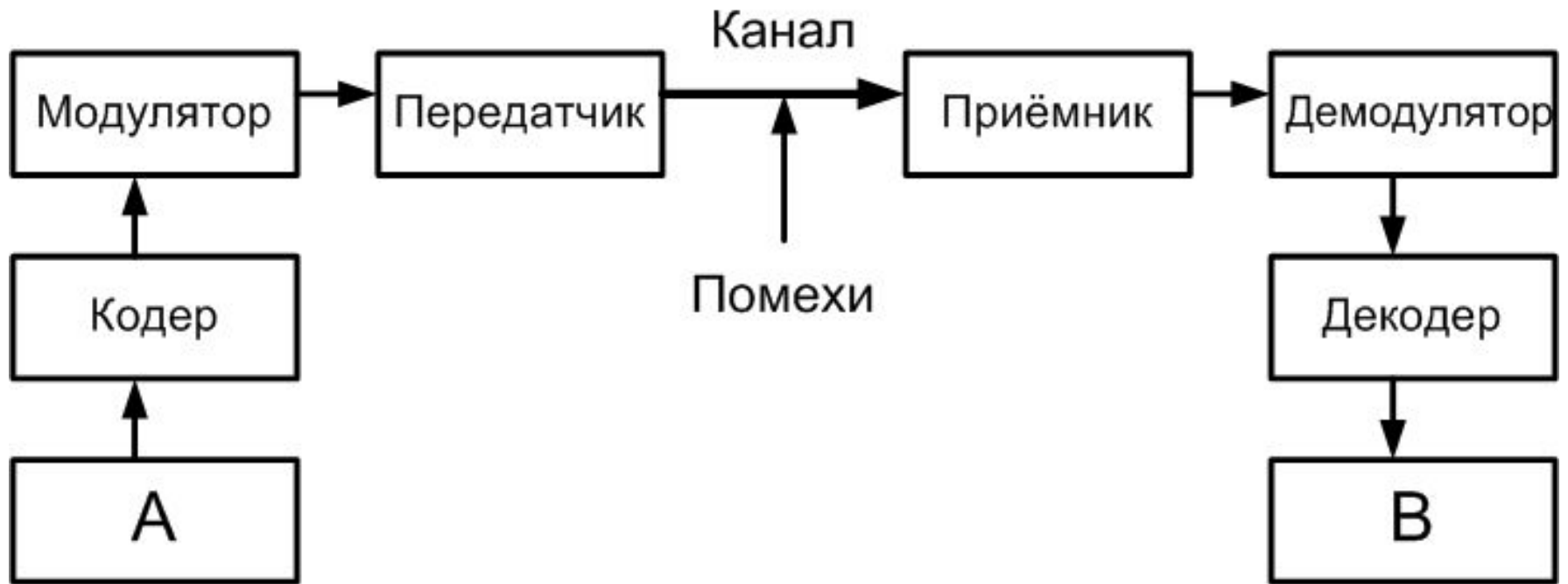
# Дальность действия

---

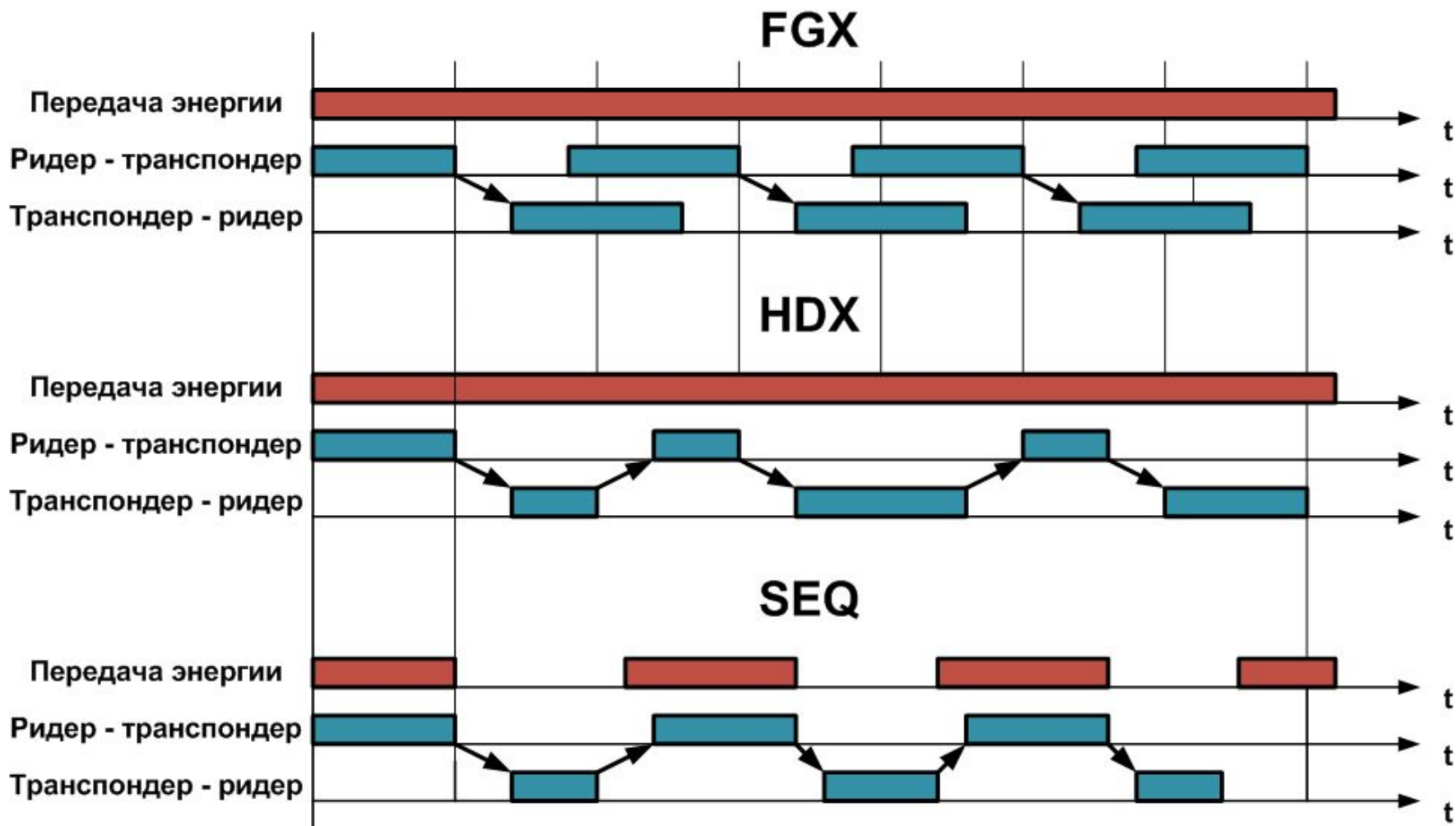


# Структурная схема информационной системы

---

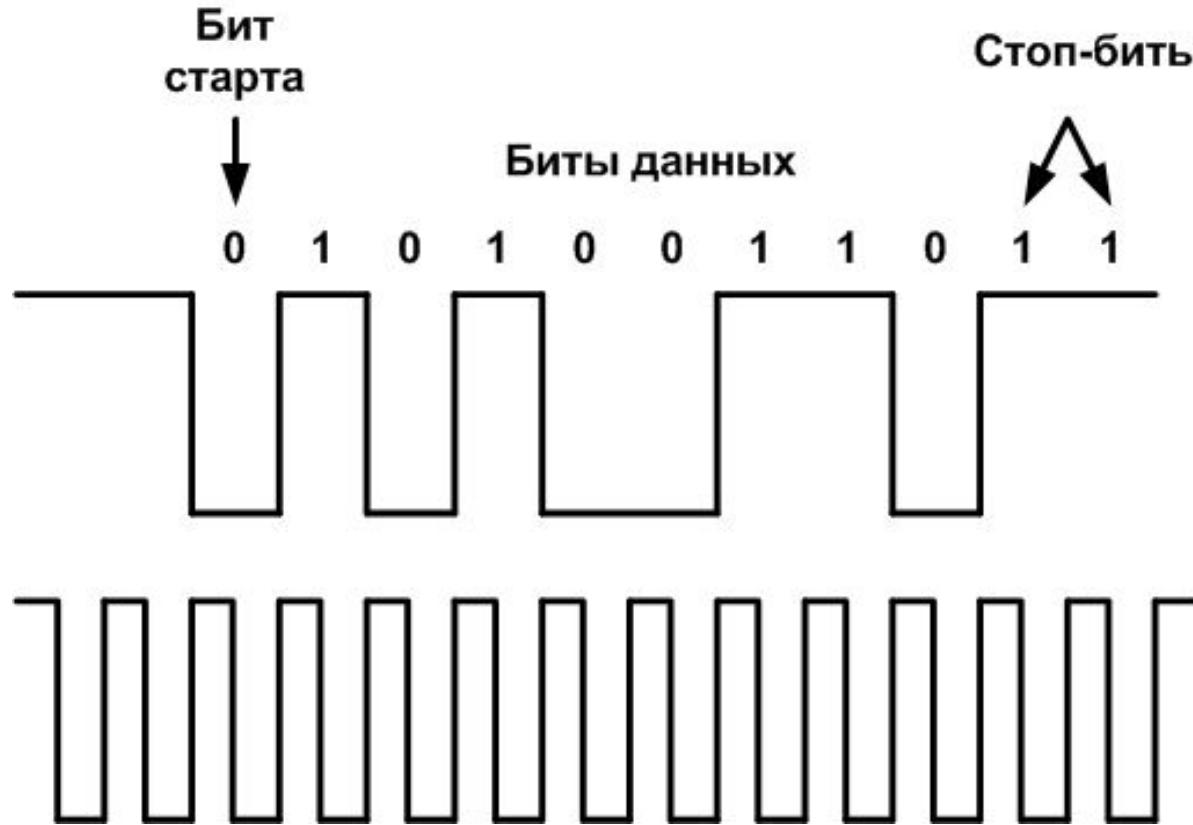


# Временные диаграммы

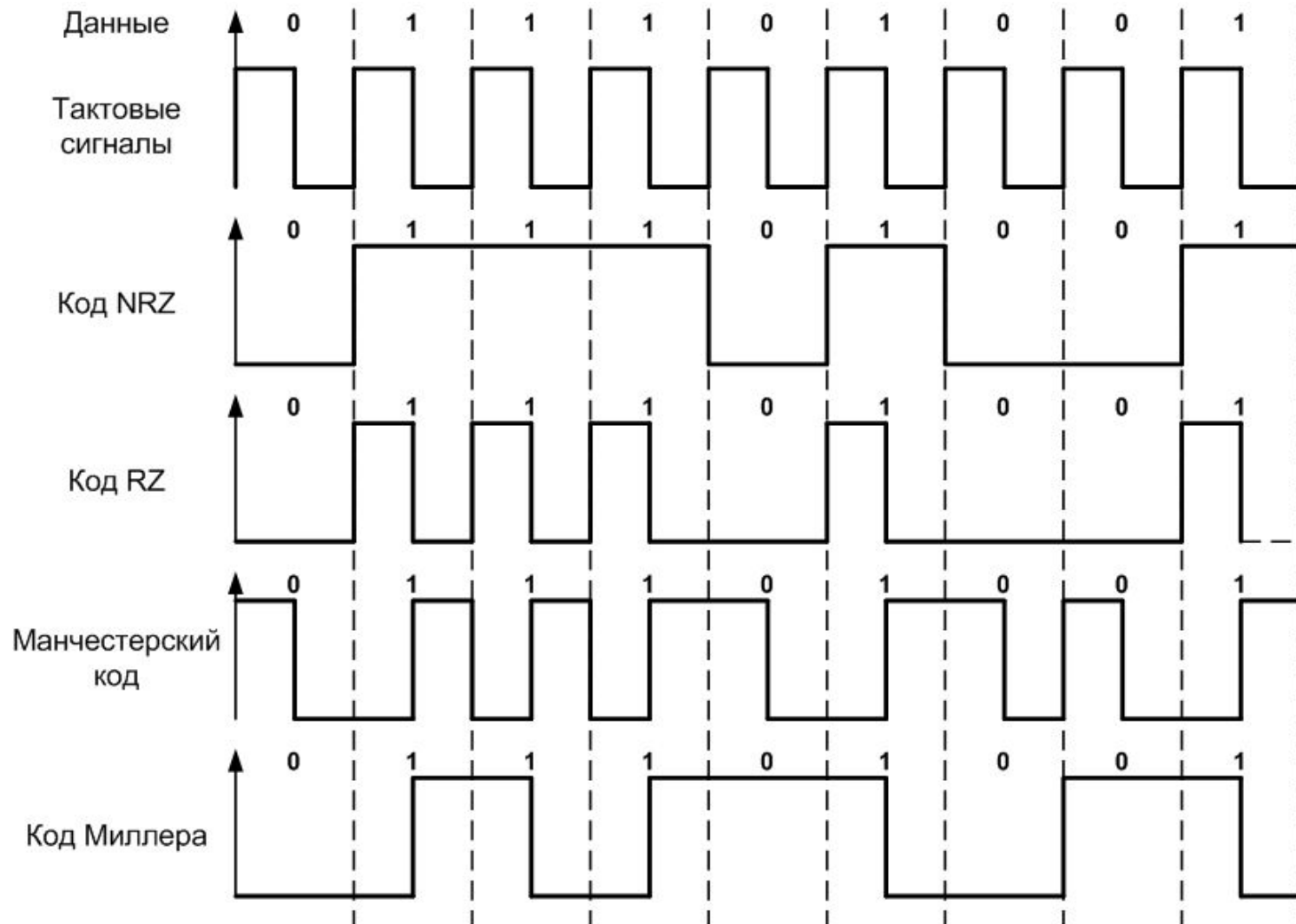


# Асинхронный режим

---



# Цифровые коды





# Модуляция сигналов

---

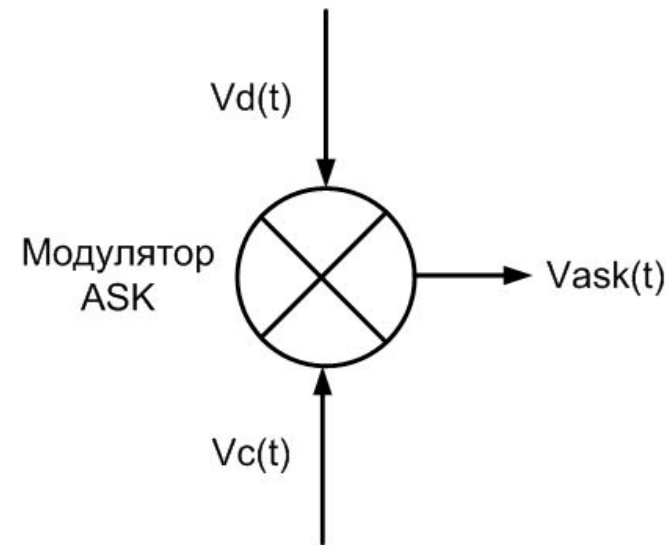
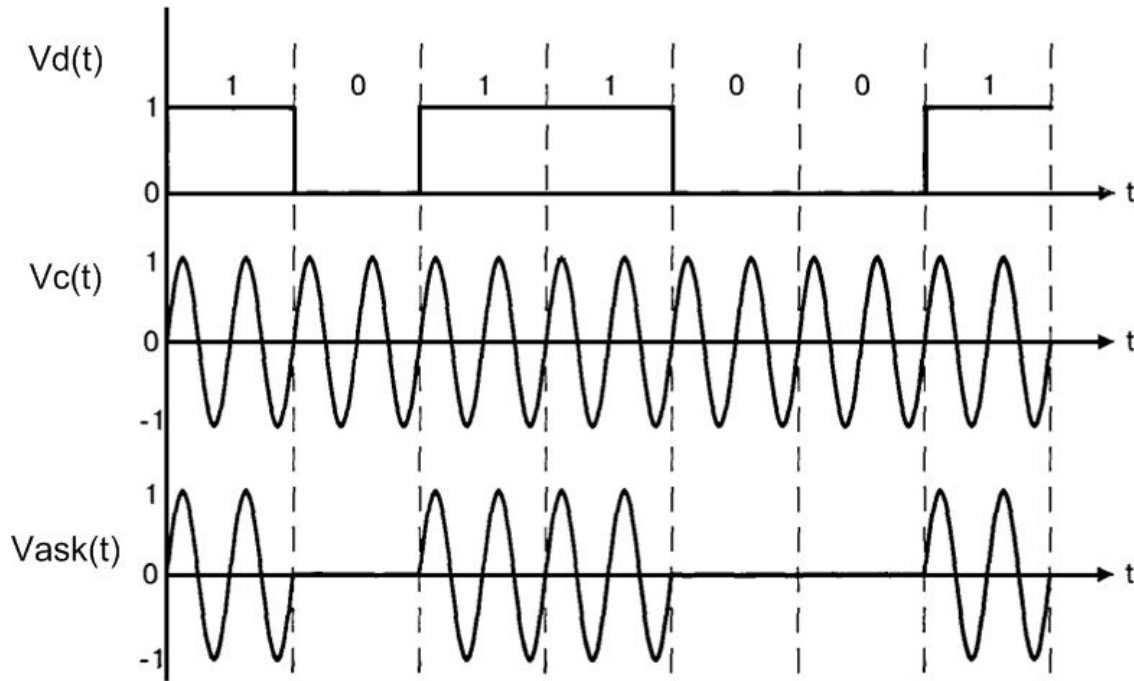
$$x(t) = A(t) \cos[\omega_0 t + \theta(t)]$$

- ASK
- FSK
- PSK

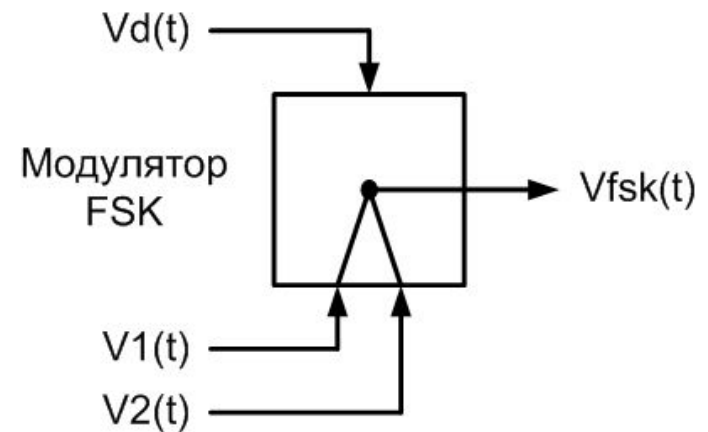
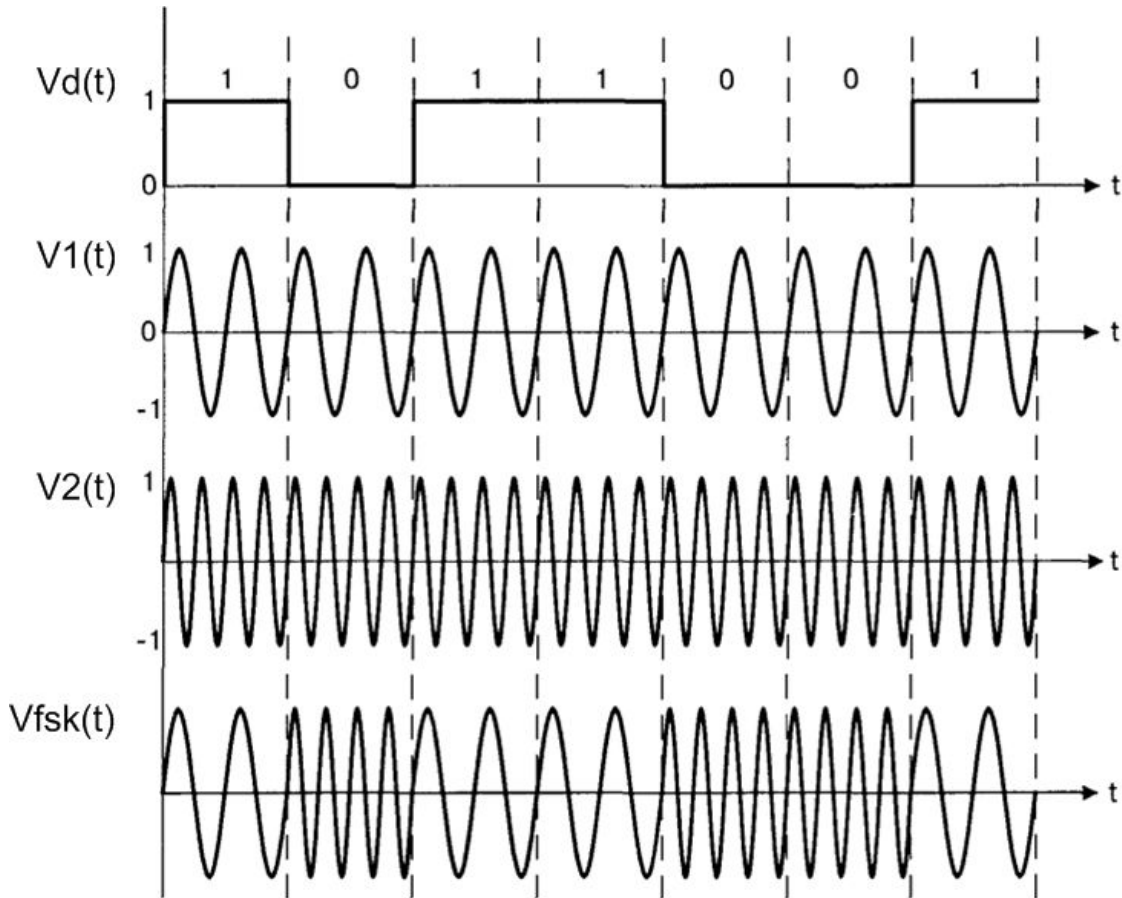


# Амплитудная модуляция

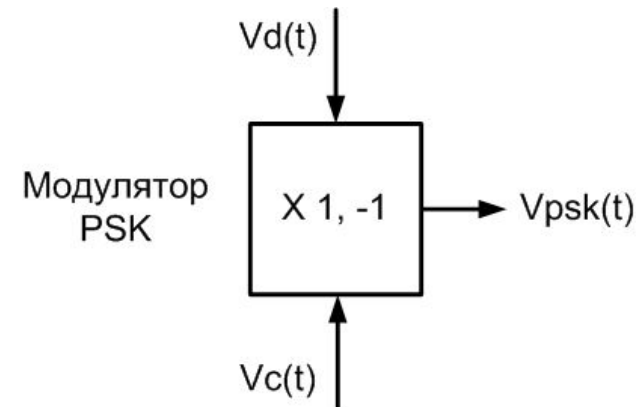
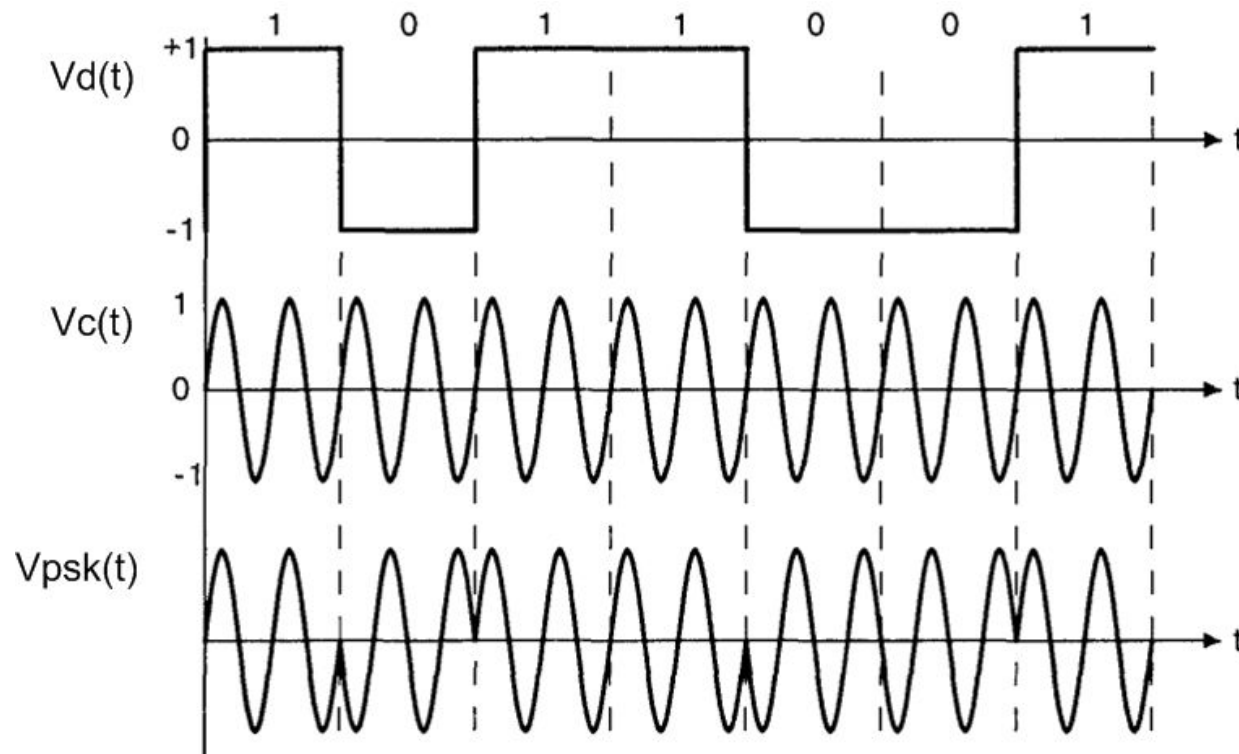
---



# Частотная модуляция



# Фазовая модуляция



# Транспондеры

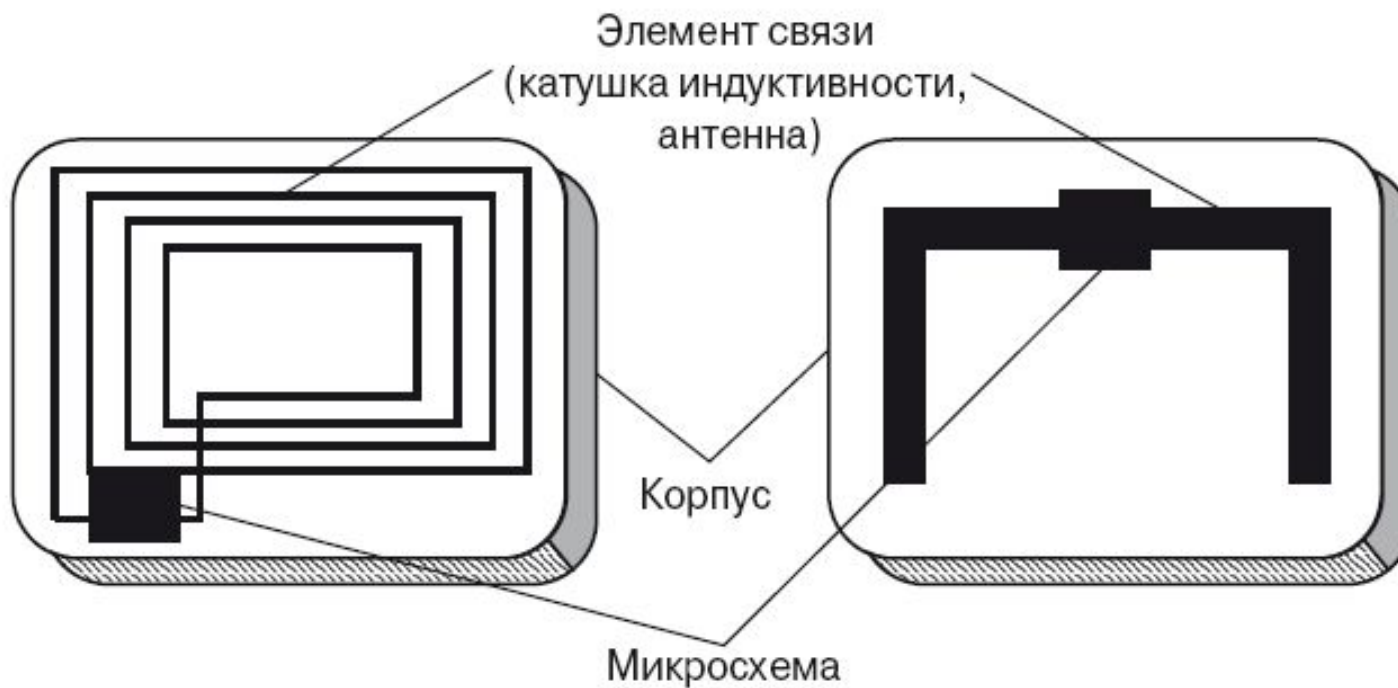
# Конструкции транспондеров:

---



# Транспондер

---



# Одноритмные транспондеры

---

- LC-контур
- Микроволновые системы
- Делитель частоты
- Электромагнитные системы
- Акустомагнитные системы





# ИНДУКТИВНОСТЬ

---

$$L = N^2 \mu_0 R \times \ln\left(\frac{2R}{d}\right)$$

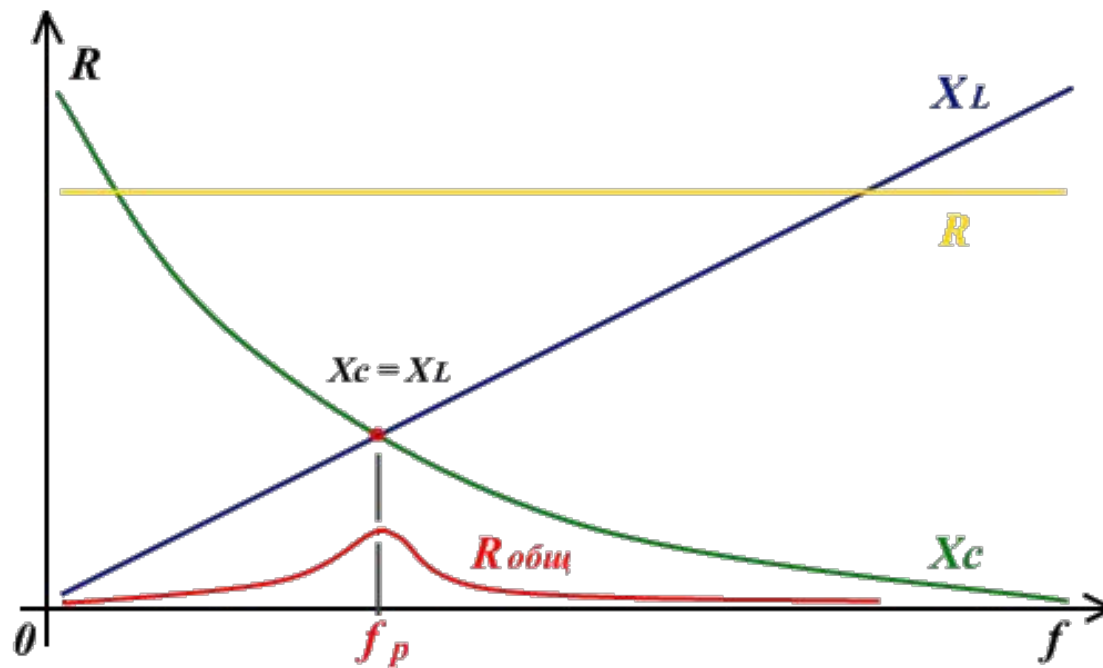
$$k = \frac{M}{\sqrt{L_1 \times L_2}}$$



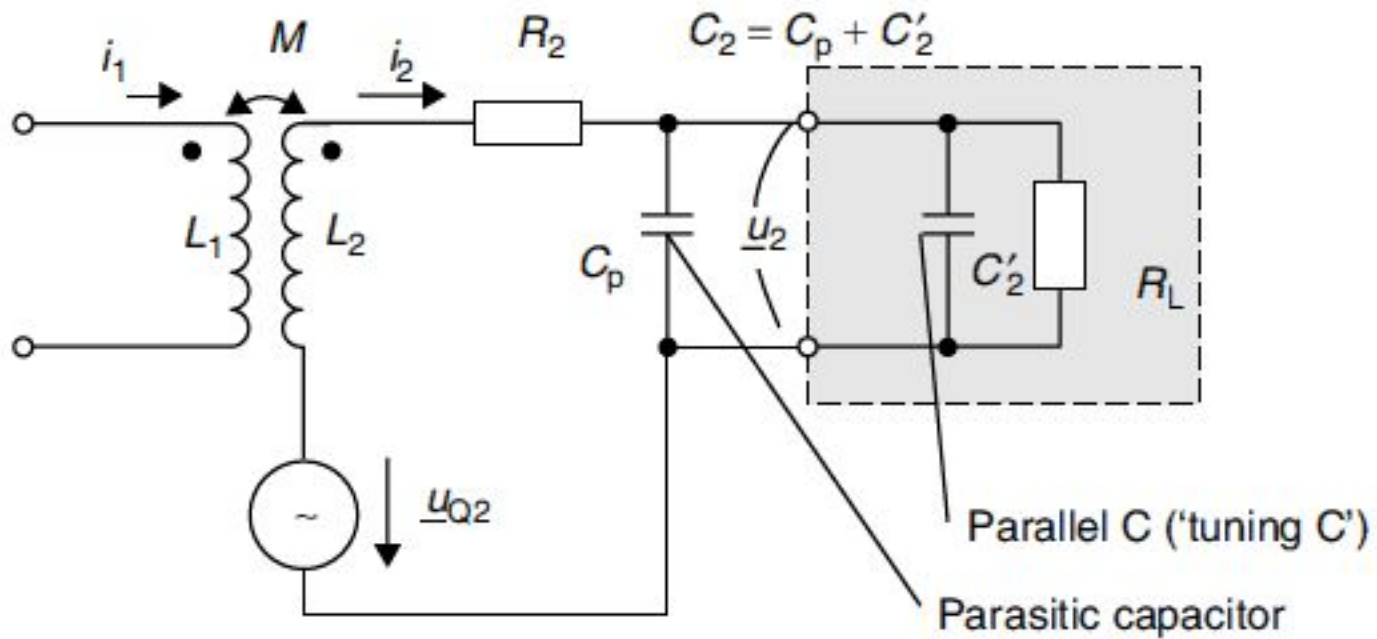
# Резонанс

---

$$f = \frac{1}{2\pi\sqrt{LC}}$$



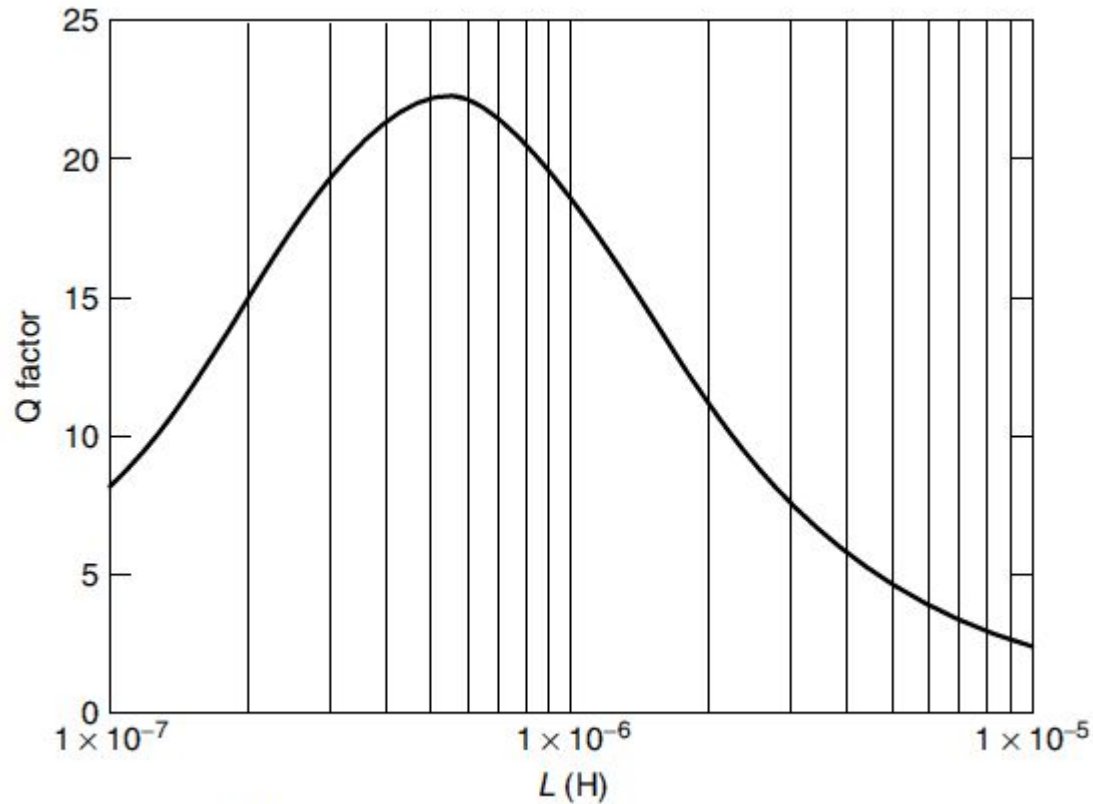
# Эквивалентная схема с магнитной связью



$$u_2 = \frac{j\omega M \cdot i_1}{1 + (j\omega L_2 + R_2) \cdot \left( \frac{1}{R_L} + j\omega C_2 \right)}$$



# Добротность контура

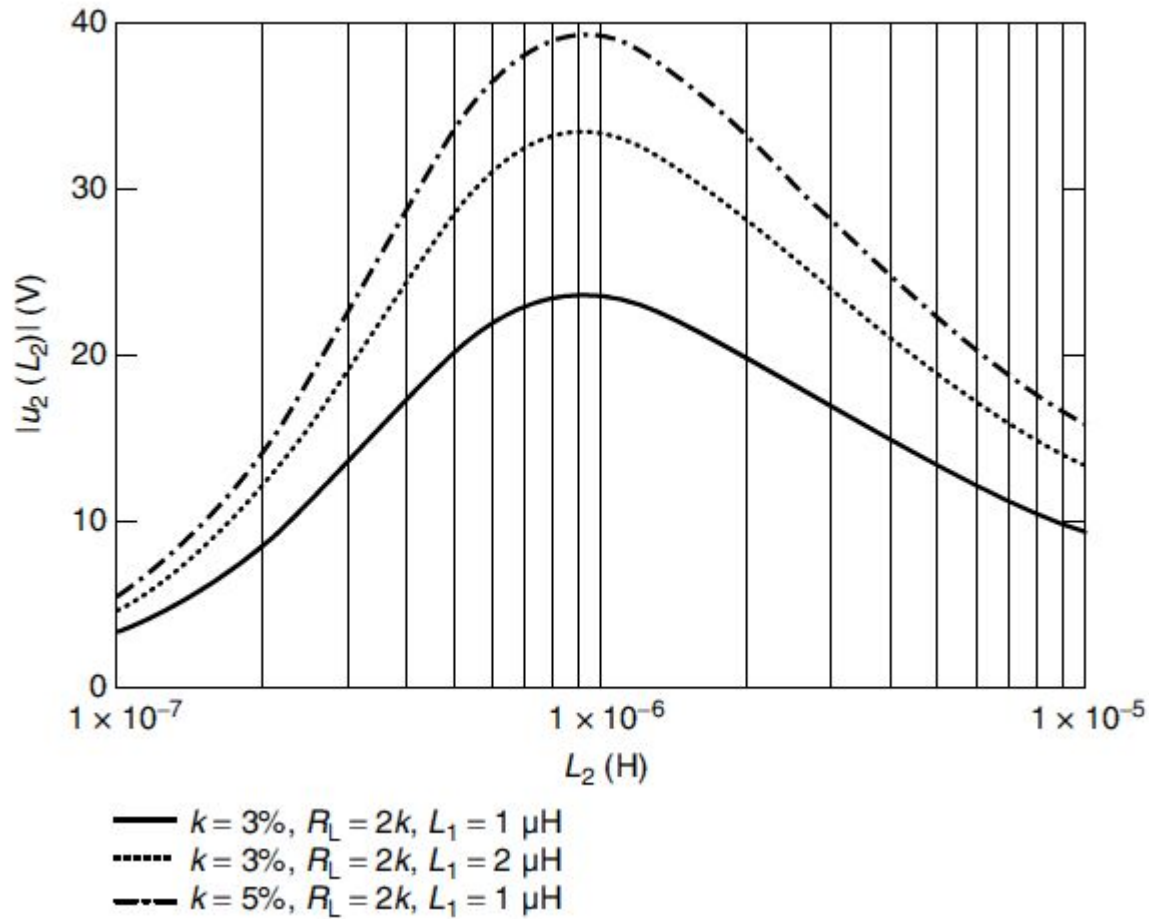


—  $Q = f(L_2)$

$$Q = \frac{1}{R_2 \cdot \frac{\sqrt{C_2}}{L_2} + \frac{1}{R_L} \cdot \frac{\sqrt{L_2}}{C_2}} = \frac{1}{\frac{R_2}{\omega L_2} + \frac{\omega L_2}{R_L}}$$



# Зависимость $U$ от $L$ катушки



# Минимальная чувствительность

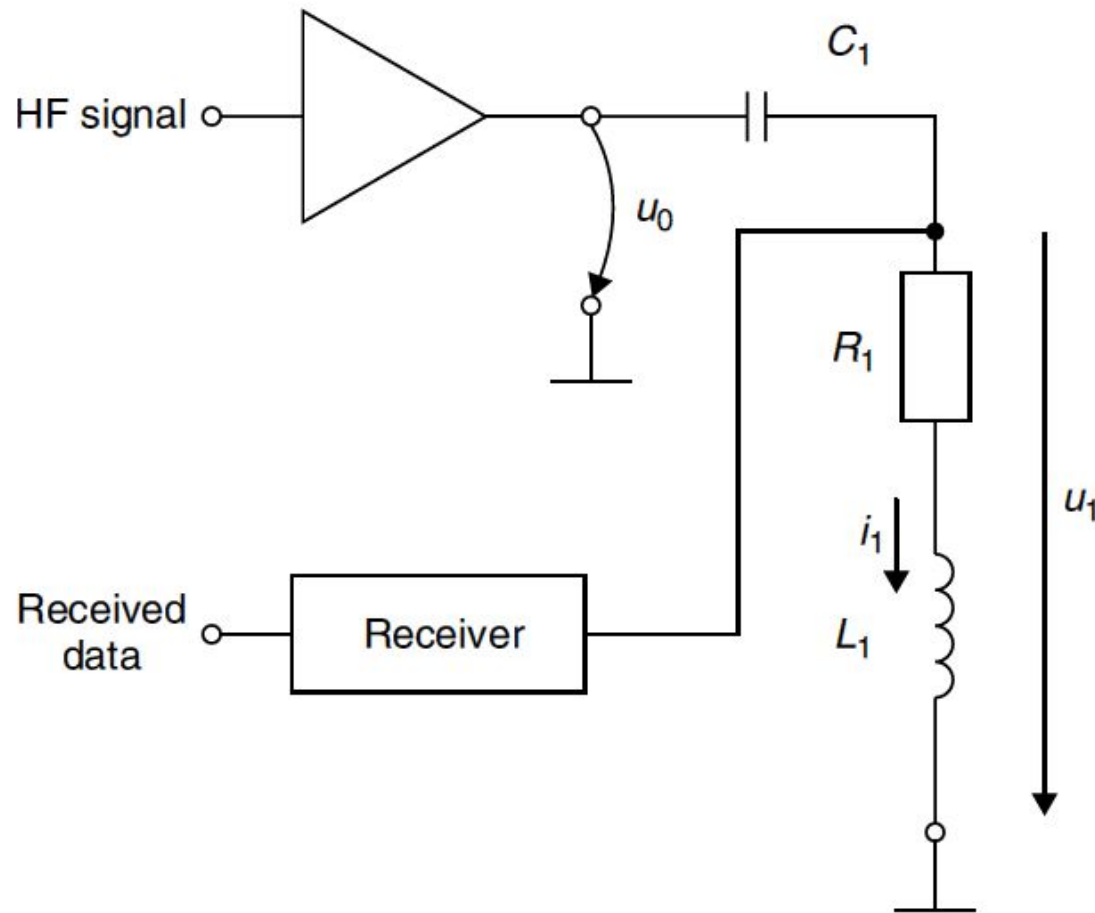
---

$$H_{\min} = \frac{u_2 \cdot \sqrt{\left(\frac{\omega L_2}{R_L} + \omega R_2 C_2\right)^2 + \left(1 - \omega^2 L_2 C_2 + \frac{R_2}{R_L}\right)^2}}{\omega \cdot \mu_0 \cdot A \cdot N}$$



# Эквивалентная схема считывателя

---



# Трансформированный импеданс

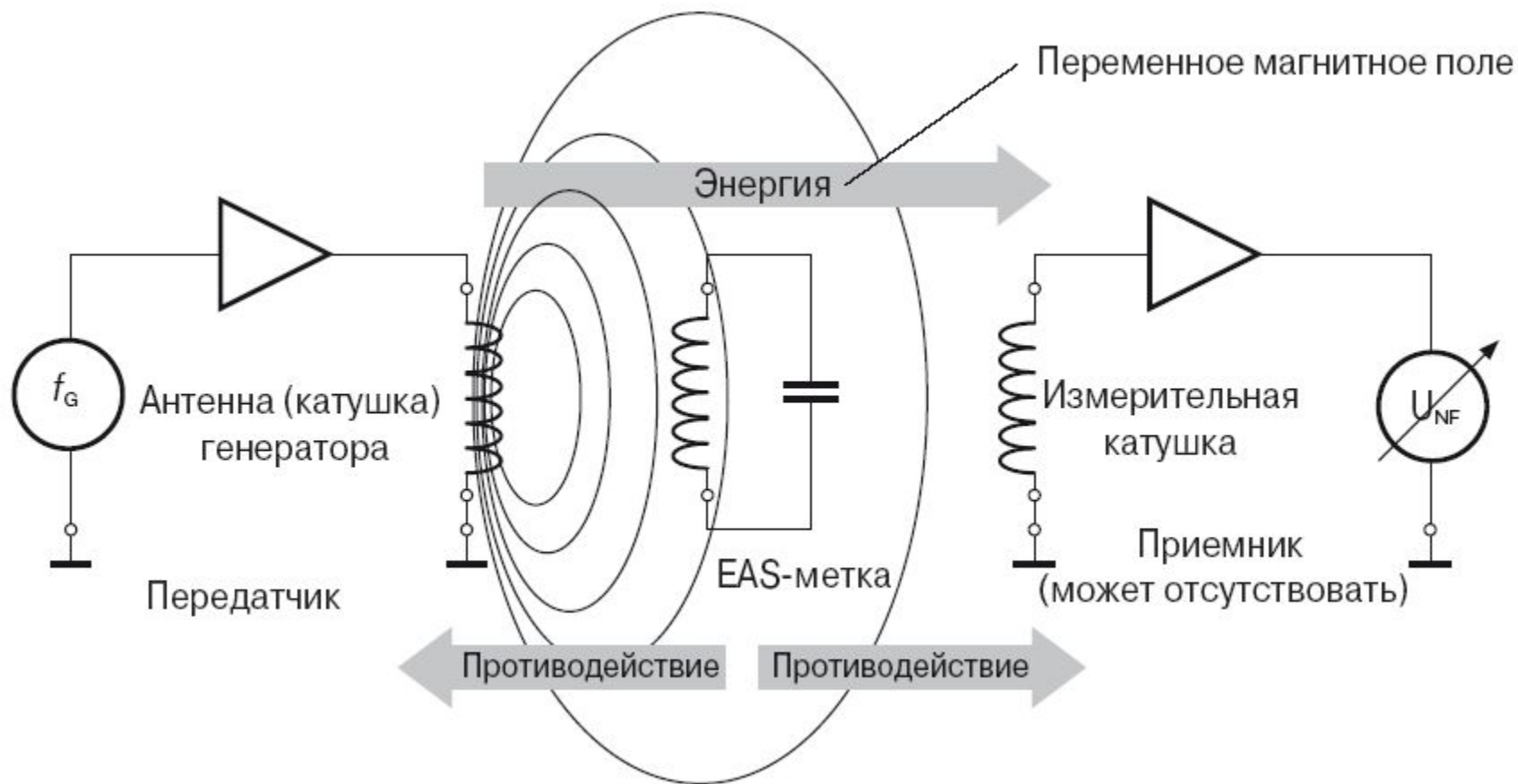
---

$$Z_T' = \frac{\omega^2 k^2 L_1 L_2}{R^2 + j\omega L_2 + \frac{R_L}{1 + j\omega R_L C_2}}$$





# Принцип действия радиочастотного EAS-транспондера



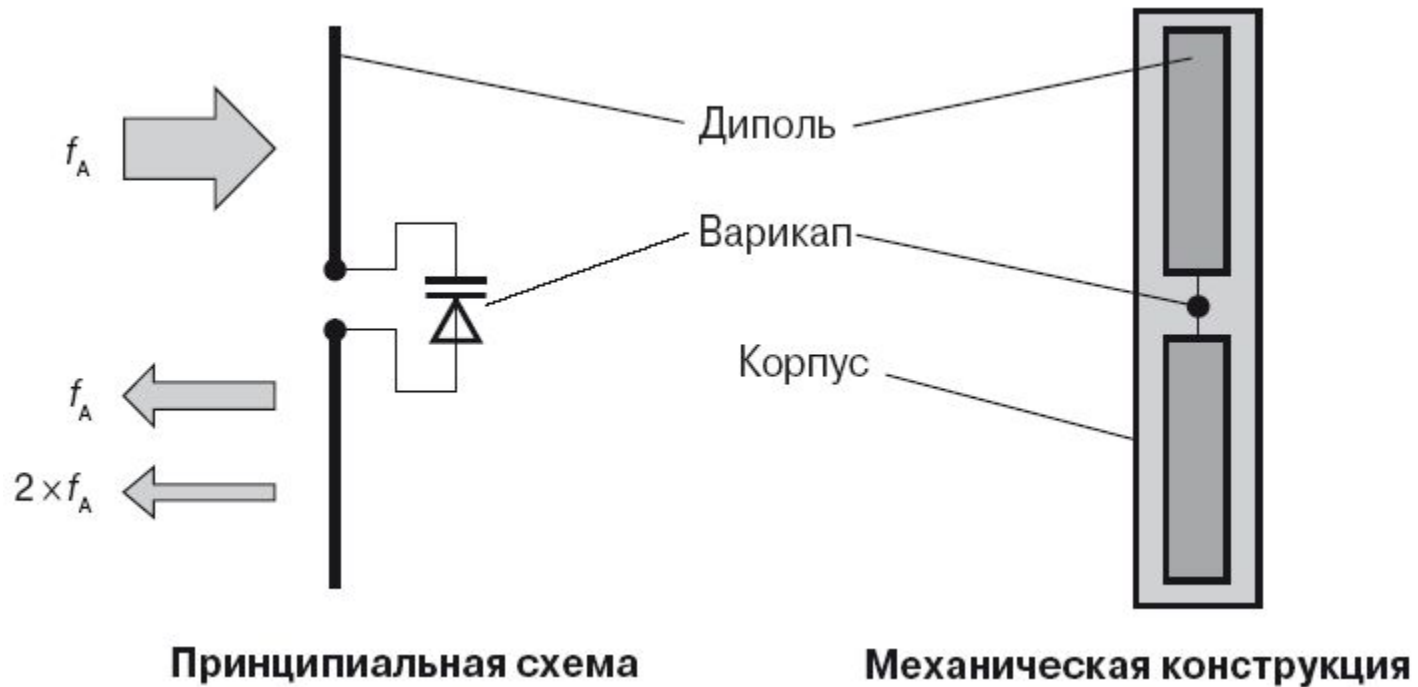
# Рамочная антенна

---

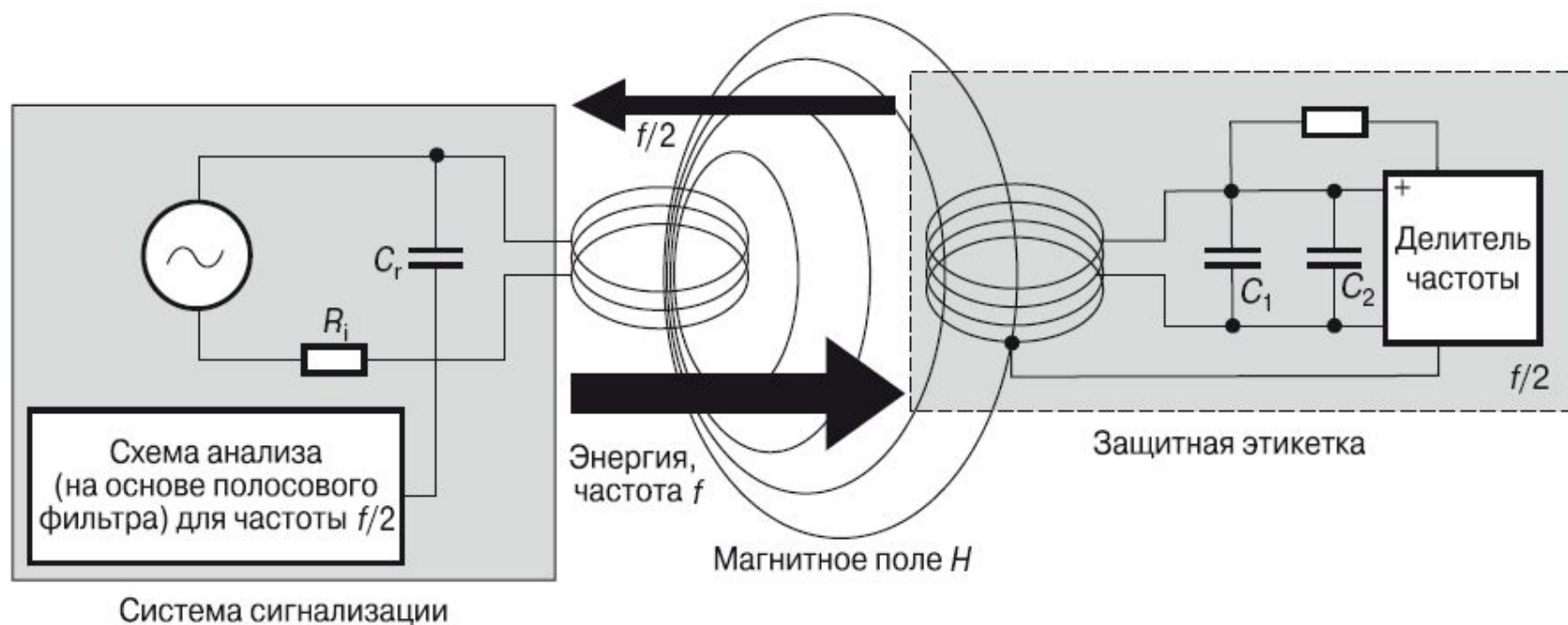


# Микроволновая система

---

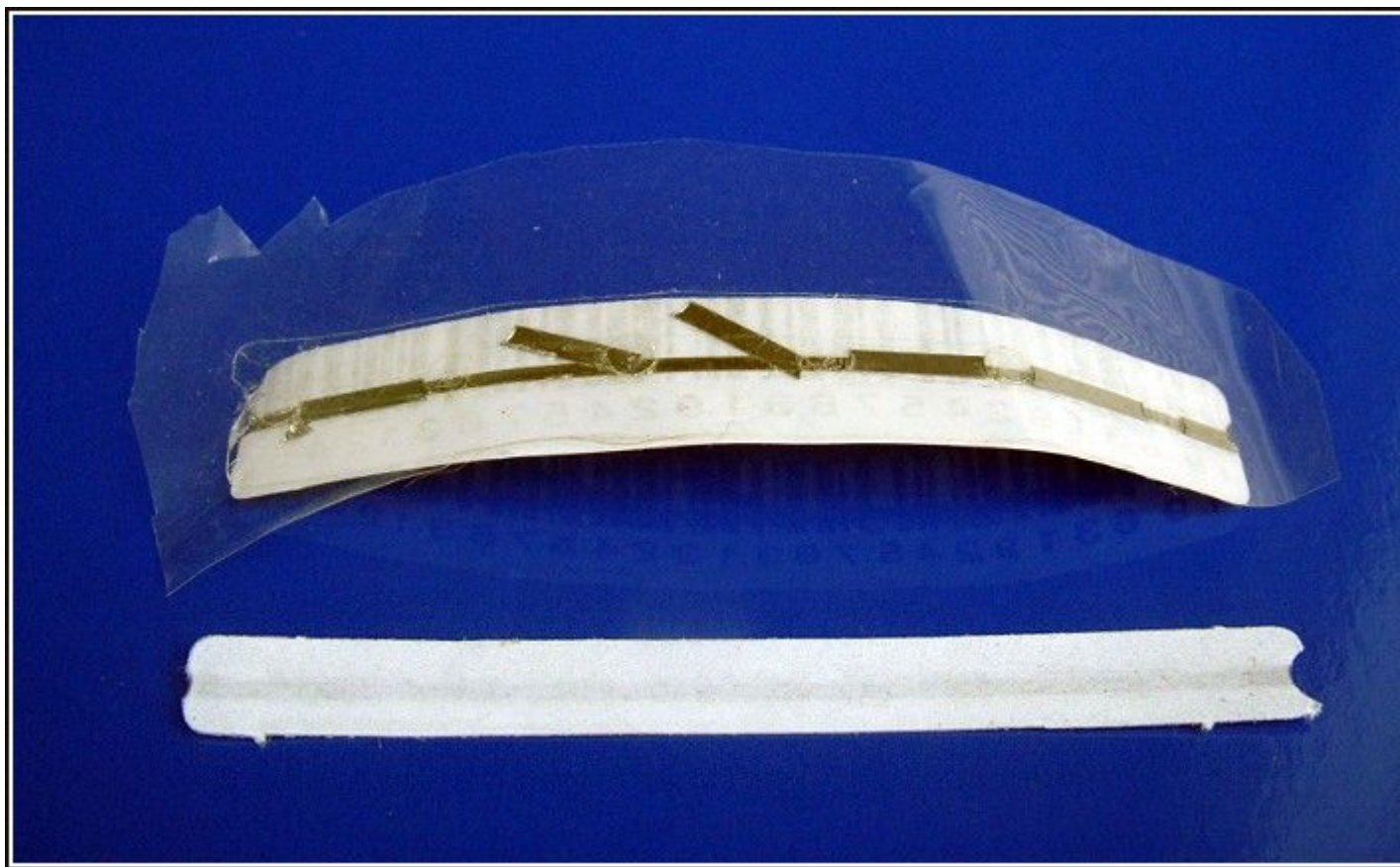


# Транспондер с делением частоты

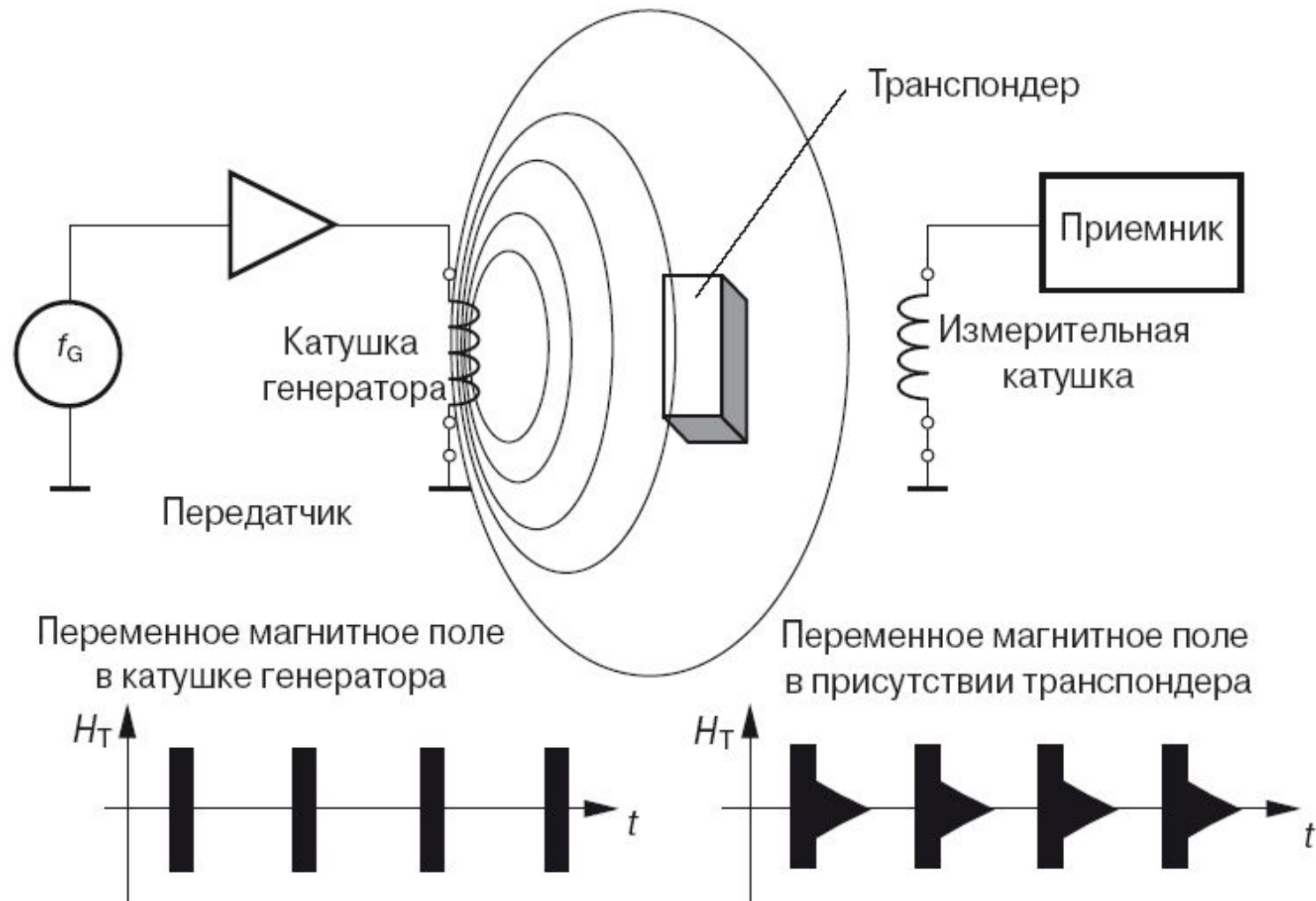


# Электромагнитная метка

---

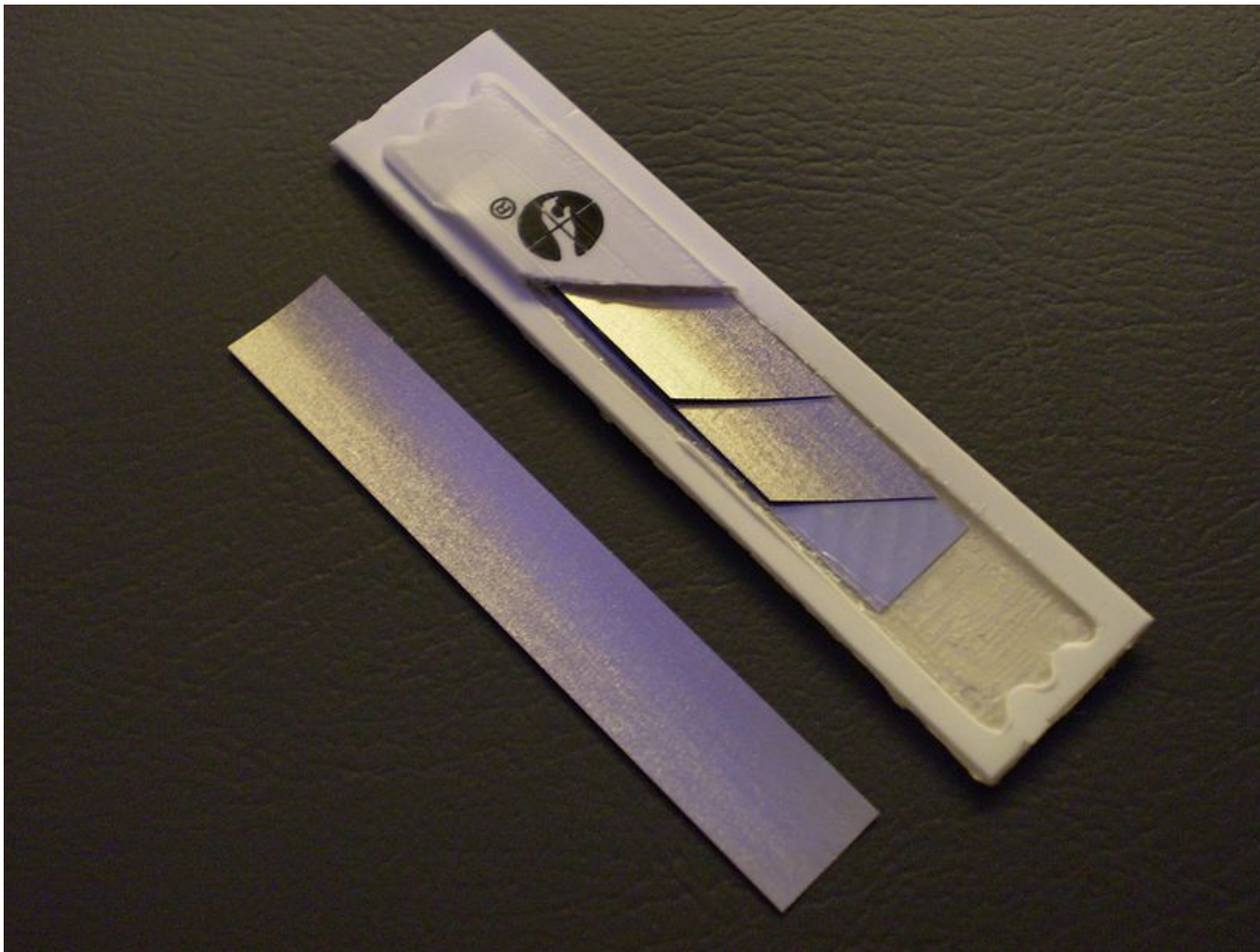


# Акустоманнитная система

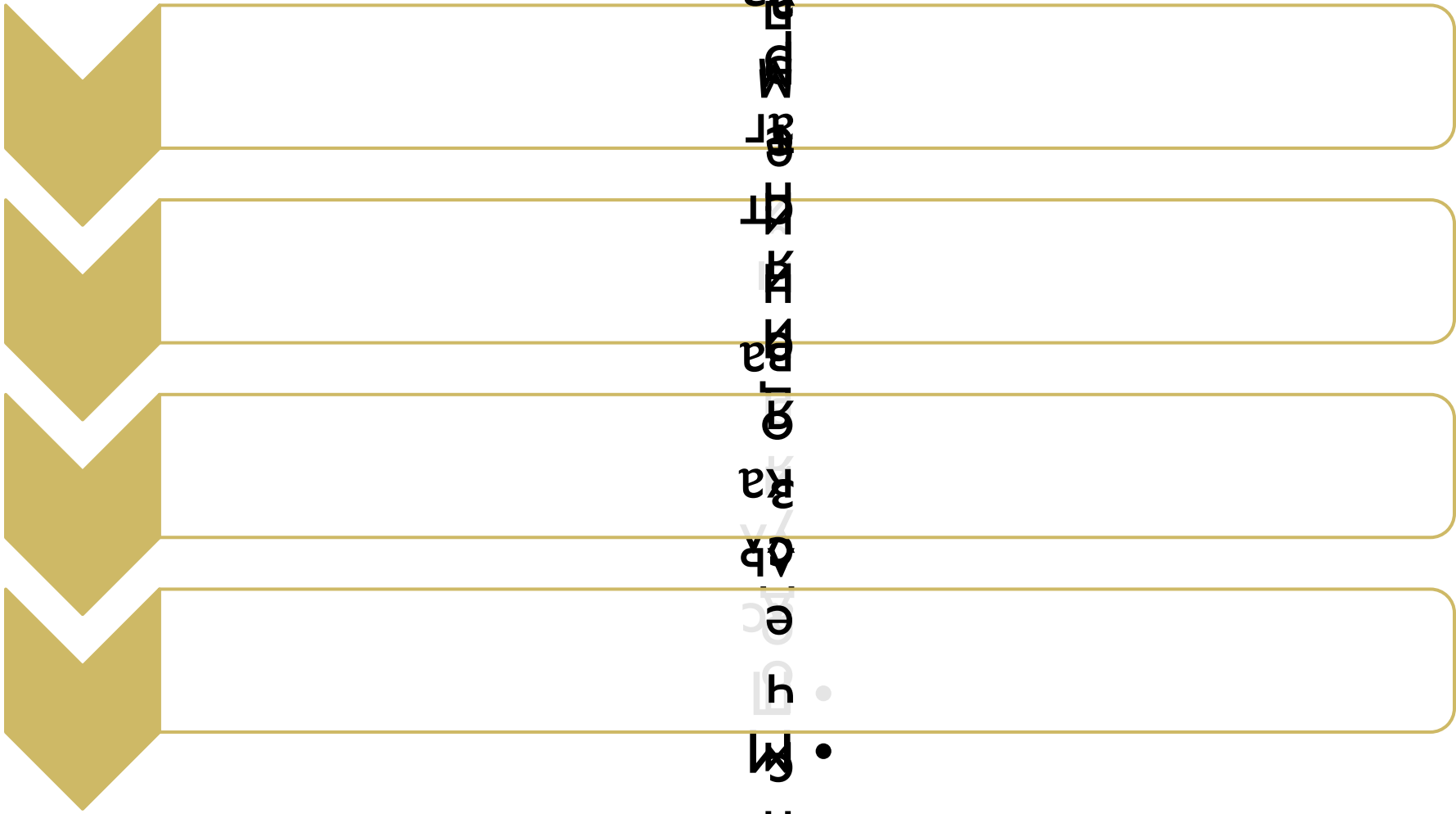


# Акустомагнитная метка

---



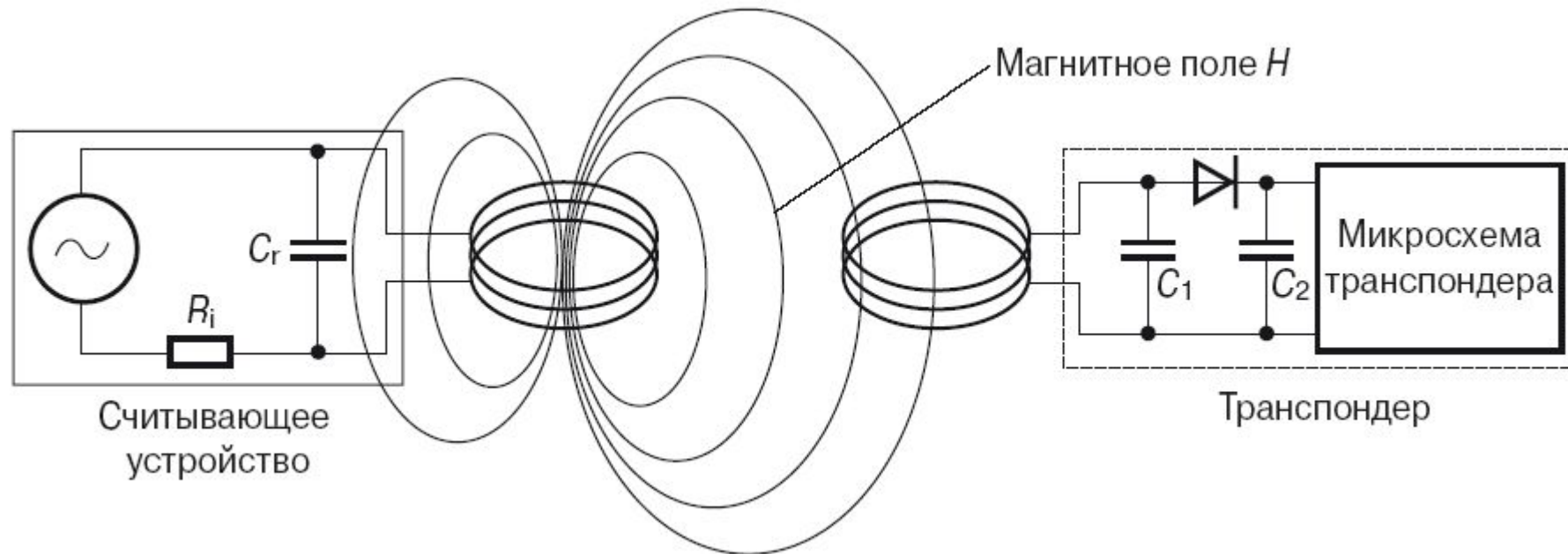
# Системы с индуктивной связью



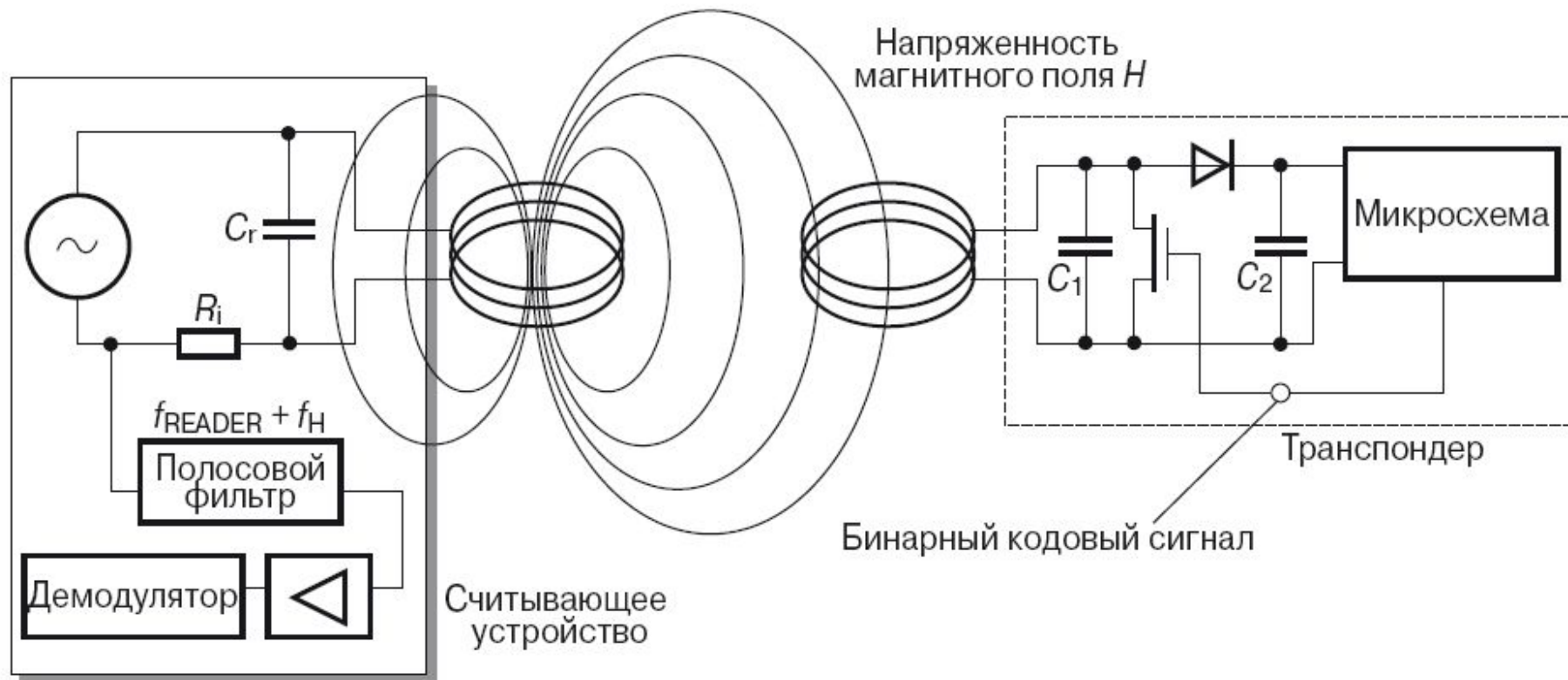
6  
И  
М  
•  
с  
е  
с  
ь  
ка  
о  
го  
в  
а  
т  
е  
р  
т  
у  
р  
ы



# Система с пассивным транспондером

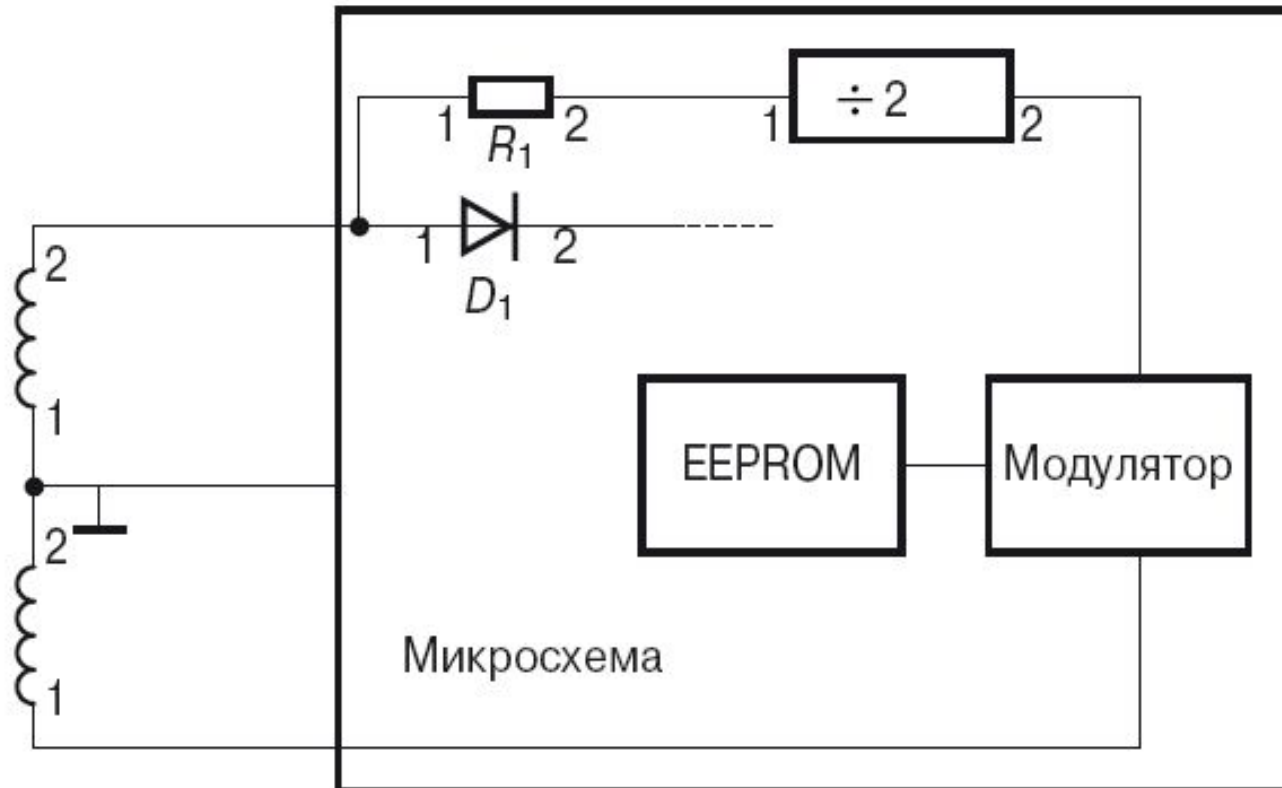


# Схема модуляции нагрузкой



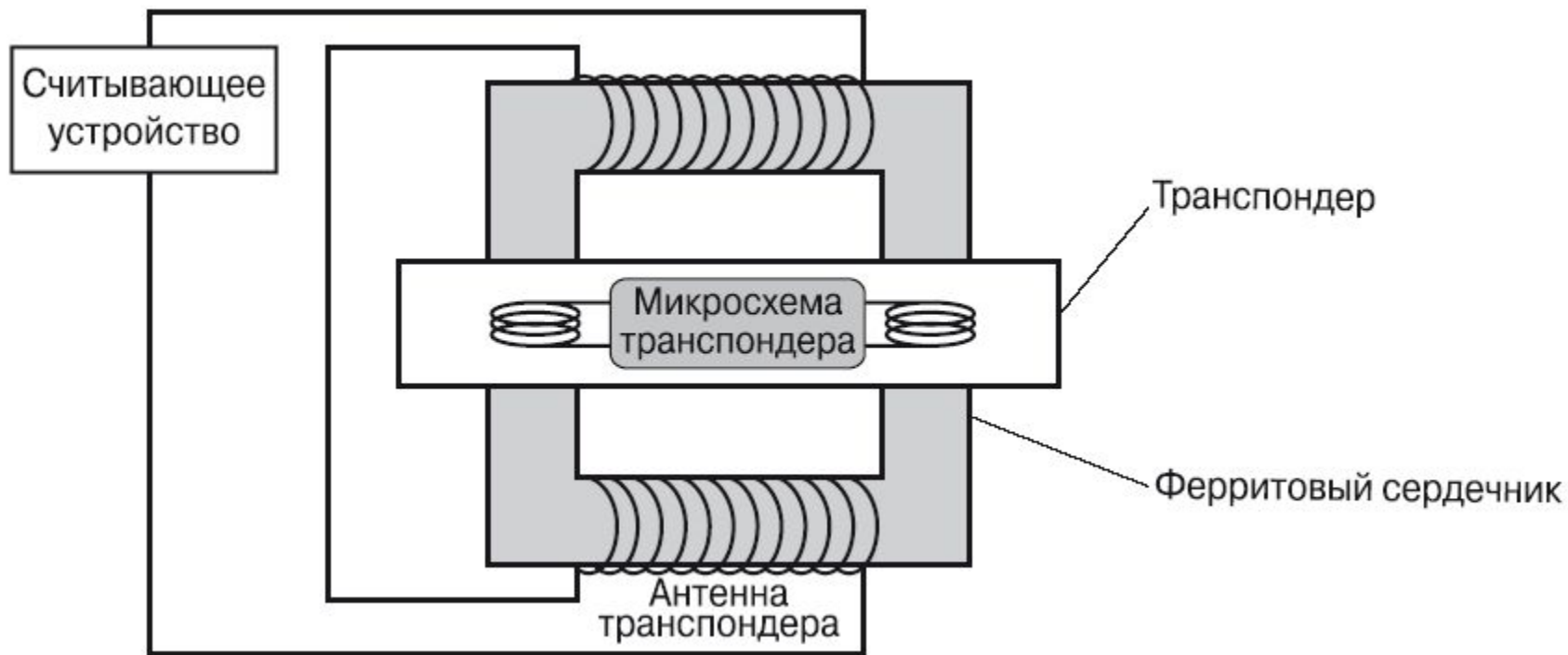
# Субгармонический транспондер

---



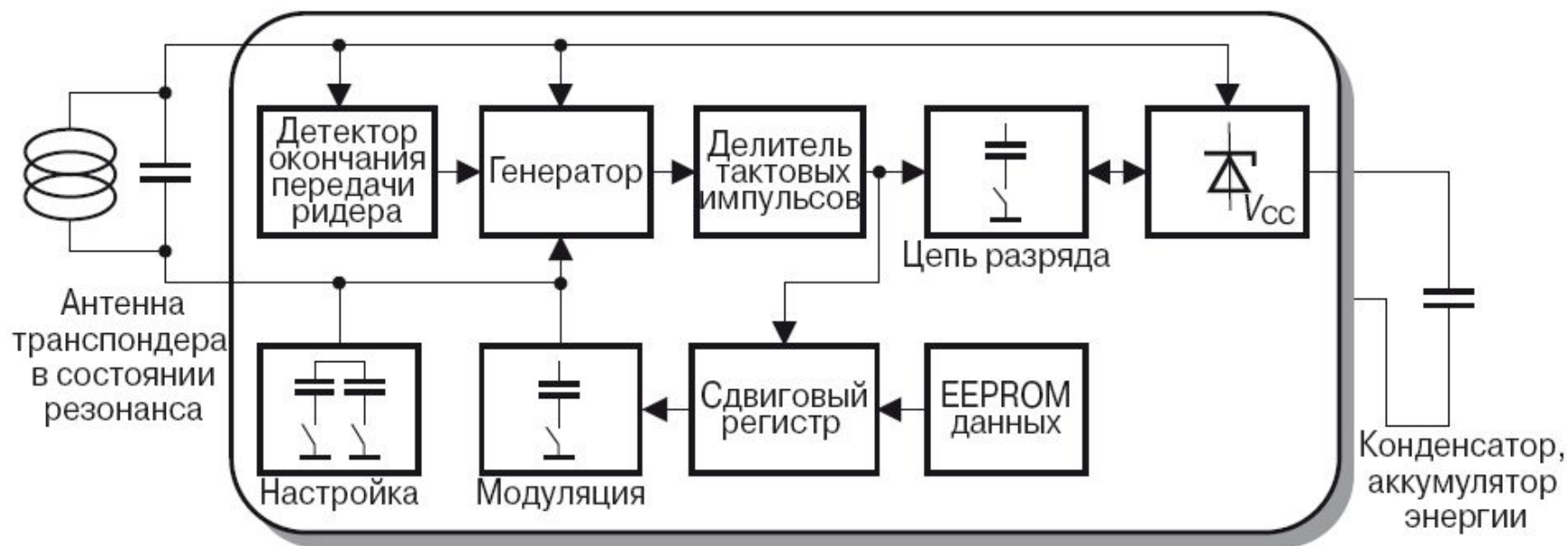
# Close-coupling

---



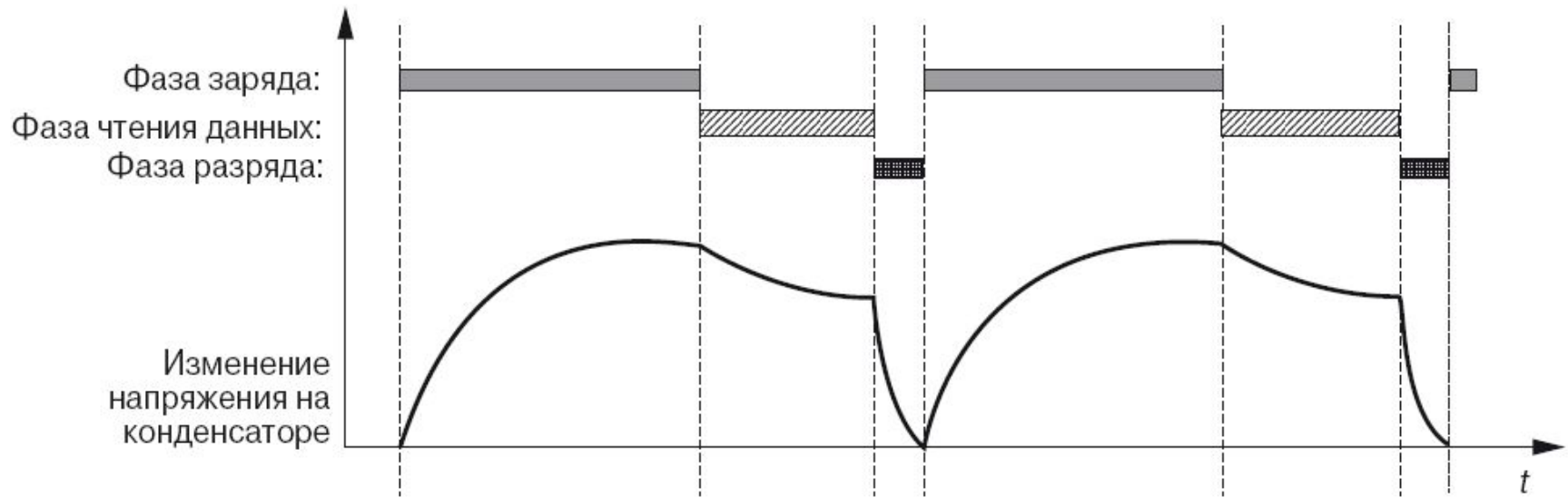
# SEQ-транспондер

## Блок-диаграмма транспондера TIRIS



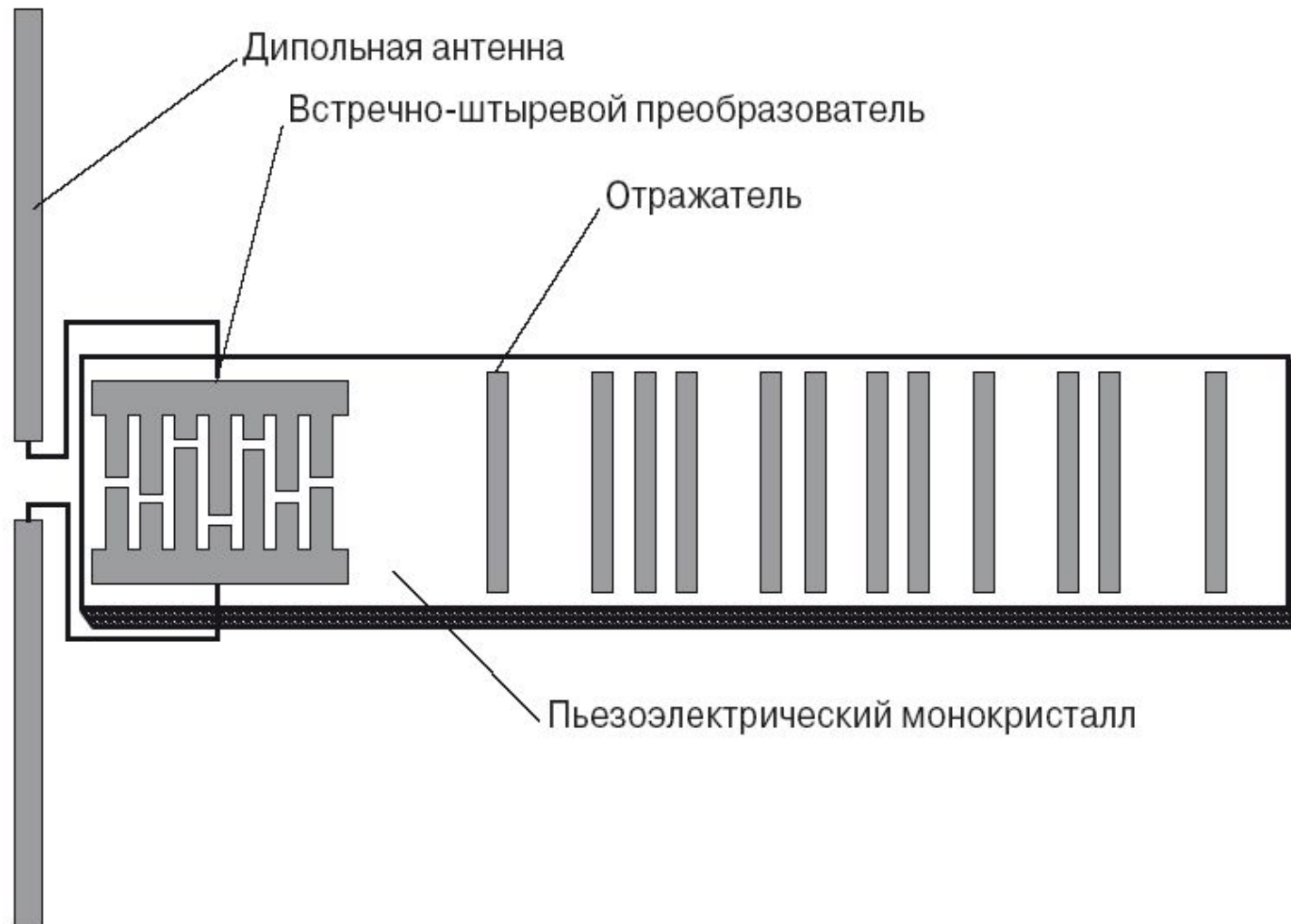
# Изменение напряжения на конденсаторе транспондера

---



# ПАВ транспондер

---



# Формула Фрииса

---

$$\frac{P_T}{P_p} = G_p G_T \left( \frac{\lambda}{4\pi} \right)^2$$





# Расстояние чтения транспондера

---

$$P_{minT} = P_p G_p G_T \left( \frac{\lambda}{4\pi} \right)^2$$

$$r = \frac{\lambda}{4\pi} \sqrt{\frac{P_p G_p G_T \tau}{P_{minT}}}$$



# Чувствительность транспондера

---

$$P_T = P_p \frac{A_e}{4\pi r^2}$$

$$A_e = G \left( \frac{\lambda^2}{4\pi} \right)$$



# Максимальная дальность

---

$$P_T = \frac{\tau P_p G_p^2 G_T^2 \lambda^4}{(4\pi r)^4}$$

$$r = \frac{\lambda}{4\pi} \sqrt[4]{\frac{P_p G_p^2 G_T^2 \tau}{P_{\min p}}}$$



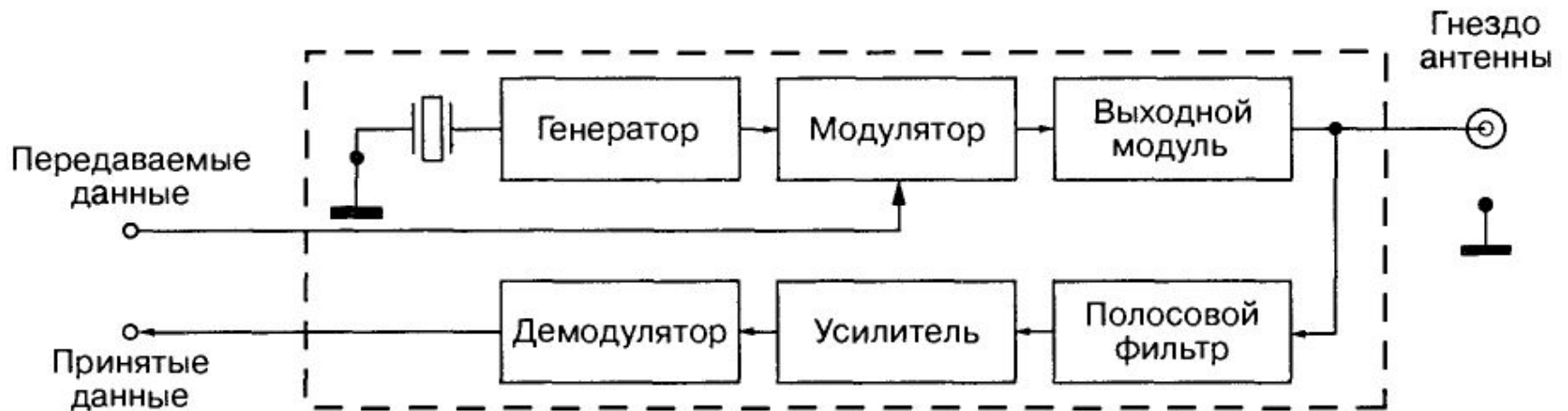
# СЧИТЫВАТЕЛИ

# Считыватели

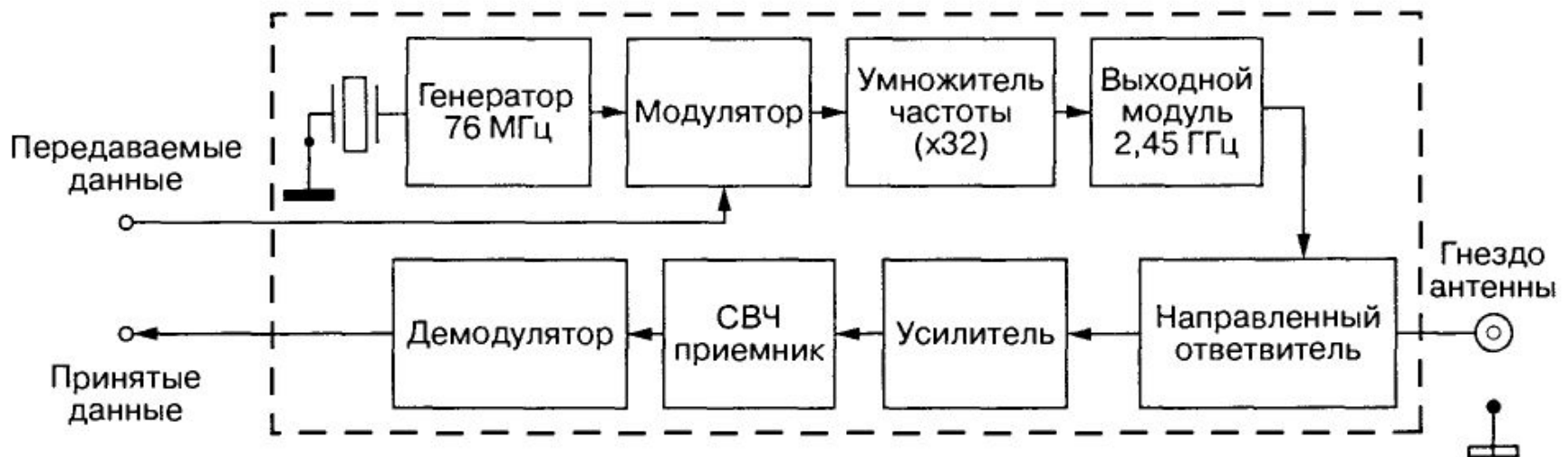
---



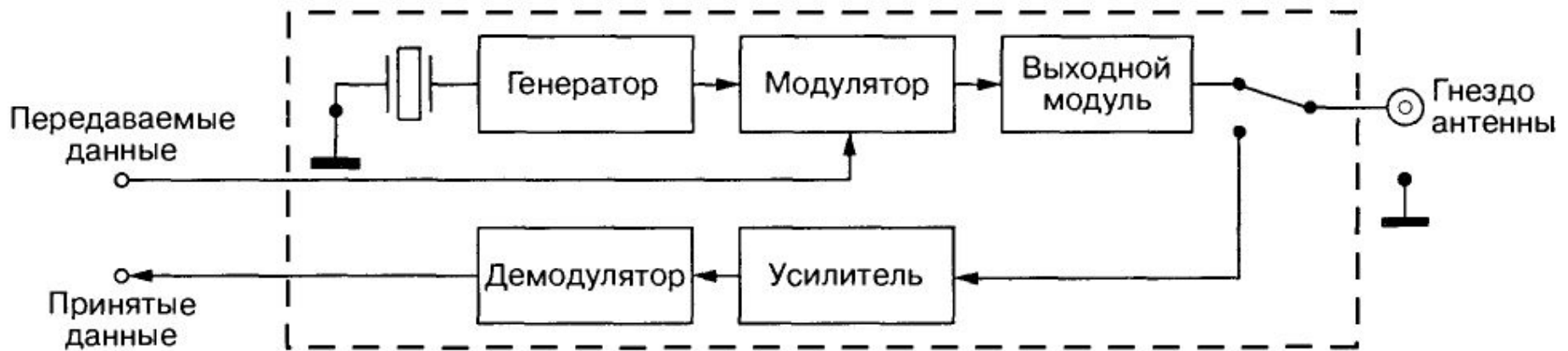
# Схема РЧ-интерфейса с ИНДУКТИВНОЙ СВЯЗЬЮ



# Схема интерфейса для микроволновых систем

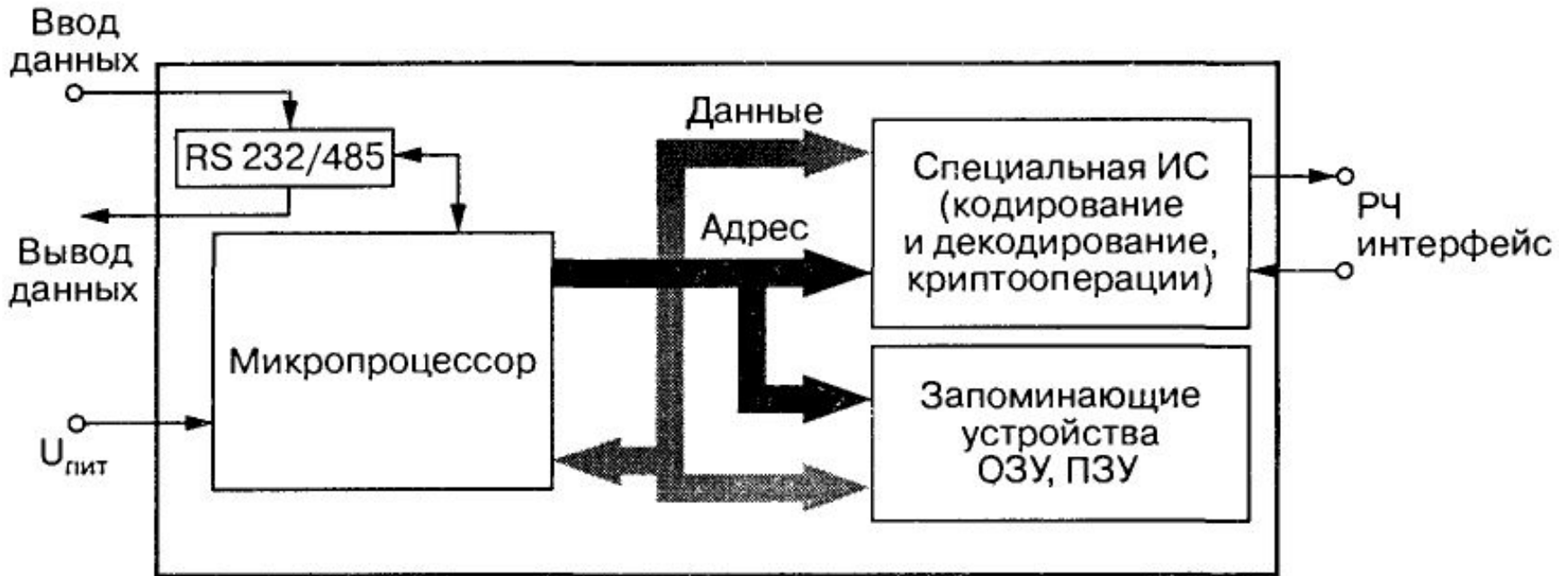


# Схема интерфейса для последовательных систем





# Блок управления



# Антенны:

---



••





СИСТЕМЫ



ЗАЩИТЫ

# Критерии безопасности

---

- целостность

- конфиденциальность

- доступность



# Защита информации

---

Антиколлизии

Помехоустойчивое кодирование

Шифрование

- Симметричные криптосистемы
- Асимметричные крипто системы
- Комбинированные криптосистемы

Хэширование

Цифровая подпись

---



# Параметры кодов:

---

- Разрядность кода
- Число информационных символов
- Избыточность кода
- Корректирующая способность



# АНТИКОМБИЗИОННЫЙ МУЛЬТИДОСТУП

---

SDMA

•space division  
multiple access

FDMA

•code division  
multiple access


TDMA

•time domain multiple  
access

CDMA

•frequency domain  
multiple access

---



# Криптография:

---

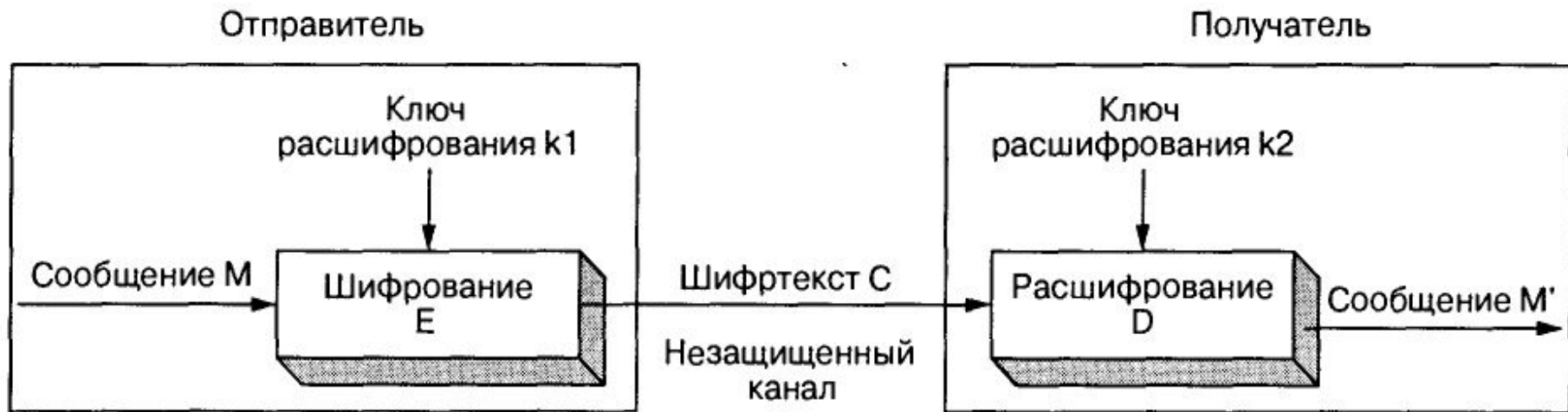
- Шифрование данных, передаваемых по каналам связи или хранимых в памяти
  - Идентификация/аутентификация пользователя
  - Контроль/разграничение доступа к ресурсам системы/сети
  - Управление криптографическими ключами
  - Контроль целостности
- 





# Симметрично шифрование

---



$$C = E_{k_1}(M)$$

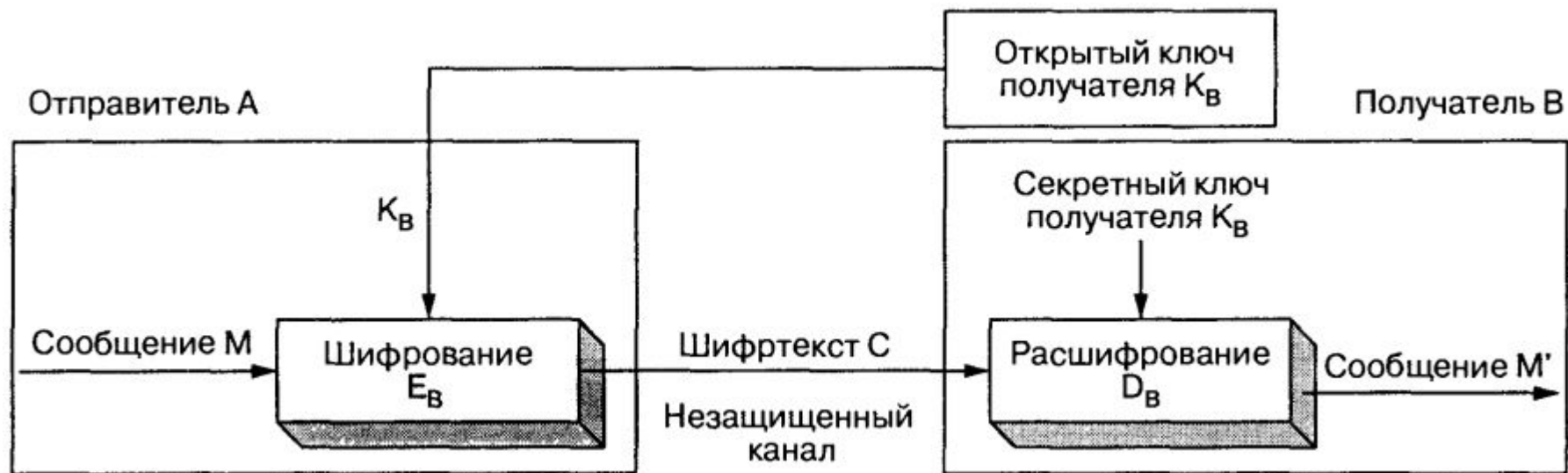
$$M' = D_{k_2}(C)$$

---

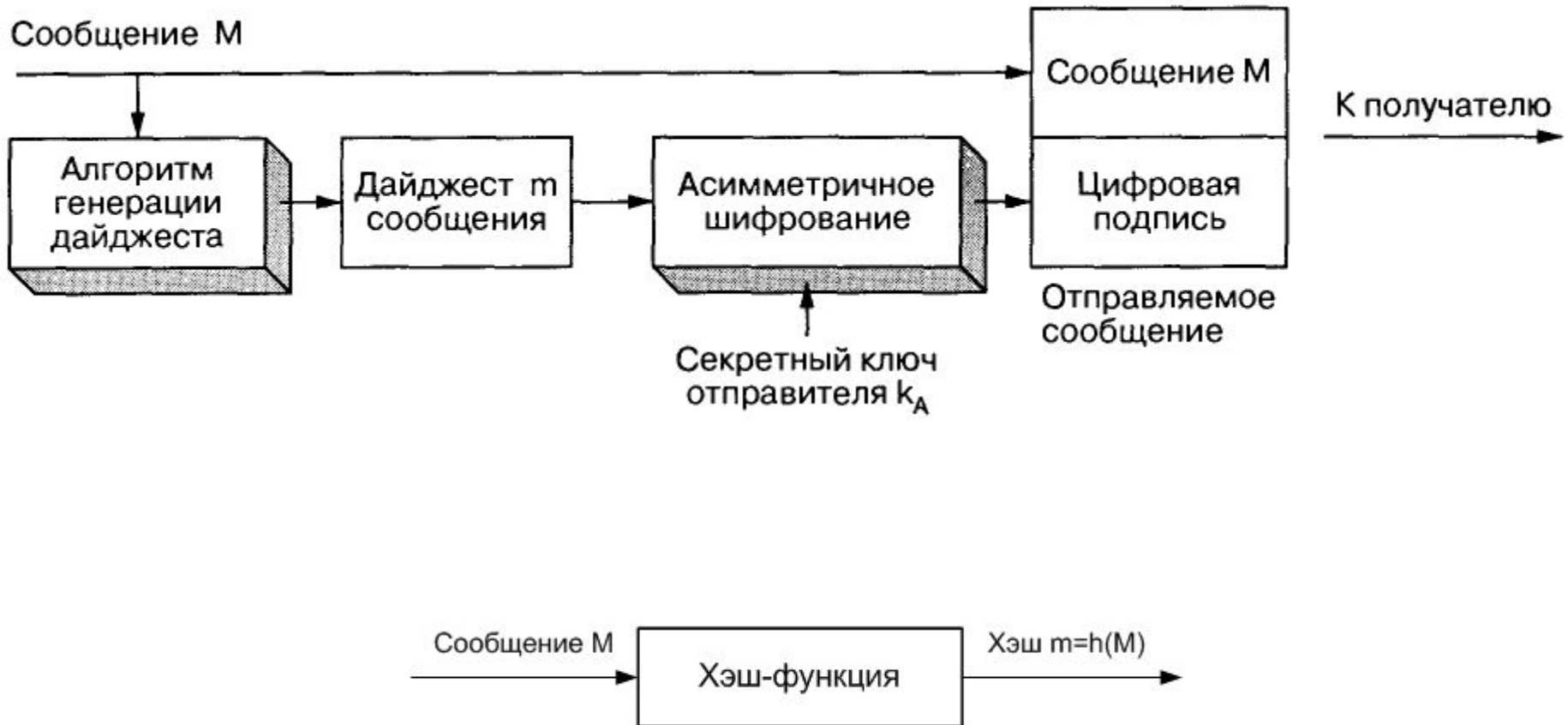


# Асимметричное шифрование

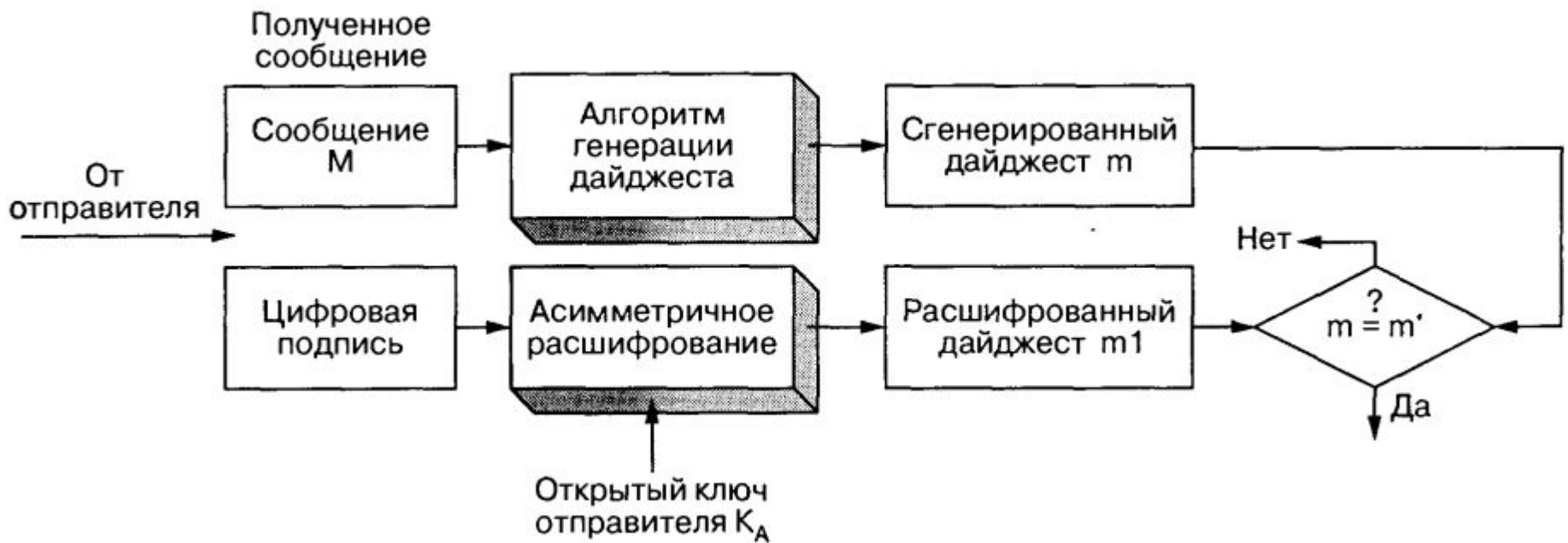
---



# Формирование ЭЦП



# Проверка ЭЦП




# Данные ЭЦП


---

- Дата подписи
- Срок действия ключа ЭЦП
- Информация о владельце
- Имя открытого ключа
- Цифровая подпись

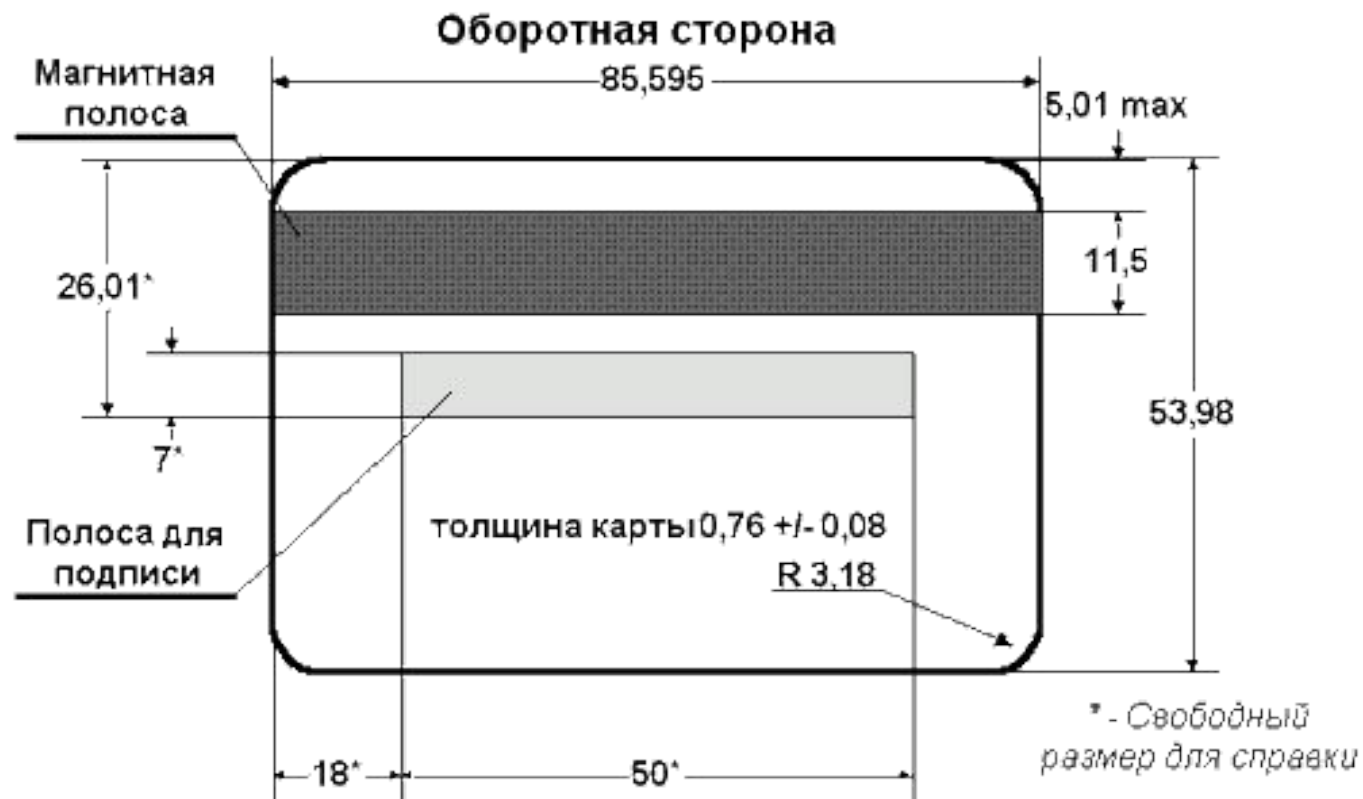




# Смарт-карты



# Карта с магнитной полосой



# Преимущества смарт-карт

---

- Максимальная емкость памяти
- Встроенная система защиты
- Шифрование данных
- Долговечность





# Классификация смарт-карт

---

По типу интерфейса между смарт-картой и терминалом

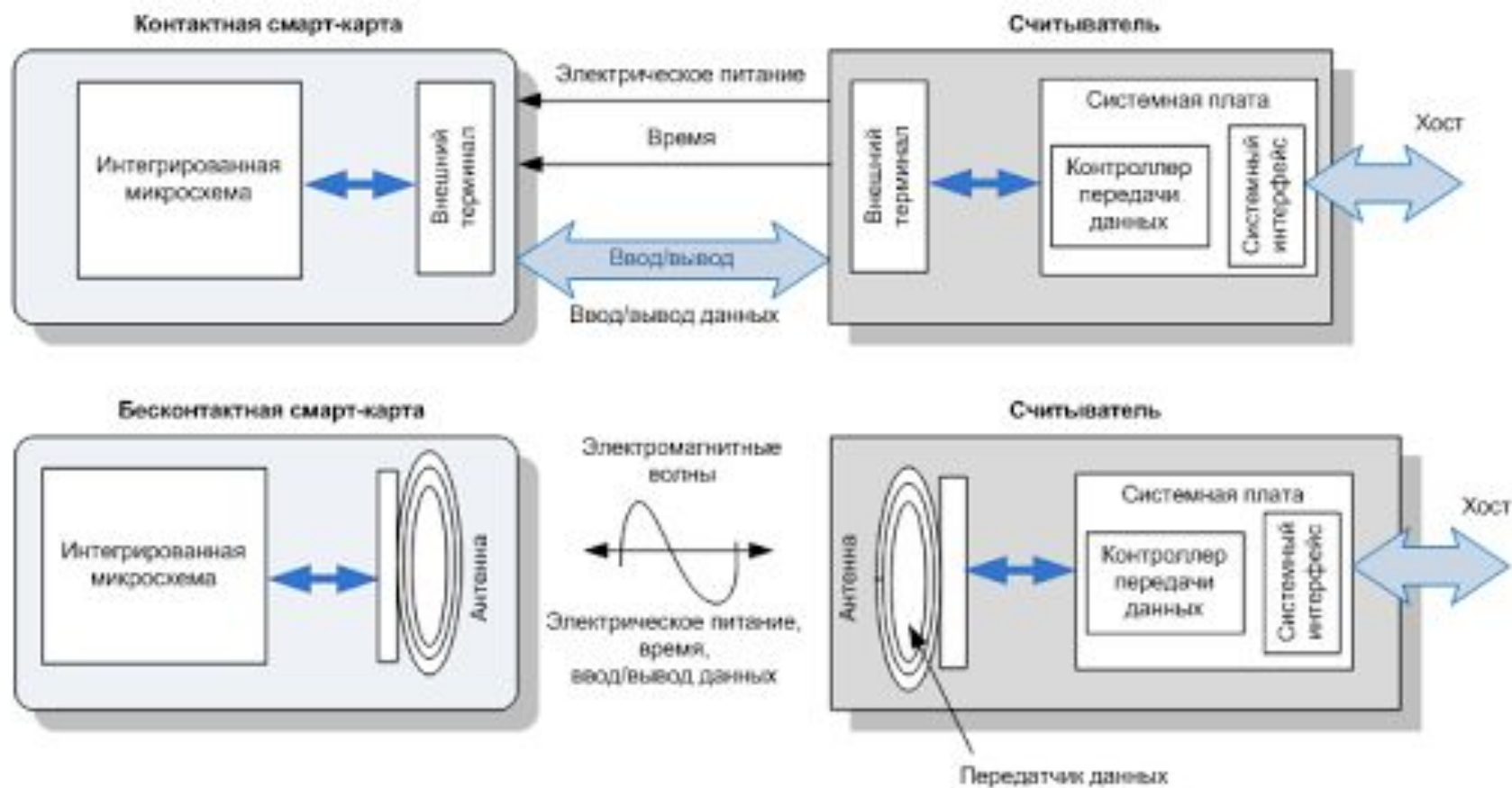
По типу интегральной схемы

По средствам обеспечения безопасности

- ИС памяти
- ИС микроконтроллера:
  - с сопроцессором
  - без сопроцессора
- Контактный
- Бесконтактный
- Комбинированный (двойной)

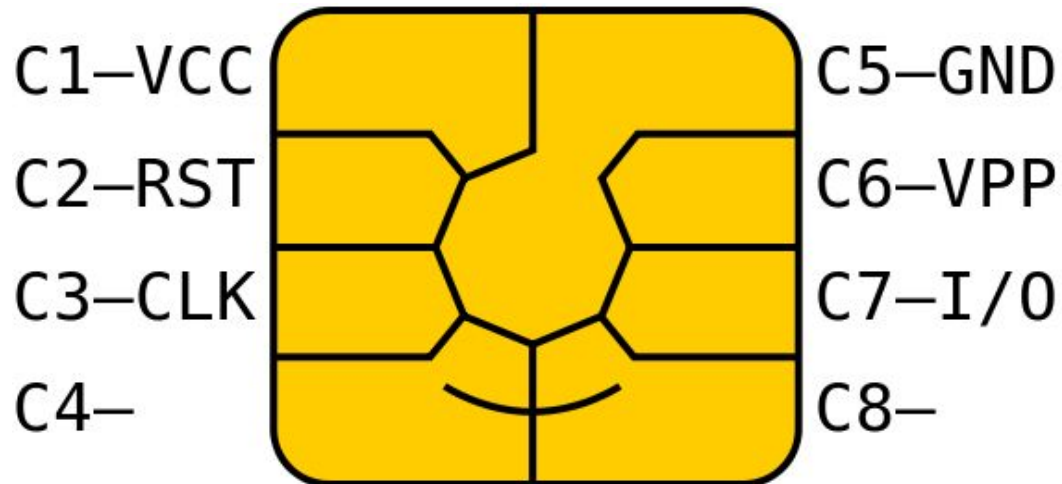


# Интерфейсы смарт-карты



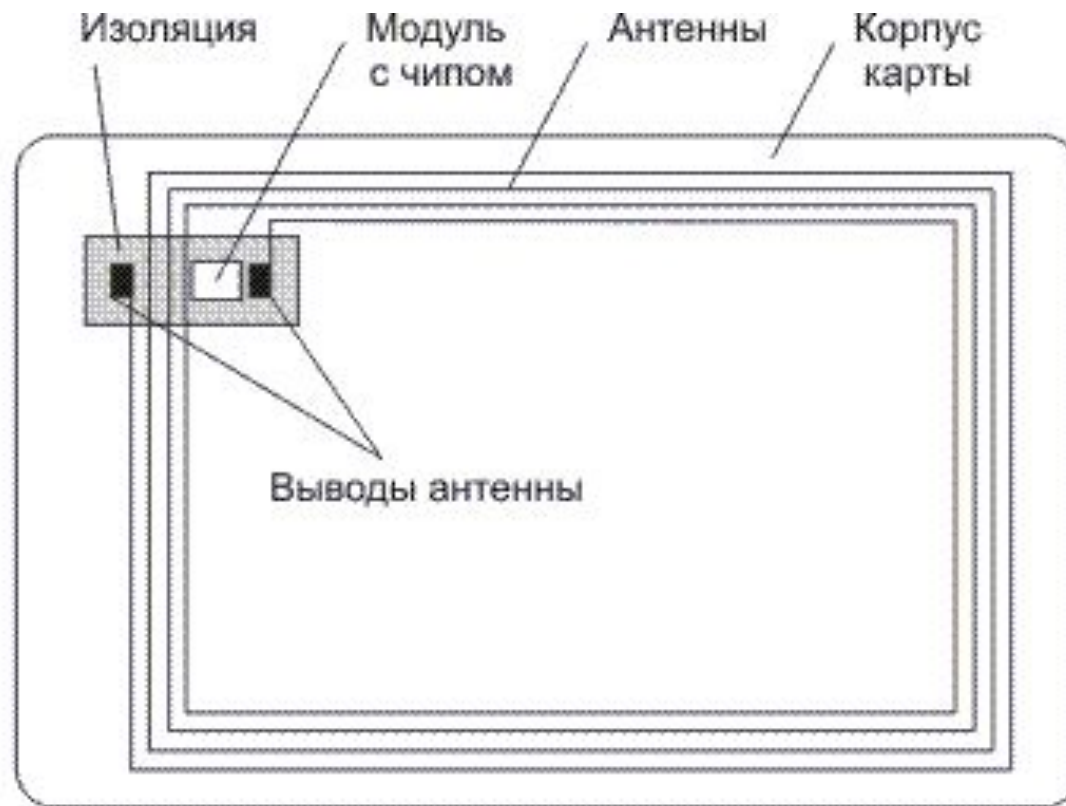
# Структура контактной смарт-карты

---



# Бесконтактная смарт-карта

---



# Связь с терминалом

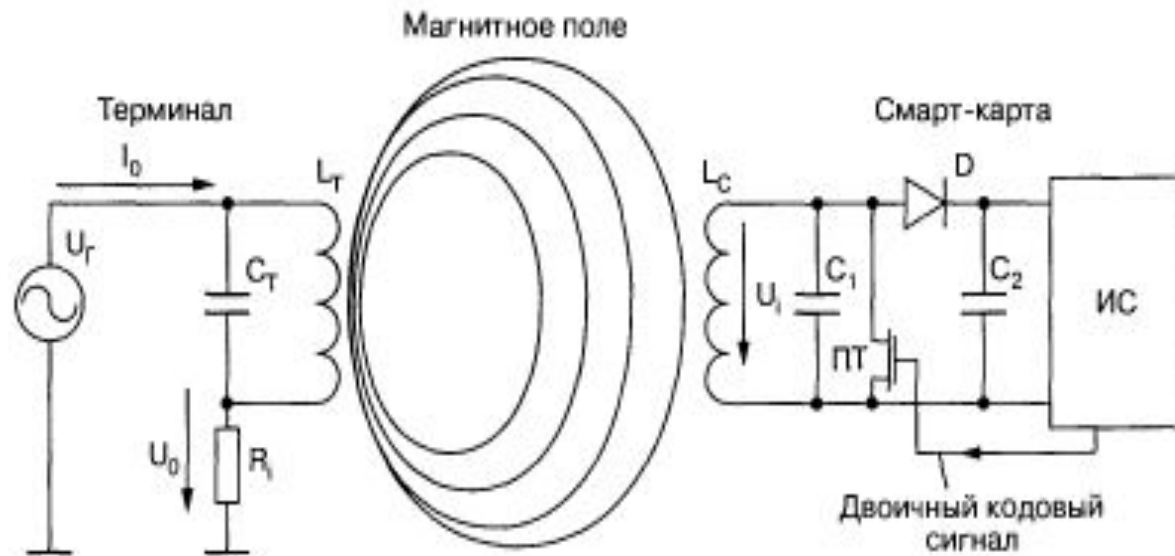
---

- Передача энергии
- Передача тактового сигнала
- Передача данных на смарт-карту
- Передача данных на терминал



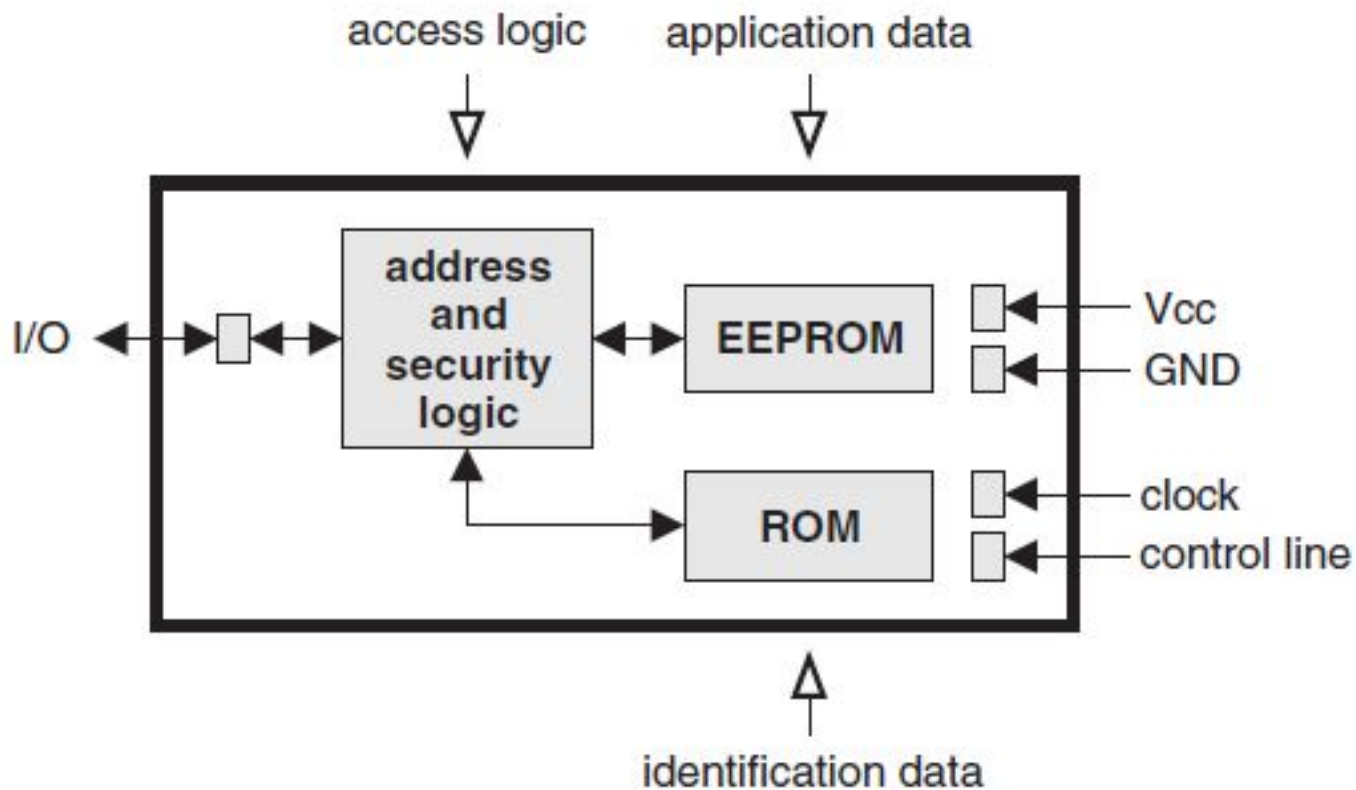
# Связь с терминалом

---

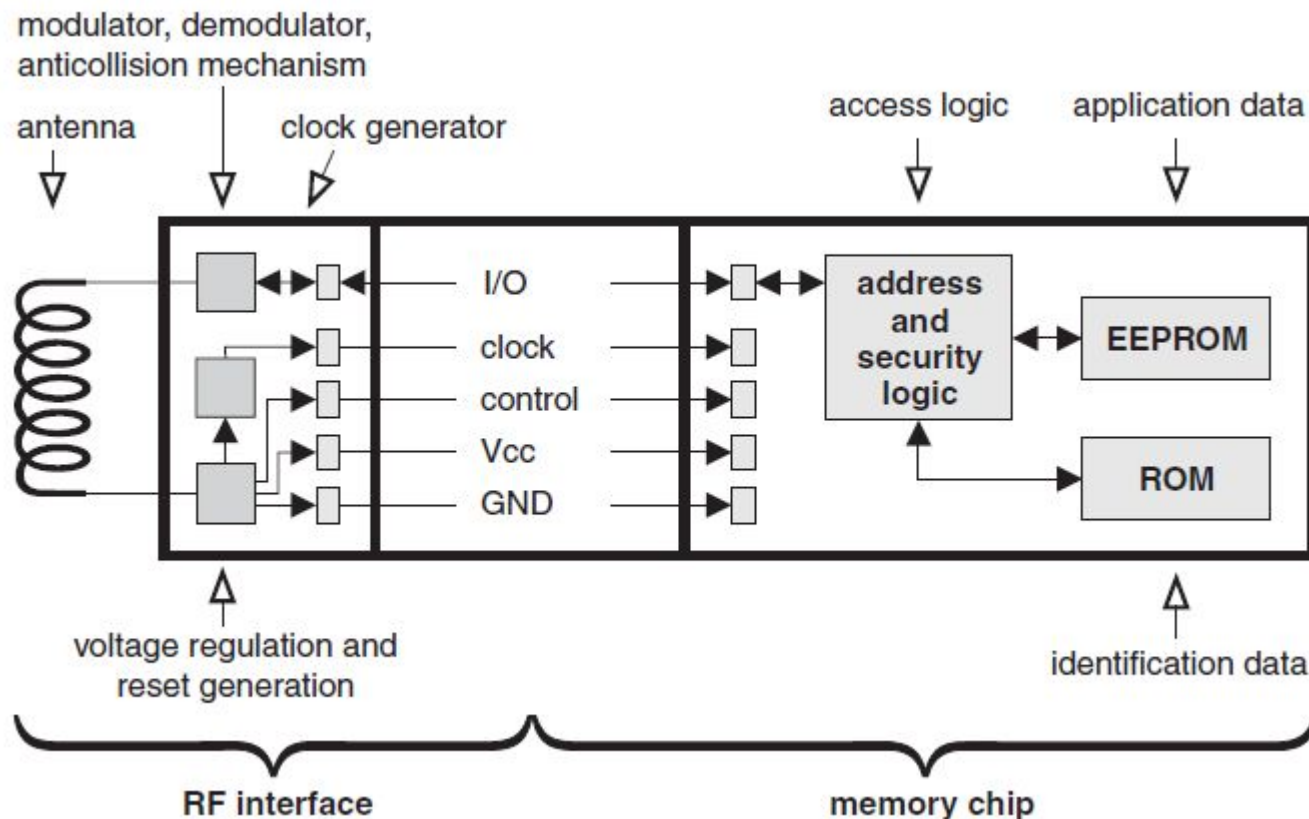


# Смарт-карты с микросхемой памяти

---

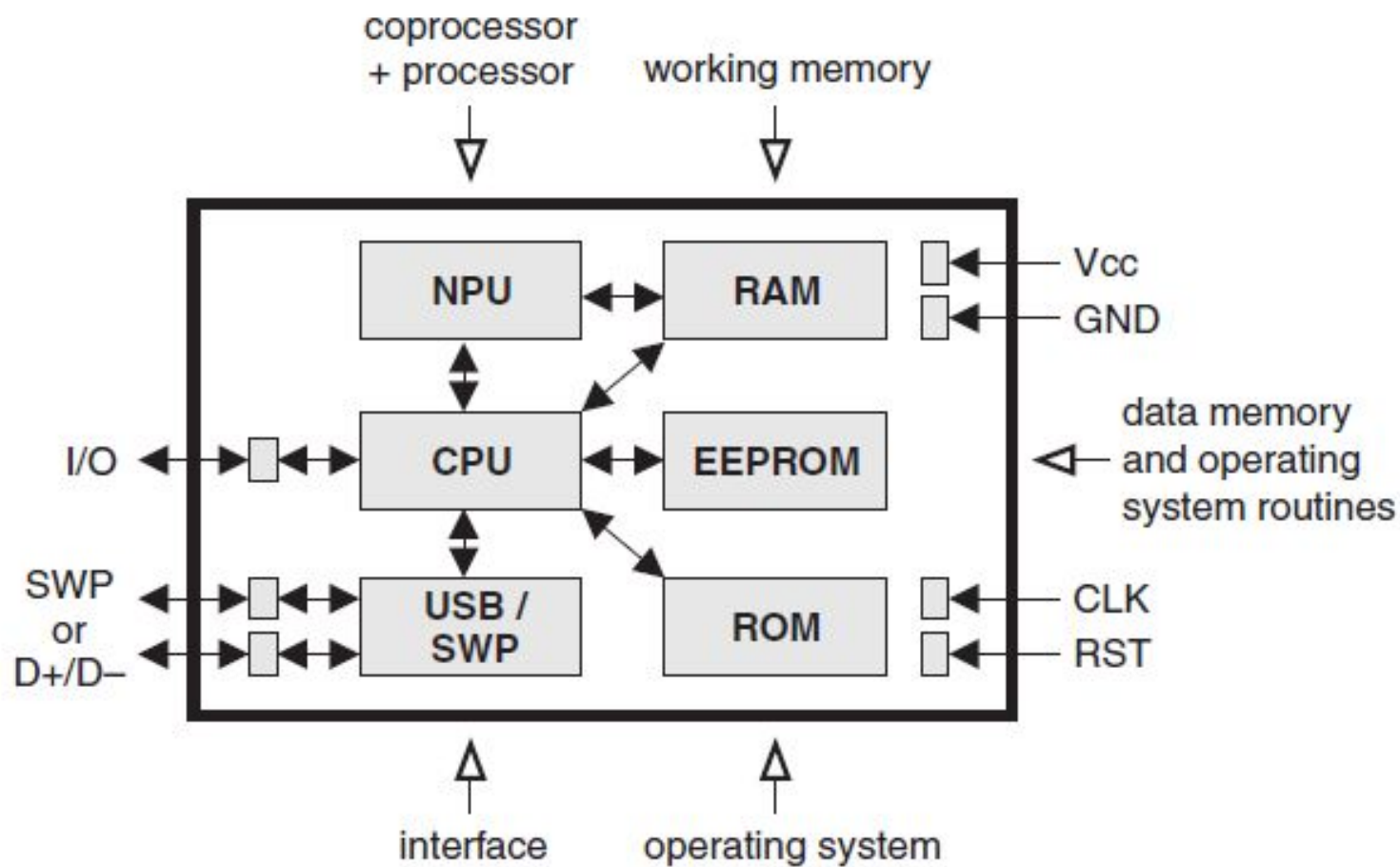


# Смарт-карты с микросхемой памяти

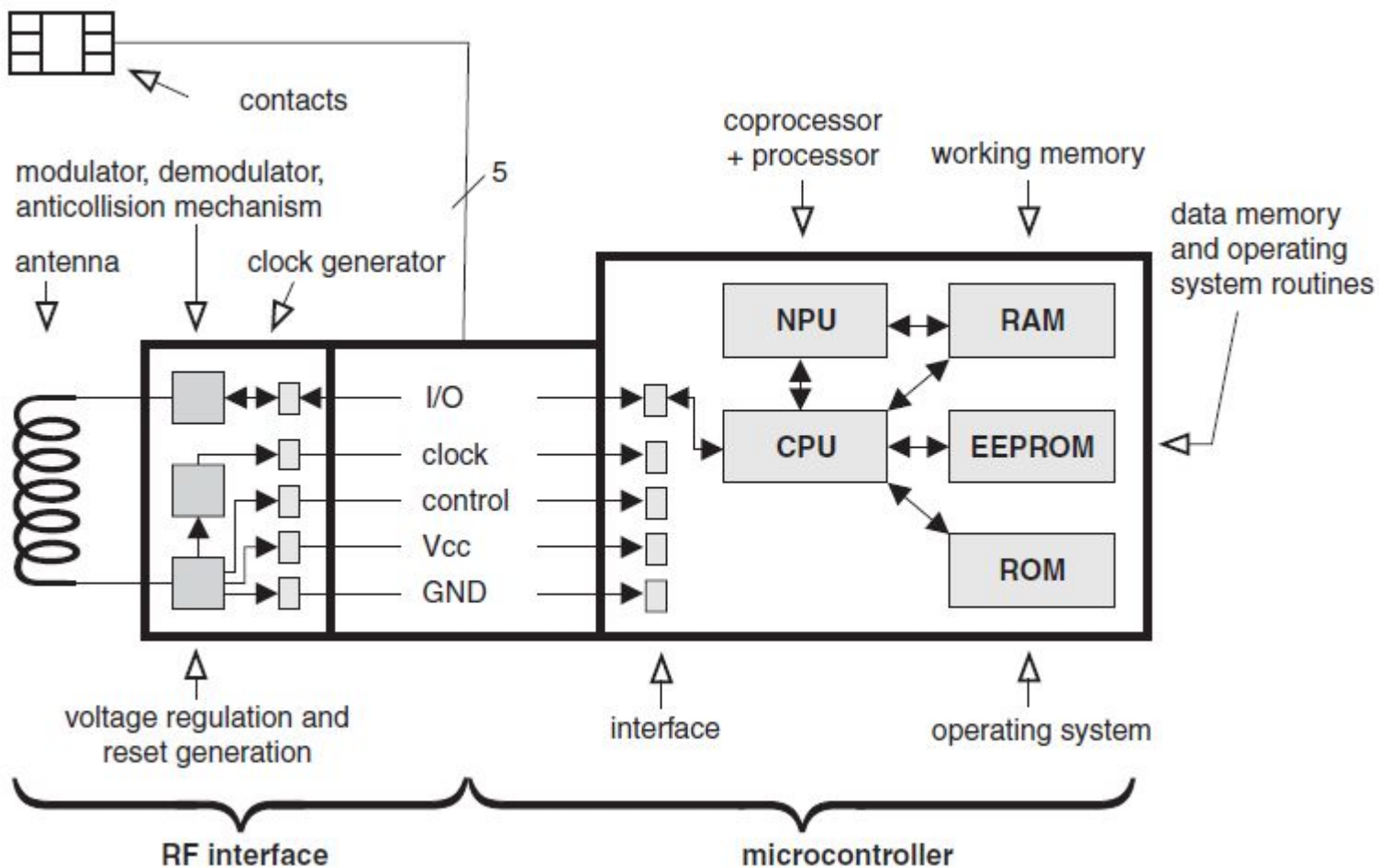




# Смарт-карта с процессором



# Смарт-карта с процессором



# Виды памяти

---

- ОЗУ
- ПЗУ
- ЭСППЗУ
- Flash-ЭСППЗУ
- FRAM



# ПО смарт-карт

---

## ПО хост-терминала:

- системные программы
- прикладные программы

## ПО смарт-карты:

- операционная система
- утилита
- приложение



# Задачи ОС смарт-карты

---

- управление передачей данных
- управление исполнением команд
- управление файлами
- управление криптографическими алгоритмами



# Функции считывателя

---

- подача электропитания
- установление соединения для передачи данных



# Компоненты считывателя

---

## Блок интерфейса:

- контактный интерфейс
- радиочастотный интерфейс

## Блок управления:

- процессор
  - память
  - генератор синхроимпульсов
  - схема ввода-вывода данных
  - блок питания
- 
- 