СИСТЕМЫ ГАРАНТИРОВАННОЙ СЕКРЕТНОСТИ

(ТЕОРЕТИЧЕСКИ СТОЙКИЕ КРИПТОСИСТЕМЫ)

Понятие стойкости

- Теоретическая стойкость (принципиальная невозможность атаки)
- Практическая стойкость (необходимость для атаки таких ресурсов, стоимость которых многократно превышает стоимость приобретаемой в случае успеха выгоды)

Криптосистема Цезаря (Вижинера)

$M \qquad (a_i)_{i=1,2,\dots,n} \qquad A \qquad a_i \in A,\ i = 1, 2, \dots, n$

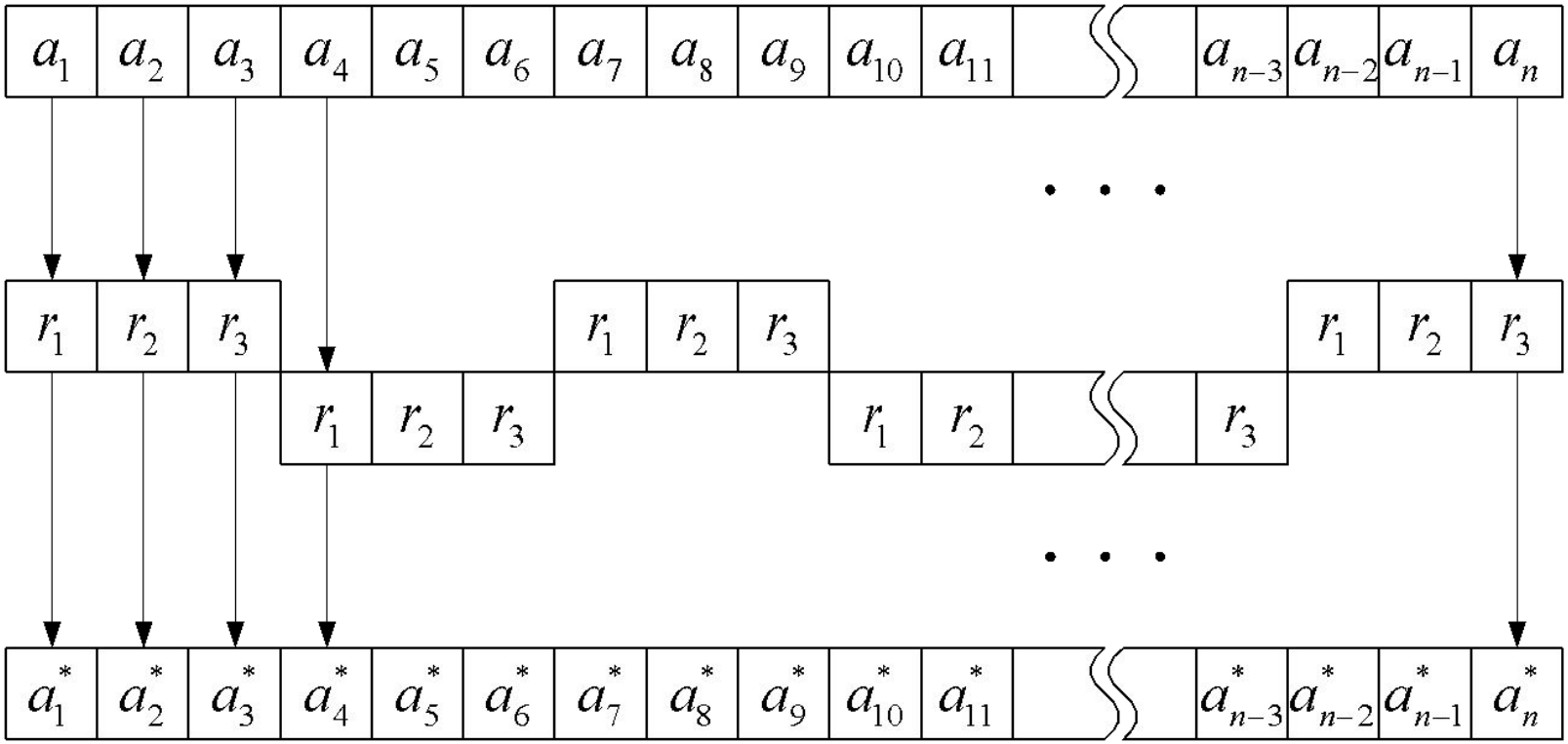
$k \qquad (r_i)_{i=1,2,\dots,n} \qquad R^{(0)} \qquad r_i \in R^{(0)},\ i = 1, 2, \dots, n$

$m \qquad m \geq |A| \qquad m \geq |R^{(0)}|$

$$a_i^* = \left| a_i + r_i \right|_m,\ i = 1, 2, \dots, n$$

$$a_i = \left| a_i^* - r_i \right|_m = \left| a_i^* + m - r_i \right|_m,\ i = 1, 2, \dots, n$$

Короткопериодический ключ



Системы гарантированной секретности

1) $\left| R^{(0)} \right| \geq \left| A \right|$

2) $\left(r_i \right)_{i=1,2,\dots,n}$ $R^{(0)}$

3) $\left(r_i \right)_{i=1,2,\dots,n}$

Проблема получения случайных равномерно распределенных над заданным алфавитом последовательностей на компьютерах с **фон Неманновской архитектурой**

Принципы фон Неймана

1. Принцип двоичности
2. Принцип программного управления
3. Принцип однородности памяти
4. Принцип адресуемости памяти
5. Принцип последовательного программного управления
6. Принцип условного перехода

Burks A. W., Goldstine H. H., Neumann J. Preliminary Discussion of the Logical Design of an Electronic Computing Instrument. — Institute for Advanced Study, Princeton, N. J., July 1946.

Принстонская и гарвардская архитектуры компьютеров

- **Принстонская архитектура** (фон Неймана)
- **Гарвардская архитектура** — архитектура ЭВМ, отличительным признаком которой является раздельное хранение и обработка команд и данных. Архитектура была разработана Говардом Эйкеном в конце 1930-х годов в Гарвардском университете.

На компьютерах с полностью фон Неймановской архитектурой генерация случайности не возможна!!!

Все ли компьютеры имют архитектуру фон Неймана?

Наивные подходы к получению случайности в вычислительных системах

- Использование «не фон Неймановости» человеко-машинных систем
- Использование векового таймера

Физические источники случайности

- Сцинтилляционные источники

Спинтарископ

- Механические источники случайности

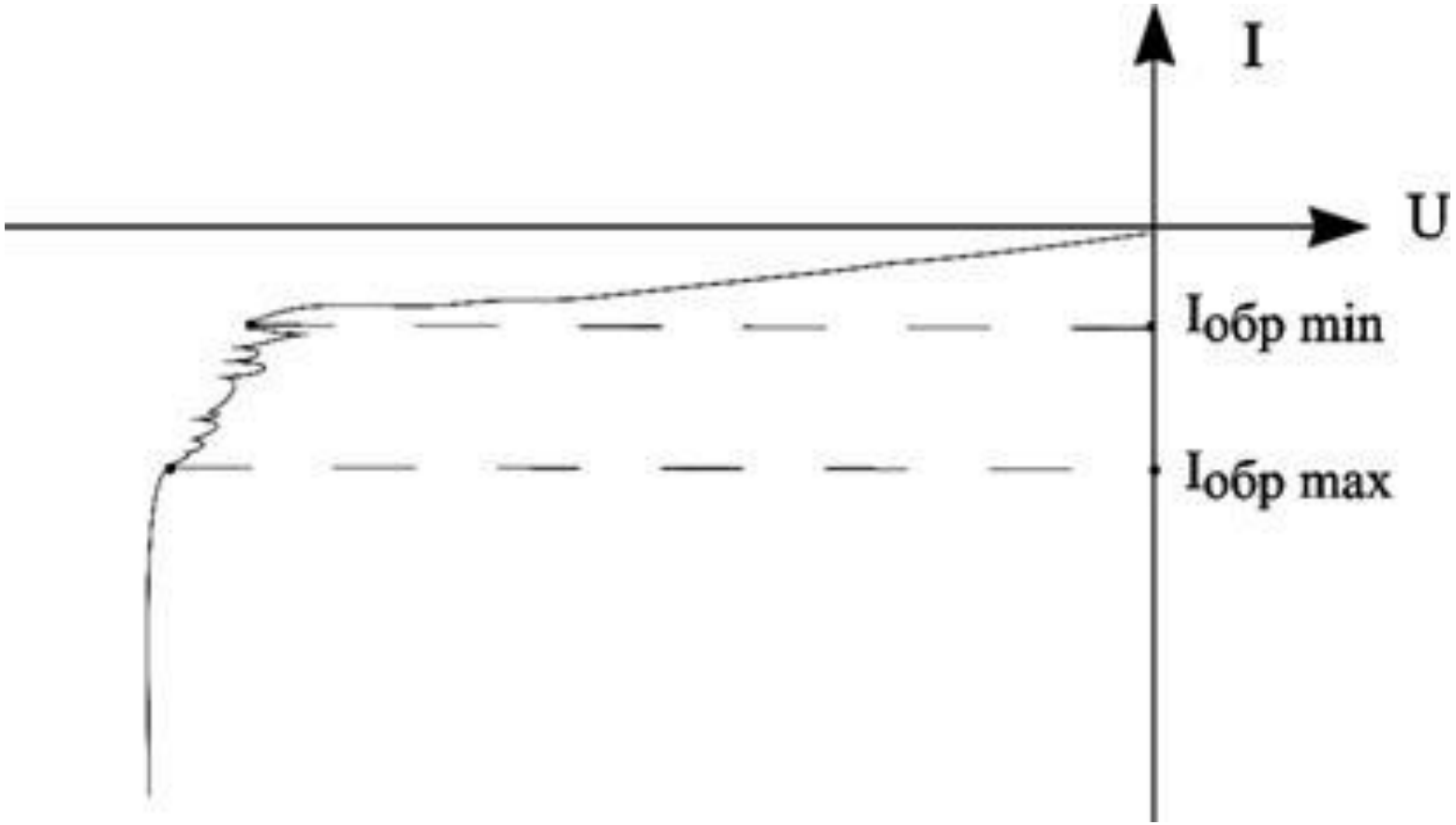
Лототроны

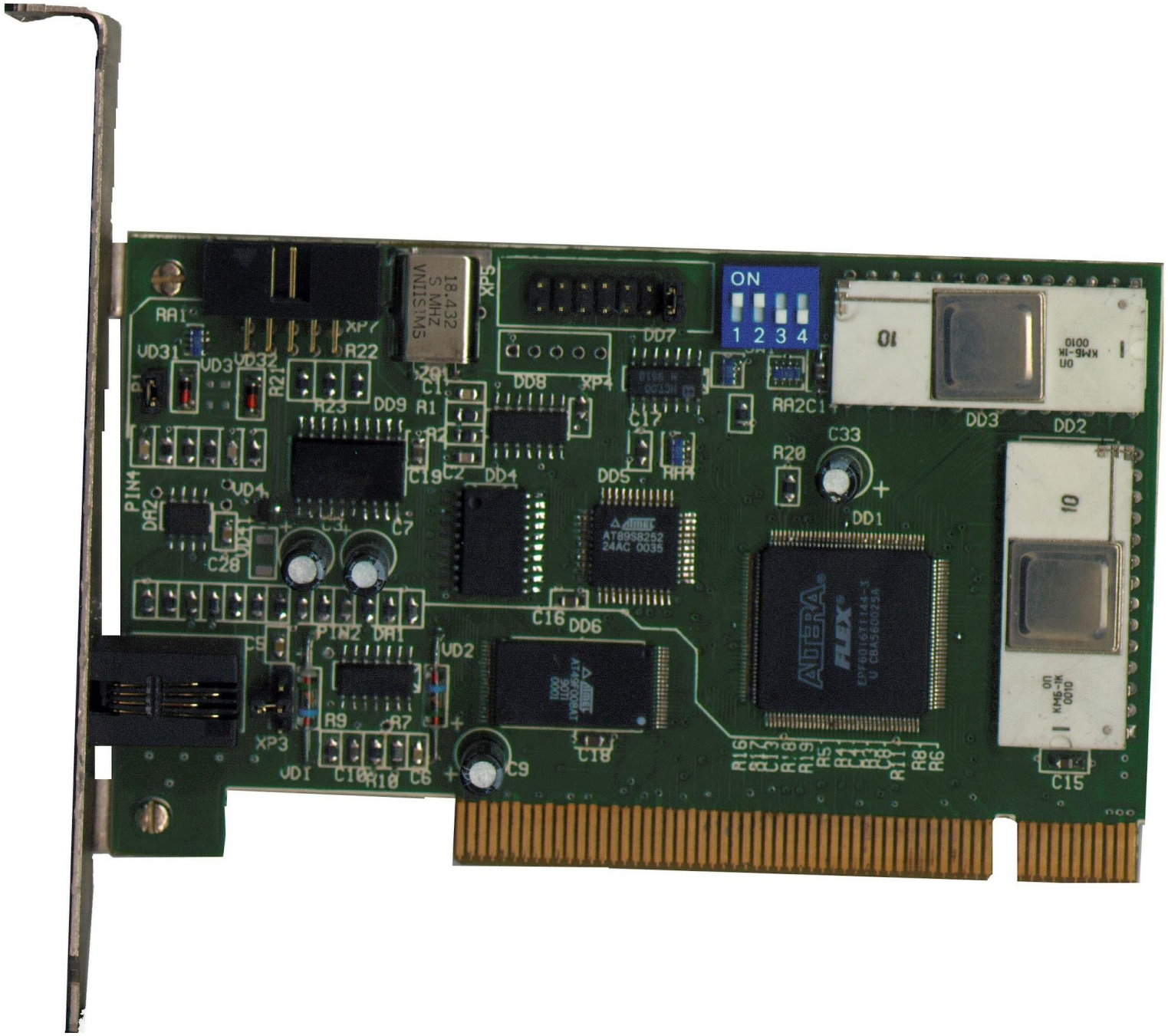
- Электрические источники
  - Шум газового разряда

- Шумовые вакуумные диоды

Шумовой вакуумный диод 2Д2С

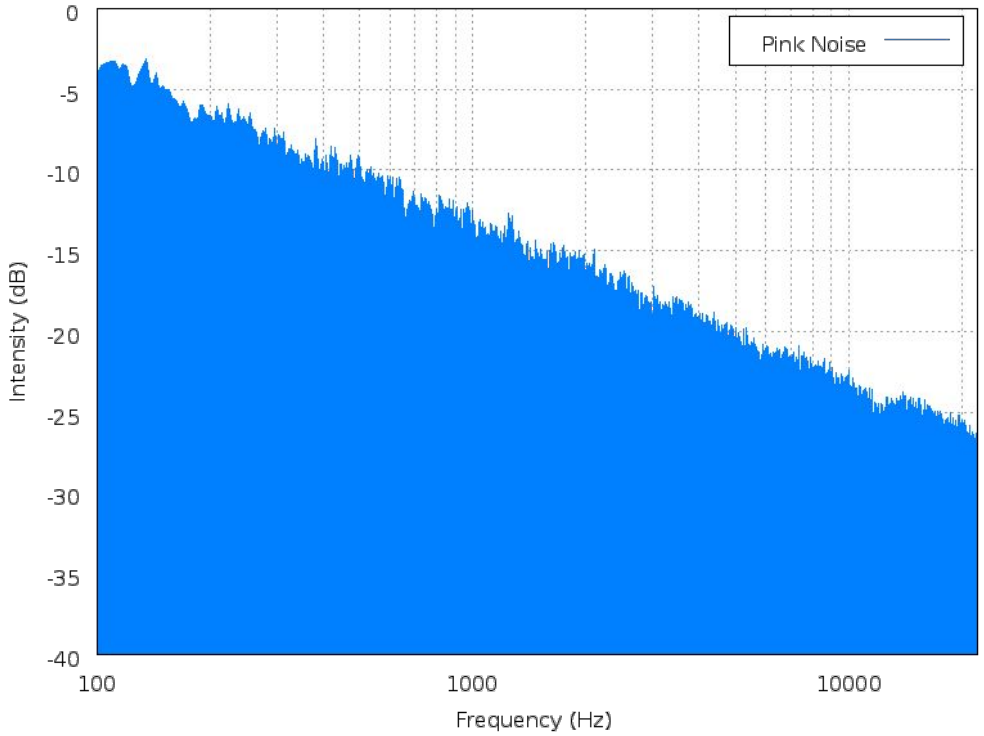
- Шумовые полупроводниковые диоды




ON
1 2 3 4
AT89S8252
24AC 0035
ALTERA
FLEX
18.432
S MHZ
VNIIS'MS
RA1
XP7
VD31
VD3
VD32
R22
R21
R23
DD9
R1
C19
C2
DD4
DD5
RA4
DD7
DD8
XP4
C17
RA2
C1
C33
R20
DD1
DD3
DD2
PIN1
DA2
VD1
VD4
C7
C28
C16
DD6
PIN2
DA1
VD2
R9
R7
XP3
VD1
C10
R10
C6
C9
C18
R16
R13
R8
R19
R5
R11
R17
R8
R6
C15

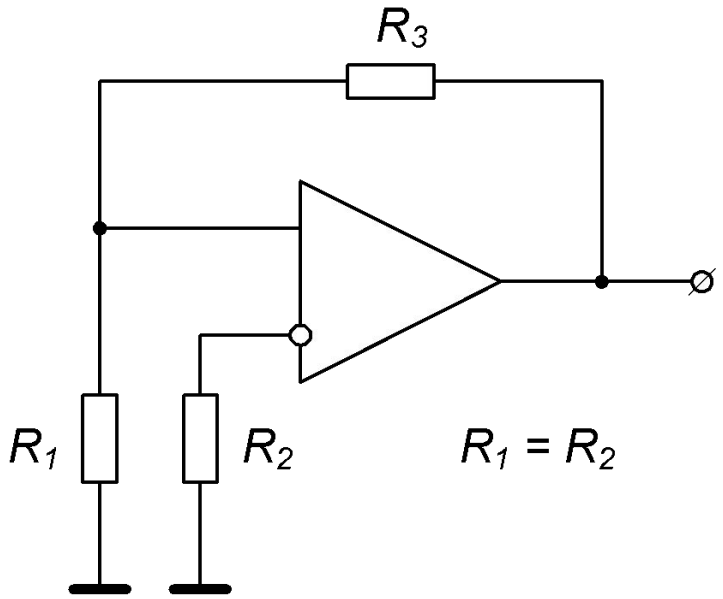
ФЛИККЕР-шум

Фликкер-шум (фликкерный **шум**, 1/f **шум**, иногда розовый **шум** в узком прикладном понимании такого термина)



Спектральная плотность розового шума определяется формулой ~1 / f (плотность обратно пропорциональна частоте), то есть он является равномерным в логарифмической шкале частот.

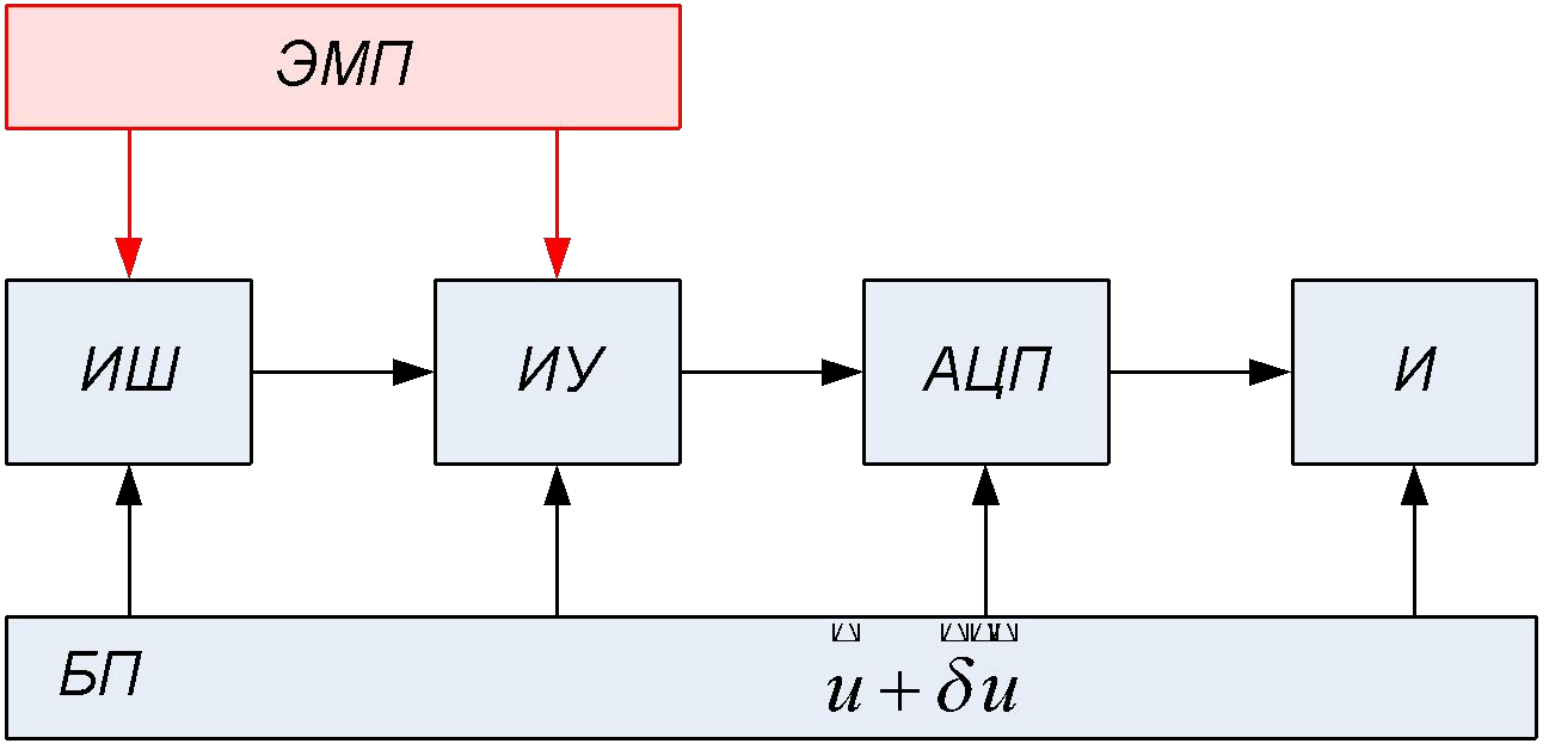
- Тепловой шум проволочных резисторов



Бородин А. В., МиСЗКИ, 2010

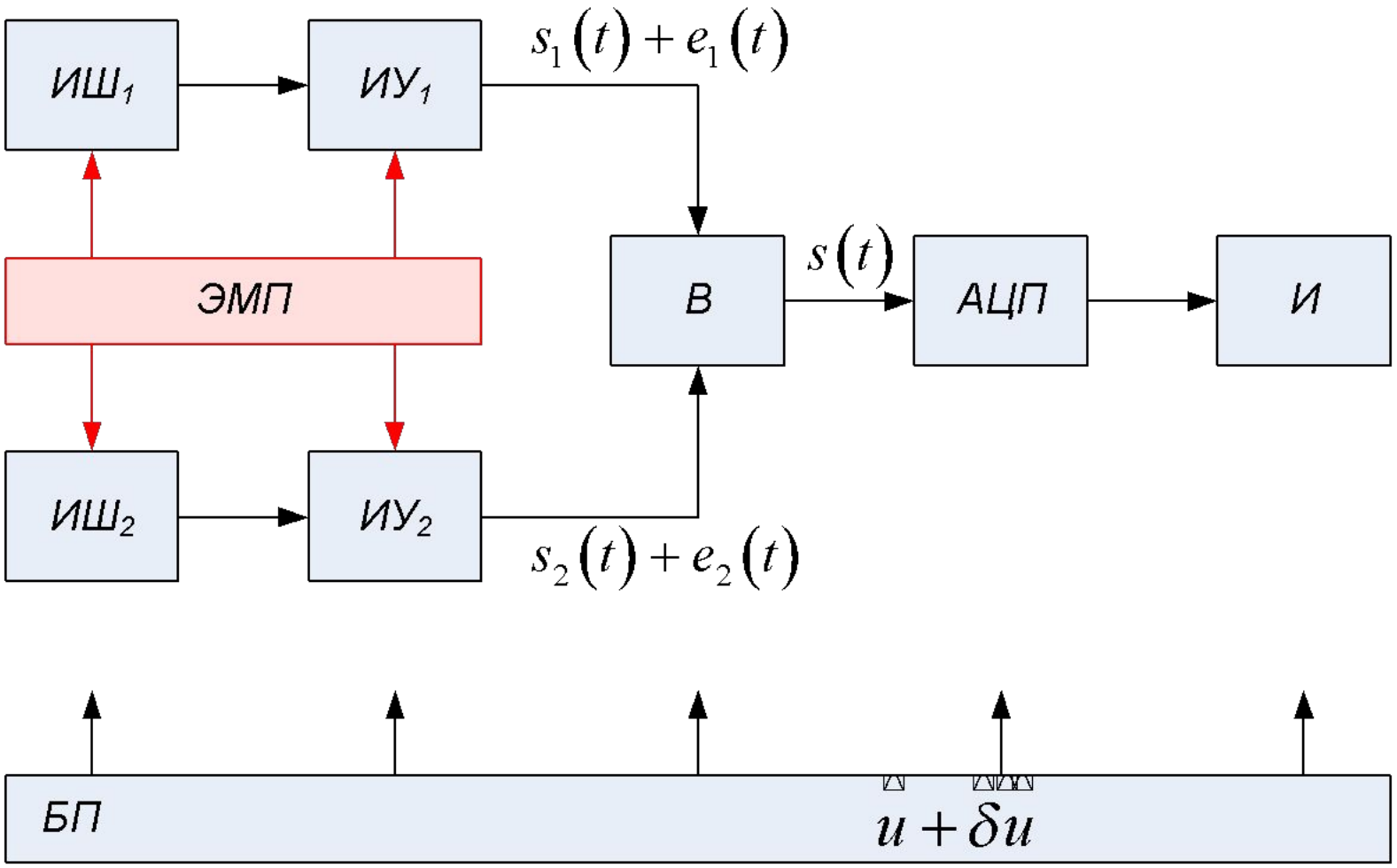
Математические основы и системотехнические решения извлечения случайности в условиях наличия ЭМП различной природы

Решение «в лоб»



Бородин А. В., МиСЗКИ, 2010

Решение с компенсацией ЭМП



Решение с компенсацией ЭМП

$$s(t) = \left(s_1(t) + e_1(t)\right) - \left(s_2(t) + e_2(t)\right) =$$

$$= \left(s_1(t) - s_2(t)\right) + \left(e_1(t) - e_2(t)\right)$$

$$\left.\begin{array}{c} s(t) = \left(s_1(t) - s_2(t)\right) - \left(e_1(t) - e_2(t)\right) \\ e_1(t) \approx e_2(t) \end{array}\right\} \Rightarrow s(t) \approx s_1(t) - s_2(t)$$

Математическое обоснование выбора принципа АЦП

Проблемы:

1) Переход от нормального распределения к равномерному
2) «Качания» питающих напряжений

Теорема

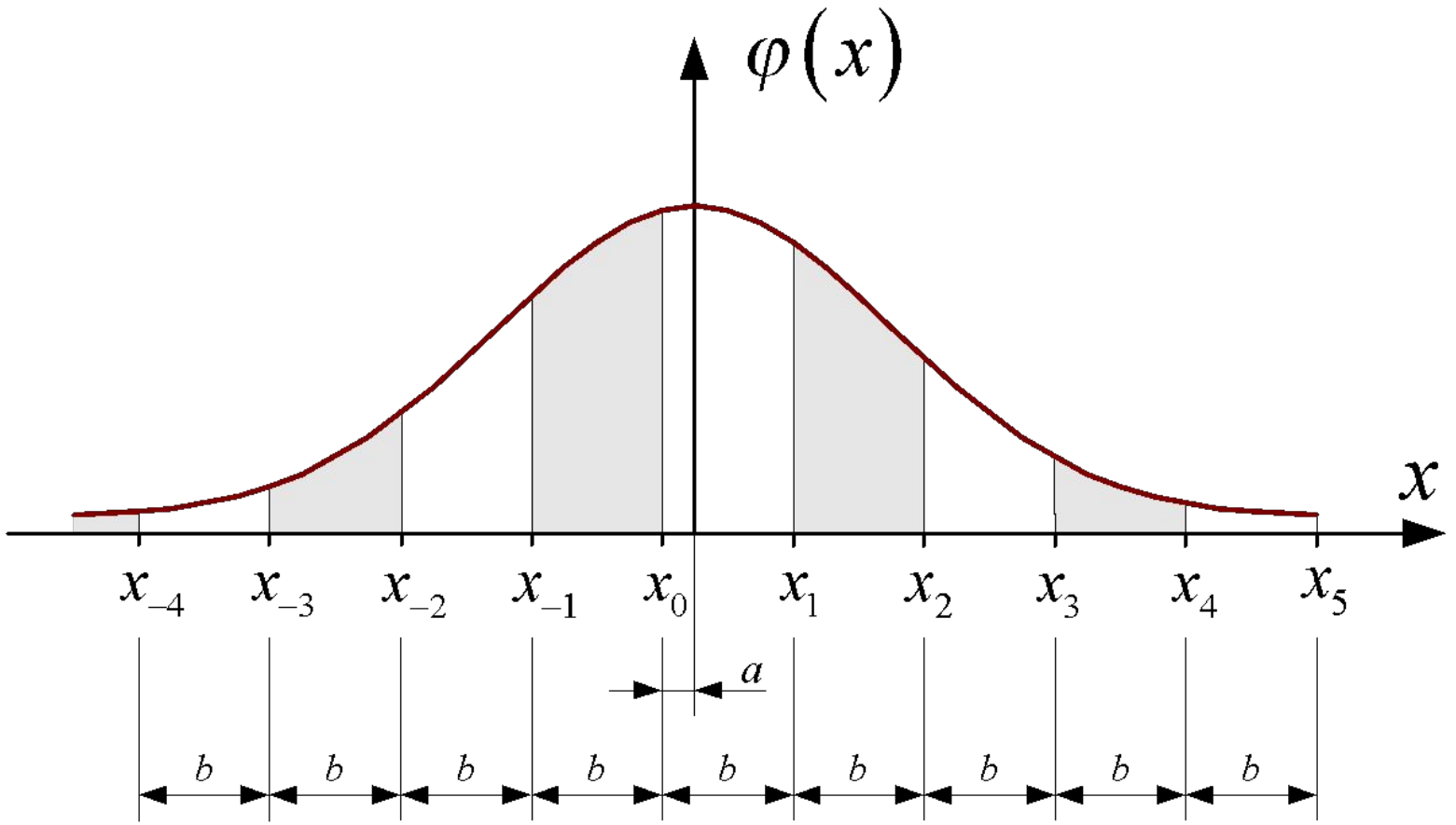
$$\forall k \left(k \in \mathbf{Z} \right) \left[x_{k+1} - x_k = b > 0 \right]$$

$$\varphi(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{x-\xi}{\sigma} \right)^2 \right]$$

$$\boxtimes_{k \in \mathbf{Z}} \left(x_{2k-1}, x_{2k} \right)$$

$$\boxtimes_{k \in \mathbf{Z}} \left(x_{2k}, x_{2k+1} \right)$$

Геометрическая интерпретация теоремы



План доказательства теоремы

$$F = P\left[x \in \boxtimes_{k \in \mathbf{Z}} \left(x_{2k}, x_{2k+1} \right) \right] - P\left[x \in \boxtimes_{k \in \mathbf{Z}} \left(x_{2k-1}, x_{2k} \right) \right]$$

$$x_k = k\,b + a, \;\; k \in \mathbf{Z}$$

$$F\left(0\right) = 0$$

$$\frac{\partial F}{\partial a} = 0$$

$$F\left(a\right) = 0 \quad \forall\, a$$

АЦП принадлежности

Z

$$\mathbf{Z}_{\pm n} = \{ -n, -n+1, \ldots , -1, 0, 1, 2, \ldots , n-1, n \}$$

Криптоанализ систем гарантированной секретности

ВОЗМОЖНО или **НЕ ВОЗМОЖНО** ?

Два подхода:

1) Ни что не случайно.
2) Идея модуляции среды.

О попытках:

источник **22** по «старым» лекциям!

Памятка о формате файлов для сдачи лабораторных работ

- Синтаксис именования
- Семантика содержания

Формальная грамматика именования

<Имя архивного файла> ::= *<Идентификатор лабораторной работы>*.**zip**

<Имя файла пояснительной записки> ::= *<Идентификатор лабораторной работы>*.**rtf**

<Идентификатор лабораторной работы> ::= *<Группа>*.*<Работа>*.*<ФИО>*.*<Версия>*
<Группа> ::= *<Поток><Номер>*
<Работа> ::= **LR***<Номер>*
<ФИО> ::= *<Фамилия><И><О><Полный тезка>*
<Версия> ::= **v***<Номер>*
<Поток> ::= **PS** | **VM** | **IVT**
<Номер> ::= *<Цифра><Цифра>*
<Фамилия> ::= *<Прописная буква><Последовательность строчных букв>*
<И> ::= *<Прописная буква>*
<О> ::= *<Прописная буква>*
<Полный тезка> ::= ∅ | *<Цифра>*

<Последовательность строчных букв> ::= ∅ | *<Последовательность строчных букв><Строчная буква>*
<Прописная буква> ::= **A** | **B** | ... | **Z**
<Строчная буква> ::= **a** | **b** | ... | **z**
<Цифра> ::= **0** | **1** | ... | **9**

Здесь: ∅ – «пустой» символ