

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)

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

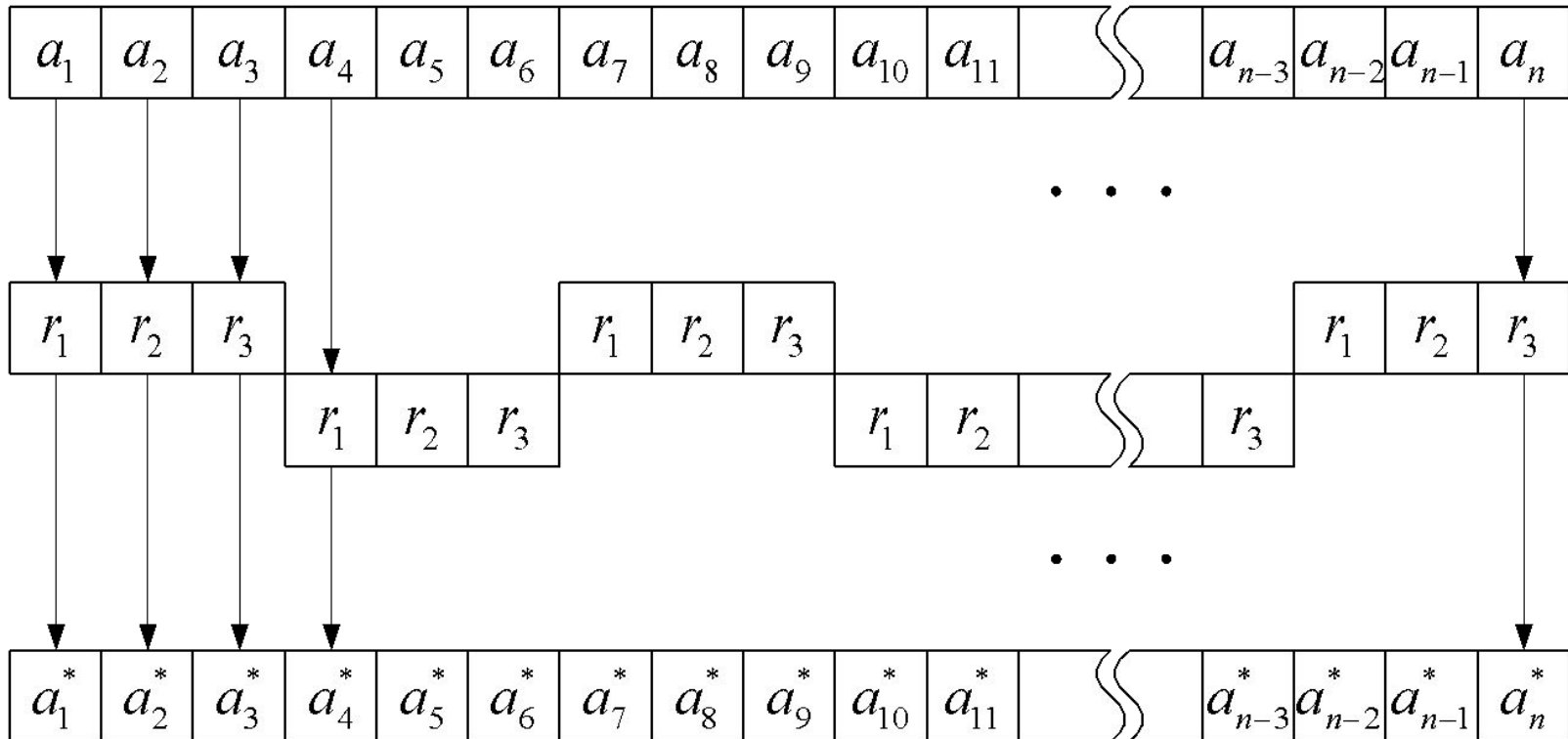
$$k \quad (r_i)_{i=1,2,\dots,n} \quad R^{(0)} \quad r_i \in R^{(0)}, \quad i=1,2,\dots,n$$

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

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

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

Короткопериодический ключ



Системы гарантированной секретности

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

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

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

Проблема получения
случайных равномерно
распределенных
над заданным алфавитом
последовательностей
на компьютерах с **фон**
Немановской 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 имеют 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



Feinwerktechnik
ELEKTROMECHANIK - FEINMECHANIK
701 LEIPZIG Karl-Liebknecht-Straße 11 · Telefon 30440

Spinthariskop



Länge 85 mm

max. Durchmesser . . . 40 mm

Gewicht mit Etui . . . 80 g

Im Spinthariskop kann man die Lichterscheinungen, welche durch das Auftreffen von α -Teilchen (Heliumkerne) auf die Zählzelle entstehen, beobachten.

Das Gerät wird im Etui geliefert.

Aktivität des RaD-Präparates etwa $0,5 \mu\text{C}$

Wirkung und Handhabung des Spinthariskopes:

Radioaktive Strahlen treffen beim Durchgang durch Materie mit Atomen zusammen. Sie treffen dabei zumeist nur die Atomhülle, wobei das getroffene Atom „angeregt“ und Energie in Form von Licht oder durch Auslösung chemischer Reaktionen frei wird. Solche Erscheinungen eignen sich zum Nachweis radioaktiver Substanzen.

s. Rückseite!
www.periodictable.ru

- Механические источники случайности



Лототроны

- Электрические источники
 - Шум газового разряда

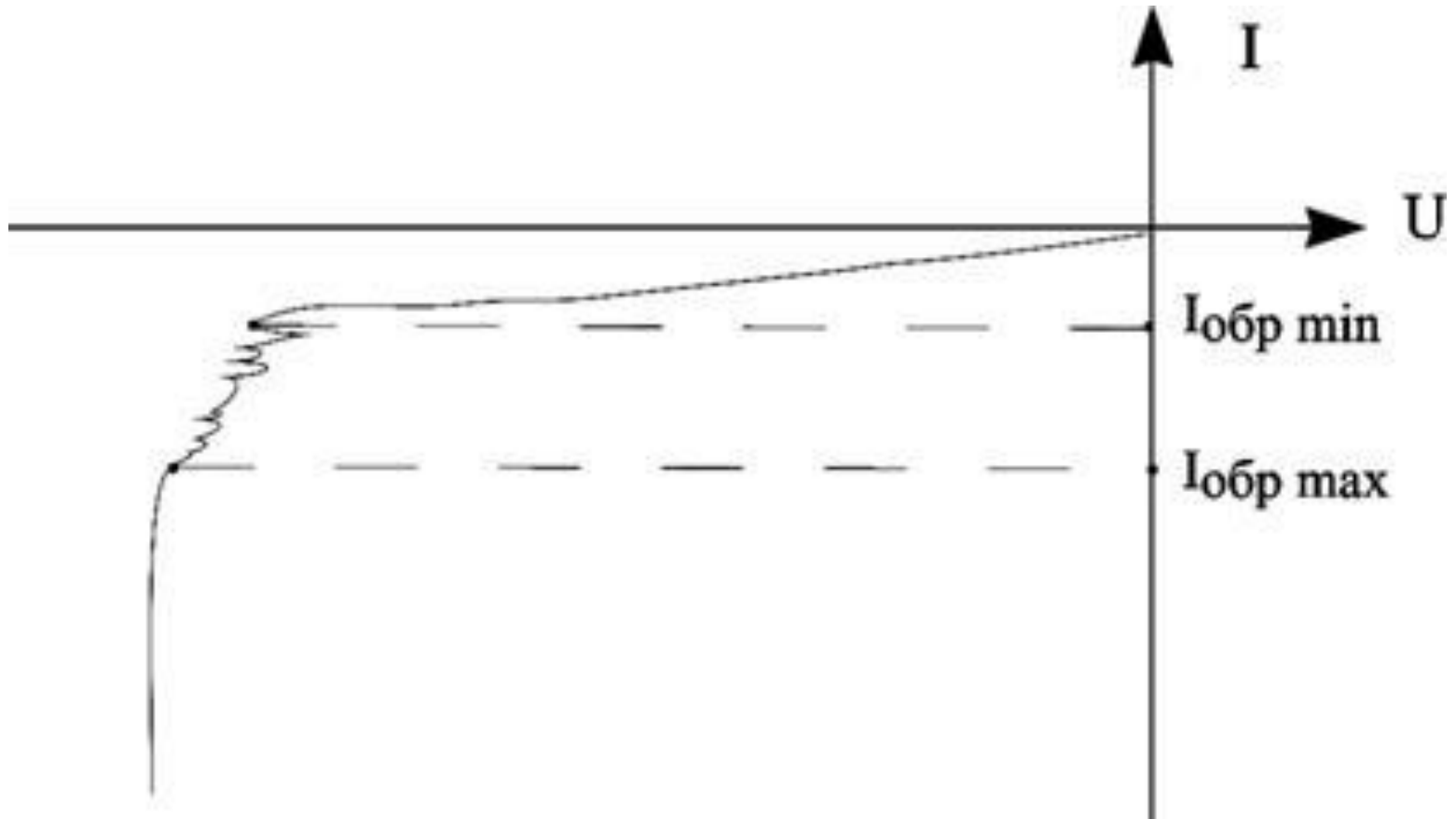


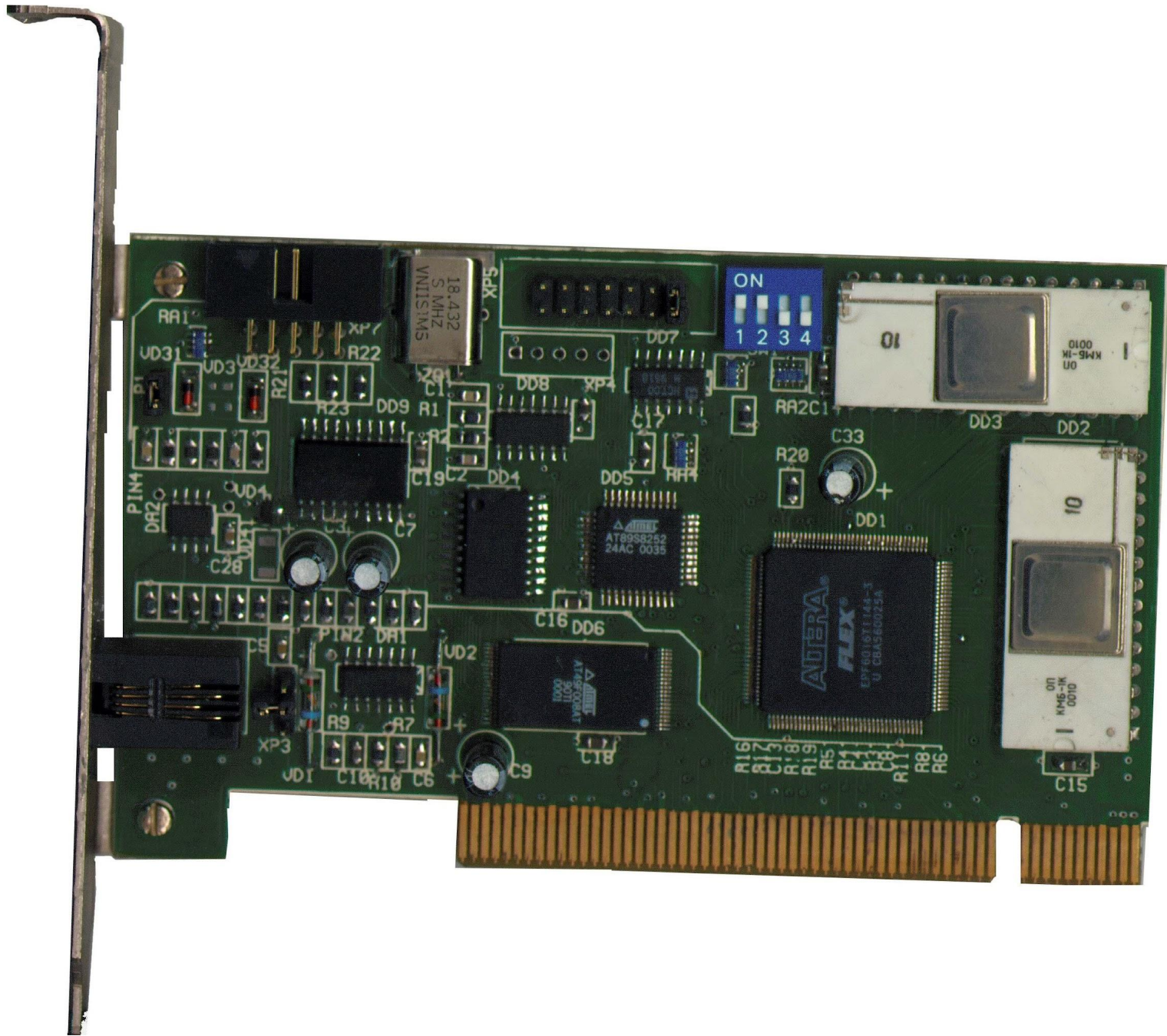
- Шумовые вакуумные диоды



*Шумовой
вакуумный
диод 2Д2С*

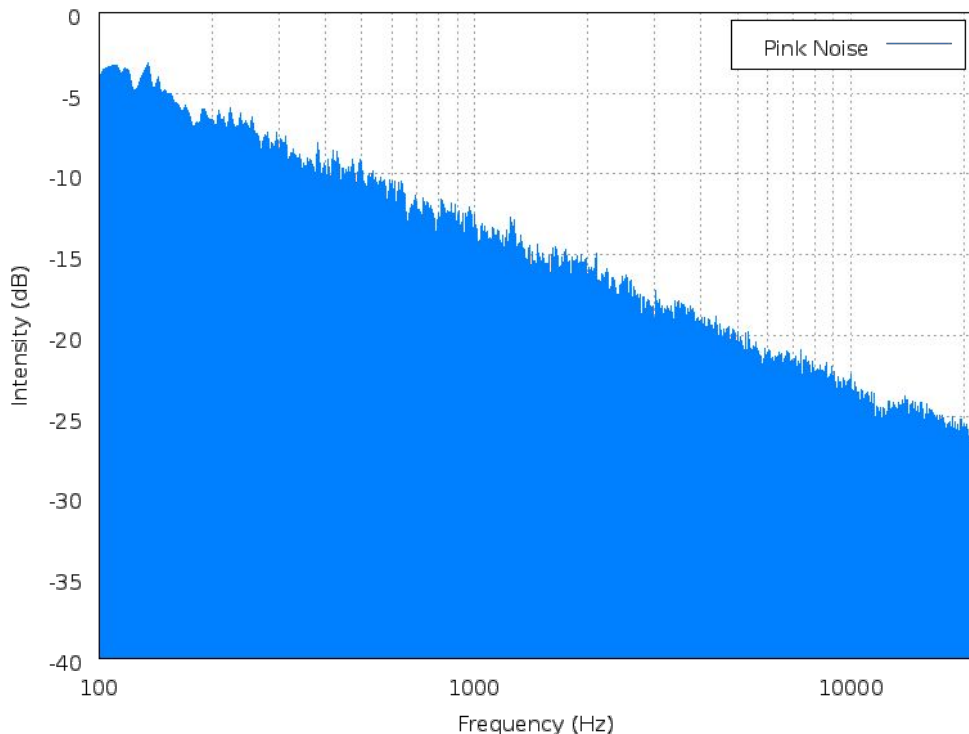
- Шумовые полупроводниковые диоды





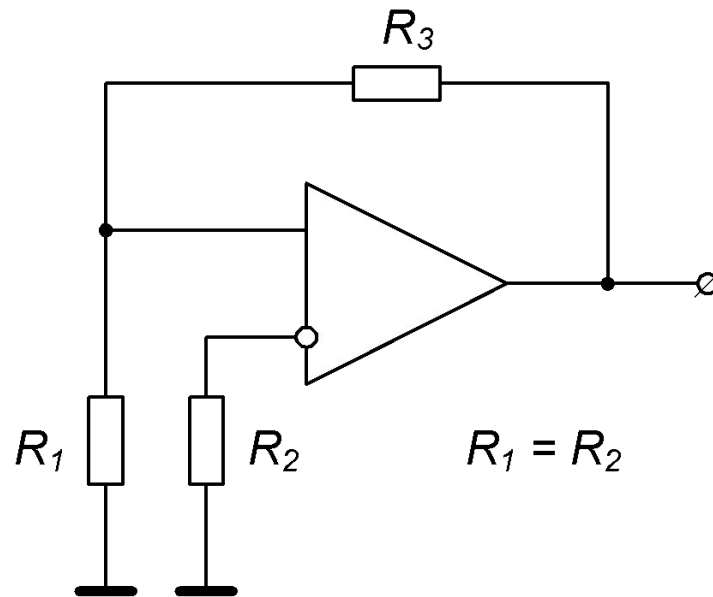
ФЛИККЕР-шум

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



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

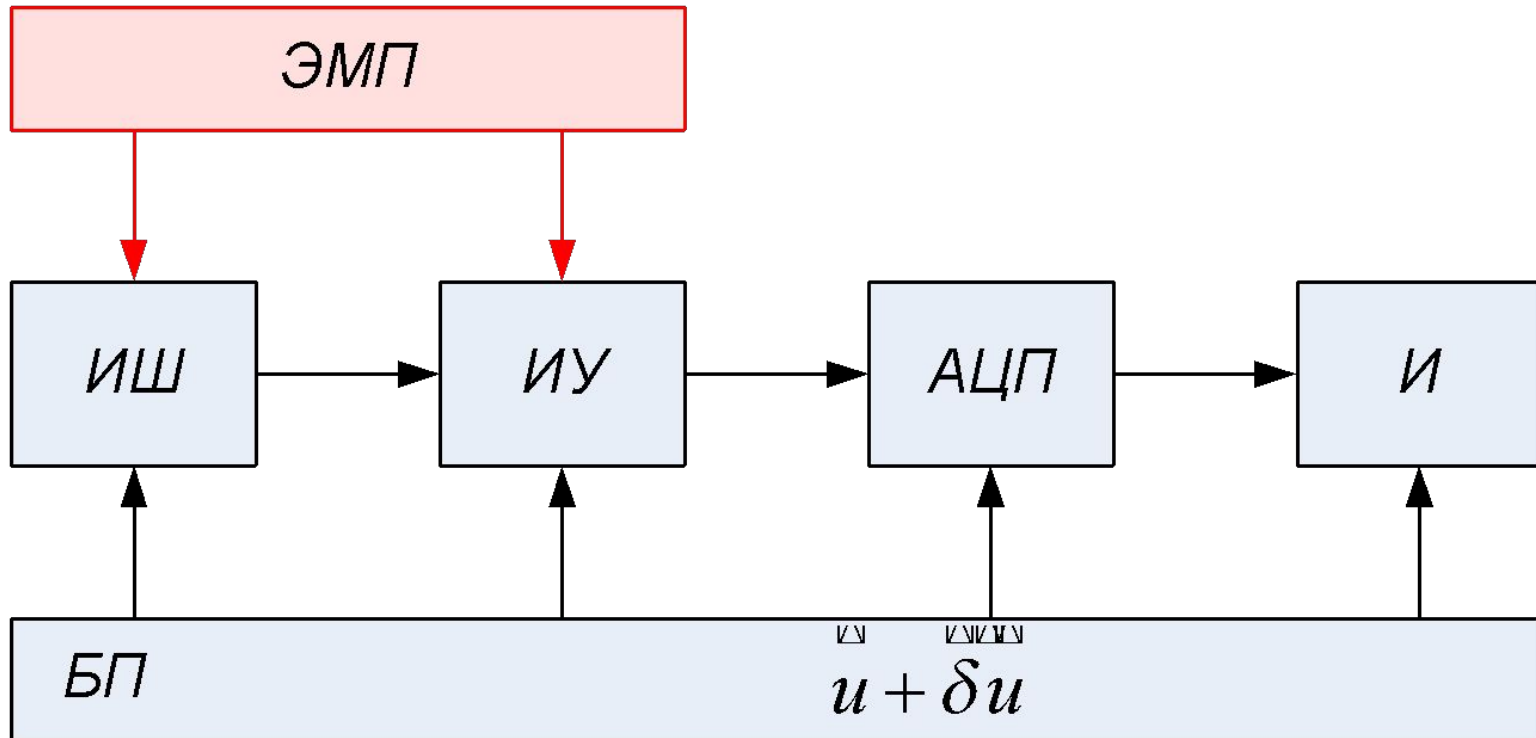
- Тепловой шум проволочных резисторов



Бородин А. В., МиСЗКИ, 2010

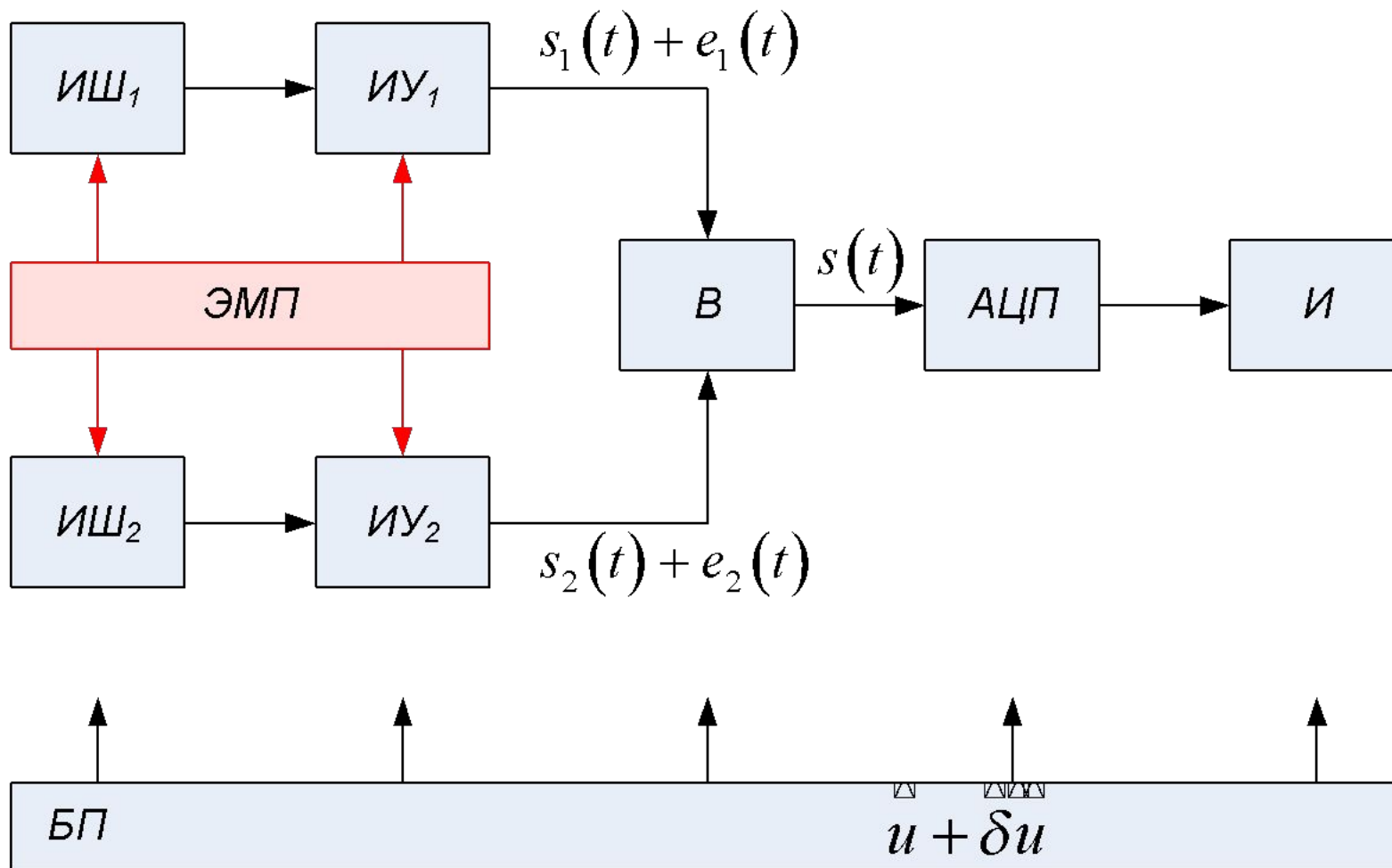
**Математические основы
и системотехнические решения
извлечения случайности в условиях
наличия ЭМП различной природы**

Решение «в лоб»



Бородин А. В., МиСЗКИ, 2010

Решение с компенсацией ЭМП



Решение с компенсацией ЭМП

$$\begin{aligned} s(t) &= (s_1(t) + e_1(t)) - (s_2(t) + e_2(t)) = \\ &= (s_1(t) - s_2(t)) + (e_1(t) - e_2(t)) \end{aligned}$$

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

Математическое обоснование выбора принципа АЦП

Проблемы:

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

Теорема

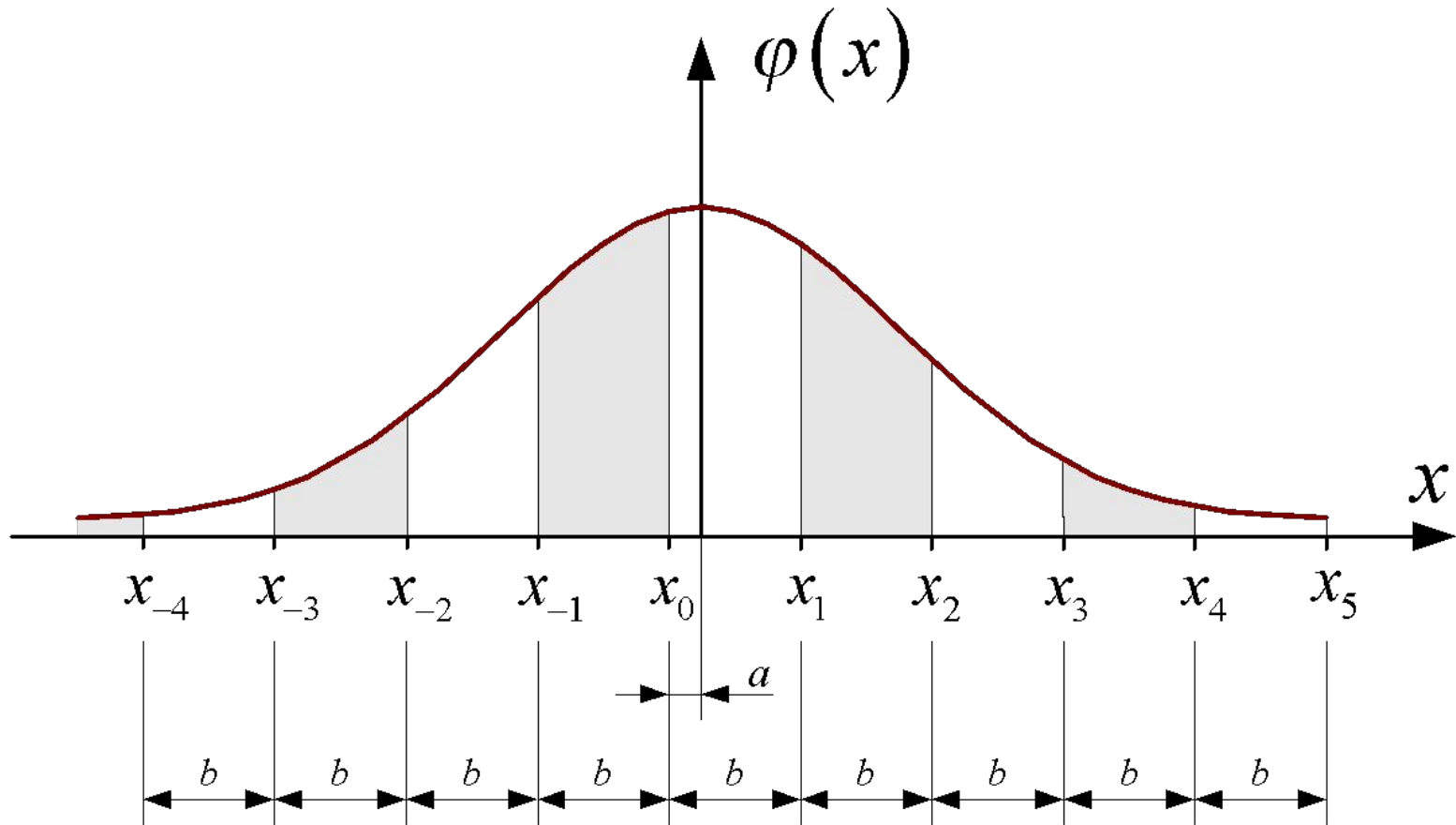
$$\forall k (k \in \mathbf{Z}) [x_{k+1} - x_k = b > 0]$$

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

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

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

Геометрическая интерпретация теоремы



План доказательства теоремы

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

$$x_k = kb + a, \quad k \in \mathbf{Z}$$

$$F(0) = 0$$

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

$$F(a) = 0 \quad \forall a$$

АЦП принадлежности

Z

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

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 именовани
- 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