

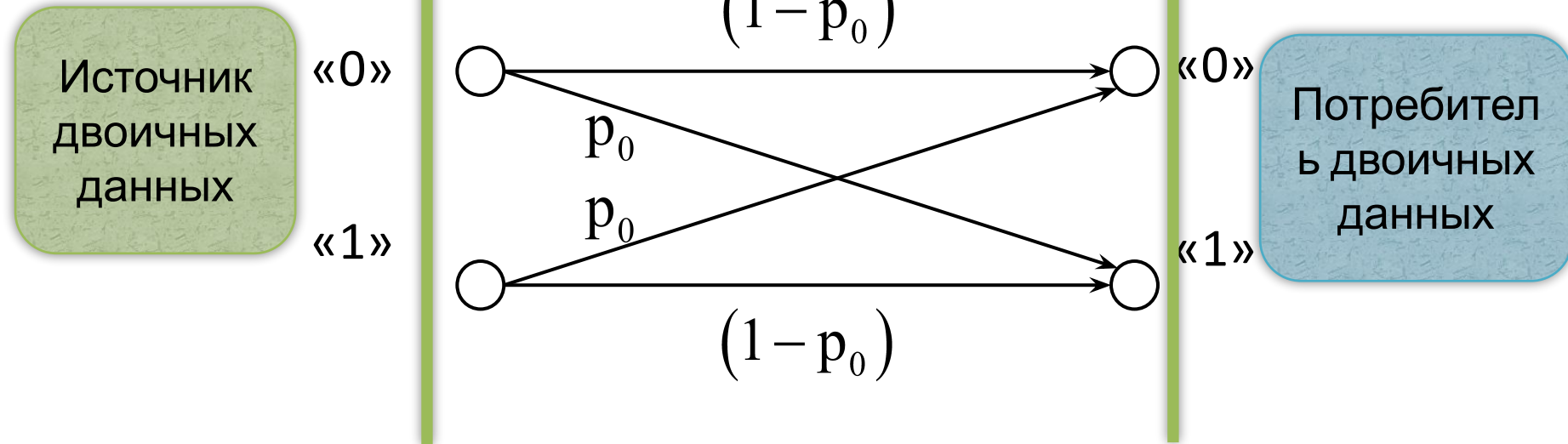
Введение в специальность

Лекция № 7

**Защита от случайных угроз (продолжение).
Защита целостности данных.**

1. Двоичная симметричная модель независимых

Среда распространения данных
в пространстве или во времени



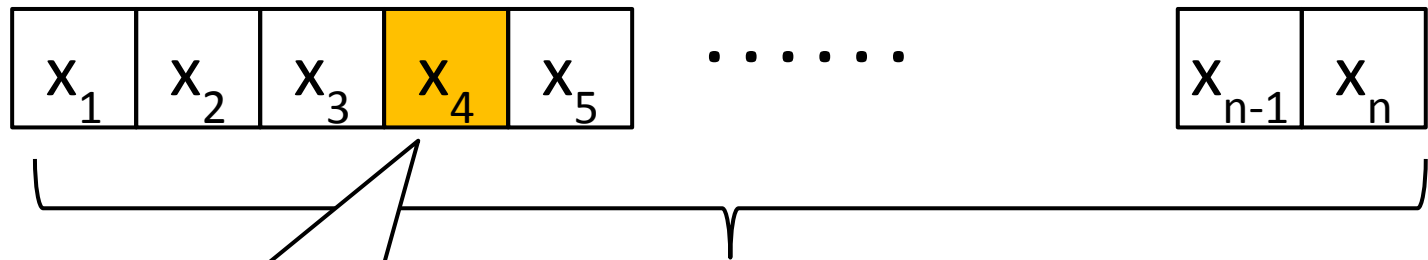
Вероятность искажения любого (произвольного) символа не зависит его значения (0 или 1) и от факта наличия или отсутствия искажений остальных символов потока:

$$\lim_{n \rightarrow \infty} \left(\frac{N_{\text{иск}}}{n} \right) = p_0$$

Искажение (инвертирование) отсутствует в любом двоичном символе с вероятностью:

$$1 - p_0$$

ПОТОК ДВОИЧНЫХ СИМВОЛОВ

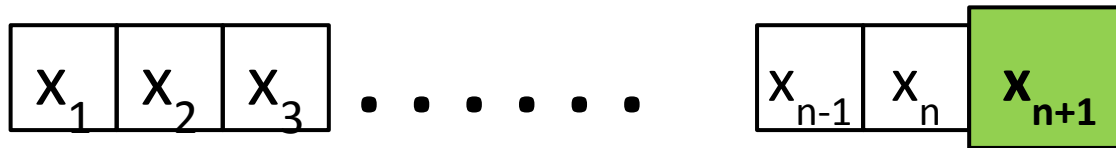


Искаженный
(инвертированный)
СИМВОЛ

$$x_i = [0, 1], \quad i = 1, 2, \dots, n$$

2. Код с проверкой на четность

Блок X содержащий " n " двоичных символов

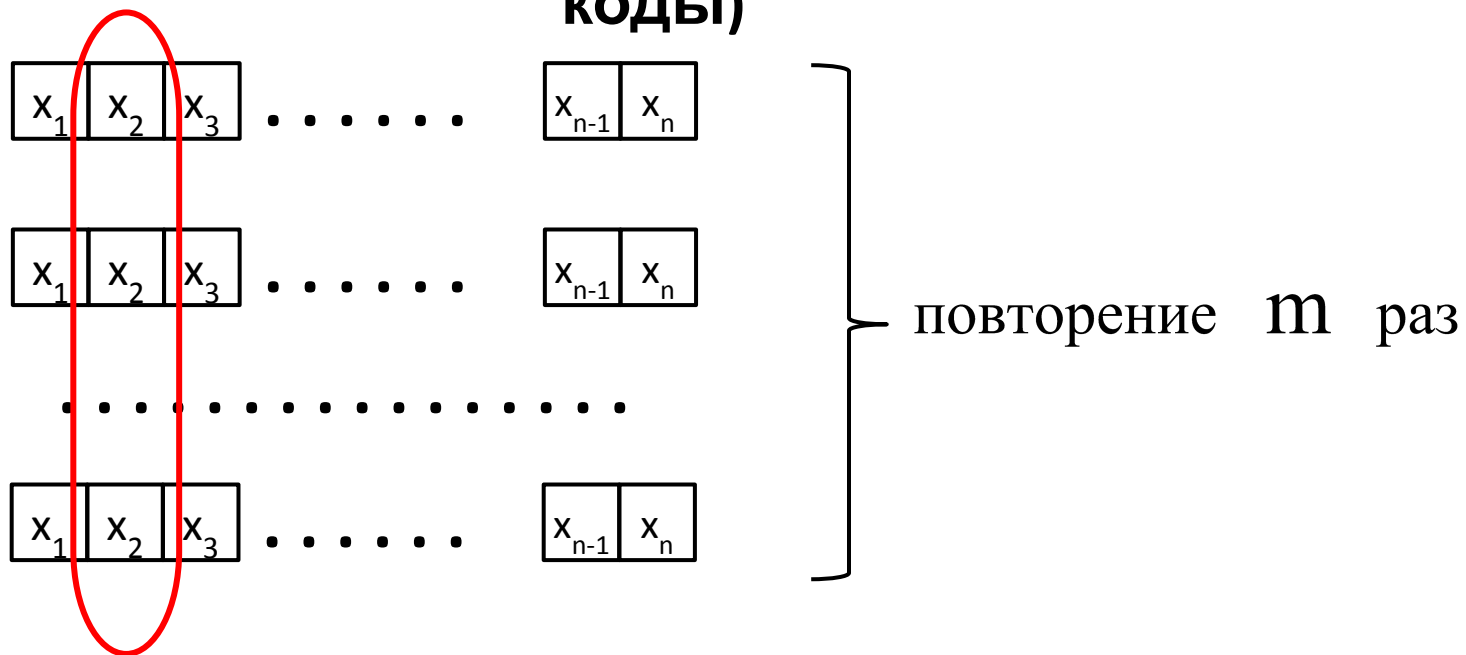


$$x_i = [0, 1], \quad i = 1, \dots, n.$$

Дополнительный
символ проверки
на четность

$$x_{n+1} = \begin{cases} 1, & \text{если число единичных символов блока } X \text{ нечетно;} \\ 0, & \text{если число единичных символов блока } X \text{ четно.} \end{cases}$$

3. Коды с повторением (мажоритарные коды)



Если $m = 2$ – возможно только обнаружение ошибок.

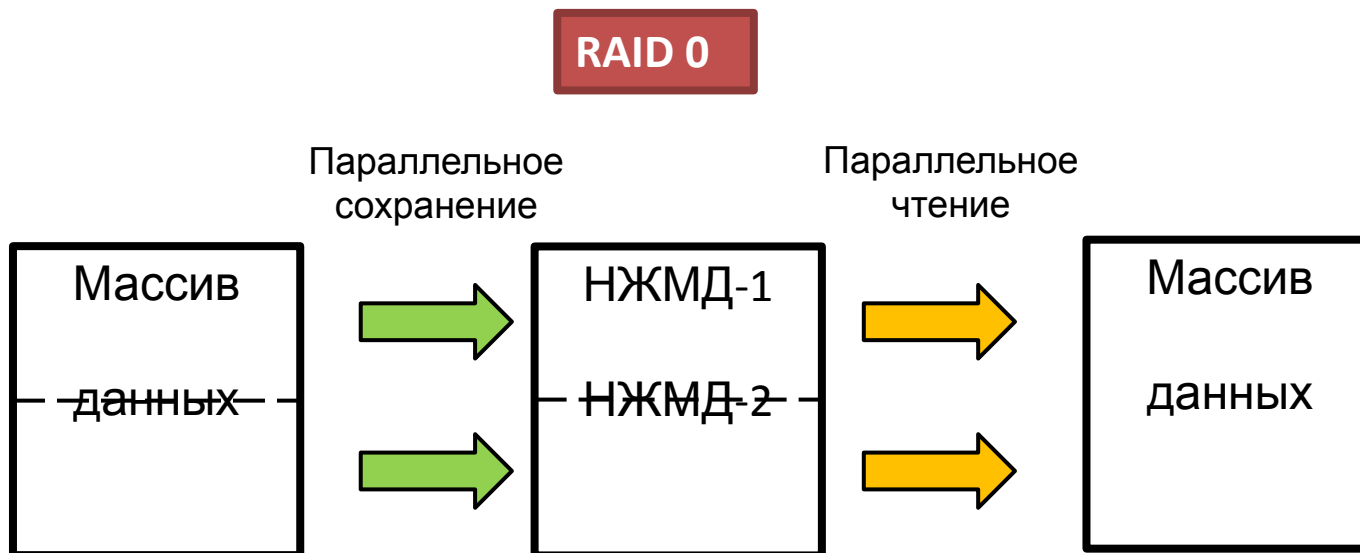
При $m > 2$ – возможно исправление ошибок.

Правило «голосования»:

$$x_i = \text{Round} \left\{ \frac{1}{m} \sum_{j=1}^m (x_i)_j \right\}$$

4. RAID - массивы хранения данных

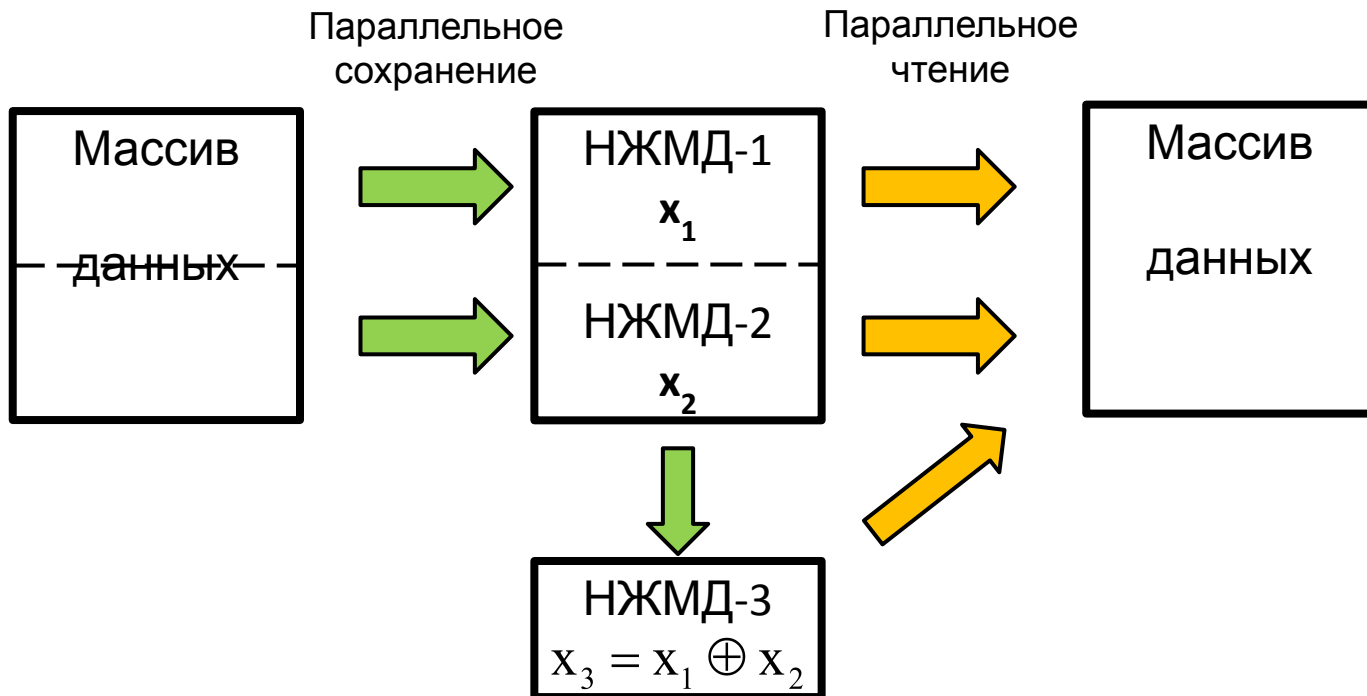
RAID – «redundant array of inexpensive disks» (избыточный (резервный) массив недорогих дисков)



Результат: ускорение процедуры обращения к жесткому диску, но **без защиты целостности**

RAID 1

- модификация кода с проверкой на четность



\oplus - оператор суммирования по модулю 2

$$x_3 = x_1 \oplus x_2 \quad \longrightarrow \quad \left\{ \begin{array}{l} x_1 = x_3 \oplus x_2 \\ x_2 = x_1 \oplus x_3 \end{array} \right.$$