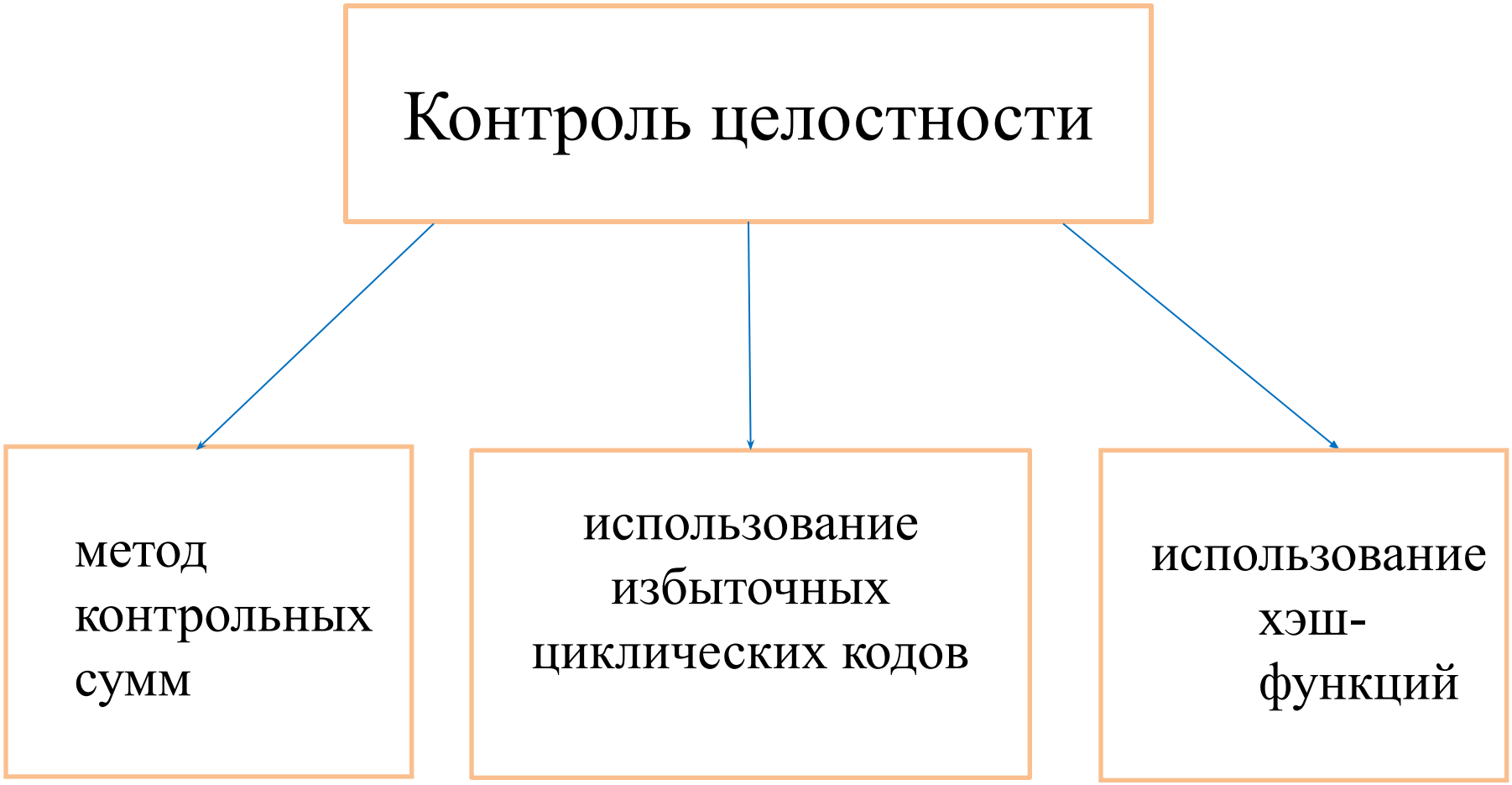
Контроль целостности


Контроль целостности
метод контрольных сумм
использование избыточных циклических кодов
использование хэш-функций


остаток от деления суммы всех чисел из входных данных на максимально возможное значение контрольной суммы
метод контрольных сумм
недостатки
несовпадение эталонного и рассчитанного значения контрольной суммы является явным доказательством изменения сообщения
неизменное значение контрольной суммы не является достаточным доказательством неизменности сообщения

Использование избыточных циклических кодов

избыточный код основан на полиноминальном распределении

каждый разряд последовательности данных соответствует коэффициенту полинома:

$0x^7+1x^6+0x^5+1x^4+0x^3+1x^2+0x^1+1x^0=x^6+x^4+x^2+1$

если полином разделить на специально подобранный полином, то получится полином-частное и полином-остаток

полином-остаток используется в качестве контрольной суммы

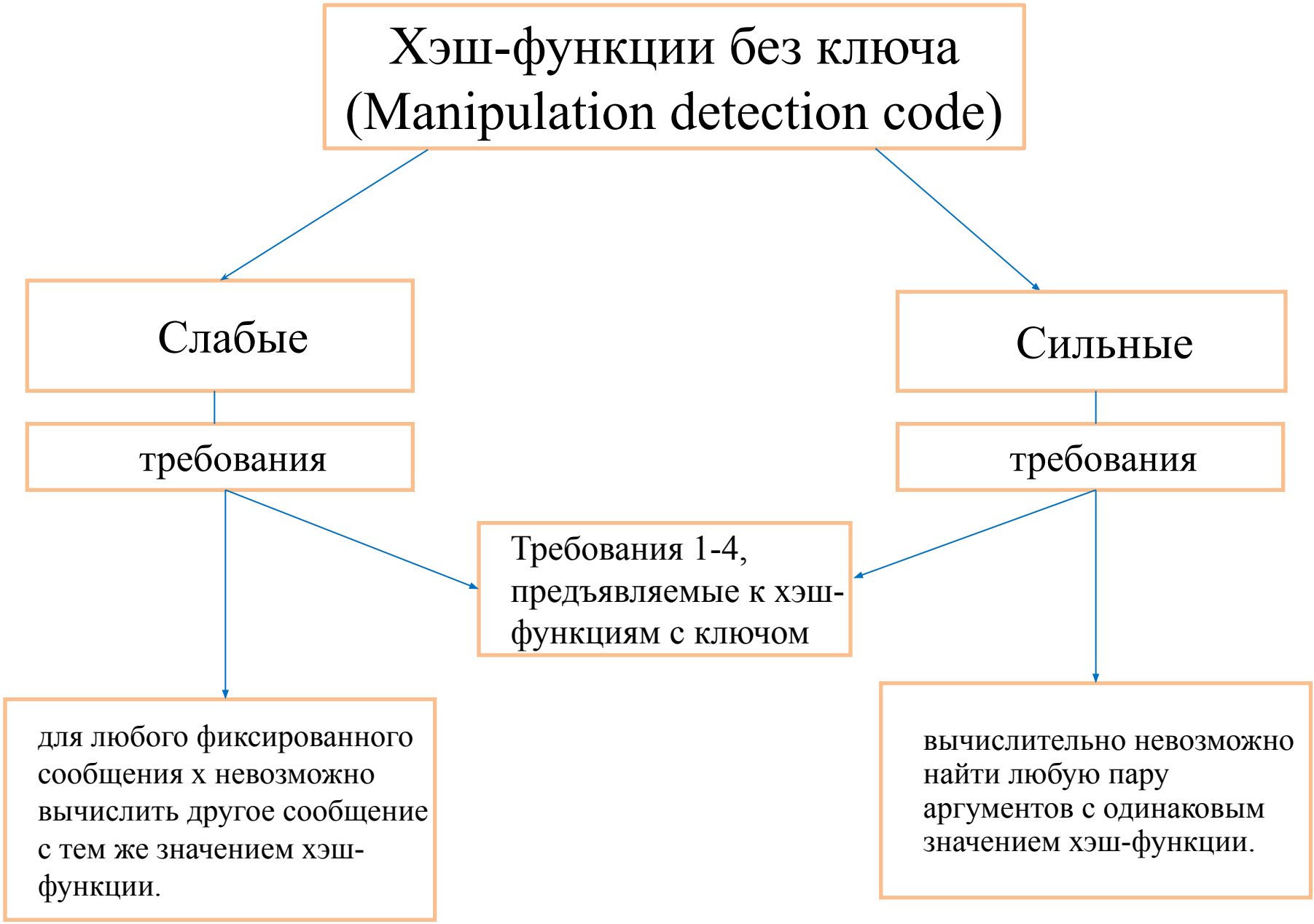
Особенности избыточных циклических кодов

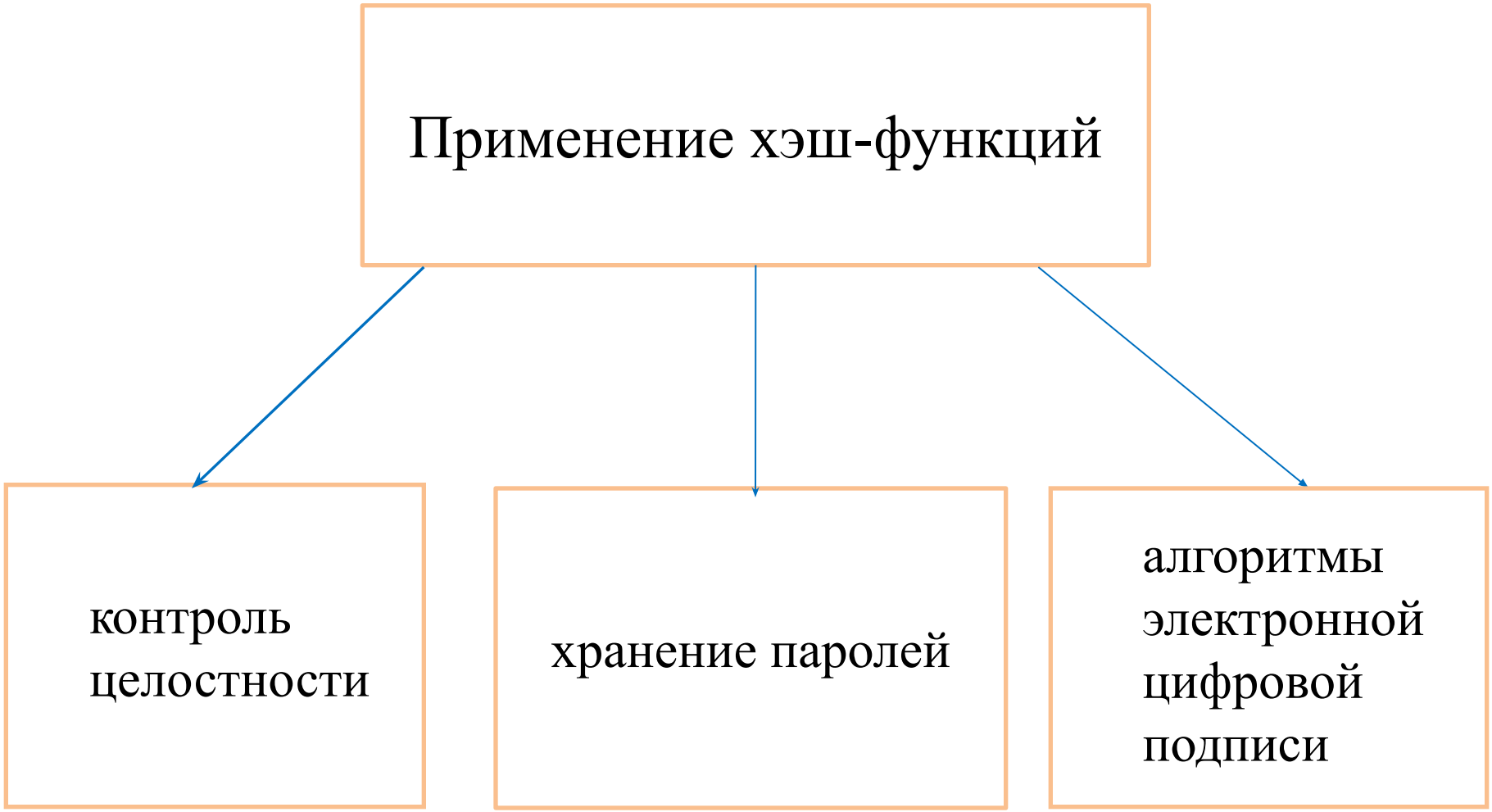
- обеспечивают большую надежность
- обнаруживаются любые перестановки битов (любое случайное изменение информации
- недостаточно надежны в случае преднамеренного изменения информации


односторонние функции, преобразующие строку произвольного размера в строку определенной длины
Хэш-функции
делятся на 2 класса
хэш-функции с ключом
хэш-функции без ключа

Хэш-функция с ключом H(k,x), где k – ключ, x – сообщение удовлетворяет требованиям:

- описание функции является открытым, ключ является секретным
- аргумент ***x*** – строка произвольного размера, а значение функции имеет фиксированную длину 256 бит
- по значению аргумента легко вычислить значение функции
- по значению функции невозможно восстановить значение аргумента
- должно быть трудно определить значение ключа по большому числу пар, состоящих из открытого текста и соответствующей ему хэш-функции, и невозможно вычислить хэш-функцию для иного значения аргумента


Хэш-функции без ключа
(Manipulation detection code)
Слабые
Сильные
требования
требования
Требования 1-4,
предъявляемые к хэш-
функциям с ключом
для любого фиксированного
сообщения x невозможно
вычислить другое сообщение
с тем же значением хэш-
функции.
вычислительно невозможно
найти любую пару
аргументов с одинаковым
значением хэш-функции.


Применение хэш-функций
контроль целостности
хранение паролей
алгоритмы электронной цифровой подписи