Размер вопроса алгоритму, значение счетчика

Размер вопроса алгоритму

Вопрос алгоритму – это блок данных определенной длины, которую аппаратный алгоритм может преобразовать за один прием (ср. с понятием Размер вопроса GrdTransform).

Для ввода размера вопроса служит одноименное поле в верхней правой части диалога. Рядом с полем указывается система счисления.

Размер вопроса зависит от типа алгоритма:

Тип алгоритма	**Размер вопроса, байтов**
Симметричный AES128	16
Асимметричный ECC160	20
Однонаправленный SHA256	32
Симметричный GSII64	8
Однонаправленные HASH64, RND64	8
Однонаправленный Stealth. *Однонаправленный алгоритм Stealth на сегодняшний день является морально устаревшим, его рекомендуется только для поддержания существующей системы защиты.*	4 – 255 (желательно использовать четные числа)

Значение счетчика

Счетчик алгоритма – специальное 4-байтовое поле, входящее в состав дескриптора алгоритма. Счетчик обычно используется для ограничения числа запусков алгоритма, а также в режимах зависимости алгоритма от счетчика.

Поле ввода **Значение счетчика** становится доступным при использовании флагов **Зависит от счетчика** или **С уменьшением счетчика**. Оно располагается в верхней правой части диалога. Рядом с полем указывается система счисления.