infotecs

Новости стандартизации в ТК 26

Алексей Уривский
секретариат ТК26
urivskiy@infotecs.ru

Новые национальные криптографические стандарты

ГОСТ Р 34.12-2015

Блочные шифры

ГОСТ Р 34.13-2015

Режимы работы блочных шифров

Дата введения: 01-01-2016

Новые национальные стандарты

ГОСТ Р 34.12-2015

- 128-битный шифр – «Кузнечик»
- 64-битный шифр – «Магма»

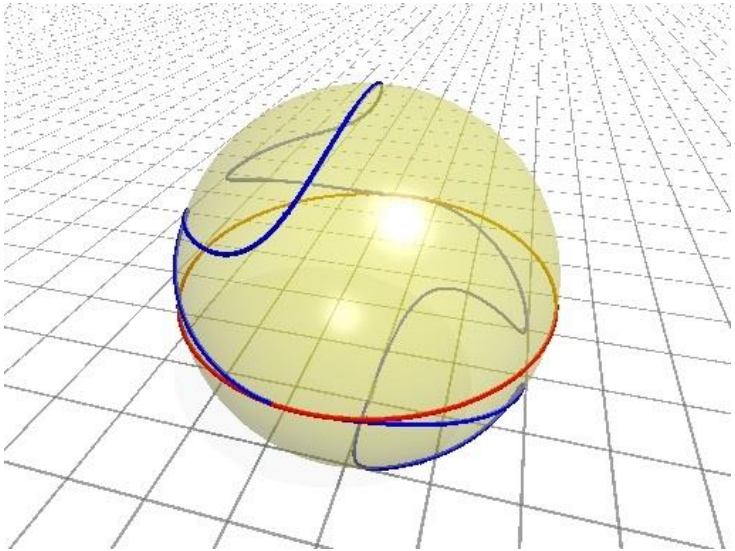
ГОСТ Р 34.13-2015

- 5 режимов шифрования
- режим выработки имитовставки

infotecs®

Параметры для ГОСТ Р 34.10-2012

"Рекомендации по стандартизации. Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012"



Международная стандартизация

3rd Working Draft
ISO/IEC 10118-3 Hash-functions –
Part 3: Dedicated hash-functions

International Organization for Standardization

Dedicated Hash-Function 11 (STREEBOG-512)
Dedicated Hash-Function 12 (STREEBOG-256)

infotecs

Спасибо!
Вопросы?

Алексей Уривский
urivskiy@infotecs.ru