

---

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

---



НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ

ГОСТ Р  
34.10—  
2012

---

**Информационная технология**

**КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА  
ИНФОРМАЦИИ**

**Процессы формирования и проверки электронной  
цифровой подписи**

Издание официальное



Москва  
Стандартинформ  
2013

## Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

### Сведения о стандарте

1 РАЗРАБОТАН Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТекС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст

4 ВЗАМЕН ГОСТ Р 34.10—2001

*Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет*

© Стандартинформ, 2013

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

## Содержание

1	Область применения . . . . .	1
2	Нормативные ссылки . . . . .	1
3	Термины, определения и обозначения . . . . .	1
3.1	Термины и определения . . . . .	1
3.2	Обозначения . . . . .	3
4	Общие положения . . . . .	3
5	Математические объекты . . . . .	4
5.1	Математические определения . . . . .	4
5.2	Параметры цифровой подписи . . . . .	5
5.3	Двоичные векторы . . . . .	6
6	Основные процессы . . . . .	6
6.1	Формирование цифровой подписи . . . . .	7
6.2	Проверка цифровой подписи . . . . .	9
	Приложение А (справочное) Контрольные примеры . . . . .	11
A.1	Пример 1 . . . . .	11
A.1.1	Параметры схемы цифровой подписи . . . . .	11
A.1.2	Процесс формирования цифровой подписи (алгоритм I) . . . . .	12
A.1.3	Процесс проверки цифровой подписи (алгоритм II) . . . . .	12
A.2	Пример 2 . . . . .	13
A.2.1	Параметры схемы цифровой подписи . . . . .	13
A.2.2	Процесс формирования цифровой подписи (алгоритм I) . . . . .	14
A.2.3	Процесс проверки цифровой подписи (алгоритм II) . . . . .	15
	Библиография . . . . .	16

## Введение

Настоящий стандарт содержит описание процессов формирования и проверки электронной цифровой подписи (ЭЦП), реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.

Необходимость разработки настоящего стандарта вызвана потребностью в реализации электронной цифровой подписи разной степени стойкости в связи с повышением уровня развития вычислительной техники. Стойкость электронной цифровой подписи основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11—2012.

Настоящий стандарт разработан с учетом терминологии и концепций международных стандартов ИСО 2382-2 [1], ИСО/МЭК 9796 [2]—[3], ИСО/МЭК 14888 [4]—[7] и ИСО/МЭК 10118 [8]—[11].