

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ

**ГОСТ Р  
34.11—  
2012**

**Информационная технология**

**КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**

**Функция хэширования**

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. № 216-ст

4 ВЗАМЕН ГОСТ Р 34.11—94

*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 . . . . .	2
4 Общие положения . . . . .	3
5 Значения параметров . . . . .	3
5.1 Инициализационные векторы . . . . .	3
5.2 Нелинейное биективное преобразование множества двоичных векторов . . . . .	3
5.3 Перестановка байт . . . . .	4
5.4 Линейное преобразование множества двоичных векторов . . . . .	4
5.5 Итерационные константы . . . . .	4
6 Преобразования . . . . .	5
7 Функция сжатия . . . . .	5
8 Процедура вычисления хэш-функции . . . . .	6
8.1 Этап 1 . . . . .	6
8.2 Этап 2 . . . . .	6
8.3 Этап 3 . . . . .	6
Приложение А (справочное) Контрольные примеры . . . . .	7
Библиография . . . . .	18

## Введение

Настоящий стандарт содержит описание алгоритма и процедуры вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах защиты информации, в том числе в процессах формирования и проверки электронной цифровой подписи.

Стандарт разработан взамен ГОСТ Р 34.11—94. Необходимость разработки настоящего стандарта вызвана потребностью в создании хэш-функции, соответствующей современным требованиям к криптографической стойкости и требованиям стандарта ГОСТ Р 34.10—2012 к электронной цифровой подписи.

Настоящий стандарт терминологически и концептуально увязан с международными стандартами ИСО 2382—2 [1], ИСО/МЭК 9796 [2—3], серии ИСО/МЭК 14888 [4—7] и серии ИСО/МЭК 10118 [8—11].

**Примечание** — Основная часть стандарта дополнена одним приложением:  
Приложение А (справочное) Контрольные примеры.