МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)

INTERSTATE COUNCIL FOR STANDARDIZATION. METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ

СТАНДАРТ

ГОСТ 34,10— 2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное

Москва
Стамдартимформ
2018

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стан* дартизации установлены в ГОСТ 1.0—2015 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2015 «Межгосударственная система стандартизации. Стандарты межгосударственные. правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия. обновления и отмены»

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 ПРИНЯТ Межгосударственным советом по метрологии, стандартизации и сертификации (протокол от 29 ноября 2018 г. № 54)

За принятие проголосовали:

Краткое наименование страны по МК {ИСО 31вв) 004-97	Ков страны по МК <ИСО31вв) 004-97	Соирашвнное наимекоммле национального органа по стандартизации
Армения	**AM**	**Минэкономики Республики Армения**
Киргизия	**KG**	**Кыргыэсгандарт**
Россия	**RU**	**Россгандарт**
Таджжистан	**TJ**	**Таджиксгандарт**

4 Приказом Федерального агентства по техническому регулированию и метрологии от 4 декабря 2018 г. N? 1059-ст межгосударственный стандарт ГОСТ 34.10—2018 введен в действие в качестве национального стандарта Российской Федерации с 1 июня 2019 г.

5 Настоящий стандарт подготовлен на основе применения ГОСТ Р 34.10—2012

6 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном 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 (www.gost.ru)

Содержание

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 34.11.

Настоящий стандарт разработан с учетом терминологии и концепций международного стандарта ИСО 2382 [1]. а также международных стандартов серий ИСО/МЭК 9796 [2]. (3]. ИСО/МЭК14888 [4]—(6) и ИСО/МЭК 10118 (71—{Ю].

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Information technology. Cryptographic data security.
Signature and verification processes of electronic digital signature

Дата введения — 2019—06—01

1 Область применения

Настоящий стандарт определяет схему электронной цифровой подписи (ЭЦП) (далее — цифровая подпись), процессы формирования и проверки цифровой подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения.

Внедрение цифровой подписи на основе настоящего стандарта повышает по сравнению с ранее действовавшей схемой цифровой подписи уровень защищенности передаваемых сообщений от подделок и искажений.

Настоящий стандарт рекомендуется применять при создании, эксплуатации и модернизации систем обработки информации различного назначения.

2 Нормативные ссылки

8 настоящем стандарте использована нормативная ссылка на следующий межгосударственный стандарт:

ГОСТ 34.11—2016 Информационная технология. Криптографическая защита информации. Функция хэширования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочного стандарта в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется 8 части, не затрагивающей згу ссылку.

3 Термины, определения и обозначения

3.1 Термины и определения

8 настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 дополнение (appendix): Строка бит. формируемая из цифровой подписи и произвольного текстового поля.

Примечание — Адаптировано из ИСО/МЭК 14888-1 [4].

Издание официальное

3.1.2 ключ подписи (signature key): Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом е процессе формирования цифровой подписи.

Примечание — Адаптировано из ИСО/МЭК 14888-1 (4).

3.1.3 ключ проверки подписи (verification key): Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.

Примечание — Адаптировано из ИСО/МЭК 14888-1 (4).

3.1.4 параметр схемы ЭЦП (domain parameter): Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам.

Примечание — Адаптировано из ИСО/МЭК 14888-1 (4].

3.1.5 подписанное сообщение (signed message): Набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения.

Примечание — Адаптировано из ИСО/МЭК 14888-1 (4).

3.1.6 последовательность псевдослучайных чисел (pseudo-random number sequence): Последовательность чисел, полученная в результате выполнения некоторого арифметического (вычислительного) процесса, используемая в конкретном случае вместо последовательности случайных чисел.

Примечание — Адаптировано из ИСО 2382 [1].

3.1.7 последовательность случайных чисел (random number sequence): Последовательность чисел, каждое из которых не может быть предсказано (вычислено) только на основе знания предшествующих ему чисел данной последовательности.

Примечание — Адаптировано из ИСО 2382 [1].

3.1.8 процесс проверки подписи (verification process): Процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки подписи и параметры схемы ЭЦП. результатом которого является заключение о правильности или ошибочности цифровой подписи.

Примечание — Адаптировано из ИСО/МЭК 14888-1 (4J.

3.1.9 процесс формирования подписи (signature process): Процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП. а в результате формируется цифровая подпись.

Примечание — Адаптировано из ИСО/МЭК 14888-1 (4].

3.1.10 свидетельство (witness): Элемент данных, представляющий соответствующее доказательство достоверности (недостоверности) подписи проверяющей стороне.

3.1.11 случайное число (random number): Число, выбранное из определенного набора чисел таким образом, что каждое число из данного набора может быть выбрано с одинаковой вероятностью.

Примечание — Адаптировано из ИСО 2382 [1].

3.1.12 сообщение (message): Строка бит произвольной конечной длины.

Примечание — Адаптировано из ИСО/МЭК 14888-1 (4J.

3.1.13 хэш-код (hash-code): Строка бит. являющаяся выходным результатом хэш-функции.

Примечание — Адаптировано из ИСО/МЭК 10118-1 [7].

3.1.14 хэш-функция (collision-resistant hash-function): Функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

1) по данному значению функции сложно вычислить исходные данные, отображаемые в это значение;

2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции;

3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

Примечания

1 Адаптировано из ИСО/МЭК 10118-1 [7].

2 Применительно к области электронной цифровой подписи свойство по перечислению 1) подразумевает. что по известной электронной цифровой подписи невозможно восстановить исходное сообщение: свойство по перечислению 2) подразумевает, что для заданного подписанного сообщения трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же электронную цифровую подпись: свойство по перечислению 3) подразумевает, что трудно подобрать какую-либо пару сообщений, имеющих одну и ту же подпись.

3 В настоящем стандарте в целях сохранения терминологической преемственности с нормативными документами. действующими на территории государства, принявшего настоящий стандарт, и опубликованными ранее на русском языке научно-техническими изданиями установлено, что термины «хэш-функция», «криптографическая хэш-функция», «функция хэширования* и «криптографическая функция хэширования» являются синонимами.

3.1.15 [электронная цифровая] подпись (signature); ЭЦП: Строка бит. полученная е результате процесса формирования подписи.

Примечания

1 Адаптировано из ИСО/МЭК 14888-1 [4].

2 Строка бит. являющаяся подписью, может иметь внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

3 В настоящем стандарте в целях сохранения терминологической преемственности с нормативными документами. действующими на территории государства, принявшего настоящий стандарт, и опубликованными ранее на русском языке научно-техническими изданиями установлено, что термины «электронная подпись*, «цифровая подпись» и «электронная цифровая подпись» являются синонимами.

3.2 Обозначения

8 настоящем стандарте применены следующие обозначения:

V, — множество всех двоичных векторов длиной / бит;

V* — множество всех двоичных векторов произвольной конечной длины:

Z — множество всех целых чисел;

p — простое число, *p* > 3;

F_p — конечное простое поле, представляемое как множество из р целых чисел {0.1..... р- 1);

Pfirtod р) — минимальное неотрицательное число, сравнимое с *b* по модулю р;

M — сообщение пользователя. *M* ь V;

(ftj' ||Л^) — конкатенация (объединение) двух двоичных векторов:

a. *b* — коэффициенты эллиптической кривой:

m — порядок группы точек эллиптической кривой;

q — порядок подгруппы группы точек эллиптической кривой;

О — нулевая точка эллиптической кривой;

P — точка эллиптической кривой порядка *q;*

d — целое число — ключ подписи:

Q — точка эллиптической кривой — ключ проверки подписи;

£ — цифровая подпись под сообщением *М.*

4 Общие положения

Общепризнанная схема (модель) цифровой подписи [4] охватывает следующие процессы:

- генерация ключей (подписи и проверки подписи);
- формирование подписи;
- проверка подписи.

6 настоящем стандарте процесс генерации ключей (подписи и проверки подписи) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами. которые устанавливают соответствующие параметры по взаимному согласованию.

Механизм цифровой подписи определяется посредством реализации двух основных процессов (см. раздел 6):

- формирование подписи (см. 6.2);
- проверка подписи (см. 6.3).

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче е системе подписанного сообщения:

- осуществление контроля целостности передаваемого подписанного сообщения:
- доказательное подтверждение авторства лица, подписавшего сообщение;
- защита сообщения от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 1.

Дополнение

Рисунок 1 — Схема подписанного сообщения

Поле «Текст», показанное на данном рисунке и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем. а также хэш-функции.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритмы вычисления хэш-функции установлены в ГОСТ 34.11.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки, определены в 5.3. 8 настоящем стандарте предусмотрена возможность выбора одного из двух вариантов требований к параметрам.

Настоящий стандарт не определяет процесс генерации параметров схемы цифровой подписи. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы цифровой подписи, исходя из требований к аппаратно-программным средствам, реализующим электронный документооборот.

Цифровая подпись, представленная е виде двоичного вектора длиной 512 или 1024 бита, должна вычисляться с помощью определенного набора правил, изложенных в 6.2.

Набор правил, позволяющих принять либо отвергнуть цифровую подпись под полученным сообщением. установлен в 6.3.

5 Математические объекты

5.1 Общие положения математических объектов

Для определения схемы цифровой подписи необходимо описать базовые математические объекты, используемые в процессах ее формирования и проверки. 8 настоящем разделе установлены основные математические определения и требования, предъявляемые к параметрам схемы цифровой подписи.

5.2 Математические определения

Эллиптической кривой *E.* определенной над конечным простым полем F_p (где p > 3 — простое число), называется множество пар чисел (x. y), x, *y* ь F_p, удовлетворяющих тождеству

$$y^2 \text{ в } x^3 \blacklozenge ax + b \pmod p. \quad (1)$$

где *a. b* 6 F_p и $4a^3 + 27 Ь^2$ не сравнимо с нулем по модулю p.

Инвариантом эллиптической кривой называется величина *J(E),* удовлетворяющая тождеству

J<£)r1728^W(mo<I'>,■ ®

Коэффициенты a. *b* эллиптической кривой *E* по известному инварианту J(£) определяются следующим образом:

f ’ as3A(modp).

lbe2A(modp).

где A' J £) (modp). J(£)*0 **WW1728.**
1728-J(£

Пары *(x,* y), удовлетворяющие тождеству (1). называются «точками эллиптической кривой *E»; x* и y — соответственно x- и /-«координатами точки».

Точка эллиптической кривой обозначается **O(x.** y) или просто *Q.* Две точки эллиптической кривой равны, если равны их соответствующие x- и y-координаты.

На множестве всех точек эллиптической кривой *E* введем операцию сложения, которую будем обозначать знаком «+». Для двух произвольных точек ОДх,, у,) и $\mathbf{0_2\{x_2.}$ y_2) эллиптической кривой *E* рассмотрим несколько случаев.

Для точек Q, и Q_2, координаты которых удовлетворяют условию x_1 # их суммой называется ючка $Q_3\{x_3. y_3)$, координаты которой определяются сравнениями

$$x_3=X^2 -x, -x_2(\text{mod}p),$$
$$y\text{^}Xf\text{^}-x\text{^}-y\text{^}\text{mod}p). \quad (4)$$

где *Ksi* $\frac{y_2 - y}{x_2 - x_1}$(mod p).

Если выполнены равенства x_1 в x_2 и *y,* в y_2 * 0. то координаты точки O_3 определяются следующим образом:

$$x\text{^}sX^2 -2x, (\text{mod}p),$$
$$y_3aX(x,-x_3)-y_1(\text{mod}p). \quad (5)$$

гц« Ха $\frac{3xf+a}{^2y|}$ (modp).

Если выполнены условия $x_1 = x_2$ и у, а ~y_2 (modp), то сумма точек О, и O_2 называется нулевой точкой О без определения ее **х- и** /-координат. 8 этом случае точка O_2 называется отрицанием точки O_r Для нулевой точки О выполнены равенства

$$Q+O=O + Q=Q. \quad (6)$$

где *Q* — произвольная точка эллиптической кривой *E.*

Относительно введенной операции сложения множество всех точек эллиптической кривой *E* вместе с нулевой точкой образуют конечную абелеву (коммутативную) группу порядка *m,* для которого вы* полнено неравенство

$$p+1-2\sqrt{p}\le m\le p + 1 + 2\sqrt{p}. \quad (7)$$

Точка О называется «точкой кратности Х» или просто «кратной точкой эллиптической кривой Е». если для некоторой точки *P* выполнено равенство

$$\underbrace{Qa P + ... + Pa}_{k} XP. \quad (8)$$

5.3 Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

* простое число р — модуль эллиптической кривой;
* эллиптическая кривая *E,* задаваемая своим инвариантом *J{E)* или коэффициентами а. Ьь F_p;
* целое число *m* — порядок группы точек эллиптической кривой *E;*
* простив число *д* — порядок циклической подгруппы группы точек эллиптической кривой *E,* для которого выполнены следующие условия:

$$\text{гл » пр. л е Z. л a l}$$
$$2^{2м}<p<2»в \text{ или } 25°8<p<2«1^2; \quad (9)$$

- точка Р # О эллиптической кривой *E* с координатами (x_p, y_p), удовлетворяющая равенству рР - *О:*

■ хэш-функция /):У*-»$У_p$ отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные векторы длины / бит. Хэш-функция определена в ГОСТ 34.11. Если $2^{254}<p<2^{25в}$, то/=256. Если $2^{50а}<p<2^{512}$. то/=512.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

- ключом подписи — целым числом tf. удовлетворяющим неравенству 0< *d*< р:

« ключом проверки подписи — точкой эллиптической кривой Q с координатами (x_g. y_Q). удовлетворяющей равенству *dP - Q.*

К приведенным выше параметрам схемы цифровой подписи предъявляют следующие требования:

« должно быть выполнено условие p^1 * 1 (mod p), для всех целых f = 1. 2. ... в. где *B* - 31. если $2^{254} < p < 2^{256}$. и *B* = 131, если $2^{508} < p < 2^{512}$;

* должно быть выполнено неравенство *m*p;*

« инвариант кривой должен удовлетворять условию *J(E)* * 0 и J(£) # 1728.

5.4 Двоичные векторы

Для определения процессов формирования и проверки цифровой подписи необходимо установить соответствие между целыми числами и двоичными векторами длины *l* бит.

Рассмотрим следующий двоичный вектор длиной / бит, в котором младшие биты расположены справа, а старшие — слева:

$$Л»(о_{м}.....Лф),\ heUp \qquad (10)$$

где в;, / = 0.....У - 1 равно либо 1. либо 0.

Число aeZ соответствует двоичному вектору *Л,* если выполнено равенство

$$a«Sa,2\text{-}. \qquad (11)$$

Для двух двоичных векторов

$$.....“»’• \qquad (12)$$

$$*2= (P\text{-}1..... Pe)\text{-}$$

соответствующих целым числам аир. операция конкатенации (объединения) определяется следующим образом:

$$..... “o\text{-}P/\text{--}t.....Po)\text{-} \qquad (18)$$

Объединение представляет собой двоичный вектор длиной *21* бит. составленный из коэффициентов векторов и $Л_2$.

Формулы (12) и (13) определяют способ разбиения двоичного вектора А, || *Ь? агмнем 2!* бит на два двоичных вектора длиной *1* бит. конкатенацией которых он является.

6 Основные процессы

6.1 Общие положения

В настоящем разделе определены процессы формирования и проверки цифровой подписи под сообщением пользователя.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, соответствующие требованиям 5.3.

Кроме того, каждый пользователь должен иметь ключ подписи *d* и ключ проверки подписи $Q(x_q, y_g)$. которые также должны соответствовать требованиям 5.3.

6.2 Формирование цифровой подписи

Для получения цифровой подписи под сообщением *м* ь *V** необходимо выполнить следующие действия (шаги) по алгоритму I:

Шаг 1 — вычислить хэш-код сообщения *M: h* я й(М). (14)

Шаг 2 — вычислить целое число а. двоичным представлением которого является вектор *h.* и определить

$$e = a(mod<j). \qquad (15)$$

Если е = 0. то определить *в* - 1.

Шаг 3 — сгенерировать случайное (псевдослучайное) целое число *К* удовлетворяющее неравенству

$$Q<k<q. \qquad (16)$$

Шаг 4 — вычислить точку эллиптической кривой С = *кР* и определить

$$г = x_c\ (mod\ q). \qquad (17)$$

где x_c — х-координата точки С.

Если *г* - 0. то необходимо вернуться к шагу 3.

Шаг 5 — вычислить значение

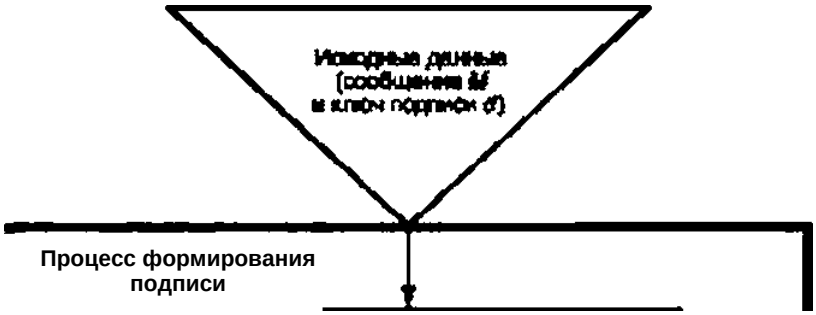
$$s = (rc/+Ae)(modg). \qquad (16)$$

Если s = 0. то необходимо вернуться к шагу 3.

Шаг **в —** вычислить двоичные векторы Г и ?, соответствующие / и в. и определить цифровую подпись £ *(Г Ц s) как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи *d* и подписываемое сообщение *М.* а выходным результатом — цифровая подпись

Схема процесса формирования цифровой подписи приведена на рисунке 2.



Шаг 1 - **вычислить яигчад сообщаем М**

I —

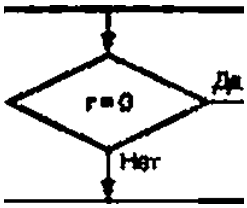
Шаг 2 - вычисление « и огредоени» е

I --

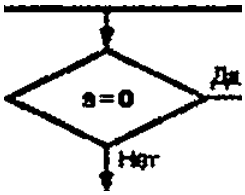
Шаг 3 - owaatqxaan» опуайЫое тшадоегомайм»э) малое чиале *к*

I

Uta г 4 - вычисление кия, алл ятгичаосй Ф«о0 С «АР,



Шаг 5 - вычисление *в*



Ши* в - определение цифровой подписи 5

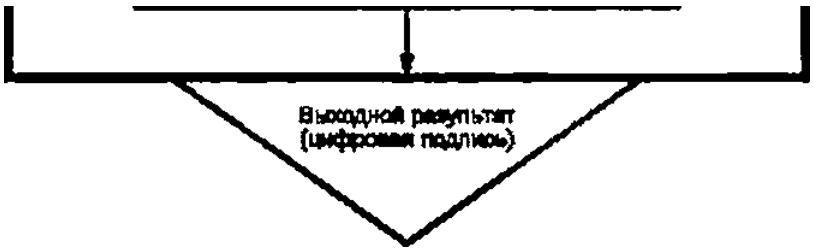


Рисунок 2 — Схема процесса формирования цифровой подписи

6.3 Проверка цифровой подписи

Для проверки цифровой подписи £ под полученным сообщением *M* необходимо выполнить следующие действия (шаги) по алгоритму II:

Шаг 1 — по полученной подписи £ вычислить целые числа г **и** s. Если выполнены неравенства 0 < *г* < Q. 0 < s < o. то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2 — вычислить хэш-код полученного сообщения *M*

(19)

Шаг 3 — вычислить целое число а. двоичным представлением которого является вектор *h,* и определить

eea(modQ). (20)

Если е = 0. то определить е - 1.

Шаг 4 — вычислить значение иве ’(modp). (21)

Шаг 5 — вычислить значения

z, в sn(mod o).^ **в** -/v(mod q). (22)

Шаг 6 — вычислить точку эллилтичесхой кривой С « z,P + z_2Q и определить

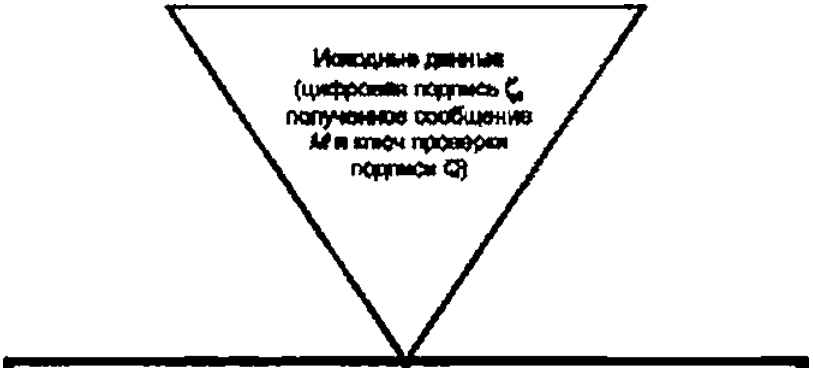
RBX_c(mod<j), (23)

где x_c — X'координата точки С.

Шаг 7 — если выполнено равенство ***R - /,*** **1О(юдписы1ринимае1си. и промином случае— подпись** неверна.

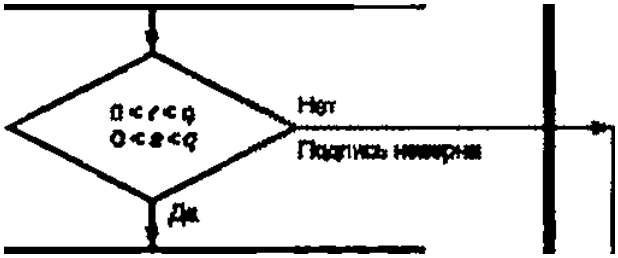
Исходными данными этого процесса являются подписанное сообщение *M.* цифровая подпись *Q* и ключ проверки подписи О. а выходным результатом — свидетельство о достоверности или ошибочности данной подписи.

Схема процесса проверки цифровой подписи приведена на рисунке 3.



Процесс проверим
поцгмпи

Шаг 1 -вьаввпвннеги «по полученной подписи £



Шаг *2* - вычислить х»uM«fl полученного сообщай ин j **W**

Шаг а • вычисление а н адрааюаниа а

швг 4 - **яычивлвнм *v***

I

Шаг 6-вычислены» а,

I...

Шаг в - *вымапан* ив точи алл иптнчкасй фвС"Х)Я* *а&* иоцмиалммЯ

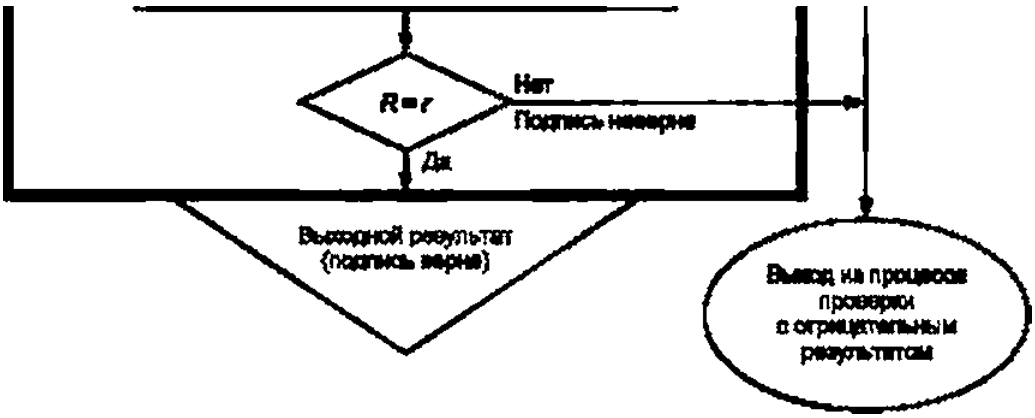


Рисунок 3 — Схема процесса проверки цифровой подписи

Приложение А
(справочное)

Контрольные примеры

А.1 Общие положения

Настоящее приложение носит справочный характер и не является частью нормативных положений настоящего стандарта.

Приводимые ниже значения параметров р. а. *Ь. т, д. Р. а* также значения ключей подписи и проверки подписи *<3* и *Q* рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящем стандарте.

Все числовые значения приведены 8 десятичной и шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления. Символ «ft» обозначает перенос числа на новую строку. Например, запись

12345ft
Б7890$_{1y}$.
499602D2$_{1b}$

представляет целое число 1234567890 в десятичной и шестнадцатеричной системах счисления соответственно.

А.2 Пример 1

А.2.1 Параметры схемы цифровой подписи

А.2.1.1 Условие

Для формирования и проверки цифровой подписи должны быть использованы параметры, приведенные 8 5.3.

А.2.1.2 Модуль эллиптической кривой

В настоящем примере параметру *р* присвоено следующее значение:

р - 57896044618658097711785492504343953926ft
634992332820282019728792003956564821041^.
р = 8000000000000000000000000000000000000000000000000000000000000431$_{1в}$.

А.2.1.3 Коэффициенты эллиптической кривой

В настоящем примере параметры *а* и £> принимают следующие значения:

$^{й = 7}$щ.
$^{e = 7}$ie-
Ь - 433088765467672769057659045956509319 95ft
9421117944510395832529688420338495804 14, $_{y}$.
Ь - 5FBFF498AA938CE739B8E022FBAFEF4Q563F6E6A3472FC2A514C0CE9DAE23B7E$_{1e}$.

А.2.1.4 Порядок группы точек эллиптической кривой

В настоящем примере параметр *т* принимает следующее значение:

m = 57896044618658097711785492504343953 92ft
708293458372545062238097359213763106961 9$_{)0}$.
m = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3,$_{e}$.

А.2.1.5 Порядок циклической подгруппы группы точек эллиптической кривой

В настоящем примере параметр *д* принимает следующее значение:

д= 57896044618658097711785492504343953 92ft
708293458372545062238097359213763106961 9$_{10}$.
q - 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$.

А.2.1.6 Коэффициенты точки эллиптической кривой

В настоящем примере координаты точки *Р* принимают следующие значения:

$\overline{X}_{P} = 2_{10}$.
2 ft.
у - 40189740565390375033354494229370597ft
756357393899055450806909793652134315662 80$_{10}$.
у = 8E2A8A0E65147O4BD6316030E16O19ft
C85C97F0A9CA267122B96ABBCEA7E8FC8$_{u}$.

А.2.1.7 Ключ подписи

В настоящем примере считается, что пользователь обладает следующим ключом подписи *d*

d= 55441196085363246126355624130324 1831ft
965767092223400165721080977500060975 25544
d = 7A929ADE789BB9BE10ED359OD39A72CW
11B60961F49397EEE1D19CE9891EC3B28$_{ie}$.

А.2.1.8 Ключ проверки подписи

В настоящем примере считается, что пользователь обладает ключом проверки подписи *Q*. координаты которого имеют следующие значения:

x= 57520216126176B084436314050233380 71W
1766301049063136321828967413422066048594 03,и.
x„ - 7F2B49E270DB6O90D8595BEC458B5U
0C58585BA1D4E9B788F6689DBD8E56FD80B,e.
y - 176149444192137815438093919496540 80W
0319426620453636392607098478594382867639 94, и.
y - 26F1B489O6701DD185C8413A977B3W
CBBAF64D1C593D26627DFFB101A87FF77DA,6.

А.2.2 Процесс формирования цифровой подписи (алгоритм 1)

Пусть после выполнения шагов 1—3 по алгоритму I (см. 6.2} были получены следующие числовые значения:

e = 20798893674476452017134061561508270 13W
0637142515379653289952617252661468872421$_{10}$,
***в* - 2DFBC1B372D89A1188C09C52E0EEU**
C61FCE52032AB1022E8E67ECE6672B043EE5,e.
***к* - 53854137677348463731403841147996619 2V**
4150400343430202071296063 8S28893196233395, o.
***к* - 77105C9B20BCD3122823C8CF6FCCW**
7B956OE33814E95B7FE64FED924594DCEAB3,6.

При этом кратная точка *C = кР* имеет координаты:

= 29700980915817952874371204983938256 9W
9042275210799431965163268798205921093339 5$_{10}$,
x$_c$ = 41AA28D2F1AB148280CD9ED56FEDW
A41974053554A42767B83A0043FD39DC0493,e.
***y$_c$* = 32842535278684663477094665322517084 5W**
0680472103245454326813285455653927406091 0,0.
***y$_c$* - 489C375A9941A3049E33B34361DDW**
204172AD98C3£5916OE27695D22A61FAE46E$_{1\$}$.

Параметр *г s x$_e$* (mod o) принимает значение:

***г*-29700980915817952874371204983938256 9W**
9042275210799431965163268798205921093339 5,
г= 41AA28D2F1AB148280CD9ED56FEDW
A41974053554A42767B83A0043FD39DC0493,e.

Параметр ss (rtf+ Jce|(modq) принимает значение:

S= 57497340027008465417892531001914703W
8455227042649098563933718999175515839552,
5 = 1456C64BA4642A1653C235A98A60249BCD6O3F746B631DF928014F6C5BF9C40$_{ie}$.

А.2.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1—3 по алгоритму II (см. 6.3) были получены следующие числовые значения:

e = 20798893674476452017134061561508270 13W
0637142515379653289952617252661468872421$_{10}$.
e = 2DFBC1B372D89A1188C09C52E0EEW
C61FCE52032AB1022E8E67ECE6672B043EE5$_{1\$}$.

При этом параметр ue e ' (mod д) принимает значение:

v =17686683605934468677301713824900268 5W
6274688308067549671528803657243114571897 8,$_0$.
***v* - 271A4EE429F84EBC423E388964555BBW**
29O3BA53C7BF945E5FAC8F381706354C2$_{1\$}$.

Параметры z, в su (mod *q)* и *z$_2$* в -rv(modp) принимают значения:

Z, = 37699167500901938556841057293512656 1U
0884134519049194261930453241274372099975 9,y.

z, - 5358F8FFB38F7C09ABC782A2DF2A11
3927DA4077D07205F763682F3A76C9019B4F,$_{e}$.
Zj = 14171998427343472112515917969500765711
69246655838972862114499932653333671092 21,$_{0}$,
Zj - 3221B4FBBF6D101074EC14AFAC2D4F711
EFAC4CF9FEC1ED11BAE336D27D527665$_{le}$.

Точка + имеет координаты;

x_e - 29700980915817952874371204983938256991 1
04227521079943196516326879820592109333 95,д.
x_e = 41AA28D2F1AB148280CD9ED56FE011
A41974053554A42767B83AD043FD39OC0493$_{ie}$,
y_e - 32842535278684663477094665322517084501 1
68047210324545432681328545565392740609 10,q .
y_c = 489C375A9941A3049E33B34361DD11
204172AD98C3E5916DE27695D22A61FAE46E,$_{e}$.

Тогда параметр R » x_f (mod <7) принимает значение:

R =29700980915817952874371204983938256 99W
04227521079943196516326879820592109333 95,0.
R - 41AA28D2F1 AB148280C D9ED56FED11
A41974053554A42767B83AD043FD39OC0493,$_{e}$.

Поскольку выполнено равенство $R = г.$ то цифровая подпись принимается.

А.3 Пример 2

А.3.1 Параметры схемы цифровой подписи

А.3.1.1 Условие

Для формирования и проверки цифровой подписи должны быть использованы параметры, приведен ныв в 5.3.

А.3.1.2 Модуль эллиптической кривой

В настоящем примере параметру p присвоено следующее значение:

p - 36239861022290036359077887536838743060213209255346786050 11
86546150450856166624002482588482022271496854025090823603051 1
6735163734263822371964987 22&582907372 40Э,д.
p - 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D11
F1D852741AF4704A0458047E80E4546D35B8336FAC224DD81664BBF528BE6373,$_{b}$.

А.3.1.3 Коэффициенты эллиптической кривой

В настоящем примере параметры a и $Ь$ принимают следующие значения:

$^{в = 7}$Ю-
в = 7,$_{в}$.
$Ь$ - 15186550692108285345089500347140431549287475277402064 3611
19401882335280998244379373282975691478597467486604160539 78в36775\\
9662632641399013695904743581182639 6$_{10}$.
b - 1CFF0806A31116DA29D8CFA54E57EB7488C5F377E49400FD07888649ECA1AC411
36183401362AO7322480A89CA58E0CF74BC9£540C2AOD6897FAO0A3084F302AOC$_{ie}$.

А.3.1.4 Порядок группы точек эллиптической кривой

В настоящем примере параметр тп принимает следующее значение:

тп =36239861022290036359077887536838743060213209255346786050865461 11
50450856166623969164898305032863068499961404079437936585455865192212 11
97073480881261812061974 3,у.
m = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D11
A82F2D7ECB1OBAC7199O5C5EECC423F1O86E2SEDBE23C595D644AAF187E6E6OF$_{ie}$.

А.3.1.5 Порядок циклической подгруппы группы точек эллиптической кривой

В настоящем примере параметр q принимает следующее значение:

q - 36239861022290036359077887536838743060213209255346786050865461 11
50450856166623969164898305032863068499961404079437936585455865192212 11
97073480881261812061974 3,0.
q = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D11
A82F2D7ECB1DBAC719905C5EECC423F1D86E25EOBE23C595D644AAF187E6E6DF,$_{e}$.

А.3.1.6 Коэффициенты точки эллиптической кривой

В настоящем примере координаты точки *Р* принимают следующие значения:

x_p = 1928356944067022849399309401243137598997786635459507974357075491307766 5W
926858354410655576810031848748196580049032123328842523358302507295276323 8X1
3493573274$_{10}$,

x_ - 24D19CC64572EE30F396BF6EBBFD7A6C5213B3B3D7057CC825F91093A68CD762W
FD60611262C0838DC6B60AA7E£E804E28BC849977FAC33B4B530F1B120248A9A$_{ie}$.

y_p - 2288728693371972859970012155529478416353562327329506180 3XX
1449742593110286030157281414199707227170880706659385065033415238 18XX
5734779888586480760509872401385 4,y,

y_0 - 2BB312A43BD2CE6E0D020613C857ACDDCFBF061E91E5F2C3F32447C259F39B2XX
C83AB156D77F1496BF7EB3351E1EE4E43OC1A18B91B24640B6D8B92CB1AOD371E$_{1e}$.

А.3.1.7 Ключ подписи

В настоящем примере считается, что пользователь обладает следующим ключом подписи *Л*

tf= 6100818041363730982195381532398475830068455190695315629 82Э88135XX
3548906063017822553836083934233723790576655275951168273070250464588311
744076612118046687586$0_{lo}$.

d = BA6Q48AADAE241BA40936D47756D7C93091AOE8514669700EE7508E508B102072XX
E8123B2200A0563322DAO2827E2714A2636B7BFD18AAOFC62967821FA16OO4_{ie}.

А.3.1.8 Ключ проверки подписи

В настоящем примере считается, что пользователь обладает ключом проверки подписи *Q.* коордтаты которого имеют следующие значения:

$x_{„}$ = 9095468530025365965566907686698303100069292725465562815963 11
729653703124985631823204368928700528428086082628324568582235801X
713780290717986855863433431150561$_w$.

$x_я$ - 115DC5BC96760C7B48598D8AB9E740D4C4A85A65BE33C1B1585C320C&54621DXX
D5A515856D13314AF69BC5B924C8B4DDFF75C45415C1D9DD9DD33612CD530EFE1$_{1e}$.

y = 2921457203374425620632449734248415455640700823559488705164895 8X1
375095391342 97Э27397380287741428246088626609329139441895016863758 11
984106326600572476822372076,$_0$.

y = 37C7C90CD40BOF5621DC3AC1B751CFA0E2634FA0503B3D52639F5D7FB72AFD611
1EA199441D943FFE7F0C70A2759A3CDB84C114E1F9339FDF27F35ECA93677BEEC$_{1tt}$.

А.3.2 Процесс формирования цифровой подписи (алгоритм I)

Пусть после выполнения шагов 1—3 по алгоритму I (см. 6.2) были получены следующие числовые значения:

в - 28979638816B286&5755628272785538650491737451978718251995629 47XX
419041388950970536661109553499954248733088719748844538964641281654 4XX
6351329697382770627204596 4,y,

в = 3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591W
7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C,$_e$,

*=1755163560258504995406282799211252803334510317477377916502X1
0814424318205707503444610 29B675096250890922723586612687247351680781054 17XX
47529710309879958632945$_{10}$.

*= 359E7F4B1410FEACC570456C68014969463121 20B3900190455986E364F31X
65886748ED7A44B3E794434006011842286212273A6D14CF70£A3AF71BB1AE679F1$_{1e}$.

При этом кратная точка С = *кР* имеет координаты:

x_c = 2489204477031349265072864643032147753667451319282131444027498637 3XX
576110928102217951018714129288237168059598287083302842436534530853X1
22004442442534151761462, y.

x_c = 2F86FA60A081091A23DO795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCACXX
035492558486620F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173A£36$_{ie}$.

y_c = 7701738899289918360478447987809604416820626318760961376739468015 0X1
2442229353276517652844283783245693642266254651370214816293307951 7X1
0843005015210864150831 0, y.

y_c= EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831OA27X1
C8100DAA876F9AOC0O28A82DD3826O4OC7F92E471DA23E55E0EBB3927C856O6_{1e}.

Параметр *г* = x_e (mod g) принимает значение:

***г*-2489204477031349265072864643032147753667451319282131444027498637W**
576110928102217951018714129288237168059598287083302842436534530853ll
22004442442534151761462$_{10}$,
r^s 2F86FA60A081091A23OD795E1E3C689EE512A3C82EE0OCC2643C78EEA8FCAC11
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{lB}$.

Параметр ss(rd + fte)(modq)npMHHMaегзначение:

s= B64523221707669519038849297382936917075023735848431579919598711
9931338518056474687719503967246017942176077089327803095680769011 5W
8227099038536828318351593 70^.
s - 1081B394696FFE8E6585E7A9362D26B6325F56778AADBC081C0BFBE933D52FF5811
23CE288E8C4F362526080DF7F70CE406A6EEB1F56919CB92A9853BDE73E584A$_{ie}$.

А.3.3 Процесс проверки цифровой подписи (алгоритм 11}

Пусть после выполнения шагов 1—3 по алгоритму Н (см. 6.3) были получены следующие числовые зна чвния:

***в* - 289796388168286857556282727855386504917374519787182519956294711**
419041388950970536661109553499954248733088719748844538964641281654411
635132969738277062720459641o,
e - 3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C59111
7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D297207588C$_{1b}$.

При этом параметр *v* = s^{-1} (mod g) принимает знамение:

***V*-25569421539460522226607408431640861538776922344007831911469284911**
356194345732344708924001925205698280688153534004145821243990606136ll
707223818593481596025267l$_{10}$.
***v* - 30D212A9E25O1A80AOF238532CADF3E64D7EF4E782B6AD140AAF8BBD9BB472911**
84595EEC87B2F3448A1999D5F0A6OE0E14A55AD875721EC8CFD5O4O0OB3A840FF$_u$.

Параметры z, в sv(mod g) и z_2 в -/vfmod g) принимают значения:

z, = 32064708273367686296869071018734752503433064480890303112144841l
385872743205045180345208826552901003496732941049780357793541942055ll
60008495619817370719790257 5$_{10}$.
z, = 3038E7262069682AD240081EEA2F92E6348D619FA45007B175837CF13B02607911
051A48A1A379188F37BA46CE12F7207F2A8345459FF960E1EBD5B4F2A34A6EEF,$_e$.
z_2=13667709118340031081429778480218475973204553475356412734827W
32082047028342168006031261814273230879203690726448631222679743757511
6163726695805680585960300820 3$_{10}$.
z_2 = 1A18A31602E6EACOA9888C01941082AEFE296F840453D2603414C2A16EB6FC52911
O8D8372E50DC49D6C612CE1FF65BD58E1D2029F2269O438CC36A76DOA444ACB$_{ie}$.

Точка С = z,P + z_2O имеет координаты:

***x_e* - 2489204477031349265072864643032147753667451319282131444027498637ll**
357611092810221795101871412928823716805959828708330284243653453085311
22004442442534151761462$_{l0}$.
x_c = 2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC11
D3549255B486B20F1C9EC197C90699850260C93BCBCO9C5C3317E19344E173AE36$_{16}$,
y_c=770173889928991836047844798780960441682062631876096137673946801 5
02442229353276517652844283783245693642266254651370214616293307951701l
8430050152108641508310$_{10}$.
***y_c* - EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BOE80A91831DA2711**
C8100OAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD6$_{ie}$.

Тогда параметр *R* s x_c(тсх1д)принимэег значение:

R = 2489204477031349265072864643032147753667451319282131444027498611
373576110928102217951018714129288237168059598287083302842436534530851l
32200444244253415176146 2,$_{l0}$.
R = 2F86FA60A081091A23OD795E1E3C689EE512A3C82EE0OCC2643C78EEA8FCAC11
D35492558486B20F1C9EC197C90699850260C93BCBCO9C5C3317E19344E173AE36,&.

Поскольку выполнено равенство R = *г,* то цифровая подпись принимается.

Библиография

Примечание — Оригиналы международных стандартов ИСО и ИСО/МЭК находятся в национальных {государственных} органах по стандартизации* государств, принявших настоящий стандарт.

(1]	**ИСО 2382:2015 (ISO 2382:2015}**	**Информационная технология. Словарь (Information technology — Vocabulary)**
(2]	**ИСО/МЭК 9796-2:2010 (ISO/1EC 9796-2:2010)**	**Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации {Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms)**
(3] ИСО/МЭК 9796-3:2006	**(ISO/1EC 9796-3:2006)**	**Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 3. Механизмы на основе дискретного логарифма (information technology — Security techniques — Digital signature schemes giving message recovery — Pari 3: Discrete logarithm based mechanisms)**
(4]	**ИСО/МЭК 14888-1:2008 (ISO/IEC 14886-1:2008}**	**Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения {Information technology — Security techniques — Digital signatures with appendix — Pari 1: General)**
(5]	**ИСО/МЭК 14888-2:2008 (ISO/IEC 14688-2:2008}**	**Информационная технология. Методы обеспечения защиты. Цифровые подписи с приложением. Часть 2. Механизмы, основанные на разложении на множители (Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms)**
(6] ИСО/МЭК 14888-3:2016	**(ISO/1EC 14888-3:2016}**	**Информационная технология. Методы и средства обеспечения безопасности. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма (Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms)**
(7] ИСО/МЭК 10118-1:2016	**(ISO/1EC 10118-1:2016)**	**Информационная технология. Методы защиты информации. Хэш-функции. Часть 1. Общие положения {Information technology — Security techniques — Hash-functions — Part 1: General)**
{8] ИСО/МЭК 10118-2:2010	**(ISO/1EC 10118-2:2010)**	**Информационные технологии. Методы защиты информации. Хэш-функции. Часть 2. Хэш-функции с использованием алгоритма шифрования п-битными блоками (Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-brt block cipher)**
(9]	**ИСО/МЭК 10118-3:2004 (ISO/IEC 10118-3:2004)**	**Информационные технологии. Методы защиты информации. Хэш-функции. Часть 3. Выделенные хэш-функции (Information technology — Security techniques — Hash-functions — Pari 3: Dedicated hash-functions)**
(10]	**ИСО/МЭК 10118-4:1998 (ISO/1EC 10118-4:1998)**	**Информационные технологии. Методы защиты информации. Хэш-функции. Часть 4. Хэш-функции с применением арифметических операций над абсолютными значениями чисел (Information technology — Security techniques — Hash-functions — Pari 4: Hash-functions using modular arithmetic)**

*** В Российской Федерации оригиналы международных стандартов ИСО и ИСО/МЭК находятся в Федеральном информационном фонде стандартов.**

УДК 681.3.06:006.354 МКС 35.040

Ключевые слова: обработка данных, передача данных, обмен информацией, сообщения, цифровые подписи, защита информации, формирование цифровой подписи, проверка цифровой подписи

БЗ 1—2019/66

Редактор *П.В. Коретникоеа*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 05.12.2019. Подписано а печать М.01.2019. Формат 60 » Гарнитура Ариал.
Усл. пом. л. 2.33. Уч -им. л. 2,10.

Подготовлено на основе электронном версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе. 11.
www.juriatzdal.ru y-book@mailnj

Создано а единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов.

117418 Москва. Нахимовский пр-т, д. 31. к. 2.
www.gostinfo.ru info@gostinfo.ru