ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.019 — 2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ Акционерным обществом «РАМЭК-ВС» (АО «РАМЭК-ВС»)

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 026 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 мая 2018 г. № 282-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

*Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Условные обозначения 3
5 Дополнительные криптографические преобразования 4
5.1 Операции в конечном поле $\mathbf{F}_2^{256}$ 4
5.2 Функция формирования производного ключа 5
5.3 Функция преобразования двоичного вектора 5
6 Характеристики участников 5
7 Ключевая система 6
8 Процедуры взаимной аутентификации, формирования ключа фискального признака и защиты фискальных данных 8
9 Действия средства формирования фискального признака при работе в автономном режиме 11
Приложение А (справочное) Контрольные примеры 13
Библиография 19

Введение

В настоящих рекомендациях содержится описание криптографических механизмов аутентификации и выработки ключа фискального признака, основанного на использовании блочного шифра «Кузнечик», определенного ГОСТ Р 34.12—2015, реализованного в режиме гаммирования, определенном ГОСТ Р 34.13—2015, а также функции выработки имитовставки (кода аутентификации), определенной Р 50.1.113—2016.

В приложении А приведены контрольные примеры выполнения процедур выработки фискальных признаков документа, архива, сообщения и оператора.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных

Information technology. Cryptographic data security. Cryptographic mechanisms for authentication and generation fiscal feature key for use in the means for the formation and verification of fiscal characteristics supporting the operation of cash registers, operators and authorized bodies for processing fiscal data

Дата введения — 2018—11—01

1 Область применения

Предлагаемое в настоящих рекомендациях решение направлено на обеспечение аутентификации и контроля целостности фискальных данных, передаваемых по каналам связи между фискальными накопителями и операторами фискальных данных, а также между операторами фискальных данных и уполномоченным органом.

Форматы передаваемых фискальных данных, способы передачи фискальных данных и механизмы обеспечения конфиденциальности передаваемых фискальных данных определяются уполномоченным органом и не входят в область применения настоящих рекомендаций.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие документы:

ГОСТ Р 34.11—2012 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.12—2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13—2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

Р 50.1.113—2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Р 1323565.1.012—2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных документов 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 заменен ссылочный документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящих рекомендациях применены следующие термины с соответствующими определениями:

3.1

заводской номер: Уникальный номер экземпляра модели контрольно-кассовой техники, фискального накопителя, средства формирования фискального признака, средства проверки фискального признака, автоматического устройства для расчетов, присвоенный изготовителем.

[1, статья 1.1]

3.2

контрольно-кассовая техника; *ККТ*: Электронные вычислительные машины, иные компьютерные устройства и их комплексы, обеспечивающие запись и хранение фискальных данных в фискальных накопителях, формирующие фискальные документы, обеспечивающие передачу фискальных документов в налоговые органы через оператора фискальных данных и печать фискальных документов на бумажных носителях в соответствии с правилами, установленными законодательством Российской Федерации о применении контрольно-кассовой техники.

[1, статья 1.1]

3.3

мастер-ключ; *МК*: Ключевой документ, предназначенный для создания серии ключей фискального признака, а также проверки фискальных признаков, сформированных с использованием ключей фискального признака этой серии.

[1, статья 1.1]

3.4

номер фискального документа; *FDN*: Порядковый номер фискального документа с момента формирования отчета о регистрации *ККТ* или отчета об изменении параметров регистрации *ККТ* в связи с заменой фискального накопителя.

[2, приложение № 2, таблица 4]

3.5

оператор фискальных данных: Организация, созданная в соответствии с законодательством Российской Федерации, находящаяся на территории Российской Федерации, получившая в соответствии с законодательством Российской Федерации о применении контрольно-кассовой техники разрешение на обработку фискальных данных.

[1, статья 1.1]

3.6 **средство проверки фискального признака:** Фискальный накопитель, обеспечивающий возможность проверки фискальных признаков, расшифровывание и аутентификацию фискальных документов, подтверждающих факт получения оператором фискальных данных фискальных документов, переданных контрольно-кассовой техникой, направляемых в контрольно-кассовую технику оператором фискальных данных.

3.7 **средство формирования фискального признака:** Фискальный накопитель, обеспечивающий возможность формирования фискальных признаков, запись фискальных данных в некорректируемом виде (с фискальными признаками), их энергонезависимое долговременное хранение, а также обеспечивающее возможность шифрования фискальных документов в целях обеспечения конфиденциальности информации, передаваемой оператору фискальных данных.

3.8

фискальные данные; *FD*: Сведения о расчетах, в том числе сведения об организации или индивидуальном предпринимателе, осуществляющих расчеты, о контрольно-кассовой технике, применяемой при осуществлении расчетов, и иные сведения, сформированные контрольно-кассовой техникой или оператором фискальных данных.

[1, статья 1.1]

3.9

фискальный накопитель: Программно-аппаратное шифровальное (криптографическое) средство защиты фискальных данных в опломбированном корпусе, содержащее ключи фискального признака, обеспечивающее возможность формирования фискальных признаков, запись фискальных

данных в некорректируемом виде (с фискальными признаками), их энергонезависимое долговременное хранение, проверку фискальных признаков, расшифровывание и аутентификацию фискальных документов, подтверждающих факт получения оператором фискальных данных фискальных документов, переданных контрольно-кассовой техникой, направляемых в контрольно-кассовую технику оператором фискальных данных, а также обеспечивающее возможность шифрования фискальных документов в целях обеспечения конфиденциальности информации, передаваемой оператору фискальных данных.

[1, статья 1.1]

3.10

фискальный признак; *FS*: Достоверная информация, сформированная с использованием фискального накопителя и ключа фискального признака или с использованием средств формирования фискального признака и мастер-ключа в результате криптографического преобразования фискальных данных, наличие которой дает возможность выявления корректировки или фальсификации этих фискальных данных при их проверке с использованием фискального накопителя и (или) средства проверки фискального признака.

[1, статья 1.1]

3.11

фискальный признак архива; FS_{FSCa}: Фискальный признак, формируемый с использованием фискального накопителя для проверки достоверности архива фискальных данных, защищенных фискальным признаком.

[2, Приложение № 2]

3.12

фискальный признак документа; FS_{FSCd}: Фискальный признак, формируемый с использованием фискального накопителя для проверки достоверности фискальных данных, защищенных фискальным признаком, с использованием средств проверки фискального признака, используемых уполномоченным органом.

[1, статья 1.1]

3.13

фискальный признак оператора; FS_{FSCo}: Фискальный признак, формируемый с использованием средств формирования фискального признака оператора фискальных данных для проверки достоверности фискальных данных, защищенных фискальным признаком, с использованием средств проверки фискального признака, используемых уполномоченным органом.

[1, статья 1.1]

3.14

фискальный признак подтверждения; FS_{FSV}:Фискальный признак, формируемый с использованием средств формирования фискального признака оператора фискальных данных для проверки достоверности фискальных данных, защищенных фискальным признаком, с использованием фискального накопителя.

[1, статья 1.1]

3.15

фискальный признак сообщения; FS_{FSCm}: Фискальный признак, формируемый с использованием фискального накопителя для проверки достоверности фискальных данных, защищенных фискальным признаком, с использованием средств проверки фискального признака оператора фискальных данных.

[1, статья 1.1]

4 Условные обозначения

В настоящих рекомендациях применены следующие обозначения:

V_n — множество всех двоичных векторов размерности n, где n — целое неотрицательное число. Нумерация подстрок и компонент вектора осуществляется слева направо, начиная с нуля;

V_* — множество всех двоичных векторов конечной размерности, включая пустую строку, то есть для любого $n \geq 0$ выполнено условие $V_n \in V_*$;

$[Z]_{i,...,j}$ — для двоичного вектора $Z = (z_0, ..., z_{n-1})$, $Z \in V_n$, подвектор $Z' = (z_i, ..., z_j)$, $0 \leq i \leq j \leq n - 1$;

$A \| B$ — конкатенация векторов $A = (a_0, ..., a_{n_1-1}) \in V_{n_1}$ и $B = (b_0, ..., b_{n_2-1}) \in V_{n_2}$, то есть вектор $(a_0, ..., a_{n_1-1}, b_0, ..., b_{n_2-1})$, для которого выполнены равенства $A = [A \| B]_{0, ..., n_1-1}$ и $B = [A \| B]_{n_1, ..., n_1+n_2-1}$;

$\mathbb{F}_{2n}$ — конечное поле из 2^n элементов;

$\mathbb{F}_2^n[x]$ — кольцо многочленов от одной переменной с коэффициентами из поля $\mathbb{F}_2^n$;

$\mathbb{F}_{2n}[x, y]$ — кольцо многочленов от двух переменных с коэффициентами из поля $\mathbb{F}_2^n$;

$\text{bin}_n(a)$ — функция, ставящая в соответствие целому неотрицательному числу a двоичный вектор размерности n по следующему правилу:

$$\text{bin}_n(a) = (a_0, ..., a_{n-1}),\ a_i \equiv \left\lfloor \frac{a}{2^i} \right\rfloor \pmod 2;$$

$\text{int}_n(a_0,...,a_{n-1})$ — функция, ставящая в соответствие двоичному вектору $(a_0,..., a_{n-1})$ длины n целое неотрицательное число a по следующему правилу:

$$\text{int}_n(a_0,..., a_{n-1}) = \sum_{i=0}^{n-1} a_i 2^i;$$

$\text{H}_l(a)$ — функция хэширования вектора $a \in V_*$, определяемая в ГОСТ Р 34.11 и вырабатывающая хэш-код длиной l бит, $l \in \{256, 512\}$;

$\text{HMAC}_{256}(a)$ — функция выработки кода аутентификации вектора $a \in V_*$, определяемая Р 50.1.113 и вырабатывающая код аутентификации длиной 256 бит;

$\text{ENC}(K, I, T)$ — результат зашифрования сообщения $T \in V_*$ на ключе $K \in V_{256}$ с синхропосылкой $I \in V_{128}$ с помощью блочного шифра «Кузнечик», в соответствии с ГОСТ Р 34.12 в режиме гаммирования, определенном в ГОСТ Р 34.13;

$\text{DEC}(K, I, C)$ — результат расшифрования шифртекста $C \in V_*$ на ключе $K \in V_{256}$ с синхропосылкой $I \in V_{128}$ с помощью блочного шифра «Кузнечик», в соответствии с ГОСТ Р 34.12 в режиме гаммирования, определенном в ГОСТ Р 34.13;

$\text{prf}(x)$ — функция преобразования двоичного вектора $x \in V_s$ размерности s, где $256 \leq s \leq 384$, в двоичный вектор фиксированной размерности 512, то есть отображение $V_s \to V_{512}$.

5 Дополнительные криптографические преобразования

5.1 Операции в конечном поле $\mathbb{F}_2^{256}$

Каждый двоичный вектор из V_{256} может быть представлен в виде элемента конечного поля $\mathbb{F}_2^{256}$. Данное представление взаимно однозначно и может быть задано следующим образом.

Пусть вектор $a = (a_0,..., a_{255}) \in V_{256}$, тогда ему будет соответствовать многочлен $a(x) = \sum_{i=0}^{255} a_i x^i \in \mathbb{F}_2^{256}[x]$.

Используя данное соответствие, определяют операции сложения и умножения двоичных векторов из V_{256} следующим образом.

Определяют неприводимый многочлен

$$(x) = x^{256} + x^{10} + x^5 + x^2 + 1 \in \mathbb{F}_2^{256}[x]. \quad (1)$$

Рассматривают произвольные $a = (a_0, ..., a_{255})$, $b = (b_0, ..., b_{255}) \in V_{256}$, а также соответствующие им многочлены $a(x) = \sum_{i=0}^{255} a_i x^i$, $b(x) = \sum_{i=0}^{255} b_i x^i \in \mathbb{F}_{2^{256}}[x]$, тогда:

- вектор $a + b$ определяется равенством $a + b = c$, где $c = (c_0, ..., c_{255})$ — вектор, которому соответствует многочлен

$$c(x) = \sum_{i=0}^{255} c_i x^i = a(x) + b(x) \pmod{p(x)}, \quad (2)$$

где mod $p(x)$ — взятие остатка от деления многочлена $a(x) + b(x)$ на многочлен $c(x)$;

- вектор ab определяется равенством $a + b = c$, где $c = (c_0, ..., c_{255})$ есть вектор, которому соответствует многочлен

$$c(x) = \sum_{i=0}^{255} c_i x^i = a(x)b(x)(\mathrm{mod}\ p(x)). \quad (3)$$

5.2 Функция формирования производного ключа

Функция формирования производного ключа $KP \in V_{512}$ представляет собой параметрическое отображение:

$$\mathrm{KDF}_l : V_{256} \times V^* \times V^* \to V_l, \quad (4)$$

где параметр l принимает значения из множества {256, 512}.

Допустим, что:

- $K \in V_{256}$ — ключ, из которого вырабатывается производный ключ KP;
- lab, $seed \in V_*$ — произвольные двоичные векторы конечной длины.

Тогда функция формирования производного ключа определяется следующими равенствами:

$$\mathrm{KDF}_{256}(K, lab, seed) = K(1), \quad (5)$$

$$\mathrm{KDF}_{512}(K, lab, seed) = K(1) \,||\, K(2), \quad (6)$$

где $K(i) = \mathrm{HMAC}_{256}(K, \mathrm{bin}_8(i) \,||\, lab \,||\, \mathrm{bin}_8(0) \,||\, seed \,||\, \mathrm{bin}_{16}(l))$;

$i = 1, 2$, $l \in \{256, 512\}$.

Функция KDF_l является частным случаем алгоритма диверсификации KDF_TREE_GOST3411_2012_256, определяемого в Р 50.1.113.

5.3 Функция преобразования двоичного вектора

Для вектора $x = (x_0, ..., x_{s-1}) \in V_s$ отображение prf (x) необходимо реализовать следующим образом:

а) сформировать двоичный вектор $S = (1, \underbrace{0, \ldots, 0}_{512-s-1}, x_0, \ldots, x_{s-1}) \in V_{512}$;

б) определить: prf $(x) = \mathrm{H}_{512}(S)$.

6 Характеристики участников

6.1 Все участники обмена фискальными данными выступают в качестве средства формирования фискального признака либо в качестве средства проверки фискального признака.

6.2 Заводские и серийные номера

6.2.1 Каждый участник должен обладать одним действующим и, возможно, несколькими, применяемыми последовательно в ходе эксплуатации, серийными номерами — $SN \in V_{48}$.

Серийные номера используются, в первую очередь, для идентификации ключей участников и устанавливаются в процессе записи или замены ключей. В случае если замена ключей невозможна, серийный номер участника может совпадать с его заводским номером.

Серийный номер средства формирования фискального признака и средства проверки фискального признака представляется в виде набора векторов размерностей V_{16} и V_{32}. Для передачи в ККТ серийный номер средства формирования фискального признака представляется в виде ASCII строки длиной 16 символов [3]. Далее ККТ организует их печать на текстовый документ и передачу средству проверки фискальных признаков [4].

6.2.2 Средство формирования фискального признака

Серийный номер средства формирования фискального признака $SN_{FSC} \in V_{48}$ представляет собой следующий вектор:

$$SN_{FSC} = (\underbrace{s_0, \ldots, s_{15}}_{\mathrm{bin}_{16}(t)}, \underbrace{s_{16}, \ldots, s_{47}}_{\mathrm{bin}_{32}(s)}), \quad (7)$$

где t — номер средства формирования фискального признака в серии;

здесь $(s_0, ..., s_{15}) = \mathrm{bin}_{16}(t)$, $0 \le t < 2^{16}$ и $t = \mathrm{int}_{16}([SN_{FSC}]_{0, ..., 15})$;

s — номер серии средств формирования фискального признака;

здесь $(s_{16}, ..., s_{47}) = \mathrm{bin}_{32}(s)$, $0 \le s < 2^{32}$ и $s = \mathrm{int}_{32}([SN_{FSC}]_{16, ..., 47})$.

6.2.3 Средство проверки фискального признака

Серийный номер средства проверки фискального признака $SN_{FSV} \in V_{48}$ представляет собой следующий вектор:

$$SN_{FSV} = (\underbrace{s_0,\ldots,s_{15}}_{\mathrm{bin}_{16}(I)}, \underbrace{s_{16},\ldots,s_{47}}_{r}), \quad (8)$$

где I — номер средства проверки фискального признака;

здесь $(s_0, \ldots, s_{15}) = \mathrm{bin}_{16}(I)$, $0 \le I < 2^{16}$ и $I = \mathrm{int}_{16}([SN_{FSC}]_{0,\ldots,15})$;

r — случайная последовательность длиной 32 бита (качественные свойства и механизм формирования данной последовательности должны соответствовать пункту 5.2 Р 1323565.1.012—2017).

6.3 Количественные и временные характеристики

6.3.1 Настоящими рекомендациями определяется, что срок действия мастер-ключа системы, используемой при передаче фискальных данных, не превышает $T = 8$ лет. Способ выработки мастер-ключа должен удовлетворять пункту 5.3 Р 1323565.1.012—2017. Порядок выработки, распространения, хранения и уничтожения мастер-ключа определяется уполномоченным органом и в настоящих рекомендациях не рассматривается.

6.3.2 В настоящих рекомендациях предполагается, что число одновременно действующих средств проверки фискального признака ограничено и не превышает величины $Q_{FSV} = 138$. За время эксплуатации средства проверки фискального признака ему может быть назначено несколько серийных номеров. Срок действия одного серийного номера средства проверки фискального признака и связанного с ним ключа не должен превышать 13 мес [1].

6.3.3 Число одновременно действующих средств формирования фискального признака ограничено и не превышает величины $Q_{FSC} = 2^{44}$. Число серий средств формирования фискального признака ограничено величиной $Q_S = 2^{32}$. Срок действия одного серийного номера средства формирования фискального признака не превышает 13 мес, за исключением особого случая работы в рамках патентной системы налогообложения, где срок использования ключа составляет 36 мес [1].

6.3.4 Для режима работы в рамках патентной системы налогообложения следует выполнять назначение нового серийного номера средства проверки фискального признака вместе с его сменой у оператора фискальных данных или в уполномоченном органе не реже одного раза в 13 мес.

7 Ключевая система

7.1 В настоящем разделе описана ключевая система, используемая при организации передачи фискальных признаков. Данная система представляет собой вариант схемы распределения ключей Блома и состоит из секретных ключей, приведенных в 7.2—7.5.

7.2 Мастер-ключ *MK* представляет собой симметричную матрицу A размера $(m + 1) \times (m + 1)$

$$A = \begin{pmatrix} a_{00} & a_{01}\ldots & a_{0m} \\ a_{10} & a_{11}\ldots & a_{1m} \\ & \ldots & \\ a_{m0} & a_{m1}\ldots & a_{1mn} \end{pmatrix}, \quad (9)$$

где $a_{ij} = a_{ji}$, $0 \le i \le m$, $0 \le j \le m$ и $a_{ij} \in V_{256}$. Максимальное число различных элементов матрицы равно $\frac{1}{2}(m+1)(m+2)$.

Значение параметра m определяется исходя из срока действия мастер-ключа системы защиты фискальных данных и полагается равным $m = 2048$.

Кроме того, коэффициенты матрицы A однозначно связаны с многочленом

$$f(x,y) = \sum_{i=0}^{m}\sum_{i=0}^{m} a_i x^i y^i, f(x, y) \in \mathbb{F}_{2^{256}}[x, y]. \quad (10)$$

7.3 Ключ средства проверки фискального признака K_{FSV}

Каждому средству проверки фискального признака соответствует свой собственный уникальный ключ K_{FSV}, зависящий от серийного номера средства проверки фискального признака.

Для каждого средства проверки фискального признака с серийным номером SN_{FSV} ключ K_{FSV} представляет собой вектор

$$(c_0,...,c_m),\ c_j \in V_{256},\ j = 0,\ ...,\ m, \tag{11}$$

определяемый равенством

$$f\left(\mathrm{H}_{256}\left(SN_{FSV}\right),y\right) = \sum_{j=0}^{m} c_j y^j \in \mathbb{F}_{2^{256}}[y], \tag{12}$$

где многочлен $f(x, y)$ определяется равенством (10).

Эквивалентным определением величин $c_j \in V_{256}$ является равенство

$$c_j = \sum_{i=0}^{m} a_{ij} \left(\mathrm{H}_{256}\left(SN_{FSV}\right)\right)^i, \tag{13}$$

выполненное для всех $j = 0, ..., m$.

7.4 Ключ серии средств формирования фискального признака K_S [s]

Каждой серии средств формирования фискального признака соответствует свой собственный уникальный ключ K_S [s], где s — номер серии. Общее число серий определяется эксплуатационными параметрами системы по организации выработки и проверки фискальных данных и не превышает 2^{32}.

Для каждого номера серии $0 \le s < 2^{32}$ ключ серии K_S [s] представляет собой вектор

$$(b_0,\ ...,\ b_m),\ b_i \in V_{256},\ i = 0,\ ...,\ m, \tag{14}$$

определяемый равенством

$$f\left(x, H_{256}\left(\mathrm{bin}_{32}\left(s\right)\right)\right) = \sum_{i=0}^{m} b_i x^i \in \mathbb{F}_{2^{256}}[x], \tag{15}$$

где многочлен $f(x, y)$ определен равенством (10).

Эквивалентным определением величин $b_i \in V_{256}$ является равенство

$$b_i = \sum_{j=0}^{m} a_{ij} \left(\mathrm{H}_{256}\left(\mathrm{bin}_{32}\left(s\right)\right)\right)^j, \tag{16}$$

выполненное для всех $i = 0, ..., m$.

7.5 Ключ средства формирования фискального признака K_{FSC}

Ключ средства формирования фискального признака формируется:

- из ключа серии средств формирования фискального признака $K_S[s] = (b_0,\ ...,\ b_m)$, где $b_i \in V_{256}$, $i = 0, ..., m$;
- серийного номера средства формирования фискального признака $SN_{FSC} \in V_{48}$;
- серийного номера средства проверки фискального признака $SN_{FSV} \in V_{48}$.

Способ формирования ключа K_{FSC} определяется следующим равенством:

$$K_{FSC} = \mathrm{KDF}_{256}(K^*, SN_{FSC}, SN_{FSV}), \tag{17}$$

где

$$K^* = \sum_{i=0}^{m} b_i \left(\mathrm{H}_{256}\left(SN_{FSV}\right)\right)^i \in V_{256}. \tag{18}$$

8 Процедуры взаимной аутентификации, формирования ключа фискального признака и защиты фискальных данных

8.1 Рассматриваемые процедуры выполняется между средством формирования фискального признака и средством проверки фискального признака. Они могут быть разнесены во времени и образовывать протокол взаимной аутентификации, формирования ключа фискального признака и защиты фискальных данных с точки зрения принятой последовательности шагов до момента подтверждения фискального признака, выработанного средством формирования фискального признака.

8.1.1 В ходе выполнения процедур происходят выработка общего ключа $K \in V_{512}$, аутентификация участников, формирование фискальных признаков, а также защита фискальных данных. Сформированная часть ключа $[K]_{0, \ldots, 255}$ используется для формирования фискального признака, а $[K]_{256, \ldots, 511}$ — для защиты (шифрования) фискальных данных.

8.1.2 Общая схема связи элементов системы приведена на рисунке 1.

8.1.3 Перед началом выполнения операций по формированию фискального признака и защите фискальных данных средство формирования фискального признака должно обладать:

а) серийным номером SN_{FSV} средства проверки фискального признака;

б) фискальными данными FD;

в) флагом F_{FS}, определяющим тип рассчитываемого фискального признака[1)];

г) флагом F_C, определяющим необходимость шифрования фискальных данных[2)].

8.1.4 Перед началом выполнения операций по проверке фискального признака и созданию фискального признака подтверждения средство проверки фискального признака должно обладать:

а) ключом K_{FSV} средства проверки фискального признака;

б) флагом F_{FS}, определяющим тип проверяемого фискального признака[3)];

в) фискальными данными FD либо сообщением C, содержащим зашифрованные фискальные данные;

г) флагом F_C, определяющим необходимость расшифрования фискальных данных[4)].

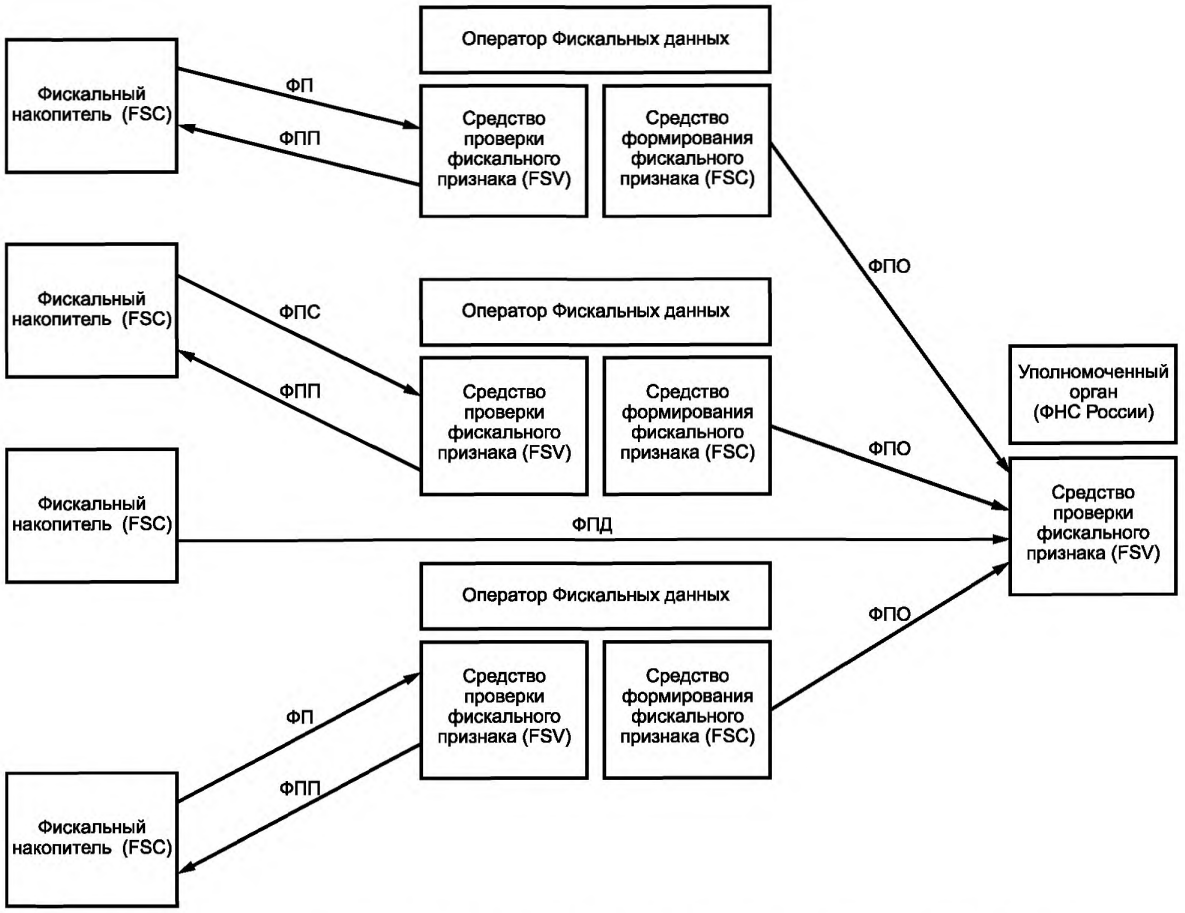
---

1) Формат и способ задания флага, определяющего тип фискального признака, определяются вне рамок настоящих рекомендаций.

2) Формат и способ задания флага, определяющего необходимость шифрования фискальных данных, определяются вне рамок настоящих рекомендаций.

3) Формат и способ задания флага, определяющего тип фискального признака, определяются вне рамок настоящих рекомендаций.

4) Формат и способ задания флага, определяющего необходимость шифрования фискальных данных, определяются вне рамок настоящих рекомендаций.



ФП — фискальный признак; ФПД — фискальный признак документа; ФПО — фискальный признак оператора; ФПП — фискальный признак подтверждения; ФПС — фискальный признак сообщения

Рисунок 1 — Схема организации связи средств формирования и проверки фискальных признаков

8.2 Шаг 1. Действия средства формирования фискального признака

Средство формирования фискального признака выполняет указанную ниже последовательность действий:

а) определяет $I = [SN_{FSV}]_{0, ..., 15}$ и осуществляет поиск связанного с ним K_{FSC} в $K_{FSC}[I]$. Если K_{FSC} не найден, то средство формирования фискального признака завершает операцию формирования фискального признака с уведомлением о неудаче;

б) устанавливает значение $FDN \in V_{32}$, размерность признака дана согласно [2], [3].

в) вычисляет вектор $Vect \in V_{512}$:

$$Vect = \text{prf}(K_{FSC} \,||\, FDN); \tag{19}$$

г) вычисляет ключ фискального признака:

$$K = \text{KDF}_{512}([Vect]_{0, ..., 255}, [Vect]_{256, ..., 383}, [Vect]_{384, ..., 511}); \tag{20}$$

д) в зависимости от значения F_{FS} формирует фискальный признак:

1) документа:

$$FS_{FSCd} = [\text{HMAC}_{256}([K]_{0, ..., 255}, FD)]_{0, ..., 47}, \tag{21}$$

где $FS_{FSCd} \in V_{48}$, на печать выводится последовательность $[FS_{FSCd}]_{15, ..., 47}$, размерность и способ вывода согласно [2]:

$$FS = FS_{FSCd}; \quad (22)$$

2) архива:

$$FS_{FSCa} = \mathrm{HMAC}_{256}([K]_{0,\ ...,\ 255}, FD), \quad (23)$$

где $FS_{FSCa} \in V_{256}$, размерность согласно [2]:

$$FS = FS_{FSCa}; \quad (24)$$

3) сообщения:

$$FS_{FSCm} = [\mathrm{HMAC}_{256}([K]_{0,\ ...,\ 255}, FD)]_{0,\ ...,\ 63}, \quad (25)$$

где $FS_{FSCm} \in V_{64}$, размерность согласно [2]:

$$FS = FS_{FSCm}; \quad (26)$$

4) оператора:

$$FS_{FSCo} = [\mathrm{HMAC}_{256}([K]_{0,...,255}, FD)]_{0,...,127}, \quad (27)$$

где $FS_{FSCo} \in V_{128}$, размерность согласно [2]:

$$FS = FS_{FSCo}; \quad (28)$$

е) в зависимости от значения F_C выполняет шифрование фискальных данных:

$$C = \mathrm{ENC}([K]_{256,\ ...,\ 511}, I, FD), \quad (29)$$

где

$$I = (\underbrace{0...0}_{32\ \text{бита}} \,||\, [FS]_{16,..,47} \in V_{64}; \quad (30)$$

ж) значения *FDN, FS*, F_C и *FD* или *C* (в зависимости от F_C) подлежат передаче в адрес средства проверки фискальных признаков, последовательность передачи данных определяется согласно [3], [4], размерность — согласно [2].

В случае отсутствия шифрования значение *FD* передается в адрес средства проверки фискального признака в открытом виде.

8.3 Шаг 2. Действия средства проверки фискального признака

Средство проверки фискального признака получает сообщение, содержащее SN_{FSC}, *FDN, FS*, F_C и *FD* или *C* (в зависимости от F_C) и выполняет указанную ниже последовательность действий:

а) вычисляет ключ K^*

$$K^* = \sum_{i=0}^{m} c_i \left(\mathrm{H}_{256}\left(\mathrm{bin}_{32}(s)\right)\right)^i \in V_{256}; \quad (31)$$

б) вычисляет ключ средства формирования фискального признака:

$$K_{FSC} = \mathrm{KDF}_{256}(K^*, SN_{FSC}, SN_{FSV}); \quad (32)$$

в) вычисляет вектор $Vect \in V_{512}$:

$$Vect = \mathrm{prf}(K_{FSC} \,||\, FDN); \quad (33)$$

г) вычисляет ключ фискального признака:

$$K = \mathrm{KDF}_{512}([Vect]_{0,\ ...,\ 255}, [Vect]_{256,\ ...,\ 383}, [Vect]_{384,\ ...,\ 511}); \quad (34)$$

д) в зависимости от значения F_C выполняет расшифрование фискальных данных:

$$FD = \mathrm{DEC}([K]_{256,\ ...,\ 511}, I, C), \quad (35)$$

где

$$I = (\underbrace{0...0}_{32\ \text{бита}} \,||\, [FS]_{16,..,47} \in V_{64}; \quad (36)$$

е) в зависимости от значения флага F_{FS} выполняет расчет контрольного значения фискального признака:

1) документа:

$$FS_{FSCd}` = [\mathrm{HMAC}_{256}([K]_{0,\ldots,255}, FD)]_{0,\ldots,47}, FS` = FS_{FSCd}`; \quad (37)$$

2) архива:

$$FS_{FSCa}` = \mathrm{HMAC}_{256}([K]_{0,\ldots,255}, FD), FS` = FS_{FSCa}`; \quad (38)$$

3) сообщения:

$$FS_{FSCm}` = [\mathrm{HMAC}_{256}([K]_{0,\ldots,255}, FD)]_{0,\ldots,63}, FS` = FS_{FSCm}`; \quad (39)$$

4) оператора:

$$FS_{FSCo}` = [\mathrm{HMAC}_{256}([K]_{0,\ldots,255}, FD)]_{0,\ldots,127}, FS` = FS_{FSCo}`; \quad (40)$$

ж) если $FS` = FS$, то средство проверки фискального признака принимает решение о корректности выработанного фискального признака и аутентификации средства формирования фискального признака. В противном случае средство проверки фискального признака завершает операцию проверки фискального признака с уведомлением о неудаче;

и) выполняет расчет фискального признака подтверждения, размерность в соответствии с [2]:

$$FS_{FSV} = [\mathrm{HMAC}_{256}([K]_{0,\ldots,255}, SN_{FSV} \| SN_{FSC} \| FDN \| FS)]_{0,\ldots,63}; \quad (41)$$

к) формирует сообщение средства проверки фискального признака, которое представляет собой двоичный вектор длины 144 бита (18 байт) (размерность вектора дана согласно [3]);

$$T = FDN \| SN_{FSV} \| FS_{FSV}; \quad (42)$$

л) передает T в адрес средства формирования фискального признака.

8.4 Шаг 3. Действия средства формирования фискального признака

Средство формирования фискального признака получает сообщение T и выполняет указанную ниже последовательность действий:

а) представляет полученное сообщение T в виде $FDN` \| SN \| FS_{FSV}$, где $FDN` \in V_{32}$, $SN \in V_{48}$ и $FS_{FSV} \in V_{64}$;

б) определяет $I = [SN]_{0,\ldots,15}$ и осуществляет поиск связанного с ним K_{FSC} в $K_{FSC}[I]$. Если K_{FSC} не найден, то средство формирования фискального признака завершает операцию проверки фискального признака подтверждения с уведомлением о неудаче;

в) на основании $FDN`$ определяет ранее рассчитанный и неподтвержденный фискальный признак FS. Если он не найден или для него уже было получено подтверждение, то средство формирования фискального признака завершает операцию проверки фискального признака подтверждения с уведомлением о неудаче;

г) вычисляет вектор $Vect \in V_{512}$:

$$Vect = \mathrm{prf}(K_{FSC} \| FDN`); \quad (43)$$

д) вычисляет ключ фискального признака:

$$K = \mathrm{KDF}_{512}([Vect]_{0,\ldots,255}, [Vect]_{256,\ldots,383}, [Vect]_{384,\ldots,511}); \quad (44)$$

е) вычисляет контрольное значение фискального признака подтверждения:

$$FS_{FSV}` = [\mathrm{HMAC}_{256}([K]_{0,\ldots,255}, SN \| SN_{FSC} \| FDN` \| FS)]_{0,\ldots,63}; \quad (45)$$

ж) если выполнено равенство $FS_{FSV} = FS_{FSV}`$, то средство формирования фискального признака принимает решение о корректности фискального признака подтверждения, аутентификации средства проверки фискального признака и подтверждения ранее выработанного фискального признака FS. В противном случае выполнение операции проверки фискального признака подтверждения заканчивается с уведомлением о неудаче.

9 Действия средства формирования фискального признака при работе в автономном режиме

В случае работы в автономном режиме средство формирования фискального признака выполняет указанную ниже последовательность действий:

а) определяет $I = [SN_{FSV}]_{0,\ldots,15}$ и осуществляет поиск связанного с ним K_{FSC} в $K_{FSC}[I]$. Если K_{FSC} не найден, то средство формирования фискального признака завершает попытку формирования фискального признака с уведомлением о неудаче;

б) устанавливает значение $FDN \in V_{32}$;

в) вычисляет вектор $Vect \in V_{512}$:

$$Vect = \text{prf}\ (K_{FSC} \| FDN); \tag{46}$$

г) вычисляет ключ фискального признака:

$$K = \text{KDF}_{512}\ ([Vect]_{0, \ldots, 255}, [Vect]_{256, \ldots, 383}, [Vect]_{384, \ldots, 511}); \tag{47}$$

д) в зависимости от значения F_{FS} выполняет расчет фискального признака:

1) документа:

$$FS_{FSCd} = [\text{HMAC}_{256}\ ([K]_{0, \ldots, 255}, FD)]_{0, \ldots, 47}; \tag{48}$$

2) архива:

$$FS_{FSCa} = \text{HMAC}_{256}\ ([K]_{0, \ldots, 255}, FD)); \tag{49}$$

3) сообщения:

$$FS_{FSCm} = [\text{HMAC}_{256}\ ([K]_{0, \ldots, 255}, FD)]_{0\ ,\ldots, 63}; \tag{50}$$

4) оператора:

$$FS_{FSCo} = [\text{HMAC}_{256}\ ([K]_{0, \ldots, 255}, FD)]_{0, \ldots, 127}. \tag{51}$$

Приложение А
(справочное)

Контрольные примеры

А.1 Ключевая система

В приведенных далее контрольных примерах используются следующие параметры:

а) величина $m = 2048$;

б) матрица $A = \{a_{ij}\}$ размера $(m + 1) \times (m + 1)$, определяющая значение мастер-ключа, имеет вид:

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} & a_{0,5} & a_{0,6} & a_{0,7} & a_{0,8} & a_{0,9} & 0 & \dots & 0 \\ a_{1,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{2,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{3,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{4,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{5,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{6,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{7,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{8,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ a_{9,0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

где 0 — вектор из V_{256}, все координаты которого равны нулю. Отличные от нуля коэффициенты матрицы A определены равенствами:

$a_{0,0} = a_{0,0}$ = 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F;
$a_{0,1} = a_{1,0}$ = 202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F;
$a_{0,2} = a_{2,0}$ = 404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F;
$a_{0,3} = a_{3,0}$ = 606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F;
$a_{0,4} = a_{4,0}$ = 808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F;
$a_{0,5} = a_{5,0}$ = A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF;
$a_{0,6} = a_{6,0}$ = C0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF;
$a_{0,7} = a_{7,0}$ = E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF;
$a_{0,8} = a_{8,0}$ = 0102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20;
$a_{0,9} = a_{9,0}$ = 212223242526272829 2A2B2C2D2E2F303132333435363738393A3B3C3D3E3F40.

Здесь и далее согласно разделу 3 настоящих рекомендаций каждый вектор из V_{256} представляется в виде строки шестнадцатеричных символов, в которой младшие индексы выводятся слева, а старшие индексы — справа.

Номер средства проверки фискального признака:

1 = 1798;

в) значение случайной последовательности r, используемой для формирования серийного номера средства проверки фискального признака:

r = 0B0A0908;

г) серийный номер средства проверки фискального признака:

SN_{FSV} = 060708090A0B;

д) значение хэш-функции от серийного номера $H_{256}(SN_{FSV})$:

$H(SN_{FSV})$: 2758C5BD20363A8483DD59DEDD132BEAB63AE12BC3D267E6A8E75253A197A08E;

е) ключ средства проверки фискального признака K_{FSV}, представленный в виде вектора (c_0, ..., c_{512}), координаты которого принимают следующие значения:

c_0 = 8712A1DD558A78448D3CCE1CA6305E7CDAC38CC77192F137C41DA1A33F4DEBC6;
c_1 = 9F2A55945A7B2527B565054E95F021510F0DD371B312FD08DF0929AA55AA2D8C;
c_2 = 69F4CEE0F386AC9D5F9912B6A25CF5D5D3CF64FD60C86358E43F54644DB67F74;
c_3 = 3BBE47336BD22BF4F932E0E14FC746569871F686D181E997F22D7FDEBABDB123;
c_4 = A04DF909A17DBFE88A603D46CD045CDC6A4A0BE4C77D5EF99253AEF87C8EDB84;
c_5 = F20770DA392938812CCBCF11209FEF5F21F4999F7634D436844185428B8515D3;
c_6 = 04D9EBAE90D4B13BC637D8E917333BDBFD362E13A5EE4A66BF77F88C9399472B;
c_7 = 5693627D08803652609C2ABEFAA88858B688BC6814A7C0A9A965D3366492897C;
c_8 = 3BB5A59E273727AC7395777966D8A751104A9FADFB4E4E0CEA67EBC5A9349615;
c_9 = 862FE8F4AF4973BBAEFB592C91D7FEF81DE327890B74D6481FBE36B04E91C3FA;

ж) номер серии средств формирования фискального признака:

s = 84148994;

и) значение хэш-функции от номера серии средств формирования фискального признака H_{256} (s):

H(s) : E5C05AA15108359056324931E627EF13569844E14A5F989A1F2C22BF3EBAB1BE;

к) ключ серии средств формирования фискального признака K_S, представленный в виде вектора (b_0, ..., b_{512}), координаты которого принимают следующие значения:

b_0 = D5B4E582B5BB86DE1A52AC2E308D5B2EFBE7557707A53824BBCD8D9D788DF3CF;
b_1 = 8DFB5656A3EBBD97DC6421AF59F4CBCB5F33134F81E066AA37CF2FBF636DC6D7;
b_2 = BA322BC23EB57580FD0EC6631E26187137D4FEA690F36DA6063B21A12BEB3FEB;
b_3 = B489FFB1B580CD721DD764D8DC9756E71089A50160FD945D169724AB13699700;
b_4 = D4A0D0EA0508E5AFBFDA08FA9182BF04E61A2575B3D57BBE64D33C9DBBE7CC92;
b_5 = DA1B04998E3D5D5D5F03AA415333F192C1477ED243DB8245747F399783656479;
b_6 = EDD2790D1363954A7E694D8D14E12228A9A0933B52C88949458B3789CBE39D45;
b_7 = E369AD7E98562DB89EB0EF36D6506CBE8EFDC89CA2C670B255273283F36135AE;
b_8 = 5AB7A9E46A2929FCCEDE2424CA9EF80B1EDD3C7AF963003F5CC65EBE1273A955;
b_9 = 9E66650E8845098EC9BDE6E11718FC7AD9AACECA27955AF432B28C7FD1CA2B2B;

л) номер средства формирования фискального признака в серии:

t = 256;

м) серийный номер средства формирования фискального признака:

SN_{FSC} = 000102030405.

А.2 Пример выполнения процедур выработки фискального признака документа FS_{FSCd}

А.2.1 Фискальные данные *FD*, для которых вырабатывается фискальный признак документа, представляются в виде строки:

FD = 807F7E7D7C7B7A79787776757473727170 6F6E6D6C6B6A69686766656463626160 5F5E

длиной 280 бит (35 байт).

Значение ключа K_{FSC}, соответствующее значению номера средства проверки 1 = 1798:

K_{FSC} = 7BA64B79B86B3996C710D36FCB2DFAC6653A4B76B5E6118951042F2C3F75E2BE.

А.2.2 Шаг 1. Формирование FS_{FSCd}

а) вектор, содержащий значение номера фискального документа:

FDN = 01000000;

б) вспомогательный вектор Vect $\in V_{512}$:

Vect = 59A25AA24D2F1E3CB8ED696DBE56EFAE6F4CC07F1587CCA59558078B1C771581060D67F921
33EEC6CEB2027E17F10F57281A6884C0CC0CA74627E51EEAA8E9FE;

в) ключ *K* фискального признака:

K = CCEF67CF3C9021CC92D1CC4ECDBEFC8E65114C9141392A46BCBBBA264665A81274163C1C609BE
B545470F3C45E7BFDD021F4FC359081648797F7CA0B852F5F80;

г) значение фискального признака документа FS_{FSCd}:

FS = 24043473FB47;

д) синхропосылка I, используемая для шифрования:

I = 000000003473FB47;

е) зашифрованные фискальные данные C:

C = BF5F9782C0805F59E39F93BD0014B7B9404B579BD14FB4AD1831624865A4B080A8C0CD.

А.2.3 Шаг 2. Проверка FS_{FSCd} и формирование фискального признака подтверждения FS_{FSV}

а) вспомогательный вектор Vect $\in V_{512}$:

Vect = 59A25AA24D2F1E3CB8ED696DBE56EFAE6F4CC07F1587CCA59558078B1C771581060D67F921
33EEC6CEB2027E17F10F57281A6884C0CC0CA74627E51EEAA8E9FE;

б) ключ K фискального признака:

K = CCEF67CF3C9021CC92D1CC4ECDBEFC8E65114C9141392A46BCBBBA264665A81274163C1C609BE
B545470F3C45E7BFDD021F4FC359081648797F7CA0B852F5F80;

в) синхропосылка I, используемая для расшифрования:

I = 000000003473FB47;

г) расшифрованные данные:

FD = 807F7E7D7C7B7A797877767574737271706F6E6D6C6B6A6968676665646362616O5F5E;

д) контрольное значение фискального признака документа:

FS_{FSCd}` = 24043473FB47;

е) фискальный признак подтверждения:

FS_{FSV} = 821B0F0A7DD82D94;

ж) сформированный вектор T:

T = 01000000060708090A0B821B0F0A7DD82D94.

А.2.4 Шаг 3. Проверка фискального признака подтверждения FS_{FSV}

а) Строка для проверки фискального признака подтверждения:

FDN` || SN_{FSV} || FS_{FSV} = 01000000060708090A0B821B0F0A7DD82D94;

б) контрольное значение фискального признака подтверждения:

FS_{FSV}` = 821B0F0A7DD82D94.

А.3 Пример выполнения процедур выработки фискального признака архива FS_{FSCa}

А.3.1 Фискальные данные FD, для которых вырабатывается фискальный признак архива представляются в виде строки:

FD = 807F7E7D7C7B7A797877767574737271706F6E6D6C6B6A6968676665646362616O5F5E

длиной 280 бит (35 байт).

Значение ключа K_{FSC}, соответствующее значению номера средства проверки 1 = 1798:

K_{FSC} = 7BA64B79B86B3996C710D36FCB2DFAC6653A4B76B5E6118951042F2C3F75E2BE.

А.3.2 Шаг 1. Формирование FS_{FSCa}

а) вектор, содержащий значение номера фискального документа — архива:

FDN = 02000000;

б) вспомогательный вектор Vect $\in V_{512}$:

Vect = F696D284A9BF7E7B5210231AD4BAB9B4F3117DED13EF3F8EE99AC42019303A3DF2DED55F9
AF3480F1739D5956EEC25A55E5351AAEA3646B1D1430A7EAE72EBFC;

в) ключ K фискального признака:

K = 61C6074142A5E0CA11D996BE876E8AE08E10A956080431E33D8BA40C93F79A1F4B7B24990AF3
77C825985A4B4338DB23AFDDCFF91DD8E47BB9F61180242CE782;

г) значение фискального признака архива FS_{FSCa}:

FS = DABFCC992EA13C6B9C89FD7280DD62B48BE2085F3CD9D6F8B5E3A6B31F0E1005.

А.3.3 Шаг 2. Проверка FS_{FSCa} и формирование фискального признака подтверждения FS_{FSV}

а) вспомогательный вектор Vect $\in V_{512}$:

Vect = F696D284A9BF7E7B5210231AD4BAB9B4F3117DED13EF3F8EE99AC42019303A3DF2DED55F9
AF3480F1739D5956EEC25A55E5351AAEA3646B1D1430A7EAE72EBFC;

б) ключ K фискального признака:

K = 61C6074142A5E0CA11D996BE876E8AE08E10A956080431E33D8BA40C93F79A1F4B7B24990AF3
77C825985A4B4338DB23AFDDCFF91DD8E47BB9F61180242CE782;

в) контрольное значение фискального признака архива:

FS_{FSCa}` = DABFCC992EA13C6B9C89FD7280DD62B48BE2085F3CD9D6F8B5E3A6B31F0E1005;

г) фискальный признак подтверждения:

FS_{FSV} = 8A302291BDD89A92;

д) сформированный вектор T:

T = 02000000060708090A0B8A302291BDD89A92.

А.3.4 Шаг 3. Проверка фискального признака подтверждения FS_{FSV}

а) строка для проверки фискального признака подтверждения:

FDN` || SN_{FSV} || FS_{FSV} = 02000000060708090A0B8A302291BDD89A92;

б) контрольное значение фискального признака подтверждения:

FS_{FSV}` = 8A302291BDD89A92.

А.4 Пример выполнения процедур выработки фискального признака сообщения FS_{FSCm}

А.4.1 Фискальные данные *FD*, для которых вырабатывается фискальный признак сообщения, представляются в виде строки:

FD = 807F7E7D7C7B7A797877767574737271706F6E6D6C6B6A6968676665646362616O5F5E длиной 280 бит (35 байт).

Значение ключа K_{FSC}, соответствующее значению номера средства проверки *I* = 1798:

K_{FSC} = 7BA64B79B86B3996C710D36FCB2DFAC6653A4B76B5E6118951042F2C3F75E2BE.

А.4.2 Шаг 1. Формирование FS_{FSCm}

а) вектор, содержащий значение номера фискального сообщения:

FDN = 03000000;

б) вспомогательный вектор Vect $\in V_{512}$:

Vect = 98DC263F09A1BAAB67C0AEBE6516EEDBF333266490831B01EAE1A0F7AC95D95C907CB7F5
56E1773C3A76015870F5EDF11B1AAA1824AD7BD44A82DD94B277C7E2;

в) ключ *K* фискального признака:

K = EF1170BEA180E195DDDD52161457181794E7DCB17D2B62D34A0836E6ACE016B4DFEF77F7A657
DB5E12BEBB6CE618AE49604F4EB29144716CE2F7729626BEC200;

г) значение фискального признака документа FS_{FSCm}:

FS = 4713374EBF2E46D3;

д) синхропосылка *I*, используемая для шифрования:

I = 00000000374EBF2E;

е) зашифрованные фискальные данные C:

C = 120AA648D2E957C00AD9963B20C9FACCA656CCDDB47DCF6F635D5A85CBB1D6DDD2D24C.

А.4.3 Шаг 2. Проверка FS_{FSCm} и формирование фискального признака подтверждения FS_{FSV}

а) вспомогательный вектор Vect $\in V_{512}$:

Vect = 98DC263F09A1BAAB67C0AEBE6516EEDBF333266490831B01EAE1A0F7AC95D95C907CB7F5
56E1773C3A76015870F5EDF11B1AAA1824AD7BD44A82DD94B277C7E2;

б) ключ *K* фискального признака:

K = EF1170BEA180E195DDDD52161457181794E7DCB17D2B62D34A0836E6ACE016B4DFEF77F7A657
DB5E12BEBB6CE618AE49604F4EB29144716CE2F7729626BEC200;

в) синхропосылка *I*, используемая для расшифрования:

I = 00000000374EBF2E;

г) расшифрованные данные:

FD = 807F7E7D7C7B7A797877767574737271706F6E6D6C6B6A6968676665646362616O5F5E;

д) контрольное значение фискального признака сообщения:

FS_{FSCm}` = 4713374EBF2E46D3;

е) фискальный признак подтверждения:

FS_{FSV} = 4944116131B958E0;

ж) сформированный вектор T:

T = 03000000060708090A0B4944116131B958E0.

А.4.4 Шаг 3. Проверка фискального признака подтверждения FS_{FSV}

а) строка для проверки фискального признака подтверждения:

FDN` || SN_{FSV} || FS_{FSV} = 03000000060708090A0B4944116131B958E0;

б) контрольное значение фискального признака подтверждения:

FS_{FSV}` = 4944116131B958E0.

А.5 Пример выполнения процедур выработки фискального признака оператора FS_{FSCo}

А.5.1 Фискальные данные *FD*, для которых вырабатывается фискальный признак оператора, представляются в виде строки:

FD = 807F7E7D7C7B7A797877767574737271706F6E6D6C6B6A6968676665646362616O5F5E длиной 280 бит (35 байт).

Значение ключа K_{FSC}, соответствующее значению номера средства проверки 1 = 1798:

K_{FSC} = 7BA64B79B86B3996C710D36FCB2DFAC6653A4B76B5E6118951042F2C3F75E2BE.

А.5.2 Шаг 1. Формирование FS_{FSCo}

а) вектор, содержащий значение номера фискального документа — оператора:

FDN = 04000000;

б) вспомогательный вектор Vect $\in V_{512}$:

Vect = 19F212BEA6F505EC6BFF5448410DD7A3B72FA470CB16F7F01A149EA58CE6CBAF6B569940C
E965B3D1B81D79F7E5F9FE407618C14200FFC4EFF899D52A75DF976;

в) ключ *K* фискального признака:

K = F51E9AB7430EB62EE40E615460EEC23D2A09026135970E467F5E75794685724BEF8A1B25BF9A
F0FB161FB6A6E6B1F811891D2C852D1C0A1BA018217B894BA400;

г) значение фискального признака оператора FS_{FSCo}:

$$FS = 5C201A6AA00D1075092985669173B754.$$

А.5.3 Шаг 2. Проверка FS_{FSCo} и формирование фискального признака подтверждения FS_{FSV}

а) вспомогательный вектор Vect $\in V_{512}$:

Vect = 19F212BEA6F505EC6BFF5448410DD7A3B72FA470CB16F7F01A149EA58CE6CBAF6B569940C
E965B3D1B81D79F7E5F9FE407618C14200FFC4EFF899D52A75DF976;

б) ключ K фискального признака:

K = F51E9AB7430EB62EE40E615460EEC23D2A09026135970E467F5E75794685724BEF8A1B25BF9A
F0FB161FB6A6E6B1F811891D2C852D1C0A1BA018217B894BA400;

в) контрольное значение фискального признака оператора:

$$FS_{FSCo}` = 5C201A6AA00D1075092985669173B754;$$

г) фискальный признак подтверждения FS_{FSV}:

$$FS_{FSV} = 662DF5CA1F85B26B;$$

д) сформированный вектор T:

$$T = 04000000060708090A0B662DF5CA1F85B26B.$$

А.5.4 Шаг 3. Проверка фискального признака подтверждения FS_{FSV}

а) строка для проверки фискального признака подтверждения:

$$FDN` \,||\, SN_{FSV} \,||\, FS_{FSV} = 04000000060708090A0B662DF5CA1F85B26B;$$

б) контрольное значение фискального признака подтверждения:

$$FS_{FSV}` = 662DF5CA1F85B26B.$$

Библиография

[1] Федеральный закон от 22 мая 2003 г. № 54-ФЗ«О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа» (в редакции Федерального закона от 3 июля 2016 г. № 290-ФЗ «О внесении изменений в Федеральный закон «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт» и отдельные законодательные акты Российской Федерации»)

[2] Приказ Федеральной налоговой службы Министерства финансов Российской Федерации от 21 марта 2017 г. № ММВ7-20/229 «Об утверждении дополнительных реквизитов фискальных документов и форматов фискальных документов, обязательных к использованию» (зарегистрирован в Министерстве юстиции Российской Федерации 13 апреля 2017 г., регистрационный № 46361)

[3] ККТ v1.1 Контрольно-кассовая техника. Описание интерфейса фискального накопителя. Версия 1.1 (от 5 мая 2016 г., введена в действие 1 июля 2016 г.)

[4] Протокол АСК ККТ Протокол взаимодействия оператора фискальных данных с подсистемой приема фискальных данных АСК КТ (ОФД — ППФД АСК ККТ)

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: криптографическая защита информации, криптографическая аутентификация, криптографический механизм, фискальные данные, контрольно-кассовая техника, хэш-функция, ключ

БЗ 7—2018/32

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 30.05.2018. Подписано в печать 08.06.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 123001 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru