

---

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

---



РЕКОМЕНДАЦИИ  
ПО СТАНДАРТИЗАЦИИ

**Р 1323565.1.017—  
2018**

---

**Информационная технология**

## **КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**

**Криптографические алгоритмы, сопутствующие  
применению алгоритмов блочного шифрования**

Издание официальное



Москва  
Стандартинформ  
2018

## Предисловие

- 1 РАЗРАБОТАНЫ Обществом с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)
- 2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»
- 3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 апреля 2018 г. № 206-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 ([www.gost.ru](http://www.gost.ru))*

© Стандартиформ, 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 Обозначения .....	1
4 Режимы работы блочных шифров с преобразованием ключа.....	2
4.1 Режим шифрования CTR-АСПКМ .....	3
4.2 Режим выработки имитовставки ОМАС-АСПКМ.....	4
5 Алгоритмы экспорта КЕхр15 и импорта КІмр15 ключа .....	5
Приложение А (справочное) Контрольные примеры для режимов работы блочных шифров с преобразованием ключа .....	7
Приложение Б (справочное) Контрольные примеры работы алгоритмов экспорта КЕхр15 и импорта КІмр15 ключа.....	15
Приложение В (рекомендуемое) Пример параметров режима шифрования CTR-АСПКМ .....	16
Библиография.....	17

## **Введение**

Настоящие рекомендации содержат описание двух режимов работы блочных шифров с внутренним преобразованием ключа и алгоритмов импорта и экспорта ключей, сопутствующих применению алгоритмов блочного шифрования по ГОСТ Р 34.12—2015 и режимов их работы согласно ГОСТ Р 34.13—2015.

Необходимость разработки настоящих рекомендаций вызвана потребностью в обеспечении совместимости криптографических протоколов, использующих алгоритмы ГОСТ Р 34.12—2015 и ГОСТ Р 34.13—2015.

**П р и м е ч а н и е** — Основная часть настоящих рекомендаций дополнена приложениями А—В.

## РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

## КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов  
блочного шифрованияInformation technology. Cryptographic data security.  
Cryptographic algorithms accompanying the use of block ciphers

Дата введения — 2018—10—01

## 1 Область применения

Настоящие рекомендации предназначены для применения в информационных системах, использующих механизмы защиты данных, определенных в ГОСТ Р 34.12—2015 и ГОСТ Р 34.13—2015, в общедоступных и корпоративных сетях для защиты информации, не содержащей сведений, составляющих государственную тайну.

## 2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

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

**П р и м е ч а н и е** — 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, применяется в части, не затрагивающей эту ссылку.

## 3 Обозначения

В настоящих рекомендациях используют следующие обозначения:

- |       |   |
|-------|---|
| $V^*$ | — множество всех двоичных строк конечной длины, включая пустую строку;  |
| $V_s$ | — множество двоичных строк длины $s$ , $s \geq 0$ ; нумерация подстрок и компонент строки осуществлена справа налево начиная с единицы; |

$V_{\geq s}$	— множество всех двоичных строк длины $l \geq s$ , где $s$ — целое неотрицательное число: $V_{\geq s} = V^* \setminus \bigcup_{i=0}^{s-1} V_i$ ;
$B_s$	— множество байтовых строк длины $s$ , $s \geq 0$ ; нумерация компонент строки осуществлена слева направо начиная с единицы. Строка $b = (b_1, \dots, b_s)$ принадлежит множеству $B_s$ , если компоненты $b_1, \dots, b_s \in \{0, \dots, 255\}$ . При $s = 0$ множество $B_s$ состоит из единственной пустой строки длины 0;
$\parallel$	— конкатенация двоичных строк; если $\alpha = (\alpha_1, \dots, \alpha_s) \in V_{s_1}$ , $\beta = (\beta_1, \dots, \beta_s) \in V_{s_2}$ , то их конкатенацией $\alpha \parallel \beta$ называется строка $\gamma = (\alpha_{s_1}, \dots, \alpha_1, \beta_{s_1}, \dots, \beta_1) \in V_{s_1+s_2}$ ;
$\oplus$	— операция покомпонентного сложения по модулю 2 двух двоичных строк одинаковой длины;
$\mathbb{Z}_{2^s}$	— кольцо вычетов по модулю $2^s$ ;
$\boxplus_s$	— операция сложения в кольце $\mathbb{Z}_{2^s}$ ;
$\alpha \ll r$	— операция логического сдвига двоичной строки $\alpha$ на $r$ компонент в сторону компонент, имеющих большие номера;
$ \alpha $	— длина битовой строки $\alpha$ ;
$\lceil x \rceil$	— наименьшее целое число, большее или равное $x$ ;
$E_K: V_n \rightarrow V_n$	— отображение, реализующее базовый алгоритм блочного шифрования на ключе $K$ ;
$n$	— параметр алгоритма блочного шифрования, называемый длиной блока. В рамках настоящих рекомендаций измеряется в битах;
$k$	— параметр алгоритма блочного шифрования, называемый длиной ключа. В рамках настоящих рекомендаций измеряется в битах и принимает значение 256;
$a^r$	— строка, состоящая из $r$ элементов $a \in \{0, 1\}$ ;
$Int_s: V_s \rightarrow \mathbb{Z}_{2^s}$	— отображение, ставящее в соответствие двоичной строке $\alpha = (\alpha_s, \dots, \alpha_1) \in V_s$ число $Int_s(\alpha) = 2^{s-1}\alpha_s + \dots + 2^0\alpha_1$ ;
$Vec_s: \mathbb{Z}_{2^s} \rightarrow V_s$	— отображение, обратное к отображению $Int_s$ ;
$Inc_s: V_s \rightarrow V_s$	— отображение, ставящее в соответствие двоичной строке $\alpha = (\alpha_s, \dots, \alpha_1) \in V_s$ строку $Vec_s(Int_s(\alpha) \boxplus_s 1)$ ;
$MSB_t: V_{\geq s} \rightarrow V_t$	— отображение, ставящее в соответствие двоичной строке $\alpha = (\alpha_s, \dots, \alpha_1) \in V_s$ строку $MSB_t(\alpha) = (\alpha_s, \dots, \alpha_{s-t+1}) \in V_t$ , $1 \leq t \leq s$ ;
$Byte_s: V_{8s} \rightarrow B_s$	— отображение, ставящее в соответствие двоичной строке $\alpha = (\alpha_{8s}, \dots, \alpha_1) \in V_{8s}$ байтовую строку $b = (b_1, \dots, b_s) \in B_s$ , где $b_i = Int_8((\alpha_{8(s+1-i)}, \dots, \alpha_{8(s+1-i)-7}))$ , $i = 1, \dots, s$ . При этом строка $b$ называется байтовым представлением двоичной строки $\alpha$ , а ее элементы $b_1, \dots, b_s$ — байтами.

**П р и м е ч а н и е** — В настоящих рекомендациях при записи байтовой строки каждый байт представлен в шестнадцатеричном виде и отделен от соседних пробелами. Предполагается, что двоичной строке  $\alpha \in V_{8s}$  соответствует байтовая строка  $b = Byte_s(\alpha)$  и наоборот. Например, двоичная строка 1100101100011000 соответствует байтовой строке СВ 18.

#### 4 Режимы работы блочных шифров с преобразованием ключа

Настоящие рекомендации определяют следующие режимы работы алгоритмов блочного шифрования, которые используют в процессе своей работы функции *АСПКМ* и *АСПКМ-Master*:

- режим шифрования CTR-АСПКМ;
- режим выработки имитовставки ОМАС-АСПКМ.

Данные режимы можно использовать в качестве режимов для блочных шифров «Магма» или «Кузнечик», определенных в ГОСТ Р 34.12—2015. В первом случае подразумевается, что в качестве отображения  $E_K$  использован блочный шифр «Магма» с длиной блока  $n = 64$ ; во втором случае подразумевается, что в качестве отображения  $E_K$  использован блочный шифр «Кузнечик» с длиной блока  $n = 128$ .

Использование двух разных блочных шифров в рамках одного режима работы алгоритма блочного шифрования не допускается. Использование двух одинаковых ключей для режима шифрования CTR-АСПКМ и режима выработки имитовставки ОМАС-АСПКМ в рамках одной криптосистемы не допускается, при этом должна быть обеспечена независимость данных ключей.

#### 4.1 Режим шифрования CTR-АСПКМ

При обработке сообщений в режиме CTR-АСПКМ каждое сообщение разбивают на секции, где под секцией понимается строка, состоящая из данных, обрабатываемых на одном секционном ключе до применения к нему функции АСПКМ, определенной в 4.1.1.

Параметром, определяющим порядок функционирования режима CTR-АСПКМ, является длина секции  $N$ . Значение  $N$  выражено в битах и фиксировано в рамках каждого конкретного протокола исходя из требований к производительности системы и нагрузке на ключ. Длина секции  $N$  должна быть кратна длине блока  $n$  используемого блочного шифра. Дополнительный параметр режима CTR-АСПКМ — это длина блока гаммы  $s$ ,  $0 < s \leq n$ , выраженная в битах. Величина  $s$  должна делить длину блока  $n$ .

Процесс обработки сообщений в режиме CTR-АСПКМ схематично представлен на рисунке 1.

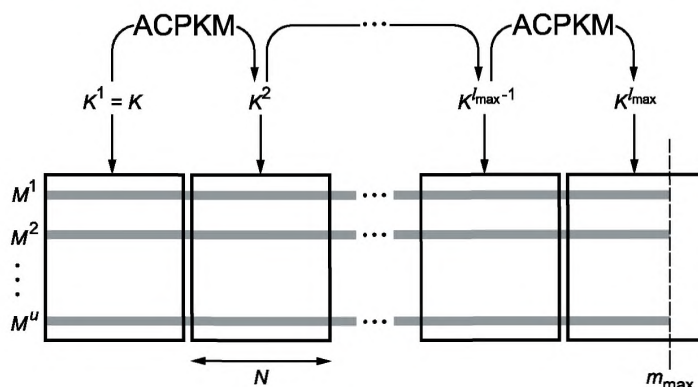


Рисунок 1 — Обработка сообщений в режиме CTR-АСПКМ

**П р и м е ч а н и е** — На рисунке 1 через  $m_{\max}$  обозначена максимальная длина сообщения, выраженная в битах,  $l_{\max} = \lceil m_{\max}/N \rceil$ .

При обработке каждого сообщения  $M = M^j$ ,  $j = 1, 2, \dots$ , в режиме CTR-АСПКМ сообщение разбивают на  $l = \lceil |M|/N \rceil$  секций и представляют в виде  $M = M_1 || M_2 || \dots || M_l$ , где  $M_i \in V_N$ ,  $i = 1, 2, \dots, l-1$ ,  $M_l \in V_w$ ,  $w \leq N$ . Первую секцию каждого сообщения обрабатывают на секционном ключе  $K^1$ , который равен начальному ключу  $K$ . Для обработки  $i$ -ой секции каждого сообщения,  $i = 2, \dots, l$ , используют секционный ключ  $K^i$ , который вычисляют из значения ключа  $K^{i-1}$  с помощью функции АСПКМ.

Результатом зашифрования сообщения  $M$  длины  $m$  в режиме CTR-АСПКМ на начальном ключе  $K$  с длиной секции  $N$  и вектором инициализации  $IV$  является строка  $C$ ,  $|C| = |M|$ , которая формируется по следующей схеме:

$$\begin{aligned}
 q &= \lceil m/s \rceil = \lceil m/N \rceil; \\
 M &= P_1 || P_2 || \dots || P_q, P_i \in V_s, i = 1, 2, \dots, q-1, P_q V_r, r \leq s; \\
 CTR_1 &= IV || 0^{n/2}; \\
 CTR_i &= Inc_n(CTR_{i-1}), i = 2, 3, \dots, q; \\
 K^1 &= K; \\
 K^j &= АСПКМ(K^{j-1}), j = 2, 3, \dots, l; \\
 C_i &= P_i \oplus MSB_{|P_i|}(E_{K^j}(CTR_i)), i = 1, 2, \dots, q, j = i \cdot s/N; \\
 C &= C_1 || \dots || C_q.
 \end{aligned} \tag{1}$$

При использовании режима CTR-АСПКМ не требуется применение процедуры дополнения сообщения. Длина  $m$  сообщения, обрабатываемого в режиме CTR-АСПКМ, не должна превышать значения  $2^{n/2-1} \cdot s$  бит.

Для обработки каждого отдельного сообщения в режиме CTR-АСПКМ на одном начальном ключе  $K$  использовано значение уникальной синхропосылки  $IV \in V_{n/2}$ .

#### 4.1.1 Функция АСРКМ

Функция АСРКМ принимает на вход ключ  $K^{i-1}$  длины  $k$  бит и преобразует его в ключ  $K^i$  той же длины. Функция АСРКМ определяется в зависимости от используемого блочного шифра «Магма» или «Кузнечик», определенного в ГОСТ Р 34.12—2015, следующим образом:

$$K^i = \text{АСРКМ}(K^{i-1}) = E_{K^{i-1}}(D_1) \parallel \dots \parallel E_{K^{i-1}}(D_J), \quad (2)$$

где  $J = k/n$ ,  $D_1 \parallel \dots \parallel D_J = D$ ,  $D_1, \dots, D_J \in V_n$ , а константа  $D \in V_k$  задана следующим образом:

$D =$  80 81 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F  
90 91 92 93 94 95 96 97 98 99 9A 9B 9C 9D 9E 9F.

#### 4.2 Режим выработки имитовставки ОМАС-АСРКМ

При вычислении имитовставки сообщения в режиме ОМАС-АСРКМ каждое сообщение разбивают на секции, где под секцией понимается строка, состоящая из данных, обрабатываемых на одном секционном ключе до применения к нему функции АСРКМ-Master, определенной в 4.2.1.

При формировании имитовставки в режиме ОМАС-АСРКМ начальный ключ  $K$  не используют непосредственно для обработки данных и задействуют только для порождения последовательности секционных ключей. Параметрами, определяющими порядок функционирования режима ОМАС-АСРКМ, являются длина секции  $N$  и частота  $T^*$  смены мастер-ключей, обозначенных на рисунке 2  $K_1^*, K_2^*, \dots, K_{l_{\max}}^*$ . Параметры  $N$  и  $T^*$  выражены в битах. Значения  $N$  и  $T^*$  фиксируют в рамках каждого конкретного протокола исходя из требований к производительности системы и нагрузке на ключ. Длина секции  $N$  должна быть кратна длине блока  $n$  используемого блочного шифра. Частота смены ключа  $T^*$  должна быть кратна  $k + n$ . Дополнительный параметр режима ОМАС-АСРКМ — это длина имитовставки  $s$ ,  $0 < s \leq n$ , выраженная в битах.

Процесс обработки сообщений в режиме ОМАС-АСРКМ схематично представлен на рисунке 2.

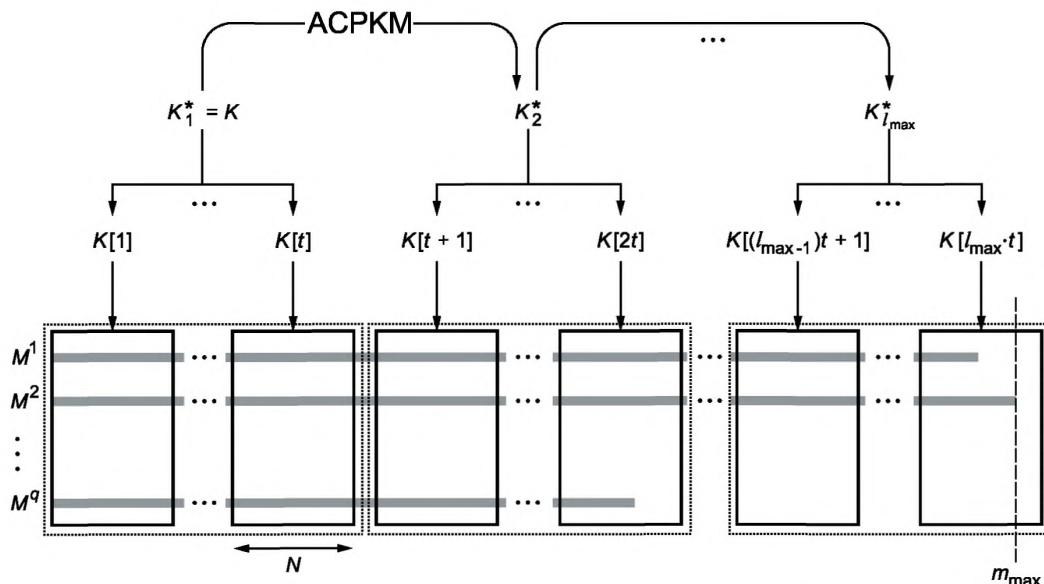


Рисунок 2 — Обработка сообщений в режиме ОМАС-АСРКМ

**Примечание** — На рисунке 2 через  $m_{\max}$  обозначена максимальная длина сообщения, выраженная в битах,  $l_{\max} = \lceil m_{\max}/N \cdot t \rceil$ ,  $t = T^*/(k + n)$ .

При обработке сообщения  $M^j$  длины  $m$  в режиме ОМАС-АСРКМ на начальном ключе  $K$  сообщение разбивают на  $l = \lceil m/N \rceil$  секций и представляют в виде  $M^j = M_1^j \parallel M_2^j \parallel \dots \parallel M_l^j$ , где  $M_i^j \in V_N$ ,  $i = 1, 2, \dots, l$ ,  $M_l^j \in V_w$ ,  $w \leq N$ . Для обработки секции из начального ключа  $K$  с помощью функции АСРКМ-Master вырабатывается последовательность ключевого материала секций  $K[1] = \{K^1, K_1^1\}$ ,  $K[2] = \{K^2, K_1^2\}$ , ...,  $K[l] = \{K^l, K_1^l\}$ . Каждая  $i$ -я секция,  $i = 1, 2, \dots, l-1$ , обрабатывается на ключе  $K^i$ . Для обработки последней  $l$ -й секции использованы ключ  $K^l$  и вспомогательный ключ  $K_1^l$ .



Результатом вычисления имитовставки сообщения  $M$  длины  $m$  в режиме ОМАС-АСРКМ на начальном ключе  $K$  с длиной секции  $N$  и частотой смены ключа  $T^*$  является строка  $MAC$  длины  $s$ , которая формируется по следующей схеме:

$$\begin{aligned}
 q &= \lceil m/n \rceil, l = \lceil m/N \rceil; \\
 M &= P_1 \parallel P_2 \parallel \dots \parallel P_q, P_i \in V_n, i = 1, 2, \dots, q-1, P_q \in V_r, r \leq n; \\
 C &= C_1 \parallel \dots \parallel C_q; \\
 K^1 \parallel K_1^1 \parallel \dots \parallel K^l \parallel K_l^1 &= \text{АСРКМ-Master}(K, T^*, l); \\
 K_2^l &= \begin{cases} K_1^l \ll 1, & \text{если } MSB_1(K_1^l) = 0 \\ (K_1^l \ll 1) \oplus B_n, & \text{иначе} \end{cases}, \\
 \text{где } B_{64} &= 0^{59} \parallel 11011, B_{128} = 0^{120} \parallel 10000111; \\
 K' &= \begin{cases} K_1^l, & \text{если } r = n; \\ K_2^l, & \text{если } r < n; \end{cases} \quad (3)
 \end{aligned}$$

$$\begin{aligned}
 C_0 &= 0^n; \\
 C_j &= E_{K^j}(P_j \oplus C_{j-1}), i = 1, 2, \dots, q-1, j = i \cdot n/N; \\
 P_q^* &= \begin{cases} P_q, & \text{если } r = n \\ P_q \parallel 1 \parallel 0^{n-1-r}, & \text{если } r < n; \end{cases}
 \end{aligned}$$

$$MAC = MSB_s(E_{K^l}(P_q^* \oplus C_{q-1} \oplus K')).$$

Длина  $m$  сообщения, обрабатываемого в режиме ОМАС-АСРКМ, не должна превышать значения  $2^{n/2-1} \cdot \frac{n \cdot N}{k+n}$  бит.

Очередная часть ключевого материала секции  $K[l]$  может быть вычислена по мере необходимости при поступлении данных на вход (может обеспечиваться потоковый режим обработки данных).

#### 4.2.1 Функция АСРКМ-Master

Функция АСРКМ-Master принимает на вход начальный ключ  $K$  длины  $k$  бит, параметр частоты смены мастер-ключа  $T^*$  и количество элементов  $l$  в последовательности ключевого материала секций, которые необходимо выработать. Функция АСРКМ-Master задана в соответствии с выбранным блочным шифром «Магма» или «Кузнечик», определенным в ГОСТ Р 34.12—2015, следующим образом:

$$\text{АСРКМ-Master}(K, T^*, l) = K^1 \parallel K_1^1 \parallel \dots \parallel K^l \parallel K_l^1 = \text{CTR-АСРКМ}(K, T^*, 1^{n/2}, 0^{l \cdot (k+n)}), \quad (4)$$

где  $K_i \in V_k, K_1^i \in V_n, i \in \{1, 2, \dots, l\}$ ,  $\text{CTR-АСРКМ}(K, N, IV, M)$  является функцией зашифрования в режиме CTR-АСРКМ, которая принимает на вход ключ  $K$ , размер секции  $N$ , значение вектора инициализации  $IV \in V_{n/2}$  и сообщение  $M$ .

## 5 Алгоритмы экспорта KExp15 и импорта KImp15 ключа

В данном разделе приведены алгоритмы экспорта и импорта ключа, использующие в своей работе один из блочных шифров, определенных в ГОСТ Р 34.12—2015 («Магма» или «Кузнечик»).

Входными параметрами алгоритма экспорта ключа KExp15 являются экспортируемый ключ  $K \in V^*$ , ключ вычисления имитовставки  $K_{MAC}^{Exp} \in V_k$ , ключ шифрования  $K_{ENC}^{Exp} \in V_k$  и значение  $IV \in V_{n/2}$ . При этом должна быть обеспечена независимость ключей  $K_{MAC}^{Exp}$  и  $K_{ENC}^{Exp}$ . Экспортное представление ключа  $K$  формируется по следующей схеме:

- вычисляют значение имитовставки  $KEYMAC$  длины  $n$  бит:

$$KEYMAC = \text{OMAC}(K_{MAC}^{Exp}, IV \parallel K), \quad (5)$$

где  $\text{OMAC}(K, M)$  — функция выработки имитовставки, описанная в ГОСТ Р 34.13—2015, на ключе  $K$  от данных  $M$ ;

- вычисляют значение  $KEXP$ :

$$KEXP = \text{encKey} \parallel \text{encKeyMAC} = \text{CTR}(K_{ENC}^{Exp}, IV, K \parallel KEYMAC), \quad (6)$$

где  $|encKey| = |K|$ ,  $|encKeyMAC| = |KEYMAC|$ ,  $CTR(K, IV, M)$  — функция зашифрования в режиме гаммирования с длиной блока гаммы  $s = n$ , представленном в ГОСТ Р 34.13–2015, принимающая на вход ключ  $K$ , вектор инициализации  $IV$  и данные  $M$

- результат работы алгоритма экспорта ключа  $K$  называется экспортным представлением ключа  $K$ , обозначается через  $KExp15(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$  и полагается равным строке  $KEXP$ :

$$KExp15(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV) = KEXP. \quad (7)$$

Импорт ключа по алгоритму  $KImp15$  (получение ключа  $K$  по экспортному представлению  $KEXP$  с помощью ключей  $K_{MAC}^{Exp}$ ,  $K_{ENC}^{Exp} \in V_K$  и значения  $IV \in V_{n/2}$ ) осуществляется по следующей схеме:

- строка  $KEXP$  расшифровывается на ключе  $K_{ENC}^{Exp}$  в соответствии с режимом гаммирования с длиной блока гаммы  $s = n$ , приведенным в ГОСТ Р 34.13—2015, при этом вектор инициализации полагается равным  $IV$ . Строка  $K \parallel KEYMAC$  полагается равной результату расшифрования;

- вычисляют значение имитовставки длины  $n$  бит в соответствии с режимом выработки имитовставки, указанным в ГОСТ Р 34.13—2015, от данных  $IV \parallel K$  на ключе  $K_{MAC}^{Exp}$ . Если результат отличен от  $KEYMAC$ , возвращается ошибка;

- результат работы алгоритма импорта ключа от его экспортного представления  $KEXP$  обозначается через  $KImp15(KEXP, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$  и полагается равным строке  $K$ :

$$KImp15(KEXP, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV) = K. \quad (8)$$

В рамках применения одной и той же пары ключей  $(K_{MAC}^{Exp}, K_{ENC}^{Exp})$  значения  $IV$ , используемые в качестве входных параметров алгоритма экспорта ключа  $KExp15$ , должны быть уникальными. Для выработки этих значений может быть использован детерминированный счетчик. Для осуществления импорта ключа в соответствии с алгоритмом  $KImp15$  каждое значение  $IV$  должно либо передаваться вместе с экспортным представлением ключа, либо являться предварительно распределенным значением.

Допускается применение алгоритмов экспорта  $KExp15$  и импорта  $KImp15$  к ключу  $K$  произвольного криптографического алгоритма.

## Приложение А (справочное)

### Контрольные примеры для режимов работы блочных шифров с преобразованием ключа

В данном приложении представлены контрольные примеры работы режимов работы блочных шифров с преобразованием ключа, приведенных в разделе 4. Параметры  $s$ ,  $m$ ,  $N$  и  $T^*$  выбраны из соображений демонстрации особенностей работы алгоритмов.

#### А.1 Режим шифрования CTR-АСРКМ для шифра «Магма»

В настоящем разделе приведены тестовые примеры работы режима шифрования CTR-АСРКМ для шифра «Магма» со следующими входными данными:

- длина блока  $n$  — 64 бита;
- длина блока гаммы  $s$  — 64 бита;
- размер секции  $N$  — 128 бит;
- ключ  $K$ :  
88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77  
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF;
- вектор инициализации  $IV$ :  
12 34 56 78;
- открытый текст  $M$ :  
11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88  
00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A  
11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00  
22 33 44 55 66 77 88 99.

Сообщение  $M$  разбивают на четыре секции  $M_1$ ,  $M_2$ ,  $M_3$ ,  $M_4$ , каждую из которых разбивают на блоки. Обработку данных производят в соответствии с таблицами А.1.1—А.1.4.

Т а б л и ц а А.1.1 — Обработка секции  $M_1$  в режиме CTR-АСРКМ для шифра «Магма»

Секция $M_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Ключ $K^1$	88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF
Обработка 1-го блока:	
Счетчик $CTR_1$	12 34 56 78 00 00 00 00
Блок гаммы	3B 9A 2E AA BE 78 3B AB
Блок открытого текста $P_1$	11 22 33 44 55 66 77 00
Блок шифртекста $C_1$	2A B8 1D EE EB 1E 4C AB
Обработка 2-го блока:	
Счетчик $CTR_2$	12 34 56 78 00 00 00 01
Блок гаммы	97 0F D9 08 06 C1 0D 62
Блок открытого текста $P_2$	FF EE DD CC BB AA 99 88
Блок шифртекста $C_2$	68 E1 04 C4 BD 6B 94 EA

Т а б л и ц а А.1.2 — Обработка секции  $M_2$  в режиме CTR-АСРКМ для шифра «Магма»

Секция $M_2$	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Ключ $K^2$	86 3E A0 17 84 2C 3D 37 2B 18 A8 5A 28 E2 31 7D 74 BE FC 10 77 20 DE 0C 9E 8A B9 74 AB D0 0C A0
Обработка 3-го блока:	
Счетчик $CTR_3$	12 34 56 78 00 00 00 02
Блок гаммы	C7 3D 45 9C 28 7B 3D 1C
Блок открытого текста $P_3$	00 11 22 33 44 55 66 77
Блок шифртекста $C_3$	C7 2C 67 AF 6C 2E 5B 6B

Окончание таблицы А.1.2

Обработка 4-го блока:	
Счетчик $CTR_4$	12 34 56 78 00 00 00 03
Блок гаммы	86 36 1C AC BC 1F 4C 24
Блок открытого текста $P_4$	88 99 AA BB CC EE FF 0A
Блок шифртекста $C_4$	0E AF B6 17 70 F1 B3 2E

Т а б л и ц а А.1.3 — Обработка секции  $M_3$  в режиме CTR-АСРКМ для шифра «Магма»

Секция $M_3$	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
Ключ $K^3$	49 A5 E2 67 7D E5 55 98 2B 8A D5 E8 26 65 2D 17 EE C8 47 BF 5B 39 97 A8 1C F7 FE 7F 11 87 BD 27
Обработка 5-го блока:	
Счетчик $CTR_5$	12 34 56 78 00 00 00 04
Блок гаммы	B0 8C 42 50 CB 8B 64 0A
Блок открытого текста $P_5$	11 22 33 44 55 66 77 88
Блок шифртекста $C_5$	A1 AE 71 14 9E ED 13 82
Обработка 6-го блока:	
Счетчик $CTR_6$	12 34 56 78 00 00 00 05
Блок гаммы	32 7E DC D4 E8 8D E6 6F
Блок открытого текста $P_6$	99 AA BB CC EE FF 0A 00
Блок шифртекста $C_6$	AB D4 67 18 06 72 EC 6F

Т а б л и ц а А.1.4 — Обработка секции  $M_4$  в режиме CTR-АСРКМ для шифра «Магма»

Секция $M_4$	22 33 44 55 66 77 88 99
Ключ $K^4$	32 56 BF 3F 97 B5 66 74 26 A9 FB 1C 5E AA BE 41 89 3C CD D5 A8 68 F9 B6 3B 0A A9 07 20 FA 43 C4
Обработка 7-го блока:	
Счетчик $CTR_7$	12 34 56 78 00 00 00 06
Блок гаммы	A6 91 B5 0E 59 BD FA 58
Блок открытого текста $P_7$	22 33 44 55 66 77 88 99
Блок шифртекста $C_7$	84 A2 F1 5B 3F CA 72 C1

Результатом зашифрования открытого текста  $M$  в режиме CTR-АСРКМ в данном случае является строка  $C_1 \parallel C_2 \parallel \dots \parallel C_7$ :

2A B8 1D EE EB 1E 4C AB 68 E1 04 C4 BD 6B 94 EA  
C7 2C 67 AF 6C 2E 5B 6B 0E AF B6 17 70 F1 B3 2E  
A1 AE 71 14 9E ED 13 82 AB D4 67 18 06 72 EC 6F  
84 A2 F1 5B 3F CA 72 C1.

## А.2 Режим шифрования CTR-АСРКМ для шифра «Кузнечик»

В настоящем разделе приведены тестовые примеры работы режима шифрования CTR-АСРКМ для шифра «Кузнечик» со следующими входными данными:

- длина блока  $n$  — 128 бит;
- длина блока гаммы  $s$  — 128 бит;
- размер секции  $N$  — 256 бит;
- ключ  $K$ :  
88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77  
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF;
- вектор инициализации  $IV$ :  
12 34 56 78 90 AB CE F0;

- открытый текст  $M$ :

```
11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33
55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33 44.
```

Сообщение  $M$  разбивают на четыре секции  $M_1, M_2, M_3, M_4$ , каждую из которых разбивают на блоки. Обработку данных производят в соответствии с таблицами А.2.1—А.2.4.

Т а б л и ц а А.2.1 — Обработка секции  $M_1$  в режиме CTR-АПКМ для шифра «Кузнечик»

Секция $M_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88 00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Ключ $K^1$	88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF
Обработка 1-го блока:	
Счетчик $CTR_1$	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00
Блок гаммы	E0 B7 EB FA 94 68 A6 DB 2A 95 82 6E FB 17 38 30
Блок открытого текста $P_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Блок шифртекста $C_1$	F1 95 D8 BE C1 0E D1 DB D5 7B 5F A2 40 BD A1 B8
Обработка 2-го блока:	
Счетчик $CTR_2$	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 01
Блок гаммы	85 FF C5 00 B2 F4 58 2A 7B A5 4E 08 F0 AB 21 EE
Блок открытого текста $P_2$	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Блок шифртекста $C_2$	85 EE E7 33 F6 A1 3E 5D F3 3C E4 B3 3C 45 DE E4

Т а б л и ц а А.2.2 — Обработка секции  $M_2$  в режиме CTR-АПКМ для шифра «Кузнечик»

Секция $M_2$	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Ключ $K^2$	26 66 ED 40 AE 68 78 11 74 5C A0 B4 48 F5 7A 7B 39 0A DB 57 80 30 7E 8E 96 59 AC 40 3A E6 0C 60
Обработка 3-го блока:	
Счетчик $CTR_3$	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 02
Блок гаммы	5A EC D8 CB 31 09 3B DD 99 BD BD EB B0 7A E2 00
Блок открытого текста $P_3$	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
Блок шифртекста $C_3$	4B CE EB 8F 64 6F 4C 55 00 17 06 27 5E 85 E8 00
Обработка 4-го блока:	
Счетчик $CTR_4$	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 03
Блок гаммы	7A 4F 09 A0 0E A7 1C A0 94 F3 F8 41 2F 8A 50 57
Блок открытого текста $P_4$	22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Блок шифртекста $C_4$	58 7C 4D F5 68 D0 94 39 3E 48 34 AF D0 80 50 46

Т а б л и ц а А.2.3 — Обработка секции  $M_3$  в режиме CTR-АПКМ для шифра «Кузнечик»

Секция $M_3$	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33
Ключ $K^3$	BB 3D D5 40 2E 99 9B 7A 3D EB B0 DB 45 44 8E C5 30 F0 73 65 DF EE 3A BA 84 15 F7 7A C8 F3 4C E8
Обработка 5-го блока:	
Счетчик $CTR_5$	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 04

Окончание таблицы А.2.3

Блок гаммы	FC 74 A0 10 F1 26 75 4B A7 30 82 CE 61 8A 98 4C
Блок открытого текста $P_5$	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
Блок шифртекста $C_5$	CF 30 F5 76 86 AE EC E1 1C FC 6C 31 6B 8A 89 6E
Обработка 6-го блока:	
Счетчик $CTR_6$	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 05
Блок гаммы	9B A8 61 9B 09 AF 9C FD C0 A1 C4 7E 34 32 34 0D
Блок открытого текста $P_6$	44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33
Блок шифртекста $C_6$	DF FD 07 EC 81 36 36 46 0C 4F 3B 74 34 23 16 3E

Т а б л и ц а А.2.4 — Обработка секции  $M_4$  в режиме CTR-АСРКМ для шифра «Кузнечик»

Секция $M_4$	55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33 44
Ключ $K^4$	23 36 2F D5 53 CA D2 17 82 99 A5 B5 A2 D4 72 2E 3B B8 3C 73 0A 8B F5 7C E2 DD 00 40 17 F8 C5 65
Обработка 7-го блока:	
Счетчик $CTR_7$	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 06
Блок гаммы	31 6F DE 4A 1B 50 73 18 87 2D 2B E7 EA F4 ED 19
Блок открытого текста $P_7$	55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33 44
Блок шифртекста $C_7$	64 09 A9 C2 82 FA C8 D4 69 D2 21 E7 FB D6 DE 5D

Результатом зашифрования открытого текста  $M$  в режиме CTR-АСРКМ в данном случае является строка  $C_1 \parallel C_2 \parallel \dots \parallel C_7$ :

F1 95 D8 BE C1 0E D1 DB D5 7B 5F A2 40 BD A1 B8  
85 EE E7 33 F6 A1 3E 5D F3 3C E4 B3 3C 45 DE E4  
4B CE EB 8F 64 6F 4C 55 00 17 06 27 5E 85 E8 00  
58 7C 4D F5 68 D0 94 39 3E 48 34 AF D0 80 50 46  
CF 30 F5 76 86 AE EC E1 1C FC 6C 31 6B 8A 89 6E  
DF FD 07 EC 81 36 36 46 0C 4F 3B 74 34 23 16 3E  
64 09 A9 C2 82 FA C8 D4 69 D2 21 E7 FB D6 DE 5D.

### А.3 Режим выработки имитовставки ОМАС-АСРКМ для шифра «Магма»

В настоящем разделе приведены тестовые примеры работы режима выработки имитовставки ОМАС-АСРКМ для шифра «Магма» со следующими входными данными:

длина блока  $n$  — 64 бита;  
длина блока гаммы  $s$  — 64 бита;  
размер секции  $N$  — 128 бит;  
частота смены ключа  $T^*$  — 640 бит;  
ключ  $K$ :

88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77  
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF.

#### А.3.1 Пример работы режима ОМАС-АСРКМ для шифра «Магма» с открытым текстом длины 1,5 блока

Открытый текст  $M$  длины 1,5 блока:

11 22 33 44 55 66 77 00 FF EE DD CC.

Сообщение  $M$  состоит из одной секции  $M_1$ , которую разбивают на блоки.

При формировании ключевого материала вырабатывается строка  $K^1 \parallel K_1^1 = \text{АСРКМ-Master}(K, T^*, 1)$ :

0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58  
A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A  
70 63 8E 3D E8 B3 57 1E.

Обработку данных производят в соответствии с таблицей А.3.1.1.

Т а б л и ц а А.3.1.1 — Обработка секции  $M_1$  в режиме ОМАС-АСРКМ для шифра «Магма»

Секция $M_1$	11 22 33 44 55 66 77 00 FF EE DD CC
Ключ $K^1$	0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58 A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A
Ключ $K_1^1$	70 63 8E 3D E8 B3 57 1E

Окончание таблицы А.3.1.1

Обработка 1-го блока:	
Блок открытого текста $P_1$	11 22 33 44 55 66 77 00
Входной блок $P_1 \oplus C_0$	11 22 33 44 55 66 77 00
Выходной блок $C_1$	A0 2B D0 1D 04 5A 9E 45
Обработка 2-го блока:	
Ключ $K'$	E0 C7 1C 7B D1 66 AE 3C
Блок открытого текста $P_2^*$	FF EE DD CC 80 00 00 00
Входной блок $P_2^* \oplus C_1 \oplus K'$	BF 02 11 AA 55 3C 30 79
Выходной блок $C_2$	A0 54 0E 37 30 AC BC F3

Результатом вычисления имитовставки сообщения  $M$  в режиме ОМАС-АСРКМ в данном случае является строка  $C_2$ :

A0 54 0E 37 30 AC BC F3.

### А.3.2 Пример работы режима ОМАС-АСРКМ для шифра «Магма» с открытым текстом длины 5 блоков

Открытый текст  $M$  длины 5 блоков:

11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88  
 00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A  
 11 22 33 44 55 66 77 88.

Сообщение  $M$  разбивают на три секции  $M_1$ ,  $M_2$ ,  $M_3$ , каждую из которых разбивают на блоки.

При формировании ключевого материала вырабатывается строка  $K^1 \parallel K_1^1 \parallel K^2 \parallel K_2^2 \parallel K^3 \parallel K_3^3 = \text{АСРКМ-}$

Master ( $K$ ,  $T^*$ , 3):

0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58  
 A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A  
 70 63 8E 3D E8 B3 57 1E 8D 38 26 D5 5E 63 A1 67  
 E2 40 66 40 54 7B 9F 1F 5F 2B 43 61 2A AE AF DA  
 18 0B AC 86 04 DF A6 FE 53 C2 CE 27 0E 9C 9F 52  
 68 D0 FD BF E1 A3 BD D9 BE 5B 96 D0 A1 20 23 48  
 6E F1 71 0F 92 4A E0 31 30 52 CB 5F CA 0B 79 1E  
 1B AB E8 57 6D 0F E3 A8.

Обработку данных производят в соответствии с таблицами А.3.2.1—А.3.2.3.

Т а б л и ц а А.3.2.1 — Обработка секции  $M_1$  в режиме ОМАС-АСРКМ для шифра «Магма»

Секция $M_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Ключ $K^1$	0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58 A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A
Обработка 1-го блока:	
Блок открытого текста $P_1$	11 22 33 44 55 66 77 00
Входной блок $P_1 \oplus C_0$	11 22 33 44 55 66 77 00
Выходной блок $C_1$	A0 2B D0 1D 04 5A 9E 45
Обработка 2-го блока:	
Блок открытого текста $P_2$	FF EE DD CC BB AA 99 88
Входной блок $P_2 \oplus C_1$	5F C5 0D D1 BF F0 07 CD
Выходной блок $C_2$	1D 61 FD 38 6F E5 8E 2F

Т а б л и ц а А.3.2.2 — Обработка секции  $M_2$  в режиме ОМАС-АСРКМ для шифра «Магма»

Секция $M_2$	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Ключ $K^2$	8D 38 26 D5 5E 63 A1 67 E2 40 66 40 54 7B 9F 1F 5F 2B 43 61 2A AE AF DA 18 0B AC 86 04 DF A6 FE

Окончание таблицы А.3.2.2

Обработка 3-го блока:	
Блок открытого текста $P_3$	00 11 22 33 44 55 66 77
Входной блок $P_3 \oplus C_2$	1D 70 DF 0B 2B B0 E8 58
Выходной блок $C_3$	E7 9A E5 A1 8F 11 24 6B
Обработка 4-го блока:	
Блок открытого текста $P_4$	88 99 AA BB CC EE FF 0A
Входной блок $P_4 \oplus C_3$	6F 03 4F 1A 43 FF DB 61
Выходной блок $C_4$	A3 1E 9B 72 1F 64 88 E8

Т а б л и ц а А.3.2.3 — Обработка секции  $M_3$  в режиме ОМАС-АСРКМ для шифра «Магма»

Секция $M_3$	11 22 33 44 55 66 77 88
Ключ $K^3$	68 D0 FD BF E1 A3 BD D9 BE 5B 96 D0 A1 20 23 48 6E F1 71 0F 92 4A E0 31 30 52 CB 5F CA 0B 79 1E
Ключ $K_1^3$	1B AB E8 57 6D 0F E3 A8
Обработка 5-го блока:	
Ключ $K'$	1B AB E8 57 6D 0F E3 A8
Блок открытого текста $P_5$	11 22 33 44 55 66 77 88
Входной блок $P_5^* \oplus C_4 \oplus K'$	A9 97 40 61 27 0D 1C C8
Выходной блок $C_5$	34 00 8D AD 54 96 BB 8E

Результатом вычисления имитовставки сообщения  $M$  в режиме ОМАС-АСРКМ в данном случае является строка  $C_5$ :

34 00 8D AD 54 96 BB 8E.

#### А.4 Режим выработки имитовставки ОМАС-АСРКМ для шифра «Кузнечик»

В настоящем разделе приведены тестовые примеры работы режима выработки имитовставки ОМАС-АСРКМ для шифра «Кузнечик» со следующими входными данными:

- длина блока  $n$  — 128 бит;
- длина блока гаммы  $s$  — 128 бит;
- размер секции  $N$  — 256 бит;
- частота смены ключа  $T^*$  — 768 бит;
- ключ  $K$ :

88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77  
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF.

##### А.4.1 Пример работы режима ОМАС-АСРКМ для шифра «Кузнечик» с открытым текстом длины 1,5 блока

Открытый текст  $M$  длины 1,5 блока:

11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88  
00 11 22 33 44 55 66 77.

Сообщение  $M$  состоит из одной секции  $M_1$ , которую разбивают на блоки.

При формировании ключевого материала вырабатывается строка  $K^1 \parallel K_1^1 = \text{АСРКМ-Master}(K, T^*, 1)$ :

0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2  
C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE  
0F 2E 26 17 E4 71 48 68 0F C3 E6 17 8D F2 C1 37.

Обработку данных производят в соответствии с таблицей А.4.1.1.

Т а б л и ц а А.4.1.1 — Обработка секции  $M_1$  в режиме ОМАС-АСРКМ для шифра «Кузнечик»

Секция $M_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Ключ $K_1$	0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2 C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE
Ключ $K_1^1$	0F 2E 26 17 E4 71 48 68 0F C3 E6 17 8D F2 C1 37



## Окончание таблицы А.4.1.1

Обработка 1-го блока:	
Блок открытого текста $P_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Входной блок $P_1 \oplus C_0$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Выходной блок $C_1$	DD 01 38 F4 86 C7 07 DA F7 F4 57 76 6D A4 78 B0
Обработка 2-го блока:	
Ключ $K'$	1E 5C 4C 2F C8 E2 90 D0 1F 87 CC 2F 1B E5 82 6E
Блок открытого текста $P_2^*$	00 11 22 33 44 55 66 77 80 00 00 00 00 00 00
Входной блок $P_2^* \oplus C_1 \oplus K'$	C3 4C 56 E8 0A 70 F1 7D 68 73 9B 59 76 41 FA DE
Выходной блок $C_2$	B5 36 7F 47 B6 2B 99 5E EB 2A 64 8C 58 43 14 5E

Результатом вычисления имитовставки сообщения  $M$  в режиме ОМАС-АСРКМ в данном случае является строка  $C_2$ :

B5 36 7F 47 B6 2B 99 5E EB 2A 64 8C 58 43 14 5E.

**А.4.2 Пример работы режима ОМАС-АСРКМ для шифра «Кузнечик» с открытым текстом длины 5 блоков**

Открытый текст  $M$  длины 5 блоков:

11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88  
 00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A  
 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00  
 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11  
 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22.

Сообщение  $M$  разбивают на три секции  $M_1$ ,  $M_2$ ,  $M_3$ , каждую из которых разбивают на блоки. При формировании ключевого материала вырабатывается строка  $K^1 \parallel K_1^1 \parallel K^2 \parallel K_1^2 \parallel K^3 \parallel K_1^3 = \text{АСРКМ-Master}(K, T^*, 3)$ :

0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2  
 C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE  
 0F 2E 26 17 E4 71 48 68 0F C3 E6 17 8D F2 C1 37  
 C9 DD A8 9C FF A4 91 FE AD D9 B3 EA B7 03 BB 31  
 BC 7E 92 7F 04 94 72 9F 51 B4 9D 3D F9 C9 46 08  
 00 FB BC F5 ED EE 61 0E A0 2F 01 09 3C 7B C7 42  
 D7 D6 27 15 01 B1 77 77 52 63 C2 A3 49 5A 83 18  
 A8 1C 79 A0 4F 29 66 0E A3 FD A8 74 C6 30 79 9E  
 14 2C 57 79 14 FE A9 0D 3B C2 50 2E 83 36 85 D9.

Обработку данных производят в соответствии с таблицами А.4.2.1—А.4.2.3.

Т а б л и ц а А.4.2.1 — Обработка секции  $M_1$  в режиме ОМАС-АСРКМ для шифра «Кузнечик»

Секция $M_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88 00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Ключ $K^1$	0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2 C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE
Обработка 1-го блока:	
Блок открытого текста $P_1$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Входной блок $P_1 \oplus C_0$	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Выходной блок $C_1$	DD 01 38 F4 86 C7 07 DA F7 F4 57 76 6D A4 78 B0
Обработка 2-го блока:	
Блок открытого текста $P_2$	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Входной блок $P_2 \oplus C_1$	DD 10 1A C7 C2 92 61 AD 7F 6D FD CD A1 4A 87 BA
Выходной блок $C_2$	9C 23 7F 18 85 F8 07 64 0B 32 5B 50 16 AB EC AF

Т а б л и ц а А.4.2.2 — Обработка секции  $M_2$  в режиме ОМАС-АСРКМ для шифра «Кузнечик»

Секция $M_2$	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Ключ $K^2$	C9 DD A8 9C FF A4 91 FE AD D9 B3 EA B7 03 BB 31 BC 7E 92 7F 04 94 72 9F 51 B4 9D 3D F9 C9 46 08

Окончание таблицы А.4.2.2

Обработка 3-го блока:	
Блок открытого текста $P_3$	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
Входной блок $P_3 \oplus C_2$	8D 01 4C 5C D0 9E 70 EC 92 98 E0 9C F8 54 E6 AF
Выходной блок $C_3$	2F 08 DE 89 F1 34 1B F9 1F 24 2F 88 94 E5 4E 6F
Обработка 4-го блока:	
Блок открытого текста $P_4$	22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Входной блок $P_4 \oplus C_3$	0D 3B 9A DC 97 43 93 60 B5 9F E3 66 6B EF 4E 7E
Выходной блок $C_4$	80 2C DF AC 40 FA 27 C2 FB 9B 2E 70 22 39 1D 84

Т а б л и ц а А.4.2.3 — Обработка секции  $M_3$  в режиме ОМАС-АСРКМ для шифра «Кузнечик»

Секция $M_3$	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
Ключ $K^3$	D7 D6 27 15 01 B1 77 77 52 63 C2 A3 49 5A 83 18 A8 1C 79 A0 4F 29 66 0E A3 FD A8 74 C6 30 79 9E
Ключ $K_1^3$	14 2C 57 79 14 FE A9 0D 3B C2 50 2E 83 36 85 D9
Обработка 5-го блока:	
Ключ $K'$	14 2C 57 79 14 FE A9 0D 3B C2 50 2E 83 36 85 D9
Блок открытого текста $P_5$	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
Входной блок $P_5^* \oplus C_4 \oplus K'$	A7 44 DD B3 23 8C 17 65 7B 95 90 A1 AB 0F 89 7F
Выходной блок $C_5$	FB B8 DC EE 45 BE A6 7C 35 F5 8C 57 00 89 8E 5D

Результатом вычисления имитовставки сообщения  $M$  в режиме ОМАС-АСРКМ в данном случае является строка  $C_5$ :

FB B8 DC EE 45 BE A6 7C 35 F5 8C 57 00 89 8E 5D.

## Приложение Б (справочное)

### Контрольные примеры работы алгоритмов экспорта KExp15 и импорта KImp15 ключа

В данном приложении представлены контрольные примеры работы алгоритмов экспорта и импорта ключей, приведенных в разделе 5, со следующими входными данными:

- ключ  $K$ :

88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77  
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF;

- ключ  $K_{MAC}^{Exp}$ :

08 09 0A 0B 0C 0D 0E 0F 00 01 02 03 04 05 06 07  
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F;

- ключ  $K_{ENC}^{Exp}$ :

20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F  
38 39 3A 3B 3C 3D 3E 3F 30 31 32 33 34 35 36 37.

#### Б.1 Алгоритмы экспорта KExp15 и импорта KImp15 ключа для шифра «Магма»

Вектор инициализации  $IV$ :

67 BE D6 54.

KEYMAC:

75 A7 66 18 E9 0F 49 73.

$KEXP = KExp15(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$ :

CF D5 A1 2D 5B 81 B6 E1 E9 9C 91 6D 07 90 0C 6A  
C1 27 03 FB 3A BD ED 55 56 7B F3 74 2C 89 9C 75  
5D AF E7 B4 2E 3A 8B D9.

#### Б.2 Алгоритмы экспорта KExp15 и импорта KImp15 ключа для шифра «Кузнечик»

Вектор инициализации  $IV$ :

09 09 47 2D D9 F2 6B E8.

KEYMAC:

10 02 2A DE 94 EE 55 B4 34 D2 07 7F 5A 13 AF F4.

$KEXP = KExp15(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$ :

E3 61 84 E8 4E 8D 73 6F F3 6C C2 E5 AE 06 5D C6  
56 B2 3C 20 F5 49 B0 2F DF F8 8E 1F 3F 30 D8 C2  
9A 53 F3 CA 55 4D BA D8 0D E1 52 B9 A4 62 5B 32.

Приложение В  
(рекомендуемое)

**Пример параметров режима шифрования CTR-АСРКМ**

В принятых в настоящее время в Российской Федерации принципах разработки средств криптографической защиты информации содержатся рекомендации по использованию дополнительных мер по защите криптографически опасной информации. Данные меры должны противостоять атакам, использующим каналы распространения информативных сигналов (см. приложение А Р 1323565.1.012—2017). К таким мерам относительно рассматриваемых в настоящих рекомендациях режимов работы блочных шифров могут быть отнесены, в частности, ограничение числа блоков, которые могут быть преобразованы на одном секретном ключе, и ограничение количества сообщений, обрабатываемых с использованием одного секретного ключа.

Перечисленные ограничения необходимо устанавливать в соответствии с определяемым в Р 1323565 классом средства криптографической защиты, с учетом используемых криптографических механизмов, условий эксплуатации и возможностей, которые могут быть использованы для проведения атак на средство защиты. При этом ограничения целесообразно устанавливать согласованным образом для каждого класса криптографических механизмов.

Кроме того, приводятся возможные значения параметров режима шифрования CTR-АСРКМ при его реализации в криптографических протоколах, в том числе и в протоколе безопасности транспортного уровня (TLS).

Для средств криптографической защиты информации классов КС1, КС2 и КС3 (см. раздел 4 Р 1323565.1.012—2017), а также средств, которые не подпадают под действие [1], допустимым является использование следующих ограничений:

- при использовании алгоритма блочного шифрования «Магма» объем преобразованной на одном секретном ключе информации не должен превышать 4 Мбайт (524 288 блоков);
- размер  $N$  одной секции режима CTR-АСРКМ полагается равным 1 Кбайт (128 блоков).

Из указанных ограничений следует, что число сообщений, которые могут быть обработаны на одном секретном ключе  $K$ , не должно превышать 4096. При этом длины сообщений дополнительно не ограничены.

Для средств криптографической защиты информации классов КВ и КА допустимым является использование следующих ограничений:

- при использовании алгоритма блочного шифрования «Кузнечик» объем обработанной на одном секретном ключе информации не должен превышать 256 Кбайт (16 384 блока);
- размер  $N$  одной секции режима CTR-АСРКМ полагается равным 4 Кбайт (256 блоков).

Из указанных ограничений следует, что число сообщений, которые могут быть преобразованы на одном секретном ключе  $K$ , не должно превышать 64. При этом длины сообщений дополнительно не ограничены.

**Библиография**

- [1] Приказ ФСБ России от 9 февраля 2005 г. № 66 (в редакции приказа ФСБ России от 12 апреля 2010 г. № 173) «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ — 2005)»

УДК 681.3.06:006.354

ОКС 35. 040

Ключевые слова: режимы, шифрование, имитовставка, ключ, экспорт ключа, импорт ключа

---

**БЗ 5—2018/31**

Редактор *Л.С. Зимилова*  
Технический редактор *И.Е. Черепкова*  
Корректор *И.А. Королева*  
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 28.04.2018. Подписано в печать 11.05.2018. Формат 60×84<sup>1</sup>/<sub>8</sub>. 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.  
[www.gostinfo.ru](http://www.gostinfo.ru) [info@gostinfo.ru](mailto:info@gostinfo.ru)