ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
**(РОССТАНДАРТ)**

**Технический комитет 026**

**«Криптографическая защита информации»**

**СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ**
**ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ**

**РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ**

# ЗАДАНИЕ УЗЛОВ ЗАМЕНЫ БЛОКА ПОДСТАНОВКИ АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89

*Утверждены решением заседания*
*технического комитета по стандартизации*
*«Криптографическая защита информации»*
*(Протокол №12 от 21.11.2013 г.)*

**Москва**
**2013**

**Содержание**

## 1. Введение

Стандарт **ГОСТ 28147-89** определяет алгоритм криптографического преобразования. Этот алгоритм криптографического преобразования предусматривает заполнение узлов замены К1, К2, К3, К4, К5, К6, К7, К8 блока подстановки. Каждый узел замены Ki реализует подстановку степени 16, которая также обозначается через Ki. Блок подстановки описывается таблицей подстановок К8, К7, К6, К5, К4, К3, К2, К1, определяющей действие блока подстановки на 32-мерном бинарном векторе с нумерацией битов справа налево.

Далее под термином «таблица подстановок» подразумевается представление блока подстановки в соответствии с порядком следования узлов замены, определённом в **ГОСТ 28147-89** на странице 3.

В настоящем документе определяются узлы замены блока подстановки стандарта **ГОСТ 28147-89**, рекомендуемые к использованию с января 2013 года.

Настоящими рекомендациями не отменяется использование иных узлов замены.

## 2. Область применения

В системах шифрования данных на базе стандарта алгоритма шифрования **ГОСТ 28147-89** в общедоступных и корпоративных сетях для защиты информации, не содержащей сведений, составляющих государственную тайну.

## 3. Нормативные ссылки

Указанные в этом разделе рекомендаций ссылочные документы являются обязательными для их применения. Для датированных ссылок используют только указанное здесь издание. Для недатированных ссылок - последнее и актуальное издание со всеми изменениями и дополнениями:

**ГОСТ 28147-89** — Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации, «Государственный стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования ГОСТ 28147-89», ГОСТ 28147-89, ИПК Издательство стандартов, 1996.

**ГОСТ Р ИСО/МЭК 8825-1:2002** — ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 8825-1:2002. Информационная технология. «Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования» (ISO/IEC 8825-1:2002, Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)), Москва, Стандартинформ, 2010.

### 3.1 Информативные ссылки

**ГОСТ 34.311-95** — Межгосударственный стандарт.Информационная технология. Криптографическая защита информации. «Функция хэширования» (Information technology. Cryptographic Data Security. Hashing function). 16 апреля 1998 введён в действие на территории Российской Федерации.

**PKCS #11** — «Стандарт криптографии с открытым ключом (версия 2.30)», разработан и опубликован RSA Laboratories (PKCS #11: CRYPTOGRAPHIC TOKEN INTERFACE STANDARD (v2.30). RSA Laboratories, 16 April 2009).

## 4. Объектный идентификатор таблицы подстановок

— id-tc26-gost-28147-param-Z, «1.2.643.7.1.2.5.1.1».

## 5. Рекомендуемая таблица подстановок алгоритма криптографического преобразования ГОСТ 28147-89

Технический комитет ТК26 рекомендует использовать таблицу подстановок алгоритма **ГОСТ 28147-89**. Представление таблицы подстановок алгоритма **ГОСТ 28147-89** соответствует представлению таблицы проверочных примеров **ГОСТ 34.311-95**.

Таблица подстановок

| x | K8(x) | K7(x) | K6(x) | K5(x) | K4(x) | K3(x) | K2(x) | K1(x) |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 8 | 5 | 7 | c | b | 6 | c |
| 1 | 7 | e | d | f | 8 | 3 | 8 | 4 |
| 2 | e | 2 | f | 5 | 2 | 5 | 2 | 6 |
| 3 | d | 5 | 6 | a | 1 | 8 | 3 | 2 |
| 4 | 0 | 6 | 9 | 8 | d | 2 | 9 | a |
| 5 | 5 | 9 | 2 | 1 | 4 | f | a | 5 |
| 6 | 8 | 1 | c | 6 | f | a | 5 | b |
| 7 | 3 | c | a | d | 6 | d | c | 9 |
| 8 | 4 | f | b | 0 | 7 | e | 1 | e |
| 9 | f | 4 | 7 | 9 | 0 | 1 | e | 8 |
| a | a | b | 8 | 3 | a | 7 | 4 | d |
| b | 6 | 0 | 1 | e | 5 | 4 | 7 | 7 |
| c | 9 | d | 4 | b | 3 | c | b | 0 |
| d | c | a | 3 | 4 | e | 9 | d | 3 |
| e | b | 3 | e | 2 | 9 | 6 | 0 | f |
| f | 2 | 7 | 0 | c | b | 0 | f | 1 |

## Приложение 1: Проверочные примеры шифрования

Проверочные примеры шифрования в режиме простой замены открытого текста длины 16 байт.

Все данные приведены в байтовом представлении, байты — в hex-формате. Порядок байтов в массиве слева направо.

Ключ:

```
81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 80
d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df d0
```

Открытый текст:

```
01 02 03 04 05 06 07 08 f1 f2 f3 f4 f5 f6 f7 f8
```

Шифртекст:

```
ce 5a 5e d7 e0 57 7a 5f d0 cc 85 ce 31 63 5b 8b
```

## Приложение 2: PKCS#11 представление узлов замены

В данном разделе приводятся представления таблиц подстановок в сжатом виде для их записи в ASN.1 DER — кодировке, согласно **ГОСТ Р ИСО/МЭК 8825-1:2002** (X.690).

```
id-tc26-gost-28147-param-Z

c6 bc 75 81 48 38 fd e7 62 52 5f 2e 23 81 a6 5d
a9 2d 89 60 5a f4 12 95 b5 af 6c 18 9c d6 da c3
e1 e7 0b f4 8e 10 97 4f d4 7a 38 ba 77 45 e1 06
0b c3 b4 d9 3d 9e 43 ac f0 69 2e 3b 1f 0b c0 72
```