

---

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ  
(МГС)

INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION  
(ISC)

---



МЕЖГОСУДАРСТВЕННЫЙ  
СТАНДАРТ

**ГОСТ**  
**34.13—**  
**2018**

---

**Информационная технология**  
**КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**  
**Режимы работы блочных шифров**

Издание официальное



Москва  
Стандартинформ  
2018

## Предисловие

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

### Сведения о стандарте

1 РАЗРАБОТАН Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

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

За принятие проголосовали:

| Краткое наименование страны по МК (ИСО 3166) 004—97 | Код страны по МК (ИСО 3166) 004—97 | Сокращенное наименование национального органа по стандартизации |
|-----------------------------------------------------|------------------------------------|-----------------------------------------------------------------|
| Армения                                             | AM                                 | Минэкономики Республики Армения                                 |
| Киргизия                                            | KG                                 | Кыргызстандарт                                                  |
| Россия                                              | RU                                 | Росстандарт                                                     |
| Таджикистан                                         | TJ                                 | Таджикстандарт                                                  |

4 Приказом Федерального агентства по техническому регулированию и метрологии от 4 декабря 2018 г. № 1062-ст межгосударственный стандарт ГОСТ 34.13—2018 введен в действие в качестве национального стандарта Российской Федерации с 1 июня 2019 г.

5 Настоящий стандарт подготовлен на основе применения ГОСТ Р 34.13—2015

6 ВЗАМЕН ГОСТ 28147—89 в части раздела 2 «Режим простой замены»; раздела 3 «Режим гаммирования»; раздела 4 «Режим гаммирования с обратной связью»; раздела 5 «Режим выработки имитовставки»

*Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет ([www.gost.ru](http://www.gost.ru))*

© Стандартиформ, оформление, 2018



В Российской Федерации настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

## Содержание

|                                                                  |    |
|------------------------------------------------------------------|----|
| 1 Область применения . . . . .                                   | 1  |
| 2 Термины, определения и обозначения . . . . .                   | 1  |
| 2.1 Термины и определения . . . . .                              | 1  |
| 2.2 Обозначения . . . . .                                        | 3  |
| 3 Общие положения . . . . .                                      | 3  |
| 4 Вспомогательные операции . . . . .                             | 4  |
| 4.1 Дополнение сообщения . . . . .                               | 4  |
| 4.2 Выработка начального значения . . . . .                      | 4  |
| 4.3 Процедура усечения . . . . .                                 | 5  |
| 5 Режимы работы алгоритмов блочного шифрования . . . . .         | 5  |
| 5.1 Режим простой замены . . . . .                               | 5  |
| 5.2 Режим гаммирования . . . . .                                 | 6  |
| 5.3 Режим гаммирования с обратной связью по выходу . . . . .     | 7  |
| 5.4 Режим простой замены с зацеплением . . . . .                 | 9  |
| 5.5 Режим гаммирования с обратной связью по шифртексту . . . . . | 11 |
| 5.6 Режим выработки имитовставки . . . . .                       | 13 |
| Приложение А (справочное) Контрольные примеры . . . . .          | 16 |
| Библиография . . . . .                                           | 22 |

## Введение

Настоящий стандарт содержит описание режимов работы блочных шифров. Данные режимы работы блочных шифров определяют правила криптографического преобразования данных и выработки имитовставки для сообщений произвольного размера.

Необходимость разработки настоящего стандарта вызвана потребностью в определении режимов работы блочных шифров, соответствующих современным требованиям к криптографической стойкости.

Настоящий стандарт терминологически и концептуально увязан с международными стандартами ИСО/МЭК 9797-1 [1], ИСО/МЭК 10116 [2], ИСО/МЭК 10118-1 [3], ИСО/МЭК 18033-1 [4], ИСО/МЭК 14888-1 [5].

Примечание — Основная часть стандарта дополнена приложением А «Контрольные примеры».