



МЕЖГОСУДАРСТВЕННЫЙ
СТАНДАРТ

ГОСТ
34.12—
2018

НИФТР и СТ КЫРГЫЗСТАНДАРТ
**РАБОЧИЙ
ЭКЗЕМПЛЯР**

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Зарегистрирован

№ 14417

3 декабря 2018 г.



Издание официальное
Кыргызстандарт
Бишкек

Предисловие

Евразийский совет по стандартизации, метрологии и сертификации (ЕАСС) представляет собой региональное объединение национальных органов по стандартизации государств, входящих в Содружество Независимых Государств. В дальнейшем возможно вступление в ЕАСС национальных органов по стандартизации других государств.

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

Сведения о стандарте

1 РАЗРАБОТАН Техническим комитетом по стандартизации Российской Федерации ТК 26 «Криптографическая защита информации», Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии Российской Федерации

3 ПРИНЯТ Евразийским советом по стандартизации, метрологии и сертификации (протоколом от 29 ноября 2018 г. №54-2018)

За принятие стандарта 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
Кыргызстан	KG	Кыргызстандарт
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт

4 Настоящий стандарт подготовлен на основе ГОСТ Р 34.12—2015

© Кыргызстандарт, 2026

5 Приказом Центра по стандартизации и метрологии при Министерстве экономики и коммерции Кыргызской Республики (Кыргызстандарт) от 23 апреля 2026 г. № 31-СТ межгосударственный стандарт ГОСТ 34.12—2018 введен в действие в качестве национального стандарта Кыргызской Республики

6 ВЗАМЕН ГОСТ 28147-89 в части раздела 1 «Структурная схема алгоритма криптографического преобразования»

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных (государственных) стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных (государственных) органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация также будет опубликована в сети Интернет на сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

Настоящий документ не может быть полностью или частично воспроизведен, копирован, тиражирован и распространен без разрешения Центра по стандартизации и метрологии при Министерстве экономики и коммерции Кыргызской Республики (Кыргызстандарт)

Содержание

1 Область применения	1
2 Термины, определения и обозначения	1
2.1 Термины и определения	1
2.2 Обозначения	2
3 Общие положения	3
4 Алгоритм блочного шифрования с длиной блока $n = 128$ бит	3
4.1 Значения параметров	3
4.2 Преобразования	4
4.3 Алгоритм развертывания ключа	4
4.4 Базовый алгоритм шифрования	4
5 Алгоритм блочного шифрования с длиной блока $n = 64$ бит	5
5.1 Значения параметров	5
5.2 Преобразования	5
5.3 Алгоритм развертывания ключа	5
5.4 Базовый алгоритм шифрования	6
Приложение А (справочное) Контрольные примеры	7
Библиография	12

Введение

Настоящий стандарт содержит описание алгоритмов блочного шифрования, которые применяются в криптографических методах защиты информации.

Необходимость разработки стандарта вызвана потребностью в создании блочных шифров с различными длинами блока, соответствующих современным требованиям к криптографической стойкости и эксплуатационным качествам.

Настоящий стандарт терминологически и концептуально увязан с международными стандартами ИСО/МЭК 10116 [1] и стандартами серии ИСО/МЭК 18033 [2], [3].

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