# ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»

## Дата введения

2019-06-01 (6-ого января 2019-ого года).

## Область применения

Настоящий стандарт распространяется на криптографическую защиту информации и определяет режимы работы блочных шифров.

## Назначение стандарта

Режимы работы блочных шифров, определенные в настоящем стандарте, рекомендуется использовать при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения.

## Перечень применяемых терминов и определений

* Шифр (cipher): Криптографический метод, используемый для обеспечения конфиденциальности данных, включающий алгоритм зашифрования и алгоритм расшифрования.
* Шифртекст (ciphertext): Данные, полученные в результате зашифрования открытого текста в целях скрытия его содержания.
* Зашифрование (encryption): Обратимое преобразование данных с помощью шифра, который формирует шифртекст из открытого текста.
* Расшифрование (decryption): Операция, обратная к зашифрованию.
* Блок (block): Строка бит определенной длины.
* Открытый текст (plaintext): Незашифрованная информация.
* Блочный шифр (block cipher): Шифр из класса симметричных криптографических методов, в котором алгоритм зашифрования применяется к блокам открытого текста для получения блоков шифртекста.

## Краткое (1-2 страницы) описание содержимого ГОСТа

**Режимы работы алгоритмов блочного шифрования**

*Режим простой замены*

Общие положения

Длина сообщений, зашифровываемых в режиме простой замены, должна быть кратна длине блока базового алгоритма блочного шифрования n, поэтому при необходимости к исходному сообщению должна быть предварительно применена процедура дополнения.

Зашифрование (расшифрование) в режиме простой замены заключается в зашифровании (расшифровании) каждого блока текста с помощью базового алгоритма блочного шифрования.

Зашифрование

Открытый и при необходимости дополненный текст  представляется в виде: 

Блоки шифртекста вычисляют по следующему правилу: 

Результирующий шифртекст имеет вид: 

Расшифрование

Шифртекст представляется в виде: 

Блоки открытого текста вычисляются по следующему правилу: 

Исходный (дополненный) открытый текст имеет вид: 

*Режим гаммирования*

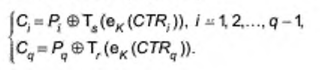
Общие положения

Параметром режима гаммирования является целочисленная величина s, 0 < s < n. При использовании режима гаммирования не требуется применение процедуры дополнения сообщения.

Для зашифрования (расшифрования) каждого отдельного открытого текста на одном ключе используется значение уникальной синхропосылки .

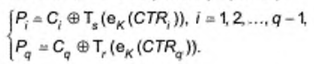
Зашифрование в режиме гаммирования заключается в покомпонентном сложении открытого текста с гаммой шифра, которая вырабатывается блоками длины s путем зашифрования последовательности значений счетчика  базовым алгоритмом блочного шифрования с последующим усечением. Начальным значением счетчика является  Последующие значения счетчика вырабатываются с помощью функции Add:  следующим образом: 

Зашифрование

Открытый текст  представляется в виде  Блоки шифртекста вычисляются по следующему правилу .

Результирующий шифртекст имеет вид: 

Расшифрование

Шифртекст представляется в виде:  Блоки открытого текста вычисляются по следующему правилу: .

Исходный открытый текст имеет вид: 

*Режим выработки имитовставки*

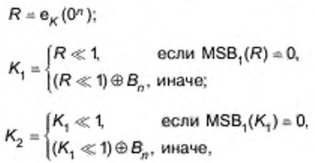
Общие положения

Режим выработки имитовставки. описание которого представлено ниже, реализует конструкцию ОМАС1 (стандартизован в ISO под названием СМАС).

Параметром режима является длина имитовставки (в битах) 0 < s <= n.

Выработка вспомогательных ключей

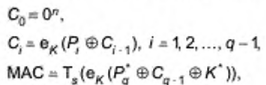
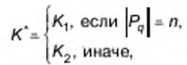
При вычислении значения имитовставки используются вспомогательные ключи, которые вычисляются с использованием ключа К. Длины вспомогательных ключей равны длине блока n базового алгоритма блочного шифрования.

Процедура выработки вспомогательных ключей может быть представлена в следующем виде: , где 

Вычисление значения имитовставки

Процедура вычисления значения имитовставки похожа на процедуру зашифрования в режиме простой замены с зацеплением при m = n и инициализации начального заполнения регистра сдвига значением 0^n: на вход алгоритму шифрования подается результат покомпонентного сложения очередного блока текста и результата зашифрования на предыдущем шаге. Основное отличие заключается в процедуре обработки последнего блока: на вход базовому алгоритму блочного шифрования подается результат покомпонентного сложения последнего блока, результата зашифрования на предыдущем шаге и одного из вспомогательных ключей. Конкретный вспомогательный ключ выбирается в зависимости от того, является ли последний блок исходного сообщения полным или нет. Значением имитовставки MAC является результат применения процедуры усечения к выходу алгоритма шифрования при обработке последнего блока.

Исходное сообщение  для которого требуется вычислить имитовставку. представляется в виде: , где 

Процедура вычисления имитовставки описывается следующим образом: , где .

 - последний блок сообщения, полученного в результате дополнения исходного сообщения.