ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.005— 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Допустимые объемы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13—2015

Издание официальное

Москва
Стандартинформ
2017

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ Центром защиты информации и специальной связи ФСБ России с участием ОАО «Информационные технологии и коммуникационные системы»

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 25 октября 2017 г. № 1518-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 (*gost.e-ecolog.ru

© Стандартинформ, 2017

Настоящие рекомендации не могут быть 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 Термины, определения и обозначения 1
4 Максимально допустимый объем материала 2

Введение

Средства защиты информации в ряде случаев реализуют криптографические протоколы, использующие национальные криптографические алгоритмы, определенные ГОСТ Р 34.12. В составе протокола данные алгоритмы функционируют в режимах, определенных ГОСТ Р 34.13. Одной из основных криптографических характеристик реализуемых режимов работы блочных шифров является величина, определяющая допустимое количество блоков открытого текста (объем материала), которые могут быть обработаны в данном режиме без изменения ключа блочного шифра.

Настоящие рекомендации определяют порядок расчета максимально допустимого количества блоков открытого текста, которые могут быть обработаны на одном ключе, для некоторых вариантов режимов работы, определенных ГОСТ Р 34.13, для блочных шифров, определенных ГОСТ Р 34.12.

Необходимость разработки настоящих рекомендаций вызвана потребностью в формировании единого подхода к оценке максимально допустимого количества блоков открытого текста, которые могут быть обработаны на одном ключе, для блочных шифров, реализуемых в системах обработки информации, в которых противник не располагает возможностью получения дополнительной информации о ключе.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Допустимые объемы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13—2015

Information technology. Information cryptographic protection. Permissible amounts of data processed under a single key for variants of block cipher modes of operation defined by GOST R 34.13—2015

Дата введения — 2018—04—01

1 Область применения

Настоящие рекомендации предназначены для оценки максимально допустимого количества блоков открытого текста, которые могут быть обработаны на одном ключе, для блочных шифров по ГОСТ Р 34.12 в режимах их работы по ГОСТ Р 34.13 при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения, в которых противник не располагает возможностью получения дополнительной информации о ключе.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 34.12 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов (рекомендаций) 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 стандарт (рекомендации), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (рекомендаций) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (рекомендации), на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта (рекомендаций) с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт (рекомендации), на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт (рекомендации) отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящих рекомендациях применены следующие термины с соответствующими определениями:

Издание официальное

3.1.1 **ключ:** Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

3.1.2 **блок:** Строка бит определенной длины.

3.1.3 **открытый текст:** Незашифрованная информация.

3.2 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

n — двоичная длина блока блочного шифра;

π_{enc} — максимально допустимое значение вероятности эффективного применения методов криптографического анализа

π_{mac} — максимально допустимое значение вероятности однократного навязывания сообщения;

N_{max} — максимально допустимое количество блоков (объем материала), которые могут быть обработаны с использованием выбранного режима работы алгоритмом блочного шифрования без изменения значения ключа;

s — параметр, определяющий двоичную длину блоков открытого текста, для режимов гаммирования, гаммирования с обратной связью по выходу, гаммирования с обратной связью по шифртексту и выработки имитовставки;

m — параметр, определяющий двоичную длину синхропосылки для режимов гаммирования с обратной связью по выходу, гаммирования с обратной связью по шифртексту и простой замены с зацеплением.

4 Максимально допустимый объем материала

Для некоторых вариантов режимов работы блочных шифров, определенных в ГОСТ Р 34.13, в таблице 1 приведены значения максимально допустимого количества блоков открытого текста (объем материала), которые могут быть обработаны на одном ключе, в зависимости от вероятностей эффективного применения методов криптографического анализа и однократного навязывания сообщения. Данные значения следует использовать при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения, в которых противник не располагает возможностью получения дополнительной информации о ключе.

Таблица 1

Название режима в соответствии с ГОСТ Р 34.13	Вариант реализации режима	Максимально допустимое количество блоков открытого текста
Простой замены		$N_{max} = 1$
Гаммирования	$s = n$	$N_{max} = 2^{\frac{n}{2}}\sqrt{\pi_{enc}}$
Гаммирования с обратной связью по выходу	$s = m = n$	$N_{max} = 2^{\frac{n-1}{2}}\sqrt{\pi_{enc}}$
Простой замены с зацеплением	$m = n$	$N_{max} = 2^{\frac{n-1}{2}}\sqrt{\pi_{enc}}$
Гаммирования с обратной связью по шифртексту	$s = m = n$	$N_{max} = \sqrt{\frac{2}{3}}2^{\frac{n}{2}}\sqrt{\pi_{enc}}$
Выработки имитовставки	$s = n$	$N_{max} = \frac{2^{\frac{n}{2}-1}}{n}\sqrt{\pi_{mac} - \frac{1}{2^n}}$

УДК 681.3.06:006.354 ОКС 35. 040

Ключевые слова: информационная технология, криптографическая защита информации, метод расчета, допустимое количество блоков, ключ, режим работы блочных шифров

БЗ 12—2017/53

Редактор *В.Н. Шмельков*
Технический редактор *В.Н. Прусакова*
Корректор *М.С. Кабашова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 27.10.2017. Подписано в печать 17.11.2017. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 0,93. Уч.-изд. л. 0,84. Тираж 21 экз. Зак. 2202.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru