Технический комитет по стандартизации
«Криптографическая защита информации»
(ТК 26)

ПРОЕКТ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ

ДОПУСТИМЫЕ ОБЪЁМЫ МАТЕРИАЛА ДЛЯ ОБРАБОТКИ НА ОДНОМ КЛЮЧЕ ПРИ ИСПОЛЬЗОВАНИИ НЕКОТОРЫХ ВАРИАНТОВ РЕЖИМОВ РАБОТЫ БЛОЧНЫХ ШИФРОВ В СООТВЕТСТВИИ С ГОСТ Р 34.13-2015

Москва
2016

Содержание

Введение

В рамках данного документа приводятся рекомендации по использованию ключей алгоритмов блочного шифрования (значения допустимого объёма материала, который может быть обработан на одном ключе) при обработке информации с использованием некоторых вариантов режимов работы алгоритмов блочного шифрования в соответствии с ГОСТ Р 34.13-2015.

Ранее в ТК 26 подобные рекомендации не разрабатывались. Они представляют несомненный интерес с точки зрения обеспечения специальных свойств режимов работы алгоритмов блочного шифрования при реализации их в различных системах обработки информации.

На основе данных методических рекомендаций могут быть созданы документы, регламентирующие использование алгоритмов блочного шифрования и режимов их работы, также они могут быть учтены при исследовании вопросов реализации указанных механизмов в криптографических протоколах и интерфейсах.

Методические рекомендации подготовлены специалистами в/ч 43753.

Примечание – Представленные в настоящих рекомендациях оценки основаны на существенных предположениях относительно свойств используемых алгоритмов блочного шифрования. В частности, ими не следует руководствоваться при проведении исследований или подготовке рекомендаций по использованию криптографических протоколов и интерфейсов, реализуемых в системах обработки информации, в которых существенное влияние на возможности противника может оказать дополнительная информация, полученная из побочных каналов утечки.

Примечание – Представленные в настоящих рекомендациях оценки справедливы только для частных случаев режимов работы, определяемых стандартом ГОСТ Р 34.13-2015. Применение данных оценок к указанным режимам в общем виде требует проведения дополнительных исследований.

Примечание – Представленные в настоящих рекомендациях оценки следует рассматривать как отправную точку для проведения дальнейших исследований конкретных реализаций. Они определяют максимальный допустимый объём материала и не предписывают обрабатывать информацию исключительно указанными объёмами.

Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

Примечание – При использовании настоящих методических рекомендаций целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства Российской Федерации по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который

опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Описание решаемых криптографических задач

Использование предлагаемых в данном документе значений позволяет определить допустимый объём материала, который может быть обработан на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015.

Описание предлагаемого решения

Введение

Исследованиям различных свойств режимов работы алгоритмов блочного шифрования посвящено большое число публикаций в отечественной и зарубежной научной периодике. Дальнейшее изложение преимущественно опирается на результаты, приведённые в работах [1] и [2], в данных работах, в том числе, приведены библиографические ссылки на используемые материалы.

Широко распространён подход, рассматривающий решение задачи оценки стойкости конкретного алгоритма блочного шифрования в конкретном режиме работы. Результаты подобных исследований часто весьма ограничены в применимости, поскольку их справедливость для алгоритма блочного шифрования, отличного от того, для которого были осуществлены исследования, даже используемого в том же самом режиме работы, может быть поставлена под сомнение. Другим вариантом решения данной задачи является использование метода редукции. Данный метод позволяет связать некоторые свойства исследуемых режимов с некоторыми свойствами используемого алгоритма блочного шифрования. Таким образом, результаты о стойкости остаются справедливыми в случае использования любого алгоритма блочно-

го шифрования с аналогичными свойствами.

Основной криптографической характеристикой какого-либо режима работы алгоритма блочного шифрования является величина, определяющая максимальный объем материала, который может быть обработан с помощью данного режима на одном ключе. Значение допустимого объема обрабатываемой информации может быть получено различными способами. В работе [1] рассматривается подход, заключающийся в выявлении и обосновании связей некоторых свойств исследуемых режимов с некоторыми свойствами используемого алгоритма блочного шифрования. В работе [2] рассматривается комбинаторно-алгоритмический подход, заключающийся в построении конкретных методов получения дополнительной информации о неизвестной части открытого текста по известному шифртексту и некоторой части соответствующих известных открытых текстов.

Максимально допустимый объем материала, который можно обрабатывать на одном ключе, будет измеряться в блоках открытого текста.

Определения и обозначения

n	длина блока алгоритма блочного шифрования;
π_{enc}	максимально допустимое значение вероятности эффективного применения методов криптографического анализа;
π_{mac}	максимально допустимое значение вероятности однократного навязывания сообщения;
$N_{\max}$	максимально допустимое число блоков, которые могут быть обработаны с использованием выбранного режима работы алгоритмом блочного шифрования на одном ключе.

П р и м е ч а н и е – Значение π_{enc} имеет иной смысл в работе [1], вместе с тем, существование эффективных методов криптографического анализа, применимых с высокой вероятностью успеха, может быть использовано при решении описанных, в том числе, в [1] задач.

П р и м е ч а н и е – Значение π_{enc} (π_{mac}) целесообразно выбирать исходя из действующих нормативных документов и технического задания на разработку криптосистемы.

Объём материала, который может быть обработан на одном ключе

С использованием результатов работ [1] и [2] для некоторых вариантов режимов, описанных в стандарте ГОСТ Р 34.13-2015 и обеспечивающих конфиденциальность, приведём зависимость между значением $N_{\max}$ и значением π_{enc}. С использованием результатов работы [1], для режима выработки имитовставки, описанного в стандарте ГОСТ Р 34.13-2015, приведём зависимость между значением $N_{\max}$ и значением π_{mac}.

Режим	**Параметры режима**	**Оценка объема материала**
простой замены		$N_{\max} = 1$
гаммирования с обратной связью по выходу	$s = m = n$	$N_{\max} = 2^{\frac{n-1}{2}}\sqrt{\pi_{\text{enc}}}$
простой замены с зацеплением	$m = n$	$N_{\max} = 2^{\frac{n-1}{2}}\sqrt{\pi_{\text{enc}}}$
гаммирования с обратной связью по шифртексту	$s = m = n$	$N_{\max} = \sqrt{\frac{2}{3}}2^{\frac{n}{2}}\sqrt{\pi_{\text{enc}}}$
гаммирования	$s = n$	$N_{\max} = 2^{\frac{n}{2}}\sqrt{\pi_{\text{enc}}}$
выработки имитовставки	$s = n$	$N_{\max} = \frac{2^{\frac{n}{2}-1}}{n}\sqrt{\pi_{\text{mac}} - \frac{1}{2^n}}$

Заключительные положения

В данном документе приведены границы на объём материала, который может быть обработан с использованием одного ключа, для некоторых вариантов режимов, описанных в стандарте ГОСТ Р 34.13-2015. Данные значения могут быть использованы при реализации и описании специальных качеств в том числе алгоритмов из стандарта ГОСТ Р 34.12-2015 в каких либо режимах из стандарта ГОСТ Р 34.13-2015. Значения приведены на основе результатов работ [1] и [2].

Список литературы

[1] Лавриков И.В. Некоторые теоретико-информационные свойства режимов работы блочных шифров. – *Представлено в редакцию журнала «Математические вопросы криптографии»*, 2015.

[2] Шишкин В.А. Некоторые свойства режимов работы блочных шифров. – *Представлено в редакцию журнала «Математические вопросы криптографии»*, 2015.