ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.006— 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Механизмы выработки псевдослучайных последовательностей

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 31 октября 2017 г. № 1608-ст

3 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 Описание механизмов 2

Введение

Криптографические протоколы, реализуемые средствами защиты информации, используют в процессе функционирования псевдослучайные числа и их последовательности, необходимые для выполнения своих целевых функций. Одним из методов формирования данных чисел является выработка псевдослучайных последовательностей с использованием криптографических механизмов.

Настоящие рекомендации определяют криптографические механизмы выработки псевдослучайных последовательностей чисел с использованием функций хэширования, в том числе определенных ГОСТ Р 34.11—2012.

Необходимость разработки настоящих рекомендаций вызвана потребностью в формировании единого подхода реализации к используемым в разрабатываемых и модернизируемых средствах защиты информации механизмам выработки псевдослучайных последовательностей с использованием функций хэширования, в том числе определенных ГОСТ Р 34.11—2012.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Механизмы выработки псевдослучайных последовательностей

Information technology. Cryptographic security of data. Pseudorandom number generation mechanisms

Дата введения — 2018—04—01

1 Область применения

Настоящие рекомендации определяют механизмы выработки псевдослучайных последовательностей с использованием функций хэширования, в том числе, определенных ГОСТ Р 34.11, и могут быть использованы при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения.

2 Нормативные ссылки

В настоящих рекомендациях использована нормативная ссылка на следующий стандарт:

ГОСТ Р 34.11 Информационная технология. Криптографическая защита информации. Функция хэширования

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 применен следующий термин с соответствующим определением:

3.1.1 **внутреннее состояние:** Значение, которое используется при выработке псевдослучайных последовательностей.

Издание официальное

3.2 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

V^* — множество всех двоичных строк конечной длины, включая пустую строку;

V_s — множество всех двоичных строк длины s, где s — целое неотрицательное число; нумерация подстрок и компонент строки осуществляется справа налево начиная с нуля;

$|A|$ — число компонент (длина) строки $A \in V^*$ (если A — пустая строка, то $|A| = 0$);

θ — пустая строка (строка длины 0);

$A||B$ — конкатенация строк A, $B \in V^*$, т. е. строка из $V_{|A|+|B|}$, в которой подстрока с большими номерами компонент из $V_{|A|}$ совпадает со строкой A, а подстрока с меньшими номерами компонент из $V_{|B|}$ совпадает со строкой B;

A^l — конкатенация l экземпляров строки A;

$LSB_s: V^* | \bigcup_{i=0}^{s-1} V_i \to V_s$ — отображение, ставящее в соответствие строке $z_{r-1} || \ldots ||z_1||z_0$, $r \geq s$ строку $z_{s-1} || \ldots ||z_1||z_0$, $z_i \in V_1$, $i = 0,1,\ldots, r-1$.

K — начальное заполнение;

s — двоичная длина начального заполнения;

$H: V^* \to V_s$ — отображение, реализующее применение функции хэширования;

m — параметр функции хэширования, называемый длиной блока;

h — параметр функции хэширования, называемый длиной хэш-кода;

U — внутренне состояние механизма выработки псевдослучайной последовательности;

t — двоичная длина вырабатываемой псевдослучайной последовательности;

R — вырабатываемая псевдослучайная последовательность.

4 Описание механизмов

В описываемых механизмах выработки псевдослучайных последовательностей предполагается использование функции хэширования с длинной блока $m \geq 512$ и длиной хэш-кода h.

Пусть необходимо осуществить выработку псевдослучайной последовательности R длины t. Представим значение t в виде $t = q \cdot h + r$, где $q, r \in Z$ и $0 \leq r < h$.

Выработка псевдослучайной последовательности осуществляется на основе следующей последовательности действий:

1) Присвоить начальное значение $R = \theta$;

2) Сформировать начальное заполнение $K \in V_s$, где $256 \leq s \leq m - 128$;

3) Положить $U_0 = (K||0^l)$, где $l = m - s - 8$;

4) Проверить условие $q = 0$. При положительном исходе перейти на шаг 5. В противном случае для $i = 1, 2,\ldots, q$ выполнять следующую последовательность действий:

- Вычислить $U_i = U_{i-1} + 1 \ (mod\, 2^{m-8})$;
- Положить $C_i = H(U_i)$;
- Положить $R = C_i||R$;

5) Проверить условие $r = 0$. При положительном исходе перейти на шаг 6. В противном случае выполнить следующую последовательность действий:

- Вычислить $U_{q+1} = U_q + 1 \ (mod\, 2^{m-8})$;
- Положить $C_{q+1} = H(U_{q+1})$;
- Положить $R = LSB_r(C_{q+1})||R$;

6) Выход: R.

Криптографические свойства данных механизмов выработки псевдослучайных последовательностей могут существенным образом зависеть от:

1) Свойств используемой функции хэширования.

2) Принципов формирования и криптографических качеств начального заполнения.

3) Длин последовательностей, которые вырабатываются с использованием одного значения начального заполнения.

При реализации данных механизмов выработки псевдослучайных последовательностей должны быть одновременно выполнены следующие два условия:

1) Формирование начального заполнения K должно осуществляться с использованием датчика случайных чисел с обоснованными криптографическими свойствами.

2) Используемые значения внутренних состояний $U_0,\ldots, U_{q+1}$ и начальное заполнение K должны сохраняться в секрете.

Для функций хэширования, определенных ГОСТ Р 34.11, параметры описанных механизмов принимают следующие возможные значения $m = 512$, $h \in \{256, 512\}$, при этом длину начального заполнения целесообразно выбирать исходя из условия $s \in \{256, 320, 384\}$.

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, псевдослучайная последовательность, функция хэширования

БЗ 11—2017/209

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

Сдано в набор 07.11.2017. Подписано в печать 23.11.2017. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 0,93. Уч.-изд. л. 0,81. Тираж 20 экз. Зак. 2377.
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