

РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ

Банковские технологии
**ПРОЦЕДУРА ВЫРАБОТКИ ПСЕВДОСЛУЧАЙНЫХ ДАННЫХ
С ИСПОЛЬЗОВАНИЕМ СЕКРЕТНОГО ПАРАМЕТРА**

Банкаўскія тэхналогіі
**ПРАЦЭДУРА ВЫПРАЦОЎКІ ПСЕЎДАВЫПАДКОВЫХ ДАДЗЕННЫХ
З ВЫКАРЫСТАННЕМ САКРЭТНАГА ПАРАМЕТРА**

Издание официальное

УДК

Ключевые слова: псевдослучайные данные, процедура выработки псевдослучайных данных

ОКС 35.240.40

Предисловие

1. РАЗРАБОТАН Государственным центром безопасности информации, Учреждением Белорусского государственного университета «Национальный научно-исследовательский центр прикладных проблем математики и информатики»

2. ВНЕСЕН Управлением безопасности и защиты информации Национального банка Республики Беларусь

3. УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Совета директоров Национального банка Республики Беларусь от 3 марта 2003 г. № 76

4. ВВЕДЕН ВПЕРВЫЕ

Настоящий руководящий документ не может быть тиражирован и распространен без разрешения Национального банка Республики Беларусь

Издан на русском языке

Содержание

1. Область применения	1
2. Нормативные ссылки	1
3. Обозначения.....	1
4. Общие положения	2
5. Процедура выработки псевдослучайных данных.....	2
5.1 Исходные данные.....	2
5.2 Используемые переменные	2
5.3 Алгоритм выработки псевдослучайных данных	3

РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ

Банковские технологии
**ПРОЦЕДУРА ВЫРАБОТКИ ПСЕВДОСЛУЧАЙНЫХ ДАННЫХ
 С ИСПОЛЬЗОВАНИЕМ СЕКРЕТНОГО ПАРАМЕТРА**

Банкаўскія тэхналогіі
**ПРАЦЭДУРА ВЫПРАЦОЎКІ ПСЕЎДАВЫПАДКОВЫХ ДАДЗЕННЫХ
 З ВЫКАРЫСТАННЕМ САКРЭТНАГА ПАРАМЕТРА**

Дата введения 2003-04-01

1. Область применения

Настоящий руководящий документ устанавливает процедуру и алгоритм выработки псевдослучайных данных с секретным параметром, которые применяются в криптографических методах защиты информации, в том числе для реализации процедуры выработки электронной цифровой подписи.

Настоящий руководящий документ применяется при разработке и сертификации средств криптографической защиты информации.

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на стандарт:
 СТБ 1176.1-99 Информационная технология. Защита информации.
 Функция хэширования.

3. Обозначения

В настоящем руководящем документе применяют следующие обозначения:

$Z(n)$ — множество всех неотрицательных целых чисел, меньших 2^n ,
 где n — натуральное число;

h^* — функция хэширования. Значения h^* вычисляются в соответствии с алгоритмом, установленным в СТБ 1176.1, в котором на шаге 15 вместо проверки $d = n + 2$ используется проверка $d = n + 1$, а значения параметров выбираются следующим образом:

$H = 4E4E9C9C 9C9C4E4E 9C9C4E4E 4E4E9C9C 9C9C4E4E 4E4E9C9C 4E4E9C9C 9C9C4E4E$

(в шестнадцатеричной системе счисления), $L = 256$;

$h^*(m_1, m_2, \dots, m_{128})$ — значение функции хэширования h^* , вычисленное от последовательности чисел m_1, m_2, \dots, m_{128} ,

где $m_i \in Z(8)$ для $i=1, 2, \dots, 128$;

\oplus — бинарная операция, определенная на множестве неотрицательных целых чисел по формуле

$$a \oplus b = \sum_{i=0}^{k-1} ((a_i + b_i) \bmod 2) \cdot 2^i, \quad (1)$$

где $a = \sum_{i=0}^{k-1} a_i 2^i$, $b = \sum_{i=0}^{k-1} b_i 2^i$, $a_0, \dots, a_{k-1}, b_0, \dots, b_{k-1} \in Z(1)$;

$c := d$ — присвоение параметру (переменной) c значения d .

4. Общие положения

Настоящий документ определяет процедуру выработки псевдослучайных данных в виде последовательности $z_1, z_2, \dots, z_T \in Z(256)$ с использованием секретного параметра из множества $Z(256)$. В алгоритме выработки псевдослучайных данных используется функция хэширования h^* .

5. Процедура выработки псевдослучайных данных

5.1 Исходные данные

Исходными данными для процедуры выработки последовательности псевдослучайных данных z_1, z_2, \dots, z_T являются:

T — натуральное число, определяющее длину последовательности данных, которую необходимо выработать;

K — $K \in Z(256)$, секретный параметр, который должен храниться в тайне;

C_0 — $C_0 \in Z(256)$, инициализирующее значение. При заданном K должны использоваться различные C_0 .

Допускается использование дополнительных входных данных, полученных произвольным образом, в том числе случайным или псевдослучайным методом.

5.2 Используемые переменные

В процедуре выработки псевдослучайных данных используются следующие переменные:

C — $C \in Z(256)$, $C = \sum_{i=0}^{31} c_i \cdot (2^8)^i$, где $c_i \in Z(8)$ для $i=0,1, \dots,31$;

Y — $Y \in Z(256)$. Если $T > 1$, то значение переменной Y должно быть уничтожено сразу после выработки псевдослучайных данных Z ;

X — $X \in Z(256)$;

t — натуральное число, $t \leq T + 1$;

M — $M \in Z(1024)$, $M = \sum_{i=1}^{128} m_i \cdot (2^8)^{i-1}$, где $m_i \in Z(8)$ для $i=1,2, \dots,128$.

5.3 Алгоритм выработки псевдослучайных данных

Алгоритм выработки последовательности данных z_1, z_2, \dots, z_T включает в себя следующие шаги:

1 $C := C_0$;

2 $Y := \sum_{i=0}^{31} (255 - c_i) \cdot (2^8)^i$;

3 $t := 1$;

4 Задать значение X на основании дополнительных входных данных.

Если дополнительные входные данные не используются, то установить $X := 0$;

5 $M := K + C \cdot 2^{256} + X \cdot 2^{512} + Y \cdot 2^{768}$;

6 $z_t := h^*(m_1, m_2, \dots, m_{128})$;

7 $t := t + 1$;

8 Если $t > T$, то перейти к шагу 12;

9 $C := (C + 1) \bmod 2^{256}$;

10 $Y := Y \oplus z_t$;

11 Перейти к шагу 4;

12 Конец работы алгоритма.