Стрибог

Исследование статистических свойств выходных последовательностей функции сжатия алгоритма *Стрибог*

Любушкина И.Е.
Главный специалист, к. т. н.

Панасенко С. П.
Заместитель генерального директора по науке и системной интеграции
к. т. н., Microsoft Certified Professional

ООО Фирма «АНКАД»

Международные исследования алгоритма Стрибог

1. R. AlTawy *et al:*
- Технология rebound-атаки;
- Коллизии для внутреннего блочного шифра, усеченного до 7,75 раунда;
- Коллизии для функции сжатия алгоритма Стрибог, усеченной до 9,5 раунда включительно.

2. Z. Wang *et al:*
- Технология rebound-атак, усиленная за счет использования Super-Sbox-методики;
- Коллизии для функции сжатия алгоритма Стрибог, усеченной до 9,5 раунда включительно;
- Различитель для функции сжатия, усеченной до 10 раундов;
- Метод построения мультиколлизий (*k*-коллизий) для полнораундовой функции сжатия с трудоемкостью, существенно меньшей трудоемкости нахождения *k*-коллизий для «идеальной» функции.

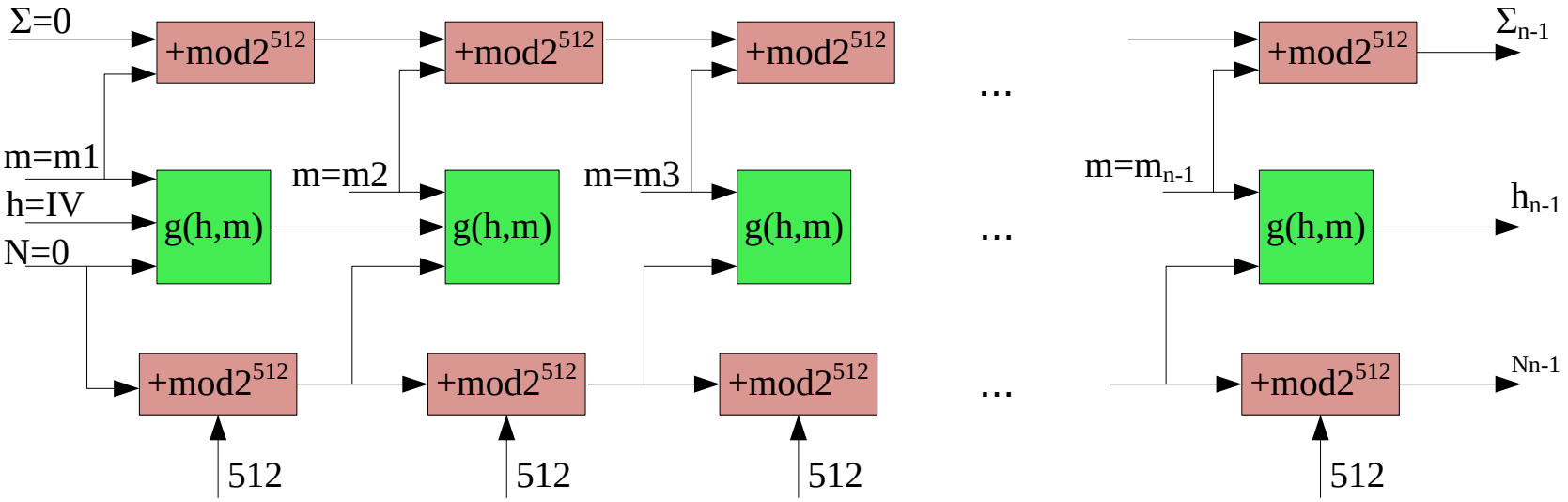
Международные исследования алгоритма Стрибог (Продолжение)

3. R. AlTawy и A. M. Youssef:
- Технология интегрального криптоанализа;
- Различитель для внутреннего блочного шифра, усеченного до 7,5 раунда включительно;
- Различитель для функции сжатия алгоритма, усеченной до 7 раундов включительно.

4. J. Guo *et al.*:
- Технология исследования хэш-функций, построенных по схеме HAIFA;
- Пример атак с нахождением вторичных прообразов за 2^{266} вызова функции вычисления хэш-значения длиной 512 бит для длинных сообщений по сравнению с 2^{512} вызовами «идеальной» хэш-функции.

Структура алгоритма Стрибог

- ✓ $M = (m_1 \| m_2 \| m_3 \| \ldots \| m_n)$ – входное сообщение M представляется как массив элементов по 512 бит;
- ✓ N - счетчик длины сообщения;
- ✓ Σ - промежуточная сумма;
- ✓ h - промежуточное значение хэш-функции.



Функция сжатия Стрибог

Функция сжатия построена по схеме Миягучи-Пренила:

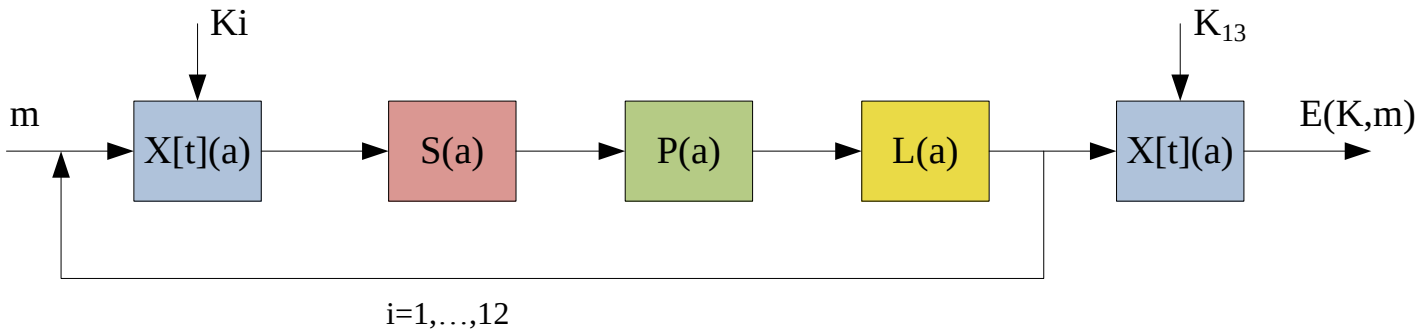
$$g_N(h, m) = E(K, m) \oplus h \oplus m$$

Шифр $E(K, m)$ является 12-раундовым AES-подобным алгоритмом:

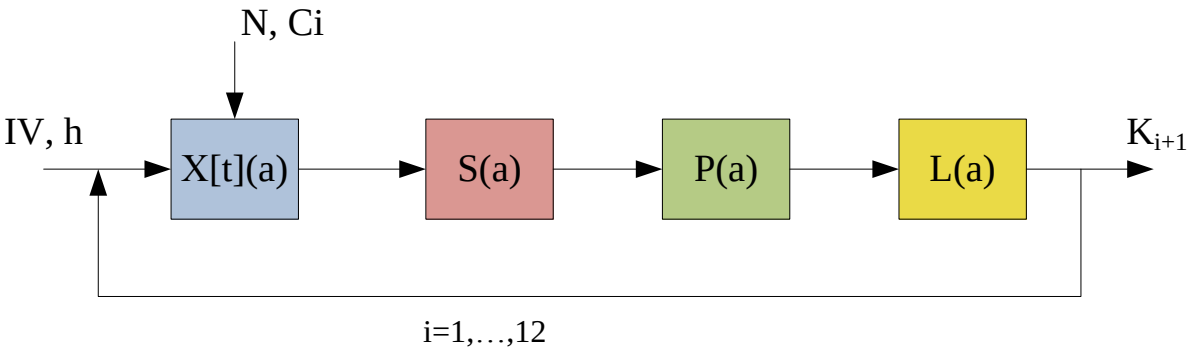
- K – псевдоключ;
- m – часть обрабатываемого сообщения длиной 512 бит.

На каждой итерации шифра используется обновленный псевдоключ K_i, где $i = 1,\ldots,12$.

Функция сжатия Стрибог



Блочный шифр E(K,M)



Функция преобразования псевдоключа

Функция сжатия Стрибог

Операции блочного шифра E:

- ✓ $X[t](a)$ – суммирование по модулю 2: $t \oplus a$;
- ✓ $S(a)$ – побайтовое замещение символов из таблицы замен;
- ✓ $P(a)$ – перестановка байтов в соответствии с вектором τ;
- ✓ $L(a)$ – умножение на матрицу A в поле GF(2).

Псевдоключ $K = K_1$ вычисляется по формуле $K = h \oplus N$. Далее значение ключа на каждом раунде складывается с константой C_i, где $i = 1,\ldots,12$.

Цель исследования статистических свойств выходной последовательности

Гипотеза: операции блочного шифра (XSPL) построены правильно и обеспечивают монотонность выходной последовательности.

Цель: поиск семейства «плохих» входных значений *m*, приводящих к вырождению рандомизирующих свойств функции сжатия.

Входные данные: последовательность *m* 512 бит, разбитая на блоки по 64 бита

$$m = (m_0 \| m_1 \| m_2 \| \ldots \| m_7)$$

Проводился полный перебор значений одного блока m_i (2^{64}). Значения остальных блоков были зафиксированы. Для каждого значения m_i вычислялось значение

$$g_0(IV, m_i)$$

Выходные данные: Преобразованное значение m_i. Выходная последовательность проверялась на соответствие критерию случайности.

Статистическое исследование: Покер-тест

$$X = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k,$$

где n – длина тестируемой последовательности, а m и k – это целые положительные числа, определяемые следующим соотношением:

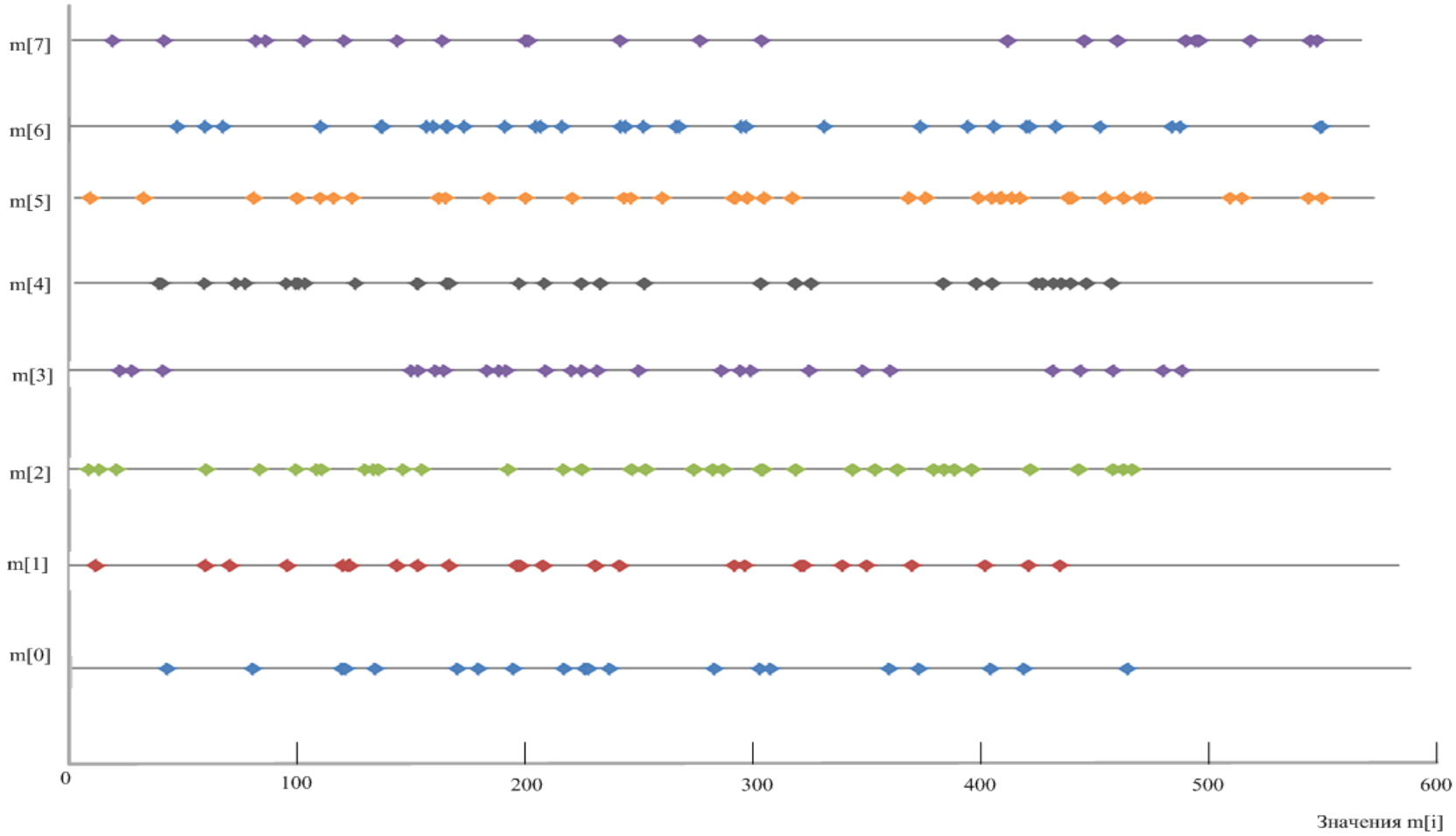
$$\left\lfloor \frac{n}{m} \right\rfloor \geq 5 * (2^m);$$

$$k = \left\lfloor \frac{n}{m} \right\rfloor.$$

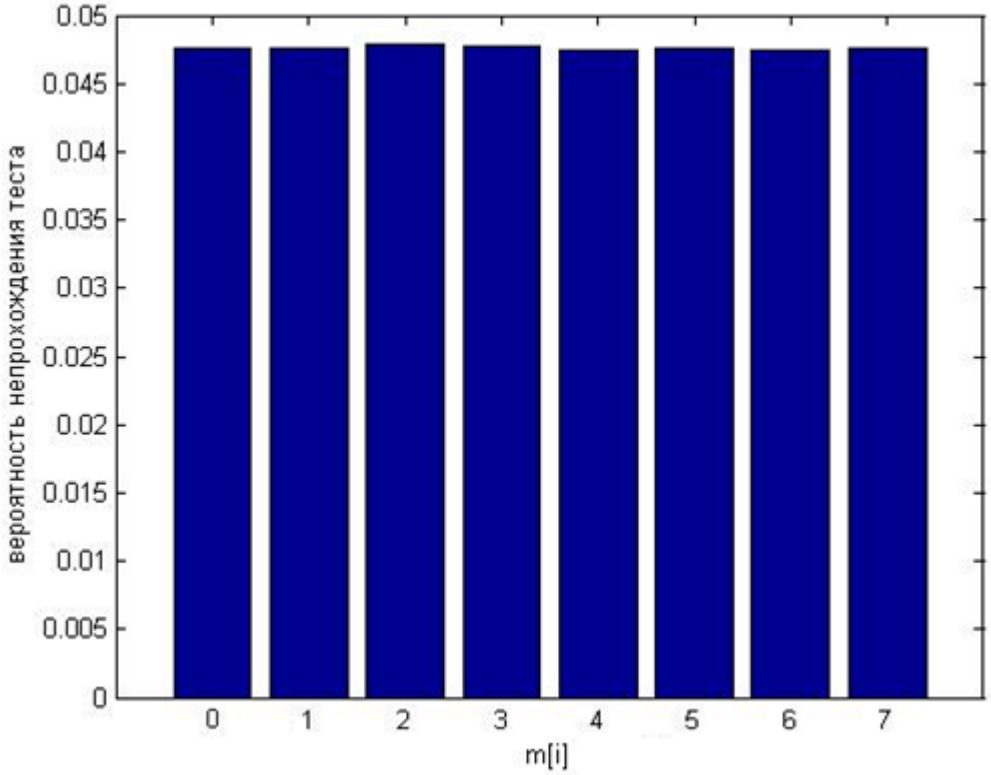
Для последовательности из 512 бит, подпоследовательностей длиной 4 бита и уровнем значимости 0,05 % для χ^2 с 2^4-1 = 15 степенями свободы

$$\sum n_i^2 \leq (25 + \left\lfloor \frac{512}{4} \right\rfloor) * \frac{128}{16} = 1224$$

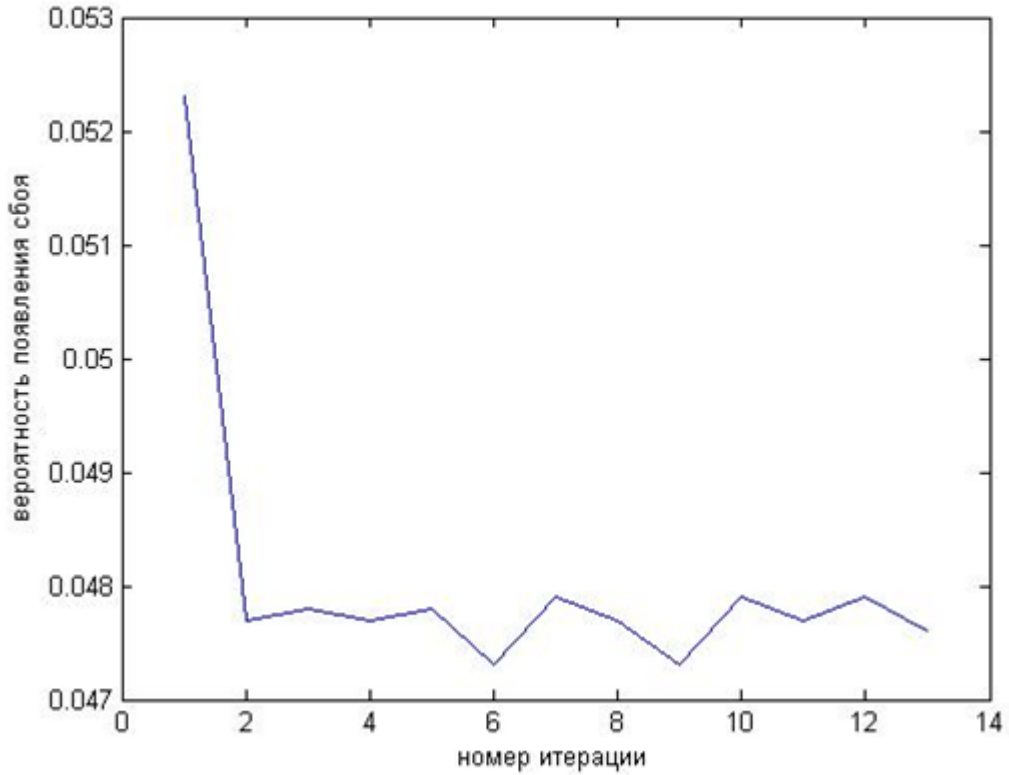
Распределение сбоев по шкале мощности m[i]



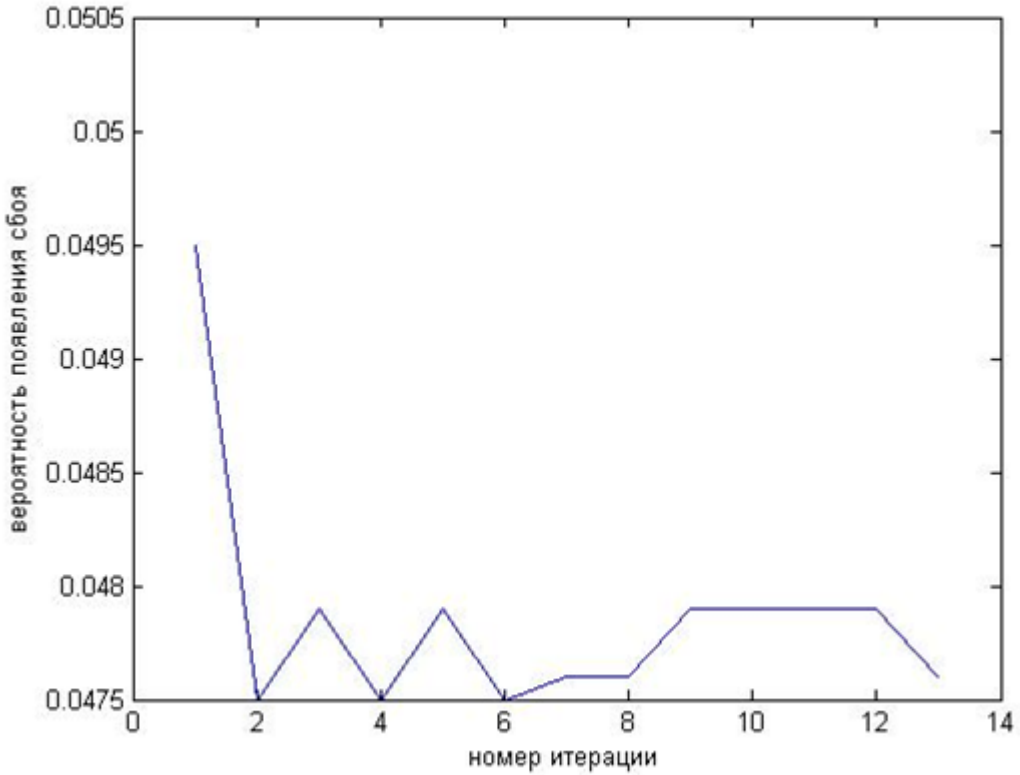
Вероятность распределения сбоев на интервалах m[i]



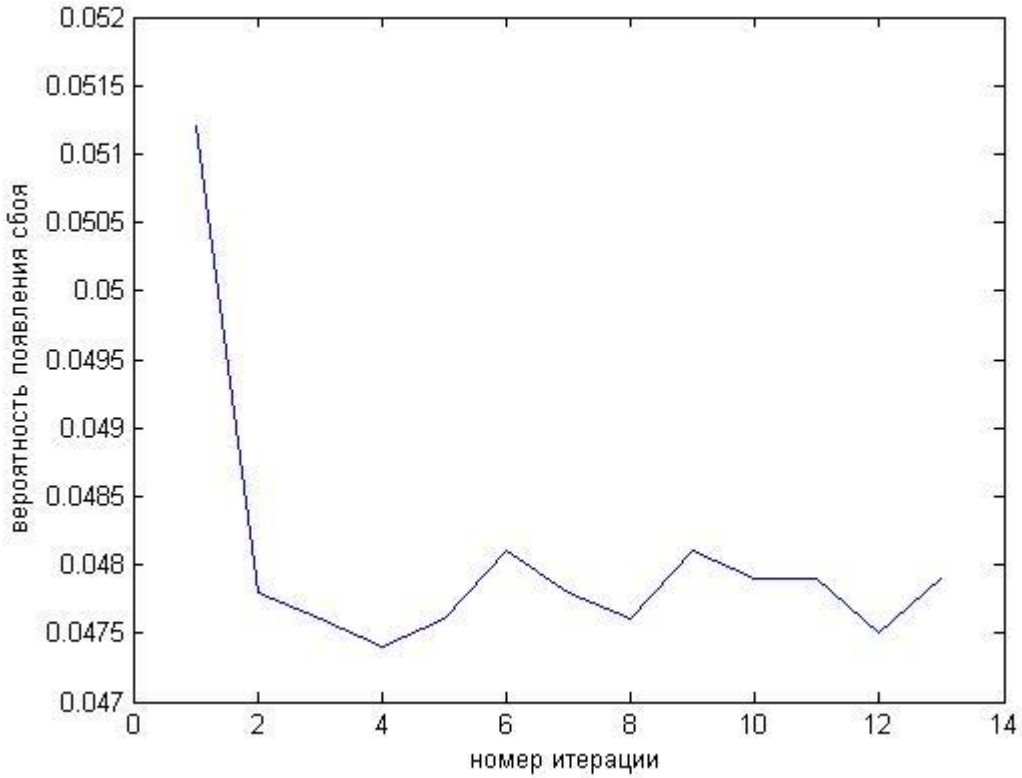
Вероятность появления сбоев в зависимости от количества итераций на интервале m[0]



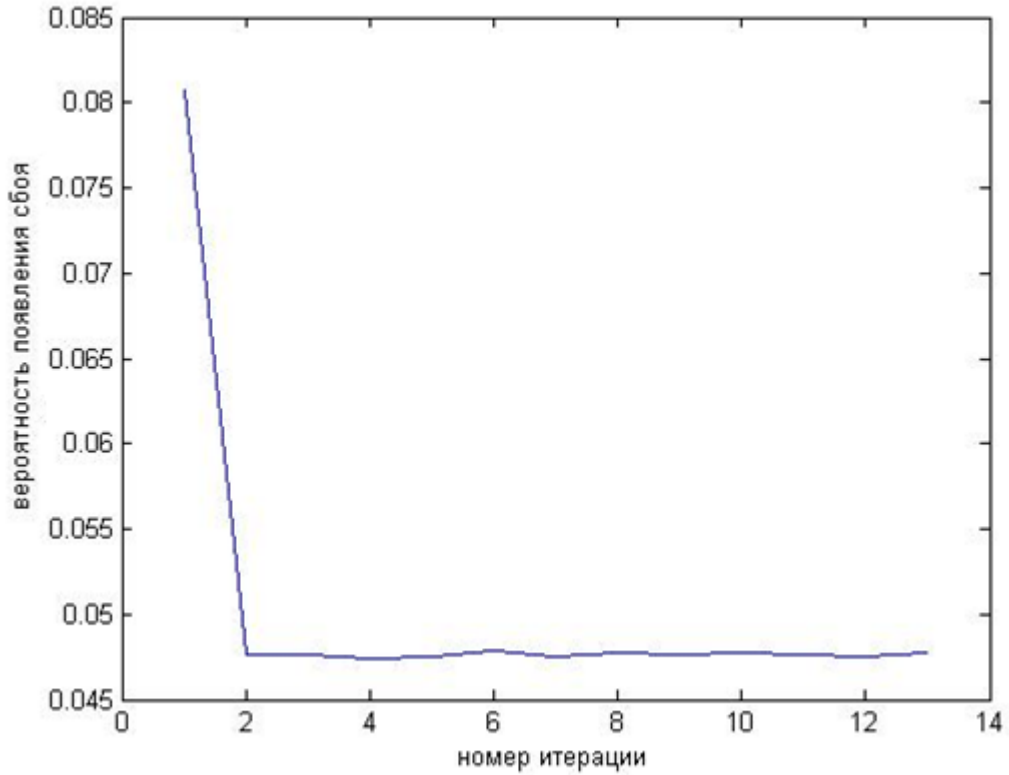
Вероятность появления сбоев в зависимости от количества итераций на интервале m[1]



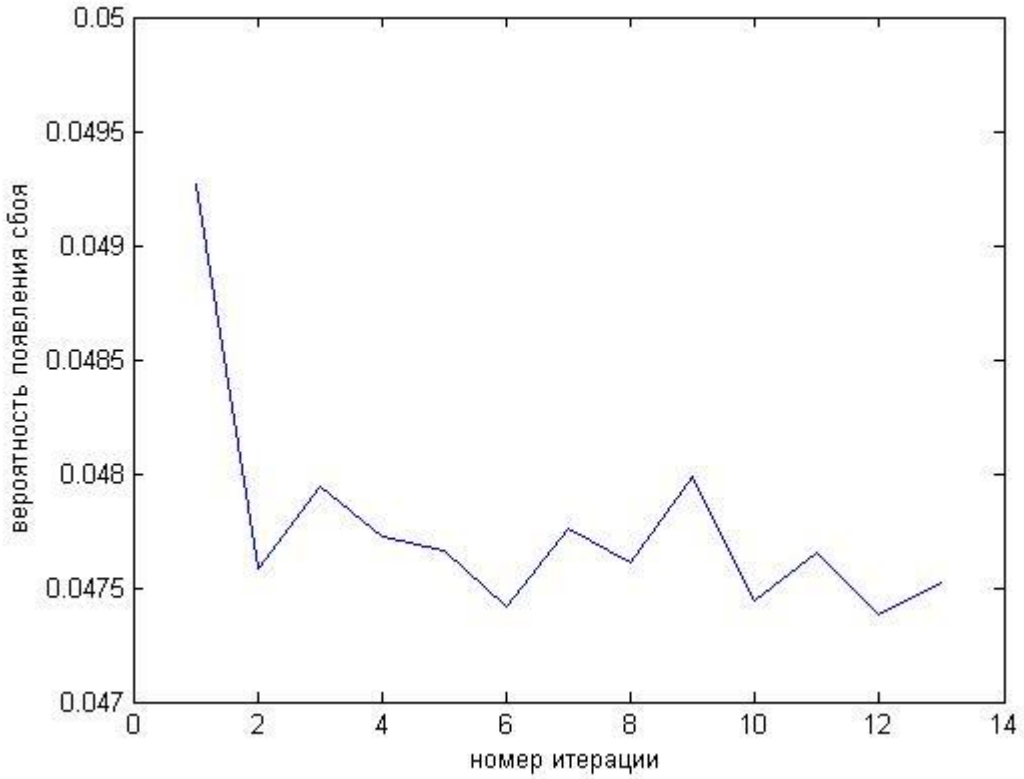
Вероятность появления сбоев в зависимости от количества итераций на интервале m[2]



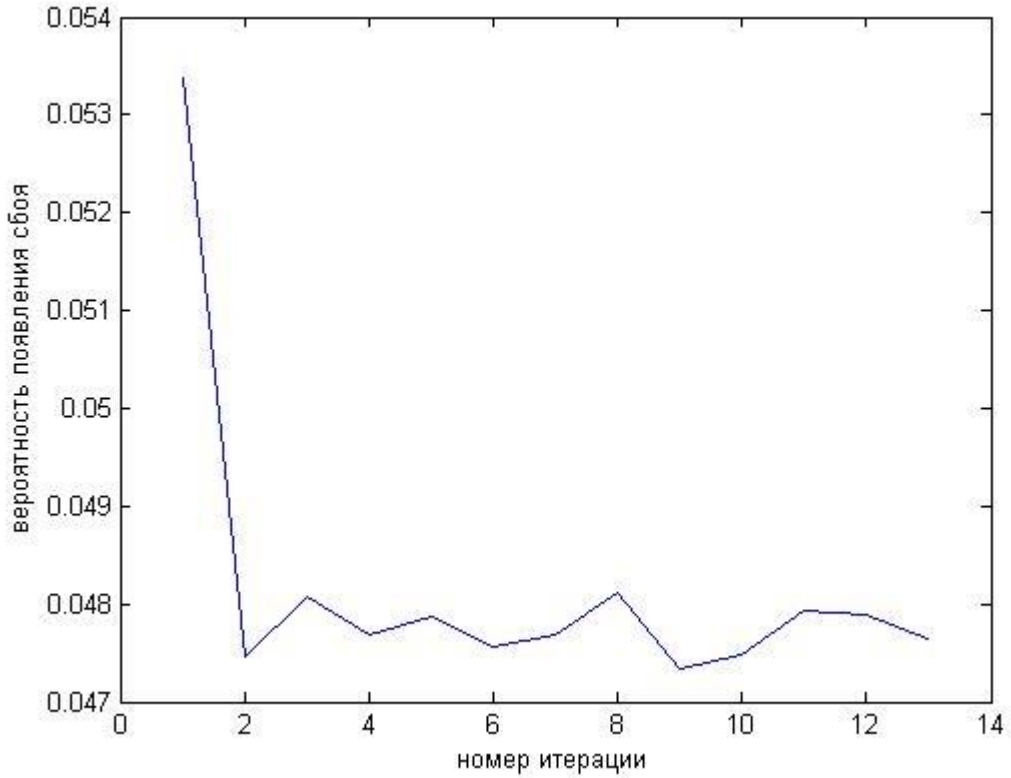
Вероятность появления сбоев в зависимости от количества итераций на интервале m[3]



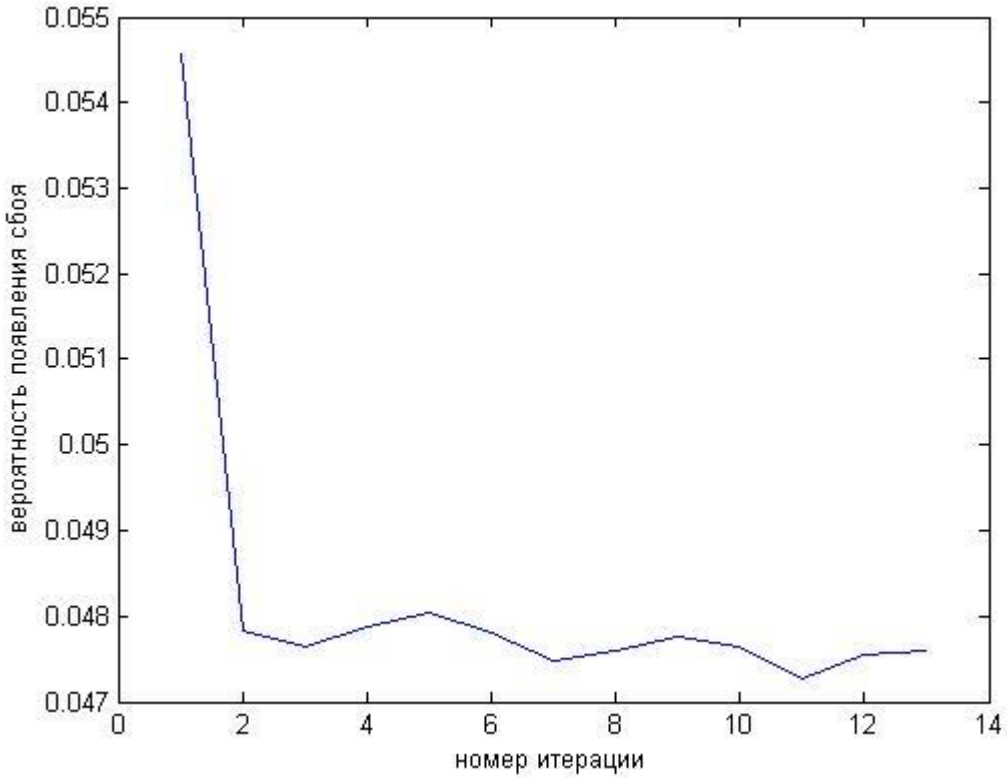
Вероятность появления сбоев в зависимости от количества итераций на интервале m[4]



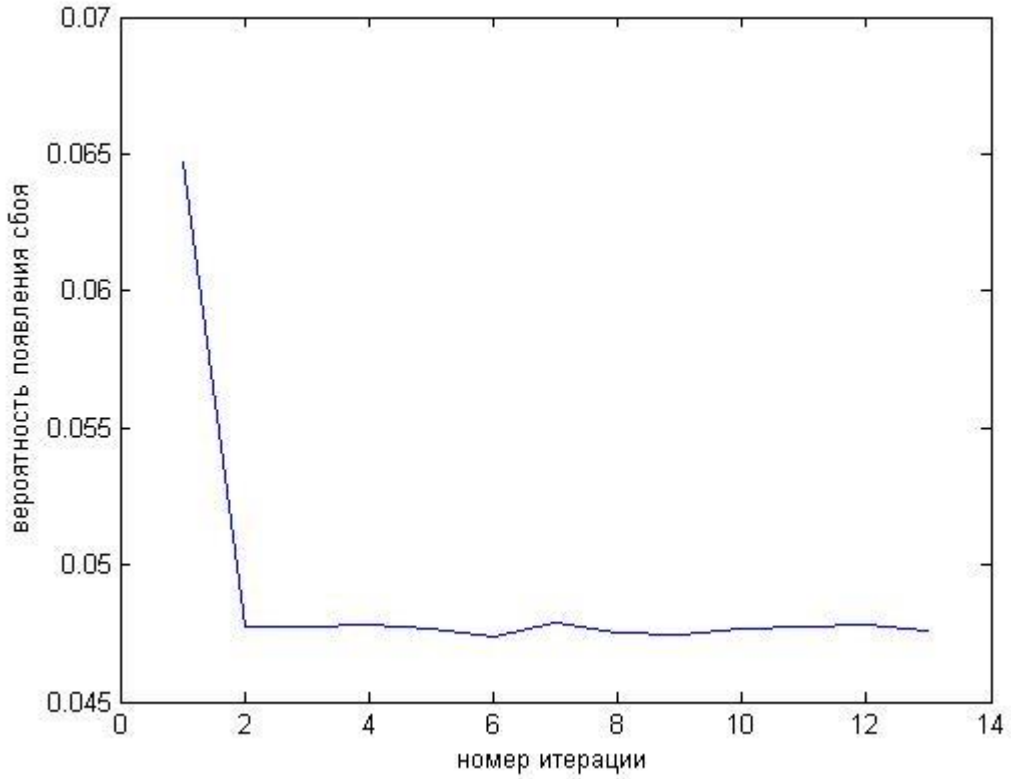
Вероятность появления сбоев в зависимости от количества итераций на интервале m[5]



Вероятность появления сбоев в зависимости от количества итераций на интервале m[6]



Вероятность появления сбоев в зависимости от количества итераций на интервале m[7]



Спасибо за внимание!

Любушкина И.Е.
Главный специалист, к. т. н.

Панасенко С. П.
Заместитель генерального директора по науке и системной интеграции
к. т. н., Microsoft Certified Professional

ООО Фирма «АНКАД»