Министерство образования Республики Беларусь
Белорусский государственный университет
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ПРИКЛАДНЫХ ПРОБЛЕМ МАТЕМАТИКИ И ИНФОРМАТИКИ

УТВЕРЖДАЮ
Директор НИИ прикладных проблем
математики и информатики

Ю.С.Харин
“___” _____ 2022 г.

МЕТОДИКА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

МИ.10127.10.03

Листов 23

Минск 2022

Предисловие

Настоящая методика испытаний предназначена для использования в испытательных лабораториях при проведении сертификационных испытаний средств криптографической защиты информации на соответствие требованиям СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности».

Содержание

1 Термины, обозначения и сокращения

В настоящей методике используются следующие термины и сокращения:

случайные числа — последовательность элементов, каждый из которых не может быть предсказан (вычислен) только на основе предшествующих ему элементов данной последовательности;

генератор случайных чисел (ГСЧ) — аппаратно-программное устройство, вырабатывающее случайные числа. Генератор включает один или несколько источников случайности и средства обработки данных от источников;

н.р.р. — независимые и равномерно распределённые (случайные величины);

СКЗИ — средства криптографической защиты информации.

В настоящей методике используются следующие обозначения:

$\mathsf{P}\{\mathcal{E}\}$ — вероятность наступления события $\mathcal{E}$;

$\mathsf{I}\{\mathcal{E}\}$ — индикатор наступления события $\mathcal{E}$;

χ^2_m — распределение хи-квадрат с m степенями свободы;

$F_L(x)$ — функция распределения закона L: $F_L(x) = \mathsf{P}\{\xi \leqslant x\}$, где случайная величина ξ распределена по закону L;

$F_L^{-1}(p)$ — квантиль уровня $p \in [0,1]$ закона L: такое x, что $F_L(x) = p$;

$\Phi(x)$ — функция стандартного нормального распределения;

$\mathsf{E}\{\xi\}$ — математическое ожидание случайной величины ξ;

C_n^m — число сочетаний из n по m;

$[z]$ — целая часть числа z.

2 Объект и цель испытаний

В СКЗИ для построения ключей, синхропосылок, других непредсказуемых или неповторяющихся объектов, используются ГСЧ. Генераторы обрабатывают данные от источников случайности и формируют по ним случайные числа — двоичные слова определенной длины. От статистического качества случайных чисел зависит надежность СКЗИ.

В компьютерных системах распространены следующие источники случайности:

— физические источники, использующие процессы в физических устройствах (например, шум в радиоэлектронных приборах);

— системные источники, использующие состояния, процессы и события операционной системы (например, системное время, сетевая активность, прерывания);

— источники, основанные на активности операторов (например, движения мышью, нажатия клавиш).

В настоящей методике рассматриваются ГСЧ, в которых используются источники только первого типа.

Объектом испытаний являются выходные последовательности ГСЧ. Эти последовательности представляют собой двоичные (бинарные) файлы, полученные объединением (конкатенацией) выходных случайных двоичных слов генератора. Выходные последовательности интерпретируются как битовые.

На испытания могут представляться несколько выходных последовательностей одного и того же генератора в разных условиях и режимах его эксплуатации.

Выходные последовательности должны сопровождаться документацией, в которой должна быть указана следующая информация:

— название генератора случайных чисел;

— перечень файлов случайных чисел;

— краткое описание способов формирования файлов случайных чисел (режим работы ГСЧ, условия его эксплуатации).

Выходные последовательности могут быть получены независимо экспертами или с участием разработчика. Если предполагается независимое снятие выходной последовательности, то разработчик дополнительно должен предоставить необходимое аппаратное и программное обеспечение ГСЧ.

Целью испытаний является проверка статистической гипотезы о н.р.р. элементов выходной последовательности ГСЧ. В математической статистике эту гипотезу принято обозначать через H_0. Выполнение H_0 означает равновероятность, независимость и однородность наблюдаемых случайных чисел, отсутствие в них периодичности.

При выполнении H_0 выходные случайные числа генератора максимально трудно предсказать и поэтому их можно использовать для формирования ключей, синхропосылок, других критических или уникальных параметров криптографических алгоритмов и протоколов.

3 Требования к выходным последовательностям

На испытания представляются $M (M \geqslant 2)$ бинарных выходных последовательностей ГСЧ длиной 1 Мб до 10 Мб ($2^{23} = 8388608$ битов соответсвует 1 Мб, а $10 \cdot 2^{23} = 83886080$ битов соответствует 10 Мб) каждая. Последовательности представляются в виде отдельных файлов или одного файла. В последнем случае файл предварительно разбивается на несколько файлов, каждый из которых представляет последовательность нужной длины (1 Мб или 10 Мб). Разбиение может выполнено с помощью следующих команд Linux, например, в частности для 1 Мб:

```
mkdir out_files
split --bytes=1M in_file ./out_files/
```

Требуется использовать не менее 10 ($M \geqslant 10$) последовательностей. Рекомендуется использовать 50 ($M = 50$) последовательностей.

При необходимости уточнения результатов тестирования могут быть затребованы статистические данные большего объема.

4 Средства и порядок испытаний

Для проверки гипотезы H_0 о независимости и одинаковой равномерной распределенности элементов выходных последовательностей ГСЧ используются статистические тесты (критерии). Это процедуры принятия решения. В них обрабатываются наблюдаемые случайные числа, в результате чего вычисляется статистика теста. По статистике теста вычисляется P-значение P.

Если H_0 верна, то P-значение имеет равномерное распределение на отрезке $[0, 1]$. В частности, для малых α событие $\mathcal{E} = \{P \leqslant \alpha\}$ наступает с малой вероятностью α. Если событие $\mathcal{E}$ не наступает, то принимается решение в пользу H_0, если наступает, то H_0 отвергается. Порог α называется уровнем значимости статистического теста. Он характеризует ошибку первого рода: вероятность отвергнуть H_0 при ее соблюдении.

В настоящей методике используется набор из 8 ($q = 8$) статистических тестов. Тесты применяются к фрагментам анализируемой выходной последовательности, в результате

чего вычисляется набор чисел (P_{ij}) — P-значений i-го теста для j-го фрагмента. Число фрагментов (m) зависит от длины аналируемой последовательности. Например, для последовательностей длины 1 Мб рекомендуется задавать 104 фрагмента, в для последовательностей длины 10 Мб рекомендуется задавать 200 фрагментов. Затем набор (P_{ij}) интерпретируется как статистические наблюдения, и по нему строится интегральное P-значение P_i для i-го теста. Интегральные P-значения тестов сравниваются с еще одним уровнем значимости β. Набор базовых тестов вместе с методом расчета интегральных P-значений называется батареей тестов. Если все интегральные P-значения батареи тестов $P_1, P_2, \ldots, P_8$ больше уровня β, то H_0 принимается, иначе — отвергается.

В методике определяются две батареи тестов: Бернулли и хи-квадрат. В обеих батареях используются одни и те же базовые статистические тесты.

Гипотеза H_0 относительно одной испытуемой последовательности принимается, если обе батареи принимают решение в пользу этой гипотезы.

Если тестируется не одна, а $M(M \geqslant 2)$ выходных последовательностей ГСЧ, то P-значения батарей обрабатываются по-другому. С учетом уровня значимости β вычисляются частоты прохождения каждого теста в отдельности. Затем, используя еще один уровень значимости γ (для статистического портрета), на основании которого вычисляется доверительный интервал для этих частот. Гипотеза H_0 относительно всех M последовательностей принимается, если для обеих батарей все частоты принятия H_0 для каждого теста попадают в построенный доверительный интервал.

При наличии различных режимов работы ГСЧ гипотеза H_0 проверяется отдельно для каждого режима. При этом используются только те выходные последовательности, которые получены в данном режиме.

Для повышения гарантий результатов тестирования рекомендуется применять данную методику к нескольким наборам выходных последовательностей, снятых с ГСЧ через достаточно большие промежутки времени.

По результатам статистического анализа эксперт оформляет протокол статистического тестирования выходных последовательностей генератора случайных чисел (см. приложение А).

5 Методы испытаний

5.1 Общие положения

В данном разделе определяются $8(q = 8)$ статистических тестов, которые используются в батареях Бернулли и хи-квадрат.

Каждый тест описывается по следующей схеме:

1) общие сведения: название, выявляемые зависимости, параметры;

2) обозначение;

3) шаги алгоритма расчета значений статистики теста и соответствующего P - значения;

4) условия применения.

Статистика теста (критерия) — это функция S от обрабатываемой последовательности. При выполнении H_0 статистика представляет собой случайную величину η с определенным распределением вероятностей. Для конкретной последовательности X статистика принимает конкретное значение s. P-значением теста называют вероятность того, что при

выполнении H_0 статистика S примет значение, большее наблюдаемого значения s:

$$P = \mathsf{P}\left\{\eta \geqslant s \mid H_0\right\}.$$

При выполнении H_0 P-значение имеет равномерное распределением на отрезке $[0,1]$.

Далее в описаниях статистических тестов $X = (x_1, x_2, \ldots, x_n)$ — анализируемая выходная бинарная последовательность ГСЧ длины n.

5.2 Тест многомерной дискретной равномерности по непересекающимся отрезкам

Общие сведения. Тест многомерной дискретной равномерности по непересекающимся отрезкам (МДРН) предназначен для проверки согласия распределения непересекающихся L-фрагментов последовательности X с L-мерным дискретным равномерным распределением.

МДРН-тест позволяет выявлять отклонения от L-мерного дискретного равномерного распределения: тест отвергает гипотезу H_0 в случае, когда отклонения эмпирических частот встречаемости фрагментов длины L от их теоретических значений значимо.

Параметр теста: длина фрагмента L.

Обозначение: МДРН$[L]$.

Входные данные. Последовательность $X = (x_1, \ldots, x_n)$.

Шаг 1. Вычислить число фрагментов разбиения: $m = [n/L]$.

Шаг 2. Построить разбиение X на последовательные непересекающиеся L-фрагменты:

$$X_t = (x_{L(t-1)+1}, \ldots, x_{Lt}), \quad t = \overline{1,m}.$$

Шаг 3. Вычислить частоты:

$$\nu_v^{(L)} = \sum_{t=1}^{m} \mathbf{I}\left\{X_t = v\right\}, \quad v \in \{0,1\}^L.$$

Шаг 4. Вычислить статистику:

$$S_{\chi^2}(m) = \sum_{v \in \{0,1\}^L} \frac{\left(\nu_v^{(L)} - m2^{-L}\right)^2}{m2^{-L}}.$$

Шаг 5. Вычислить и возвратить P-значение:

$$P = 1 - F_{\chi^2_{2^L-1}}\left(S_{\chi^2}(m)\right).$$

Условия применения. Должны выполняться условия:

$$m \geqslant 50, \qquad m \cdot \frac{1}{2^L} = \frac{n}{L2^L} \geqslant 10.$$

5.3 Тест многомерной дискретной равномерности по пересекающимся отрезкам

Общие сведения. Тест многомерной дискретной равномерности по пересекающимся отрезкам предназначен для проверки согласия распределения пересекающихся L-фрагментов наблюдаемой последовательности с L-мерным дискретным равномерным распределением [6].

МДРП-тест позволяет обнаруживать отклонения от гипотезы независимости и равновероятности типа рекуррентной, марковской зависимости порядка не больше, чем размерность вектора L, отклонения от L-мерного дискретного равномерного распределения.

Параметр теста: длина фрагмента L.

Обозначение: МДРП[L].

Входные данные. Последовательность $X = (x_1, \ldots, x_n)$.

Шаг 1. Построить разбиение X на пересекающиеся L-фрагменты:

$$X_1^{(L)} = (x_1, \ldots, x_L),\ X_2^{(L)} = (x_2, \ldots, x_{L+1}),\ \ldots,$$
$$X_{n-L+2}^{(L)} = (x_{n-L+2}, \ldots, x_n, x_1), \ldots, X_n^{(L)} = (x_n, x_1, \ldots, x_{L-1}).$$

Шаг 2. Для $v \in \{0,1\}^L$ вычислить частоты по всем фрагментам:

$$\nu_v^{(L)} = \sum_{t=1}^{n} \mathbf{I}\left\{X_t^{(L)} = v\right\}.$$

Шаг 3. На основании частот $\nu_v^{(L)}$ вычислить статистику $\gamma_L(n)$:

$$\gamma_L(n) = \sum_{v \in \{0,1\}^L} \frac{\left(\nu_v^{(L)} - n2^{-L}\right)^2}{n2^{-L}}$$

Шаг 4. Построить разбиение X на пересекающиеся $(L-1)$-фрагменты:

$$X_1^{(L-1)} = (x_1, \ldots, x_{L-1}),\ X_2^{(L-1)} = (x_2, \ldots, x_L),\ \ldots,$$
$$X_{n-L+2}^{(L-1)} = (x_{n-L+3}, \ldots, x_n, x_1), \ldots, X_n^{(L-1)} = (x_n, x_1, \ldots, x_{L-2}).$$

Шаг 5. Вычислить частоты встречаемости векторов $v \in \{0,1\}^{L-1}$:

$$\nu_v^{(L-1)} = \sum_{t=1}^{n} \mathbf{I}\left\{X_t^{(L-1)} = v\right\}.$$

Шаг 6. Вычислить статистику $\gamma_{L-1}(n)$:

$$\gamma_{L-1}(n) = \sum_{v \in \{0,1\}^{L-1}} \frac{\left(\nu_v^{(L-1)} - n2^{-(L-1)}\right)^2}{n2^{-(L-1)}}$$

Шаг 7. Вычислить статистику теста:

$$S_{МДРП} = \gamma_L(n) - \gamma_{L-1}(n).$$

Шаг 8. Вычислить и возвратить P-значение:

$$P = 1 - F_{\chi^2_{2^L - 2^{L-1}}}\left(S_{МДРП}\right).$$

Условия применения. Должно выполняться условие:

$$n \geqslant 20 \cdot 2^L \qquad \left(L \leqslant \log_2 \frac{n}{20}\right).$$

Рекомендуется выбирать: $2 \leqslant L \leqslant 23$, причем при $L = 20$ необходимая длина последовательности $n = 20 \cdot 2^{20} = 20971520$ битов.

5.4 Тест «пустых ящиков»

Общие сведения. Применение статистических тестов, использующих частоты векторов из $\{0,1\}^L$, ограничено небольшими значениями L. С увеличением L информативной статистикой становится число векторов, не встретившихся в тестируемой последовательности ни разу (или же встретившихся более одного раза). Тестом, основанным на данной статистике, является тест "пустых ящиков" [4], [5], [17, с. 121], [19].

Тест «пустых ящиков» позволяет обнаруживать отклонения от L-мерного дискретного равномерного распределения.

Параметр теста: длина фрагмента L.

Обозначение: КПЯ$[L]$.

Входные данные. Последовательность $X = (x_1, \ldots, x_n)$.

Шаг 1. Вычислить число фрагментов $m = [n/L]$.

Шаг 2. Построить разбиение X на последовательные непересекающиеся L-фрагменты: $X = (X_1, X_2, \ldots, X_m)\,,\ X_t = \left(x_{L(t-1)+1}, \ldots, x_{Lt}\right) \in \{0,1\}^L,\ t = \overline{1,m}$.

Шаг 3. Для $v \in \{0,1\}^L$ вычислить частоты:

$$\nu_v^{(L)} = \sum_{t=1}^{m} \mathbf{I}\left\{X_t = v\right\}.$$

Шаг 4. Вычислить статистику теста — число векторов, встретившихся более одного раза (число «конфликтов»):

$$S_{EB} = \sum_{v\in\{0,1\}^L} \left(\nu_v^{(L)} - 1\right) \mathbf{I}\left\{\nu_v^{(L)} > 1\right\} = m - \left(2^L - \sum_{v\in\{0,1\}^L} \mathbf{I}\left\{\nu_v^{(L)} = 0\right\}\right) = m - \left(2^L - \mu_0\right),$$

где $\mu_0 = \mu_0(m, 2^L)$ — число "пустых ящиков": векторов из $\{0,1\}^L$, не встретившихся в X ни разу.

Шаг 5. Вычислить вспомогательные параметры:

$$\lambda = \frac{m}{2^L}, \quad \lambda_{\text{П}} = \frac{m^2}{2\cdot 2^L}, \quad \mu = 2^L e^{-\lambda}, \quad \sigma^2 = 2^L e^{-\lambda}(1 - (1+\lambda)e^{-\lambda}).$$

Шаг 6. Если $\lambda \leqslant 1/32$, то P-значение вычислить по формуле:

$$P = F_{\chi^2_{2S_{EB}}}\left(2\lambda_{\text{П}}\right).$$

Шаг 7. Если $1/32 < \lambda < 5$, то P-значение вычислить по формуле:

$$P = \Phi\left(-\frac{\mu_0 - \mu}{\sigma}\right).$$

Шаг 8. Возвратить P-значение.

Условия применения. Тест «пустых ящиков» следует применять для больших L в тех случаях, когда применить тесты типа хи-квадрат нельзя.

Размерность фрагментов L и число фрагментов $m = n/L$ в X должны согласованно выбираться в соответствии с одной из указанных выше асимптотик (см. шаги 5 и 6 алгоритма).

В случае $\lambda \geqslant 5$ тест не применяется: рекомендуется использовать критерий хи-квадрат, описание которого приведено в разделе 5.11.

При $\lambda < 1/32$ рекомендуется использовать $L \geqslant 19$ и $m = 2^{L/2+3}$ векторов.

5.5 Тест серий

Общие сведения. Цель теста — проверить, соответствует ли число серий из нулей и единиц различной длины в наблюдаемой последовательности теоретически ожидаемому числу для равномерно распределенных случайных последовательностей [7, с. 182], [8].

Тест серий позволяет выявлять последовательности, которые с вероятностью больше $0,5$ сохраняют свое предыдущее значение.

Обозначение: КС.

Входные данные. Последовательность $X = (x_1, x_2, \ldots, x_n)$.

Фрагмент $(x_t, x_{t+1}, \ldots, x_{t+l-1})$ последовательности X называется *серией длины* l, если $x_t = x_{t+1} = \cdots = x_{t+l-1}$, но $x_{t-1} \neq x_t$ (или $t = 1$) и $x_{t+l-1} \neq x_{t+l}$ (или $t + l - 1 = n$).

Шаг 1. Вычислить теоретические частоты серий:

$$\mu_i = (n - i + 3)/2^{i+2}, \quad i = \overline{1, k},$$

где k определяется из условия: $\mu_k \geqslant 5$ и $\mu_{k+1} < 5$.

Шаг 2. Для $i = 1, \ldots, k$ вычислить частоты $\nu_i^{(0)}$ и $\nu_i^{(1)}$. Здесь $\nu_i^{(b)}$ — частота серий из символов b длины i в последовательности X.

Шаг 3. Вычислить значение статистики теста S_{runs}:

$$S_{runs} = \sum_{i=1}^{k} \frac{(\nu_i^{(0)} - \mu_i)^2}{\mu_i} + \sum_{i=1}^{k} \frac{(\nu_i^{(1)} - \mu_i)^2}{\mu_i}.$$

Шаг 4. Вычислить и возвратить P-значение:

$$P = 1 - F_{\chi^2_{2k-2}}(S_{runs}).$$

Условия применения теста. Рекомендуется использовать $n \geqslant 20000$ и $k \geqslant 6$.

5.6 Тест длинных серий

Общие сведения. Тест длинных серий в отличии от теста серий проверяет, соответствует ли максимальная длина серии из единиц (или из нулей) в L-битном фрагменте наблюдаемой последовательности теоретически ожидаемому значению [8, стр. 67].

Тест длинных серий позволяет выявлять такие же зависимости как и в тесте серий (см. п. 5.5).

Параметр теста: длина фрагмента $L \in \{8, 128, 512, 1000, 10000\}$.

Обозначение: КДС[L].

Входные данные. Последовательность $X = (x_1, x_2, \ldots, x_n)$.

Шаг 1. Разбить X на $m = [n/L]$ фрагментов X_i по L бит:

$$X_i = (x_{(i-1)L+1}, \ldots, x_{(i-1)L+L}), \quad i = \overline{1, m}.$$

Шаг 2. По L, используя таблицу 2, определить разбиение множества длин серий на подмножества (классы) $D_0, \ldots, D_K$.

Шаг 3. Для $i = 1, \ldots, m$ найти длину b_i максимальной серии из единиц в фрагменте X_i.

Шаг 4. Для $j = 1, \ldots, K$:

1) используя таблицу 3, определить теоретические вероятности попадания статистик b_i в класс D_j:

$$\pi_j = \mathsf{P}\left\{b_i \in D_j\right\};$$

2) вычислить частоты попадания статистик b_i в класс D_j:

$$\nu_j = \sum_{i=1}^{m} \mathbf{I}\left\{b_i \in D_j\right\}.$$

Шаг 5. Вычислить статистику теста:

$$S_{long} = \sum_{j=0}^{K} \frac{(\nu_j - m\pi_j)^2}{m\pi_j}.$$

Шаг 6. Вычислить и возвратить P-значение теста:

$$P = 1 - F_{\chi^2_K}\left(S_{long}\right).$$

Условия применения. Должно выполняться условие: $m \cdot \min_{0 \leqslant i \leqslant K} \pi_i \geqslant 10$. Откуда следует, что минимальная длина n последовательности X для различных значений параметра L должна удовлетворять значениям из таблицы 1.

Таблица 1 — Минимальные значения n теста длинных серий

L	8	128	512	1000	10000
n	427	12464	50688	100000	1490000

Примечание. Если верна H_0 и в фрагменте X_i встречается r единиц и $L - r$ нулей, то теоретические вероятности равны [8]:

$$\mathsf{P}\left\{b_i \leqslant q\right\} = \sum_{r=0}^{L} C_r^L \mathsf{P}\left\{b_i \leqslant q | r\right\} \frac{1}{2^L}, \quad \mathsf{P}\left\{b_i \leqslant q | r\right\} = \frac{1}{C_L^r} \sum_{j=0}^{U} (-1)^j C_{L-r+1}^{j} C_{L-j(q+1)}^{L-r},$$

где $0 \leqslant q \leqslant L,\ U = \min(L - r + 1, [r/(q+1)]),\ 0 \leqslant r \leqslant L$.

При больших значениях L вычисление вероятностей π_i по данным формулам требует больших вычислительных и временных ресурсов, поэтому в методике предлагается значения длин фрагментов L выбирать из множества $\Lambda = \{8, 128, 512, 1000, 10000\}$, для которого сделаны предвычисления. В таблице 2 представлены классы D_i для различных значений $L \in \Lambda$, а в таблице 3 — соответствующие им вероятности π_i.

Таблица 2 — Разбиение множества значений статистики b_i на классы

L	8	128	512	1000	10000
K	3	5	5	5	6
D_0	$\leqslant 1$	$\leqslant 4$	$\leqslant 6$	$\leqslant 7$	$\leqslant 10$
D_1	2	5	7	8	11
D_2	3	6	8	9	12
D_3	$\geqslant 4$	7	9	10	13
D_4	—	8	10	11	14
D_5	—	$\geqslant 9$	$\geqslant 11$	$\geqslant 12$	15
D_6	—	—	—	—	$\geqslant 16$

Таблица 3 — Вероятности попадания статистики b_i в классы

L	8	128	512	1000	10000
K	3	5	5	5	6
π_0	0.2148	0.1174	0.1170	0.1307	0.0882
π_1	0.3672	0.2430	0.2460	0.2437	0.2092
π_2	0.2305	0.2493	0.2523	0.2452	0.2483
π_3	0.1875	0.1752	0.1755	0.1714	0.1933
π_4	—	0.1027	0.1015	0.1002	0.1208
π_5	—	0.1124	0.1077	0.1088	0.0675
π_6	—	—	—	—	0.0727

5.7 Тест аппроксимации энтропии

Общие сведения. Тест аппроксимации энтропии основан на статистических оценках энтропии случайных фрагментов размерностей L и $L-1$ [11].

Тест позволяет обнаруживать отклонения от свойств бинарных равномерно распределенных случайных последовательностей, связанные со значимыми изменениями количества информации при переходе от фрагментов размерности $L-1$ к фрагментам размерности L.

Параметр теста: длина фрагмента L.

Обозначение: КАЭ$[L]$).

Входные данные. Последовательность $X = (x_1, x_2, \ldots, x_n)$.

Шаг 1. Для $l \in \{L-1, L\}$ построить разбиения X на пересекающиеся l-фрагменты:

$$X_t^{(l)} = (x_t, x_{t+1}, \ldots, x_{t+l-1}), \quad t = \overline{1, n+1-l}.$$

Шаг 2. Для $l \in \{L-1, L\}$ вычислить относительные частоты $\{\pi_v^{(l)}\}$ встречаемости всевозможных векторов $v \in \{0,1\}^l$:

$$\pi_v^{(l)} = \frac{1}{n+1-l} \sum_{t=1}^{n+1-l} \mathbf{I}\left\{X_t^{(l)} = v\right\}.$$

Шаг 3. Для $l \in \{L-1, L\}$ вычислить выборочные энтропии:

$$F^{(l)} = -\sum_{v \in \{0,1\}^l} \pi_v^{(l)} \log_2 \pi_v^{(l)}.$$

Шаг 4. Вычислить приращение энтропии:

$$ApEn(L) = F^{(L)} - F^{(L-1)}.$$

Шаг 5. Вычислить статистику теста $S_{AE}(n)$:

$$S_{AE}(n) = 2n\,|ln2 - ApEn(L)|\,.$$

Шаг 6. Вычислить и возвратить P-значение теста:

$$P = 1 - F_{\chi^2_{2^L-2^{L-1}}}\left(S_{AE}(n)\right).$$

Условия применения. Параметр L рекомендуется выбирать максимально возможным, удовоетворяющим условию $n/2^L \geqslant 100$.

5.8 Тест скалярного произведения

Общие сведения. Тест основан на экстремальной статистике скалярного произведения [24]. Тест позволяет обнаруживать отклонения от гипотезы независимости и равновероятности.

Параметры теста: длина подфрамента m, число подфрагментов $K \geqslant 2$. По параметрам m и K определяется длина фрагмента $L = m \cdot K$.

Обозначение: КСКП$[m, K]$.

Входные данные. Последовательность $X = (x_1, \ldots, x_n)$.

Шаг 1. Разбить X на $M = [n/L]$ фрагментов длины $L = m \cdot K$, а каждый из этих фрагментов в свою очередь разбить на K подфрагментов длины m:

$$X^{(l)} = (X_1^{(l)}, X_2^{(l)}, \ldots, X_K^{(l)}), \quad l = \overline{1, M},$$

$$X_i^{(l)} = (x_{(l-1)L+(i-1)m+1}, \ldots, x_{(l-1)L+im}), \quad i = \overline{1, K}.$$

Шаг 2. По каждому фрагменту $X^{(l)}$ $(l = \overline{1, M})$ вычислить $K - 1$ статистик $Y_2^{(l)}, \ldots, Y_K^{(l)}$:

$$Y_j^{(l)} = (X_1^{(l)}, X_j^{(l)}) = \sum_{k=1}^{m} x_{(l-1)L+k} \cdot x_{(l-1)L+(j-1)m+k}, \quad j = \overline{2, K}.$$

Шаг 3. Для каждого фрагмента $X^{(l)}$ $(l = \overline{1, M})$ по статистикам $Y_2^{(l)}, \ldots, Y_K^{(l)}$ определить экстремальную статистику $Y_{\max}^{(l)}$:

$$Y_{\max}^{(l)} = \max\{Y_2^{(l)}, \ldots, Y_K^{(l)}\}.$$

Статистика Y_j характеризует «степень похожести» 1-го и j-го фрагментов.

Шаг 4. По набору статистик $\{Y_{\max}^{(l)} : l = \overline{1, M}\}$ вычислить эмпирические частоты:

$$f_k = \sum_{l=1}^{M} \mathbf{I}\left\{Y_{\max}^{(l)} = k\right\}.$$

Шаг 5. Вычислить теоретические частоты:

$$q_0 = \mathsf{P}\{Y_{\max} = 0\} = 2^{-m} \sum_{l=0}^{m} 2^{-l(K-l)} C_m^l = 2^{-m}(1 + 2^{1-K})^m,$$

$$q_k = \mathsf{P}\{Y_{\max} = k\} = 2^{-m} \sum_{l=0}^{m} C_m^l \left(\sum_{y=0}^{k} 2^{-l} C_l^y\right)^{K-1} - 2^{-m} \sum_{l=0}^{m} C_m^l \left(\sum_{y=0}^{k-1} 2^{-l} C_l^y\right)^{K-1}, \quad k > 0.$$

Шаг 6. Вычислить статистику теста S_{χ^2}:

$$S_{\chi^2} = \sum_{k=0}^{m} \frac{(f_k - M q_k)^2}{M q_k}.$$

Шаг 7. Вычислить и возвратить P-значение теста:

$$P = 1 - F_{\chi^2_m}(S_{\chi^2}).$$

Условия применения. При выборе параметров m и K требуется обеспечить условия: 1) $m \in \{2, 3, \ldots, 8\}$; 2) $K \in \{2, 3, \ldots, 11\}$; 3) $\frac{K}{q_{\min}} \leqslant \frac{n}{10m}$, где $q_{\min} = \min_k q_k$.

5.9 Спектральный тест

Общие сведения. Спектральный тест предназначен для выявления периодичности в бинарных случайных последовательностях [8].

Параметры теста: нет.

Обозначение: СК-БПФ.

Входные данные. Последовательность $X = (x_1, \ldots, x_n)$.

Шаг 1. По X сформировать последовательность Y, заменяя $x_t = 0$ на $y_t = -1$, а $x_t = 1$ на $y_t = 1$:

$$Y = (y_1, y_2, \ldots, y_n), \quad y_t = 2x_t - 1, \quad t = \overline{1, n}.$$

Шаг 2. К Y применить алгоритм быстрого преобразования Фурье (БПФ) [12] и сформировать комплекснозначную последовательность $S = (s_0, s_1, \ldots, s_{n-1})$:

$$s_t = \sum_{k=1}^{n} y_k \exp\left(\frac{2\pi i(k-1)t}{n}\right), \quad t = \overline{0, n-1},$$

где

$$\exp\left(\frac{2\pi ikt}{n}\right) = \cos\left(\frac{2\pi kt}{n}\right) + i\sin\left(\frac{2\pi kt}{n}\right),$$

и $i = \sqrt{-1}$ — мнимая единица.

Шаг 3. По S сформировать последовательность $\{|s_t|\}$:

$$|s_t| = \sqrt{\left(s_t^{\Re}\right)^2 + \left(s_t^{\Im}\right)^2}, \quad t = \overline{0, n/2-1},$$

где $\{s_t^{\Re}\}$ и $\{s_t^{\Im}\}$ — действительная и мнимая части последовательности S (в силу симметричности суммируем половину членов последовательности).

Шаг 4. Определить порог $h = \sqrt{3n}$ и построить последовательность бинарных случайных величин — индикаторов превышения значения $|s_t|$ порога h:

$$u_t = \mathbf{I}\{|s_t| < h\}, \quad t = \overline{0, n/2-1}.$$

При выполнении H_0 95% значений $|s_t|$ должно лежать ниже порогового значения $h = \sqrt{3n}$. При этом величины u_t имеют распределение Бернулли [8]:

$$\mathcal{L}\{u_t\} = Bi(1, p), \quad p = 0.95, \quad t = \overline{0, n/2-1}.$$

Шаг 5. Вычислить значение статистики S_{SC}:

$$S_{SC} = \sum_{t=0}^{n/2-1} u_t.$$

Шаг 6. Вычислить математическое ожидание и дисперсию:

$$\mu = \frac{n}{2}p, \quad \sigma^2 = \frac{n}{2}p(1-p).$$

Шаг 7. Вычислить и возвратить P-значение теста:

$$P = 2\left(1 - \Phi\left(\left|\frac{S_{SC} - \mu}{\sigma}\right|\right)\right).$$

Условия применения. Требуется выполнение условия [22]: $\frac{n}{2} \cdot 0.95 \cdot 0.05 \geqslant 9$, то есть $n \geqslant 400$. Рекомендуется выбирать $n \geqslant 1000$ битов [8].

5.10 Батарея Бернулли

Общие сведения. При использовании батареи Бернулли по набору входных P-значений фрагментов для каждого теста строится новая случайная бинарная последовательность, элементы которой равны 1 при принятии H_0 и равны 0 при отклонении H_0 на уровне значимости теста α. При выполнении H_0 новая последовательность соответствует реализации схемы независимых испытаний Бернулли. Длина новой последовательности совпадает с числом фрагментов тестирования. Частота принятия H_0 по всем фрагментам определяет еще одну статистику, которая и является статистикой интегрального P-значения. При выполнении H_0 данная статистика имеет распределение Бернулли [8], [13], [14].

Параметры: уровень значимости тестов α.

Обозначение: Б1[α].

Входные данные. Набор P-значений $(P_{ij}), i = \overline{1,q},\ j = \overline{1,m}$ (q — число тестов; m — число фрагментов).

Шаг 1. Для $i = 1,\dots,q$ и $j = 1,\dots,m$ по набору P-значений построить индикаторы:

$$\nu_{ij} = \mathbf{I}\{P_{ij} \geqslant \alpha\}.$$

Шаг 2. Для $i = 1,\dots,q$ вычислить частоту принятия H_0:

$$\overline{\nu}_i = \sum_{j=1}^{m} \nu_{ij}.$$

Шаг 3. Для $i = 1,\dots,q$ вычислить интегральные P-значения тестов:

$$P_i^1 = 1 - \Phi\left(-\frac{\overline{\nu_i}/m - (1-\alpha)}{\sqrt{\alpha(1-\alpha)/m}}\right).$$

Шаг 4. Возвратить $(P_1^1,\dots,P_q^1)$.

Условия применения. Должно выполняться условие: $m \geqslant 1/\alpha$. Рекомендуемые значения: $\beta = 0.0001$; $m = 104$ для выборки 1 Мб и $m = 200$ для выборки 10 Мб.

5.11 Батарея хи-квадрат

Общие сведения. При использовании батареи хи-квадрат к входному набору P-значений фрагментов для каждого теста в отдельности применяется критерий согласия хи-квадрат, при этом набор P-значений интерпретируется как новые статистические наблюдения. Длина новой последовательности совпадает с числом фрагментов тестирования. По значению статистики хи-квадрат строится интегральное P-значение теста.

Параметры: k — число интервалов группировки для критерия хи-квадрат.

Обозначение: Б2[k].

Входные данные. Набор P-значений $(P_{ij}), i = \overline{1,q},\ j = \overline{1,m}$ (q — число тестов; m — число фрагментов).

Шаг 1. Разбить отрезок $[0;1]$ на k равных интервалов:

$$I_j = [(j-1)/k; j/k),\ j = \overline{1,k-1},\quad I_k = [(k-1)/k; 1].$$

Шаг 2. Для каждого теста K_i $(i = 1, \ldots, q)$ вычислить частоты попадания P- значений данного теста в интервалы I_j:

$$\nu_{ij} = \sum_{t=1}^{m} \mathbf{I}\{P_{it} \in I_j\}, \quad j = 1, \ldots, k.$$

Теоретические вероятности попадания в каждый из интервалов I_j равняются $1/k$.

Шаг 3. Для $i = 1, \ldots, q$ вычислить статистику критерия хи-квадрат i-го теста:

$$S^{(i)}_{\chi^2} = \sum_{j=1}^{m} \frac{(\nu_{ij} - m/k)^2}{m/k},$$

где m/k — теоретическая частота попадания наблюдений в j-й интервал.

Шаг 4. Для $i = 1, \ldots, q$ вычислить интегральные P-значения тестов:

$$P^2_i = 1 - F_{\chi^2_{m-1}}\left(S^{(i)}_{\chi^2}\right).$$

Шаг 5. Возвратить $(P^2_1, \ldots, P^2_q)$.

Условия применения. Должны выполняться условия: $m \geqslant 1/\alpha$, $k \geqslant 10, m/k \geqslant 10$. Рекомендуемые значения: $\beta = 0.0001$; $m = 104, k = 10$ для выборки 1 Мб; $m = 200, k = 10$ для выборки 10 Мб.

5.12 Тестирование одной последовательности

Общие сведения. Методика принятия H_0 основана на принципе гарантированного результата [20], [25]: H_0 принимается, если все интегральные P-значения каждой из батарей свидетельствуют в ее пользу.

Параметры: Набор тестов $\mathcal{B} = \{K_1, K_2, \ldots, K_q\}$, где q — число тестов в батарее; число фрагментов m; число интервалов группировки k; уровень значимости тестов α; уровень значимости батарей β.

Обозначение: ТОП$[\mathcal{B}, m, k, \alpha, \beta]$.

Входные данные. Последовательность $X = (x_1, \ldots, x_N)$.

Шаг 1. Разбить X на m фрагментов по $n = [N/m]$ битов:

$$X^{(j)} = (x_{(j-1)n+1}, x_{(j-1)n+2}, \ldots, x_{jn}), \quad j = 1, \ldots, m.$$

При таком разбиении последние биты X могут игнорироваться.

Шаг 2. Для $i = 1, \ldots, q$ и $j = 1, \ldots, m$ по батарее тестов $\mathcal{B}$ вычислить наборы P-значений:

$$P_{ij} = K_i(X^{(j)}).$$

Шаг 3. Вычислить интегральные P-значения батареи Бернулли:

$$(P^1_1, \ldots, P^1_q) = \text{Б1}[\alpha](P_{11}, \ldots, P_{1m}, P_{21}, \ldots, P_{2m}, \ldots, P_{q1}, \ldots, P_{qm}).$$

Шаг 4. Вычислить интегральные P-значения батареи хи-квадрат:

$$(P^2_1, \ldots, P^2_q) = \text{Б2}[k](P_{11}, \ldots, P_{1m}, P_{21}, \ldots, P_{2m}, \ldots, P_{q1}, \ldots, P_{qm}).$$

Шаг 5. Найти минимальное P-значение среди интегральных P-значений обеих батарей Б1 и Б2:

$$P_{\min} = \min\{P^1_1, \ldots, P^1_q, P^2_1, \ldots, P^2_q\}.$$

Шаг 6. Возвратить $\mathbf{I}\{P_{\min} < \beta\}$: 0 означает принятие H_0, 1 — отклонение.

Шаг 7. Если блок «Тестирование одной последовательности» используется в составе блока «Тестирование нескольких последовательности», то дополнительно возвратить набор $(P_1^1, \ldots, P_q^1, P_1^2, \ldots, P_q^2)$.

Схема тестирования одной последовательности представлена на рисунке 1.

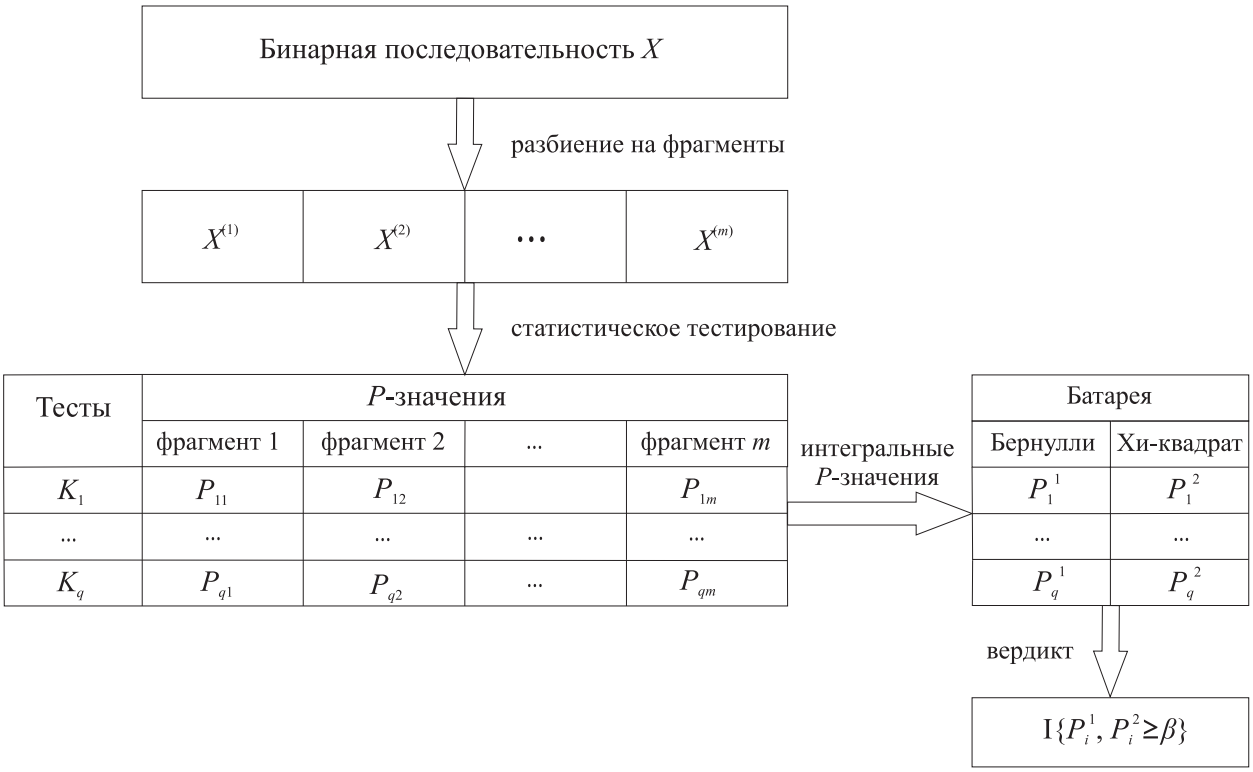

Рисунок 1 — Схема тестирования одной последовательности

5.13 Тестирование нескольких последовательностей

Общие сведения. Пусть тестируется не одна, а несколько последовательностей, и к каждой из них применяется блок ТОП с фиксированным уровнем значимости β. Тогда с ростом числа последовательностей вероятность браковки хотя бы одной из них будет увеличиваться даже при справедливости H_0. Чтобы избежать чересчур жестких вердиктов, процедура принятия решения модифицируется. Во-первых, анализируется уровень браковки каждого из тестов по-отдельности. Гипотеза H_0 отвергается, только если некоторый тест явно свидетельствует против нее. Во-вторых, при обработке уровней браковки отдельных тестов используется дополнительный уровень значимости. Этот уровень уменьшается с ростом числа последовательностей, и, таким образом, требования к уровням браковки ослабляются.

Параметры: Набор тестов $\mathcal{B} = \{K_1, K_2, \ldots, K_q\}$, где q — число тестов в батарее; число фрагментов m; число интервалов группировки k; уровень значимости тестов α; уровень значимости батареи β; уровень значимости прохождения тестов в составе батарей γ.

Обозначение: $\text{ТНП}[\mathcal{B}, m, k, \alpha, \beta, \gamma]$.

Входные данные. Последовательности $X[1], X[2], \ldots, X[M]$ длины N каждая $(M \geqslant 2)$.

Шаг 1. Для $j = 1, \ldots, M$ вычислить:

$$(P_1^1[j], \ldots, P_q^1[j], P_1^2[j], \ldots, P_q^2[j]) = \text{ТОП}[\mathcal{B}, m, k, \alpha, \beta](X[j]).$$

Полученный набор P-значений ($P_i^{1,2}$) называется *статистическим портретом*.

Шаг 2. Для $b = 1, 2$, $i = 1, \ldots, q$ и $j = 1, \ldots, M$ вычислить результаты прохождения теста K_i в составе батарей Б1 и Б2:

$$\Delta_i^b[j] = \mathbf{I}\left\{P_i^b[j] \geqslant \beta\right\}.$$

Шаг 3. Для $b = 1, 2$ и $i = 1, \ldots, q$ вычислить относительные частоты прохождения теста K_i в составе батарей Б1 и Б2:

$$\nu_i^b = \frac{1}{M}\sum_{j=1}^{M} \Delta_i^b[j].$$

Шаг 4. По M и γ построить доверительный интервал $[\Delta_{\min}, \Delta_{\max}]$ для относительных частот прохождения тестов:

$$\Delta_{\min} = 1 - \gamma - 3\sqrt{\frac{\gamma(1-\gamma)}{M}}, \quad \Delta_{\max} = 1 - \gamma + 3\sqrt{\frac{\gamma(1-\gamma)}{M}}.$$

Если полученное значение $\Delta_{\min} < 0$, то его значение следует переопределить: $\Delta_{\min} = 0$. Если $\Delta_{\max} > 1$, то его также следует переопределить: $\Delta_{\max} = 1$.

Например, при $M = 50$ и $\gamma = 0.01$ будет получен доверительный интервал $[0.948, 1]$; при $M = 50$ и $\gamma = 0.001$ — интервал $[0.986, 1]$.

Шаг 5. Найти минимальное значение относительных частот прохождения тестов для обеих батарей:

$$\nu_{\min} = \min_{b,i}\{\Delta_i^b\}.$$

Минимум берется по $b \in \{1, 2\}$ и $i \in \{1, \ldots, q\}$.

Шаг 6. Возвратить $\mathbf{I}\{\nu_{\min} \notin [\Delta_{\min}, \Delta_{\max}]\}$: 0 означает принятие H_0, 1 — отклонение.

Схема тестирования нескольких последовательностей представлена на рисунке 2.

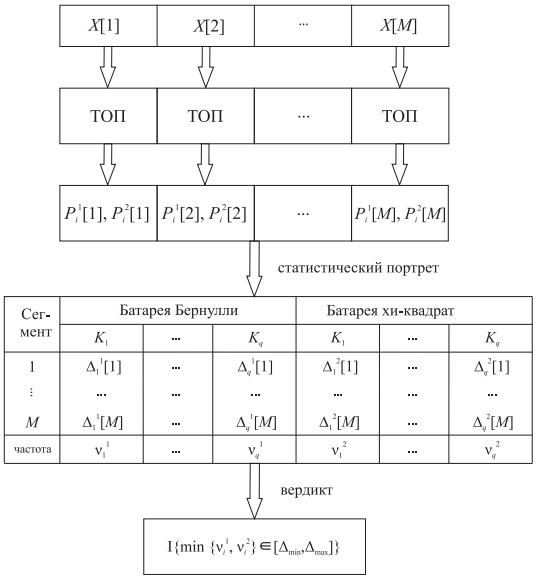

Рисунок 2 — Схема тестирования нескольких последовательностей

5.14 Проведение испытаний

Входные данные. На испытания представляется либо одна последовательность X либо $M \geqslant 2$ последовательностей $X[1], \ldots, X[M]$. Каждая последовательность состоит из 2^{23} или 10×2^{23} битов.

Базовые статистические тесты. Для последовательностей длины 1 Мб используется набор $\mathcal{B}1$ из следущих 8 тестов: МДРН[9], МДРП[11], КПЯ[18], КС, КДС[128], КАЭ[9], КСКП[4, 10], СК-БПФ.

Для последовательностей длины 10 Мб используется набор $\mathcal{B}2$ из следущих 8 тестов: МДРН[17], МДРП[20], КПЯ[22], КС, КДС[10000], КАЭ[19], КСКП[4, 10], СК-БПФ. Тесты определены в п.п. 5.2 — 5.9.

Примечание – При других длительностях последовательностей следует переопределить параметры батарей тестов.

Алгоритм тестрирования последовательностей длины 1 Мб:

Шаг 1. Если на вход подана одна последовательность, то возвратить вердикт

$$\text{ТОП}[\mathcal{B}1, 104, 10, 0.05, 0.0001](X).$$

Шаг 2. Если на вход поданы несколько последовательностей, то возвратить вердикт

$$\text{ТНП}[\mathcal{B}1, 104, 10, 0.05, 0.0001, 0.01](X[1], \ldots, X[M]).$$

Алгоритм тестрирования последовательностей длины 10 Мб:

Шаг 1. Если на вход подана одна последовательность, то возвратить вердикт

$$\text{ТОП}[\mathcal{B}2, 200, 10, 0.05, 0.0001](X).$$

Шаг 2. Если на вход поданы несколько последовательностей, то возвратить вердикт

$$\text{ТНП}[\mathcal{B}2, 200, 10, 0.05, 0.0001, 0.01](X[1], \ldots, X[M]).$$

Приложение А
Форма протокола

Экз. № {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
статистического тестирования выходных последовательностей генератора случайных чисел

Генератор случайных чисел: {Поле 4}

Выходная последовательность:

Имя файла	Число наблюдений	Хэш-значение файла согласно СТБ 34.101.31-2020
...	...	...

1. Проверка независимости и равномерной распределённости

Для выходных последовательностей ГСЧ {Поле 4} гипотеза о независимости и равномерной распределенности выходных битов {Поле 5: выполняется/не выполняется}.

2. Результаты статистического тестирования выходных последовательностей

Тесты (критерии)	Частота прохождения тестов (в %)	
	Батарея Бернулли	Батарея Хи-квадрат
МДРН	{Поле 6}	{Поле 6}
МДРП	{Поле 6}	{Поле 6}
Критерий пустых ящиков	{Поле 6}	{Поле 6}
Критерий серий	{Поле 6}	{Поле 6}
Критерий длинных серий	{Поле 6}	{Поле 6}
Критерий аппроксимации энтропии	{Поле 6}	{Поле 6}
Спектральный критерий	{Поле 6}	{Поле 6}
Критерий скалярного произведения	{Поле 6}	{Поле 6}

Оценка вероятности (частота) прохождения тестов в составе батареи: {Поле 7}.
Эксперт(ы),
{Поле 8} {Поле 9}

В поле 1 указывается номер экземпляра протокола.
В поле 2 указывается номер, однозначно идентифицирующий протокол.
В поле 3 указывается дата составления протокола.
В поле 4 указывается название ГСЧ, как заявлено производителем.
В поле 5 указывается вердикт вынесенный в соответствии с п. 5.14.

В полях 6 таблицы тестирования приводятся результаты проверки статистическими тестами для двух батарей: частота прохождения тестов (в %).

В поле 7 указывается минимальное значение оценок из полей 6.

В полях 8, 9 указываются соответственно должность и Ф.И.О. экспертов.

Библиография

[1] FIPS PUB 140-1. Security requirement for cryptographic modules. — Computer Systems Laboratory NIST, 1994.

[2] FIPS PUB 140-2. Security requirement for cryptographic modules. — Computer Systems Laboratory NIST, 1999.

[3] Geckinli N.G., Apohan M.A. Power spectrum tests of random numbers // Signal Processing. — 2001. — Vol. 81. — P. 1389-1405.

[4] Gustafson H.M. Statistical Analysis of Symmetric Ciphers // Ph.D. thesis, Information Security Research Center, Queensland University of Technology, Queensland, 1996.

[5] L'Ecuyer P., Simard R., Wegenkittl S. Sparse Serial Tests of Uniformity for Random Number Generators // GERAD Report G-98-65, 1998.

[6] Marsaglia G. Keynote Address: A Current View of Random Number Generators // Proceedings of the 16th Symposium on the Interface "Computer Science and Statistics". — Elsevier, 1985.

[7] Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. — CRC Press, 1996.

[8] NIST Special Publication 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

[9] NIST. À statistical test suite for random and pseudorandom number generators for cryptographic applications, Revised: April 2010. `http://csrc.nist.gov`.

[10] Rueppel R.A Analysis and Design of Stream Ciphers — Springer-Verlag Berlin, Heidelberg, 1986.

[11] Rukhin A. , Approximate entropy for testing randomness // Journal of Applied Probability. — 2000. — Vol. 37

[12] Singleton R.C. An Algorithm for Computing the Mixed Radix Fast Fourier Transform // IEEE Transactions on Audio and Electroacoustics. — 1969. — Vol. AU-17, № 2. — P. 93-103.

[13] Soto J. Statistical Testing of Random Number Generators // `http://csrc.nist.gov/rng/`

[14] Soto J. Randomness Testing of the AES Candidate Algorithms // `http://www.nist.gov/aes/`

[15] Soto J., Bassham L. Randomness Testing of the Advanced Encryption Standard Finalist Candidates // `http://www.nist.gov/aes/`

[16] Ивченко Г.И., Иванова Т.В. Статистика в дискретных задачах. Полиномиальная модель. — М.: Московский институт электронного машиностроения, 1990. — 66 с.

[17] Ивченко Г.И., Медведев Ю.И. Математическая статистика. — М.: Высшая школа, 1984. — 248 с.

[18] Кендалл М.Дж., Стьюарт А. Статистические выводы и связи. — М.: Наука, 1973. — 900 с.

[19] Кнут Д.Э. Искусство программирования. Т. 2: Получисленные алгоритмы. — 3-е изд., доп. — Вильямс, 2000. — 830 с.

[20] Кокс Д., Хинкли Д. Теоретическая статистика. — М: Мир, 1978. — 560 с.

[21] Коренева А.М., Фомичев В.М. Статистическое тестирование псевдослучайных последовательностей // Безопасность информационных технологий. — 2016. № 2, с. 36–42.

[22] Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. — 5-е. изд. — М.: Наука, 1984. — 836 с.

[23] Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. — Минск: БГУ, 1999. — 320 с.

[24] Харин Ю.С., Мартиневский А.В. Обнаружение N-мерной равномерности в двоичных последовательностях с использованием экстремальных статистик // Pattern Recognition and Information Processing: сборник трудов 5-ой международной конференции PRIP-99, с. 358-362.

[25] Чистяков С.П. Об определении уровней значимости статистических критериев при их совместном использовании // Труды ИПМИ КарНЦ РАН. — 1999, вып. 1, с. 55-60.