УДК 681.3.06

АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ AIS31

Татьяна Гриненко
Харьковский национальный университет радиоэлектроники

Аннотация: **Рассмотрены требования к генераторам случайных и псевдослучайных чисел. Проанализированы классы уровней оценки AIS31 и возможные области применения генераторов. Дано описание и проведен анализ применяемых статистических тестов.**
Summary: **Requirements to random and pseudorandom number sequences generators are considered. Classes of AIS31 evaluation levels and possible application area of generators are analyzed. The description and analysis of applied statistical tests are given.**
Ключевые слова: **Генератор случайных чисел, источник шума, внутренние случайные числа, дискретизированная последовательность шумового сигнала, статистический тест.**

Введение

Генераторы случайных чисел (ГСЧ) являются одними из основных компонент криптографических систем. Только при использовании ключевых данных, сформированных с применением ГСЧ, могут достигаться заявленные уровни стойкости криптографической защиты информации (КЗИ). ГСЧ формируют необходимую для функционирования криптографических систем ключевую информацию, от качества которой зависит стойкость криптографических преобразований. Поэтому одним из важных и необходимых направлений исследований и практических работ при разработке ГСЧ и генераторов псевдослучайных чисел (ГПСЧ) является разработка методов и средств оценки статистических свойств случайных последовательностей. Статистические показатели имеют важное влияние на общую оценку эффективности ГСЧ. В сущности, статистические показатели и построенные на их основе критерии оценки являются инструментом проверки правильности технических решений построения ГСЧ.

Для решения этих задач в Германии приняты нормативные документы соответственно для оценки ГСЧ AIS 20 [1] и AIS 31 [2]. При их разработке были учтены основные положения и опыт применения федеральных стандартов США FIPS 140-1 [3] и FIPS 140-2 [4].

Задача оценки генераторов случайных чисел возникла из-за необходимости использования при разработке технических решений специальных методов оценки, которые базируются на ряде руководящих принципов.

"Истинные" (аппаратные, физические) генераторы случайных чисел формируют случайные числа, основанные на истинных вероятностных процессах, например, за счет использования шумовых процессов резисторов или диодов. Они используются также для формирования параметров и синхронизирующих последовательностей. Случайность этих чисел является основой ряда криптографических приложений, например, генерация PIN-кодов, криптографических ключей.

При решении задач создания аппаратных ГСЧ, а также ГПСЧ для анализа их случайности применяются статистические методы исследований, которые могут быть в частном случае охарактеризованы их энтропией (средней неопределенностью одиночного случайного числа или последовательности чисел).

Случайные числа уже давно играют важную роль во многих криптографических приложениях. В то же время ITSEC [5] и CC [6, 7] не определяют единых критериев оценки генераторов случайных чисел. Заслуживает внимания AIS31, в котором представлены критерии оценки криптографических свойств генераторов случайных чисел. Анализ показал, что AIS31 базируется на математическо-технической основе AIS20 [1]. Целью настоящей статьи является анализ основных положений AIS31 и возможностей его применения в Украине при разработке ГСЧ.

I Основные понятия и предположения

Физический генератор случайных чисел (ФГСЧ) формирует случайные числа на основе шумового сигнала физического источника шума. Значения, получаемые непосредственно дискретизацией аналогового сигнала шума, называются дискретизированным шумовым сигналом. Внутренними случайными числами будем называть значения, получаемые после дополнительной математической обработки дискретизированной шумовой последовательности. Идеальный генератор случайных чисел выдает независимые случайные числа (СЧ), принимающие всевозможные значения с одинаковой вероятностью. Под *online*-тестами подразумеваются статистические тесты, или, точнее, совокупность правил тестирования, которые применяются при генерации СЧ на основе дискретизированной шумовой

последовательности или для анализа внутренних СЧ при верификации правильности функционирования ФГСЧ. Выявленное в процессе *online* тестирования статистическое несоответствие является основой для блокирования работы ФГСЧ. При этом необходимо полное блокирование работы генератора с того момента, когда дискретизированная шумовая последовательность становится "не случайной". Для описания свойств таких последовательностей можно использовать *энтропию на бит*, которая понимается здесь как частное: энтропия дискретизированного шумового сигнала/ширина бинарного представления дискретизированного шумового сигнала или энтропия внутреннего СЧ/количество бит в двоичном представлении СЧ.

ФГСЧ содержит внутренний физический источник шума. Чаще всего он вырабатывает аналоговый сигнал, который в дальнейшем дискретизируется. Дискретизированный шумовой сигнал при дальнейшей обработке превращается во внутреннюю последовательность случайных чисел. Это делается для улучшения распределения вероятностей дискретизированной последовательности шумовых сигналов. "Хороший" физический источник шума может без дополнительной обработки дискретизированный шумовой сигнал передавать непосредственно в выходной блок. В этом случае последовательность внутренних СЧ соответствует дискретизированной последовательности шумового сигнала. Выходной блок (буфер) синхронизирует непрерывную или апериодичную выдачу внутренней случайной последовательности с выдачей внешней последовательности СЧ (рис. 1). Неопределенность выдаваемой источником шума последовательности СЧ повышается с генерацией каждого СЧ.

ФГСЧ основаны на физических случайных процессах, которые выдают (формируют) наблюдаемые аналоговые величины для цифровой обработки. Процессы, все параметры которых (время, уровень и т. д.) дискретизируются, т. е. ограничиваются конечным числом состояний, обладают в общем случае детерминированными свойствами и подчиняются свойствам детерминированных генераторов случайных чисел (ДГСЧ). На рис. 1 показаны основные элементы ФГСЧ и ДГСЧ, а также процесс генерации начального заполнения для ДГСЧ с применением ФГСЧ. Могут также применяться структуры, использующие комбинацию различных аналоговых источников шума и уже дискретизированных сигналов, применение которых существенно усложняет анализ. Последующая обработка дискретизированного шумового сигнала, как правило, осуществляется опциями. Если она отсутствует, дискретизированный шумовой сигнал совпадает с внутренним СЧ.

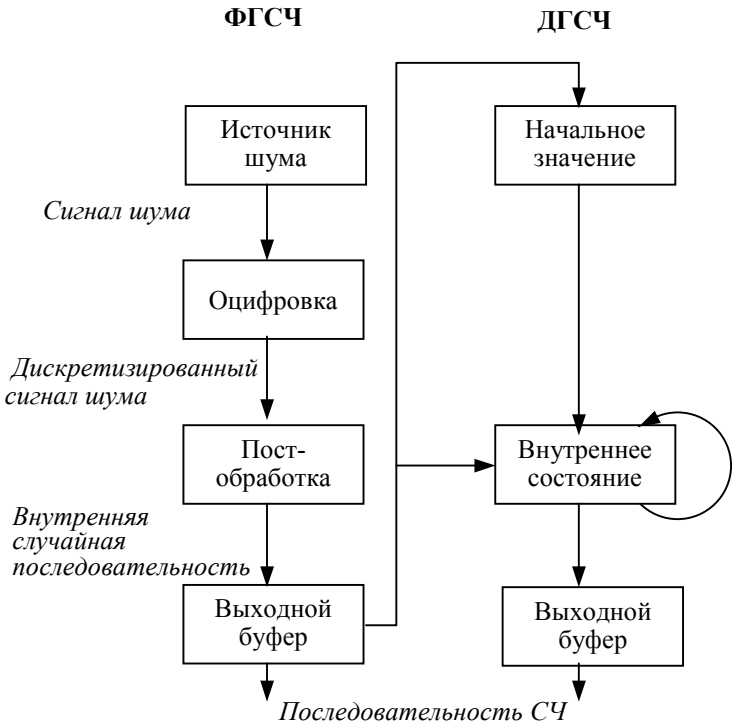

Рисунок 1 – Основные элементы ФГСЧ и ДГСЧ

Описание конечного объекта оценки, областей его применения помогают понимать требуемую среду

защиты и стратегию защиты. В зависимости от уровня безопасности разработчик специфицирует требования к функциональной безопасности. Если уже на этом уровне абстракции генерирование и использование СЧ является рациональным, для ФГСЧ задают классы функциональности [1, 2], например P1 или P2 (с указанием функции безопасности конечного объекта оценки). Зачастую ФГСЧ является только частью конечного объекта. Конечный объект может содержать ГСЧ как комбинацию ФГСЧ для получения начального заполнения и ДГСЧ – для выработки случайной последовательности. Анализ ДГСЧ в этом случае проводится в соответствии с AIS 20 и подтверждается требование C.1 (IV) [1].

II Анализ классов уровней оценки ГСЧ

Оценка ФГСЧ основывается в основном на статистических тестах. На основе различных возможных сценариев атак можно разработать требования к свойствам внешних и соответственно внутренних СЧ. Принимая во внимание эти обстоятельства, в дальнейшем рассматриваются 2 класса функциональности (P1, P2) [2]. Что касается применения, то классы P1 и P2 по существу соответствуют классам К1 – К2 и К3 – К4 AIS20 [1].

Свойство P1 требует статистического различия внутренних СЧ. P2 класс требует, чтобы было практически невозможно определить случайное число, даже если его предшественники или последующие элементы известны. Класс P2 является самым высоким возможным классом в пределах технических требований BSI AIS31 [2].

Требования на соответствие ФГСЧ классу P1.

Для соответствия классу P1 должны выполняться требования P.1d)(i)-P1.d)(vi) [2] в соответствии с механизмами [5] и функциями [6, 7] стойкости.

P.1d)(i) требует, чтобы последовательность случайных векторов, образуемая из внутренних СЧ $r_1, r_2,$K с большой вероятностью являлась попарно различной (тест T0). Для верификации требования P.1d)(ii) внутренние последовательности СЧ $r_1, r_2,$K и их проекции на отдельные биты должны удовлетворять статистическим тестам T1 – T5.

P.1d)(iii) (если стойкость механизмов или функций "средняя" или "высокая"). Если при включении ФГСЧ происходит общий останов источника шума, то этот останов должен быть тотчас же распознан, и после останова не могут быть поданы внешние СЧ.

P.1d)(iv) (если стойкость механизмов или функций "средняя" или "высокая"). Если во время работы ФГСЧ возникает общий останов источника шума, то после останова прекращается выработка случайных величин, производимых внутренней случайной последовательностью. В качестве замены достаточно, чтобы после общего останова источник шума ФГСЧ вел себя для каждой постоянной последовательности сигналов шума как К2-ДГСЧ AIS 20 [1], выходные последовательности которого соответствует предусмотренной цели применения.

P.1d)(v) (если стойкость механизмов или функций "высокая"). Требуемые в P.1d)(i) и P.1d)(ii) свойства должны быть верифицированы при предусмотренных внешних воздействиях (температура, электроснабжение и т. д.), так как они могут влиять на функционирование источника шума.

P.1d)(vi) (если стойкость механизмов или функций "средняя" или "высокая"). ФГСЧ должен содержать *online*-тест, который по внешнему вызову проверяет качество внутренних СЧ.

После запуска аппаратный генератор шума начинает производить плавнорегулируемые блоки необработанных случайных байтов. Для немедленного обнаружения неисправности физического источника шума на старте применяются полные статистические испытания (*online*-тест). Только в случае успеха ФГСЧ доходит до стандартного режима работы и становится доступным приложениям. В стандартном режиме *online*-тест применяется к каждому сгенерированному блоку случайных байтов. Если тест пройден, ФГСЧ возвратится к рабочему режиму. Иначе ФГСЧ будет блокирован, и, следовательно, все запросы, использующие ФГСЧ, будут возвращены с соответствующим кодом ошибки. Во время работы конечного объекта оценки тестирование ФГСЧ должно выполняться непрерывно для проверки правильности его работы.

Возможные применения ФГСЧ P1:

- ✓ открыто передаваемые, непостоянные векторы инициализации (синхропоследовательности) [8];
- ✓ генерация начального состояния для ДГСЧ классов К1 и К2 AIS 20 [1].

Требования на соответствие ФГСЧ классу P2.

ФГСЧ должен принадлежать классу P1 как минимум с такими же механизмами [5] и функциями [6, 7] стойкости.

P2.i)(i) Верификация свойств P1.

P2.d)(vii) Дискретизированные последовательности шумовых сигналов (ДПШС), удовлетворяющие

определенным критериям, должны проходить статистические тесты, которые помимо всего прочего должны исключить многошаговые зависимости. Кроме того, должен быть пройден энтропийный тест T8.

P2.d)(viii) Дополнительная математическая обработка не должна уменьшать энтропию на бит.

P2.d)(ix) (если стойкость механизмов или функций "средняя" или "высокая"). При каждом включении ФГСЧ должны быть удостоверены минимальные статистические свойства ДПШС. До тех пор, пока не закончится статистическое тестирование, СЧ не могут быть выданы.

P2.d)(x) (если стойкость механизмов или функций "средняя" или "высокая"). Если во время работы ФГСЧ произошел общий останов источника шума, должна исключаться выдача случайных чисел, так как соответствующие внутренние случайные последовательности были сгенерированы после останова.

P2.d)(xi) (если стойкость механизмов или функций "средняя" или "высокая"). В работу ФГСЧ должен быть имплементирован *online*-тест, с помощью которого может быть проверено статистическое качество ДПШС. *Online*-тест должен быть вызываем извне или же ФГСЧ должен сам вызывать его. Последнее должно осуществляться постоянно или по крайней мере через регулярные промежутки. *Online*-тест должен распознать в согласованное время незначительные статистические дефекты или ухудшение статистических свойств дискретизированной шумовой последовательности.

P2.d)(xii) (если стойкость механизмов или функций "высокая"). Требуемые в P2.d)(vii) свойства должны быть верифицированы для предусмотренных внешних условий применения (температура, энергоснабжение и т. д.), так как они могут влиять на функционирование источника шума.

P2.d)(xiii) (если стойкость механизмов или функций "высокая"). ФГСЧ должен сам вызывать *online*-тест.

Возможные применения ФГСЧ класса P2:

- ✓ ключи и параметры шифрования;
- ✓ случайное заполнение;
- ✓ пароли.

III Описание и применение статистических тестов

В AIS31 [2] для верификации требований P1.d)(i), (ii), (v) и P2.d(vii) и (xii) используются тесты T0 – T8, приведенные ниже.

Для верификации P1 применяются тесты T0 – T5. Свойства P1.d) (i) и (ii) являются относительно слабыми и должны быть удовлетворены почти для всех физических источников шума. В качестве нулевой гипотезы H_0 предполагается, что тестируемая последовательность СЧ выдается идеальным источником шума.

Тесты T0 – T5 применяются для внутренних СЧ [2]. Если предположить, что последовательности $w_1, ..., w_{2^{\wedge}16}$ или $b_1, ..., b_{20000}$ – выход идеального источника шума, то вероятность отклонения нулевой гипотезы для теста T0 $\approx 2^{-17}$ и для тестов T1 – T5 – $\approx 10^{-6}$.

Тесты T1 – T4 в [2] вместе с обозначениями и границами отклонений взяты из FIPS PUB 140-1 [3].

Для верификации P2 применяются дополнительно тесты T6 – T8.

Тесты T6 – T8 применяются к дискретизированным последовательностям шумовых сигналов [2]. Предполагая, что последовательности $w_1, ..., w_n$ или $b_1, ..., b_{(Q+K)L}$ выдаются идеальным источником шума, вероятности отклонения при выбранных в P2.i) параметрах пренебрежимо малы [2]. Так как дискретизированные последовательности шумовых сигналов реального ФГСЧ всегда имеют статистические дефекты (зависимости и т. д.), границы отклонений выбирают так, чтобы ФГСЧ с допустимыми слабостями прошли бы эти тесты (см. P2.j) [2]).

Для проведения технологического тестирования необходимо сгенерировать аппаратным ГСЧ случайную последовательность *b* длиной *n* = 20000 бит.

Тест T0 Дизъюнктивный тест (Disjunktheitstest).

Осуществляется проверка, что во множестве, которое формируется из не перекрывающихся слов $w_1, ..., w_{2^{\wedge}16}$, где $w_i \in \{0,1\}^{48}$, не существует ни одного последовательного одинакового слова.

Дизъюнктивный тест P.1d)(i) является простейшим критерием проверки пригодности ФГСЧ производить попарноразличные внешние СЧ. Если последовательность проходит этот тест, то свойство P1.d)(i) верифицировано. В противном случае – не верифицировано. Повторное повторение теста недопустимо.

Тест T1 Монобитный тест (Monobittest).

Целью статистического теста является определение, будет ли количество нулей и единиц в

последовательности b таким же, как ожидаемое для случайной последовательности. Пусть n_1 и n_2 обозначают число нулей и единиц в последовательности b, соответственно.

$$n_1(n_2) = \sum_{j=1}^{20000} b_j \ .$$

Если последовательность b_1, …, b_{20000} случайная, то значения n_1 и n_2 должны удовлетворять условию $9654 < n_1\,(n_2) < 10346$.

Если тест не пройден, можно сделать вывод, что в последовательности слишком много нулей или единиц.

Тест Т2 Покер тест (Pokertest).

Пусть m положительное целое число такое, что $\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \times \left(2^m\right)$, и пусть $k = \left\lfloor \frac{n}{m} \right\rfloor$. Разобьем последовательность s на k блоков, которые не перекрываются, длиной m. Пусть n_i – количество блоков i-го типа длиной m, $1 \leq i \leq 2^m$. Целью теста является определение, будут ли блоки длиной m встречаться в последовательности s с такой же частотой, как в случайной последовательности. Во время тестирования рассчитывается статистика

$$X_1 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k \ ,$$

которая приблизительно подчиняется χ^2-распределению с 2^m–1 степенями свободы. Статистический параметр, который задается уравнением, вычисляется для m = 4. Статистика должна удовлетворять условию $1{,}03 < X_3 < 57{,}4$.

Тест Т3 Тест серий (Runtest).

Под серией понимается последовательность одинаковых символов, т. е. последовательность, состоящая из последовательных единиц или нулей. Суть теста заключается в том, что на заданной длине последовательности, которая тестируется, осуществляется подсчет серий длиной 1, 2, 3, 4, 5, 6 элементов (серии длиной более чем 6 элементов рассматриваются как серии длиной 6).

Целью теста серий является определение, будет ли количество серий единиц (или нулей) разной длины в двоичной последовательности таким же, как ожидаемое для случайной последовательности. Если последовательность случайная, то количество серий каждой длины должно находиться в интервалах, приведенных в таблице 1.

Таблица 1 – Необходимые интервалы для теста серий в зависимости от длины серии

Длина серии	Необходимый интервал
1	2267 – 2733
2	1079 –1421
3	502 – 748
4	223 – 402
5	90 – 223
≥ 6	90 – 233

Тест Т4 Тест длин серий (Long Runtest)

Суть теста заключается в проверке максимальной длины серии из одинаковых элементов. Если последовательность случайная, то максимальная длина серии не должна превышать значения 34. (Вероятность события, которое заключается в появлении серии такой длины, очень мала).

Тест Т5 Автокорреляционный тест (Autokorrelationstest)

Этот тест рассчитывает корреляцию между битами последовательности и ее сдвигами.

$$Z_\tau = \sum_{j=1}^{5000} \left(b_j \oplus b_{j+\tau}\right),$$

где b_j – j-й бит; τ – степень 2, т. е. 2, 4, 8, 16, 32, 64 и т. д. до 4096. Тест считается пройденным, если для всех τ выполняется

$$2326 < Z_\tau < 2674 \, .$$

Цель теста – проверка корреляции между последовательностью s и ее не циклическими сдвигами.

Пусть d фиксированное целое число, $1 \le d \le \lfloor n/2 \rfloor$. Количество бит в последовательности s, которые не совпадают с их d-сдвигом, рассчитывается как

$$A(d) = \sum_{i=0}^{n-d-1} s_i \oplus s_{i+d} .$$

Статистика

$$X_2 = 2\left(A(d) - \frac{n-d}{2} \right) \Big/ \sqrt{n-d}$$

имеет распределение, близкое к стандартному нормальному распределению $N(0,1)$. Значения статистики X_2 должны находиться в интервале [– 4,7534; 4,7534]. Для длин n = {64, 128, 192, 256, 512, 768, 1024, 2048, 4096, 8192, 16384} осуществляется тестирование для всех $1 \le d \le \lfloor n/2 \rfloor$.

Тест Т6 Тест проверки равномерного закона распределения (Gleichverteilungstest)

Последовательность $w_1,\ldots,w_n \in \{0,1\}^k$ удовлетворяет этому тесту с параметрами (k,n,a), если выполнено

$$\frac{1}{n} \cdot \left| j \le n \mid w_j = x \right| \in \left[2^{-k} - a,\ 2^{-k} + a \right],\ x \in \{0,1\}^k \qquad (1)$$

Замечание: для k=1 выражение (1) упрощается

$$\frac{1}{n} \cdot \left| j \le n \mid w_j = 1 \right| \in \left[2^{-k} - 0{,}5,\ 2^{-k} + 0{,}5 \right].$$

Если к тому же n=20000 и a=0.0173, то этот тест соответствует монобитному тесту Т1. По сути, этот тест позволяет проверить выполняется ли монобитный тест на последовательностях $k \le n$.

Тест Т7 Сравнительный тест для полиномиальных распределений (Vergleichstest für Multinomialverteilungen).

Для каждого $i \in \{1,\ldots,h\}$ берут n-элементную выборку значений $w_{i1},\ldots,w_{in}$ из множества $\{0,1,\ldots,s\text{-}1\}$. Нулевая гипотеза говорит о том, что полиномиальное распределение лежащих в основе отдельных выборок идентично. Пусть для $t \in \{0, 1, \ldots, s\text{-}1\}$ $f_i[t] := \left| \{ j : w_{ij} = t \} \right|$. Обозначим $p_t := \left(f_1[t] + \ldots + f_h[t] \right) / (hn)$ усредненную по всему множеству выборок относительную частоту появления значения t. Для нулевой гипотезы тестируемая величина $\sum_{i=1,\ldots,h} \sum_{t=0,\ldots,s-1} \left(f_i[t] - np_t \right)^2 / np_t$ приблизительно подчиняется χ^2-распределению с $(h-1)(s-1)$ степенями свободы ([9], тест Т6).

Тест Т8 Энтропийный тест (Entropietest)

Статистика энтропийного теста – мера согласованности наблюдаемого значения энтропии источника с тем, которое теоретически ожидается для случайного источника.

Энтропийный тест проводится согласно Coron [10]. Битовая последовательность $b_1,\ldots,b_{(Q+K)L}$ разбивается на не перекрывающиеся слова $w_1,\ldots,w_{Q+K}$ длиной L. Обозначим A_n расстояние от w_n к его равнозначному предшественнику, а именно

$$A_n = \begin{cases} n & \text{если не существует } i \le n \text{ при } w_n = w_{n-i}; \\ \min\{ i \mid i \ge 1,\ w_n = w_{n-i} \} & \text{в других случаях.} \end{cases}$$

Тестируемая величина $f: \{0,1\}^{(Q+K)L} \to R$ для Coron-теста [10] задается следующим образом

$$f_c(s) = \frac{1}{K} \sum_{n=Q+1}^{Q+k} g(A_n) \quad ,$$

где $g(i) = \frac{1}{\log(2)} \sum_{k=1}^{i-1} \frac{1}{k}$.

Для $i \ge 23$ сумма в выражении для $g(i)$ может быть оценена с ошибкой $<10^{-8}$ как

$$\sum_{j=1}^{n} \frac{1}{j} = \log n + \gamma + \frac{1}{2n} + \frac{1}{12n^2} + O\left(\frac{1}{n^4} \right),\ \gamma = 0{,}577216 \text{ (постоянная Эйлера).}$$

Для стационарного двузначного случайного источника с конечной памятью математическое ожидание тестируемой величины f_c тесно связано с приростом энтропии на L-битовый блок. Если источник шума независимый, равенство выполняется. Для идеального ИШ распределение тестируемой величины f_c достаточно хорошо аппроксимируется нормальным распределением с математическим ожиданием μ_c и дисперсией $(\sigma_c)^2$

$$\sigma_c = \left(d(L) + \frac{e(L) 2^L}{K} \right) \sqrt{Var(g(A_n))/K} \cdot$$

Таблица 2 – Значения, справедливые для идеального ИШ [10]

L	Variance Var($g(A_n)$)	$d(L)$	$d(L)$
3	2.5769918	0.3313257	0.4381809
4	2.9191004	0.3516506	0.4050170
5	3.1291382	0.3660832	0.3856668
6	3.2547450	0.3758725	0.3743782
7	3.3282150	0.3822459	0.3678269
8	3.3704039	0.3862500	0.3640569
9	3.3942629	0.3886906	0.3619091
10	3.4075860	0.3901408	0.3606982
11	3.4149476	0.3909846	0.3600222
12	3.4189794	0.3914671	0.3596484
13	3.4211711	0.3917390	0.3594433
14	3.4223549	0.3918905	0.3593316
15	3.4229908	0.3919740	0.3592712
16	3.4233308	0.3920198	0.3592384
бесконечно	3.4237147	0.3920729	0.3592016

Выводы

Таким образом, используя тесты T0 – T5 можно верифицировать ГСЧ на случайность с уровнем P1. Используя тесты T0 – T8 можно верифицировать ГСЧ на случайность с уровнем P2. Тесты T6 – T8 чувствительны к возможным "слабостям". Проведенный анализ подтвердил, что заявляемые уровни P1 и P2 могут применяться во многих приложениях. Они прошли тестирование и испытания и приняты в Германии в качестве базовых рекомендаций для оценки ГСЧ. Поэтому заслуживают серьезного рассмотрения и применения.

Литература: ***1.*** *Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.* ***2.*** *Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.* ***3.*** *Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994.* ***4.*** *Federal Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999.* ***5****. Information Technology Security Evaluation Criteria (ITSEC); Provisional Harmonised Criteria, Version 1.2, June 1991.* ***6.*** *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements. 1999.* ***7.*** *ISO/IEC 15408: – Information technology – Security techniques – Evaluation criteria for IT security. Part 2. 1999.* ***8.*** *Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования ГОСТ 28147-89. Гос. Ком. СССР по стандартам, М., 1989.* ***9.*** *G. K. Kanji: 100 Statistical Tests. Sage Publications, London 1995.* ***10.*** *J.-S. Coron: On the Security of Random Sources, Gemplus' Corporate Product R&D Division, Technical Report IT02-1998. Auch in: H. Imai und Y. Zheng (Hrsg.): Public Key Cryptography. Second International Workshop on Practice and Theory in Public Key Cryptography, PKC'99. Springer, Lecture Notes in Computer Science 1560, Berlin 1999, 29-42.*