Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056:519.254

КИЕВЕЦ
Наталья Григорьевна

АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск 2019

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Научный руководитель — **Корзун Александр Иванович**, кандидат технических наук, доцент, директор закрытого акционерного общества «Центр новых интеллектуальных интегрированных систем»

Официальные оппоненты: **Бобов Михаил Никитич**, доктор технических наук, профессор, главный специалист по защите информации открытого акционерного общества «АГАТ – системы управления» – управляющая компания холдинга «Геоинформационные системы управления»

Утин Леонид Львович, кандидат технических наук, доцент, начальник кафедры связи учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Оппонирующая организация — Научно-исследовательское учреждение «Институт прикладных физических проблем имени А. Н. Севченко» Белорусского государственного университета

Защита состоится «20» июня 2019 г. в 14.00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, e-mail: dissovet@bsuir.by, тел. 293-89-89.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан « 20 » мая 2019 г.

Ученый секретарь
совета по защите диссертаций
кандидат технических наук, доцент О. В. Бойправ

ВВЕДЕНИЕ

В настоящее время в Республике Беларусь реализуется комплекс мер по созданию информационно-коммуникационной инфраструктуры, позволяющей оказывать электронные услуги потребителям на основе персонифицированной электронной пластиковой карты (ЭПК) как идентификатора личности и биометрического документа. ЭПК обладает рядом достоинств: защищенная от внешнего вмешательства компоновка интегральной схемы; процессор карты способен выполнять криптопреобразования, не вынося вычисления за пределы карты; данные могут храниться в недоступной для чтения области энергонезависимой памяти.

Неотъемлемым компонентом большинства ЭПК является генератор случайных чисел (ГСЧ), используемый при выработке криптографических ключей для целей защиты информации. Однако качество его работы может изменяться в ходе эксплуатации ЭПК, что может быть вызвано дефектами изготовления интегральной схемы, условиями использования и старением элементов. В связи с этим необходимо периодически выполнять статистическое тестирование ГСЧ, которое состоит из процессов генерирования необходимого количества случайных последовательностей (СП), расчета статистических характеристик сгенерированных СП и сравнения эмпирических распределений тестовых статистик, рассчитанных для каждой СП, с теоретическими распределениями при использовании критерия согласия.

Для анализа статистических свойств СП применяются системы тестов, которые требуют достаточно длинных СП, длины которых на несколько порядков превышают длины реально используемых криптографических ключей. Однако ГСЧ ЭПК вырабатывают СП только фиксированных длин, как правило, связанных с длинами ключей, что обусловлено приложениями ЭПК. В связи с этим актуальной является задача разработки методики тестирования, учитывающей особенности функционирования ГСЧ ЭПК, для оценки качества его работы на основе двухуровневого тестирования вырабатываемых СП. Работа посвящена вопросам разработки аппаратно-программного средства (АПС) статистического тестирования ГСЧ ЭПК, реализующего двухуровневое тестирование генерируемых СП и обеспечивающего формирование массивов СП, свойства которых соответствуют свойствам равномерно распределенных случайных последовательностей (РРСП).

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами, темами

Диссертационная работа выполнялась на инициативной основе, тема работы соответствует направлению 5 «Информатика и космические исследования» Приоритетных направлений научных исследований Республики Беларусь на 2016–2020 годы, утвержденных Постановлением Совета Министров Республики Беларусь 12.03.2015 № 190.

Также тема работы соответствует пунктам «средства технической и криптографической защиты информации» и «технологии и системы электронной идентификации» направления 7 «Информационно-коммуникационные и авиакосмические технологии» Приоритетных направлений научно-технической деятельности в Республике Беларусь на 2016–2020 годы, утвержденных Указом Президента Республики Беларусь 22.04.2015 № 166.

Цель и задачи исследования

Целью диссертационной работы является разработка аппаратно-программного средства статистического тестирования генераторов случайных чисел электронных пластиковых карт для оценки качества их работы в диапазоне рабочих температур и формирования массивов случайных последовательностей, свойства которых соответствуют свойствам равномерно распределенных случайных последовательностей. Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать методы статистического тестирования генераторов случайных чисел для криптографических приложений на основе анализа характеристик вырабатываемых случайных последовательностей.
2. Разработать методику статистического тестирования ГСЧ ЭПК, позволяющую оценивать качество работы генератора случайных чисел с использованием двухуровневого тестирования и формировать массивы случайных последовательностей со свойствами РРСП.
3. Разработать и реализовать программно в среде MATLAB алгоритм тестирования генераторов случайных чисел, обеспечивающий получение качественных характеристик сгенерированных случайных последовательностей для принятия решения о пригодности ГСЧ для применения в ЭПК.
4. Разработать структуру и создать аппаратно-программное средство статистического тестирования ГСЧ ЭПК, обеспечивающее получение и анализ случайных последовательностей в диапазоне рабочих температур ЭПК на основе предложенной методики статистического тестирования ГСЧ ЭПК.
5. Провести экспериментальные исследования качества работы ГСЧ ЭПК

с использованием разработанной методики статистического тестирования и созданного аппаратно-программного средства.

Научная новизна

1. Получены теоретические распределения тестовых статистик и вероятностей превышения возможных значений тестовых статистик при длинах случайных последовательностей 128 и 256 бит для:

– частотного теста;

– частотного теста в подпоследовательностях;

– теста на подпоследовательности одинаковых бит;

– теста на самые длинные подпоследовательности единиц в блоках;

– теста серий;

– теста аппроксимированной энтропии;

– теста кумулятивных сумм,

что позволяет применить вышеуказанные тесты для статистического анализа случайных последовательностей с длинами 128 и 256 бит при двухуровневом тестировании.

2. Теоретически доказана и экспериментально подтверждена эквивалентность одной из статистик теста серий и статистики теста аппроксимированной энтропии при стремлении длины последовательности к бесконечности, что позволяет для случайных последовательностей длиной более 1 млн бит не применять тест аппроксимированной энтропии при использовании теста серий.

Положения, выносимые на защиту

1. Методика статистического тестирования генераторов случайных чисел электронных пластиковых карт, включающая:

– тестирование последовательности, составленной из всех сгенерированных случайных последовательностей, которое позволяет оценить качество работы генератора с использованием любого статистического теста;

– двухуровневое тестирование случайных последовательностей, что позволяет оценить статистические свойства каждой сгенерированной последовательности, предназначенной для использования в качестве криптографического ключа, и проверить равновероятность вырабатываемых генератором случайных последовательностей,

отличающаяся использованием двухуровневого тестирования случайных последовательностей с длинами, равными длинам практически используемых ключей.

2. Алгоритмы нахождения теоретических распределений тестовых статистик и вероятностей превышения возможных значений тестовых статистик:

– частотного теста;
– частотного теста в подпоследовательностях;
– теста на подпоследовательности одинаковых бит;
– теста на самые длинные подпоследовательности единиц в блоках;
– теста серий;
– теста аппроксимированной энтропии;
– теста кумулятивных сумм,

позволяющие выполнить двухуровневое тестирование случайных последовательностей с длинами, равными длинам практически используемых ключей.

3. Структура и программное обеспечение аппаратно-программного средства статистического тестирования генераторов случайных чисел электронных пластиковых карт, позволяющего оценивать качество работы генераторов случайных чисел в диапазоне рабочих температур, формировать массивы случайных последовательностей со свойствами равномерно распределенных СП в соответствии с предложенной методикой.

Личный вклад соискателя ученой степени

Основные научные и практические результаты диссертационной работы, а также положения, выносимые на защиту, разработаны и получены лично автором. В совместно опубликованных работах автору принадлежат: разработка методики статистического тестирования ГСЧ ЭПК, получение теоретических распределений тестовых статистик и вероятностей превышения возможных значений тестовых статистик частотного теста, частотного теста в подпоследовательностях, теста на подпоследовательности одинаковых бит, теста на самые длинные подпоследовательности единиц в блоках, теста серий, теста аппроксимированной энтропии и теста кумулятивных сумм; теоретическое доказательство и экспериментальное подтверждение эквивалентности одной из статистик теста серий и статистики теста аппроксимированной энтропии при стремлении длины последовательности к бесконечности; разработка АПС статистического тестирования ГСЧ ЭПК, реализующего предлагаемую методику. Вклад научного руководителя кандидата технических наук, доцента А. И. Корзуна заключается в постановке целей и задач исследований, кандидата технических наук, доцента Г. И. Мельянца – в обсуждении результатов, аспиранта А. М. Ярука, студентов А. В. Босака и Э. В. Машковича – в подготовке и обработке данных для статистического тестирования ГСЧ по тестам NIST. Магистранту П. Б. Капле принадлежат результаты, не вошедшие в диссертацию.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях и семинарах: 8-я, 11-я, 12-я, 13-я, 14-я Белорусско-российские научно-технические конференции «Технические средства защиты информации» (Браслав, 2010 г., Минск, 2013, 2014, 2015, 2016 гг.); 15-я, 16-я, 17-я, 18-я, 19-я, 20-я, 21-я, 22-я Международные научно-технические конференции «Современные средства связи» (Минск, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017 гг.); Международные научно-технические семинары «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных» (Минск, 2011, 2012 гг.); Республиканский научный семинар «Математическое моделирование сложных систем, анализ данных и защита информации» (Минск, 2015 г.); 30-я Международная научно-техническая конференция «Математические методы в технике и технологиях» (Минск, 2017 г.); Международная научная конференция «Информационные технологии и системы» (Минск, 2017 г.).

Опубликование результатов диссертации

Результаты исследований представлены в 25 опубликованных работах, в том числе в 6 статьях в рецензируемых научных журналах, включенных в Перечень научных изданий Республики Беларусь для опубликования результатов диссертационных исследований, 1 статье в сборнике научных трудов, 13 работах в сборниках материалов научных конференций и семинаров, 5 работах в сборниках тезисов докладов научных конференций. Общий объем опубликованных работ, соответствующих пункту 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, составляет 2 авторских листа.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и приложений. Общий объем диссертационной работы составляет 195 страниц, из них 110 страниц текста, 37 рисунков на 18 страницах, 24 таблицы на 11 страницах, библиографический список из 138 наименований, включая 25 собственных публикаций автора, на 13 страницах, 7 приложений на 37 страницах.

ОСНОВНАЯ ЧАСТЬ

В **первой главе** проведен анализ методов получения СП и методов их статистического тестирования, позволяющих оценить качество работы ГСЧ,

вырабатывающих СП. Анализ методов показал, что для оценки качества работы ГСЧ ЭПК целесообразно применение двухуровневого тестирования СП, которое позволяет не только оценить статистические свойства единичных СП, но и сделать выводы о свойствах ГСЧ в целом. В случае применения двухуровневых тестов к СП с длинами, равными длинам ключей, появляется возможность проверить соответствие свойств каждой СП, предназначенной для использования в качестве ключа, свойствам РРСП.

Установлено, что наиболее известные системы тестирования не позволяют осуществлять статистический анализ СП с длинами, равными длинам практически используемых ключей, поскольку требуют достаточно длинных последовательностей: длиной 20 тыс. бит – для тестов стандарта FIPS 140, от 100 тыс. бит – для системы CRYPT-X, от 1 млн бит – для системы NIST. Для проверки свойств СП длиной, равной длине ключа, требуется формирование набора тестов, допускающих указанные длины СП. На основе анализа литературных источников предложена классификация статистических тестов для реализации цели и задач диссертации.

Во **второй главе** разработано аппаратно-программное средство, позволяющее извлекать из ЭПК СП заданной длины, осуществлять их тестирование для оценки качества работы ГСЧ в диапазоне рабочих температур и на основе результатов тестирования формировать массивы СП, которые по статистическим свойствам соответствуют свойствам РРСП. Для создания данного средства был решен ряд задач:

– реализован метод формирования массивов данных для тестирования ГСЧ ЭПК в диапазоне рабочих температур, позволяющий извлекать из ЭПК требуемое количество СП с длинами, которые допускает операционная система карты, и хранить полученные массивы;

– разработана методика статистического тестирования ГСЧ ЭПК;

– выбрана система статистических тестов для оценки свойств СП.

Разработанная методика статистического тестирования ГСЧ ЭПК включает следующие этапы.

1. Формирование набора тестов № 1 $\{T_{1i}\}$ для тестирования длинной битовой последовательности, составленной из всех сгенерированных СП ($i = \overline{1, X}$, где X – число тестов в наборе № 1).

2. Формирование набора тестов № 2 $\{T_{2j}\}$ для тестирования отдельных СП ($j = \overline{1, Y}$, где Y – число тестов в наборе № 2).

3. Генерация N СП, каждая из которых имеет длину n.

Длина n определяется системой шифрования. Количество СП N должно удовлетворять условиям [4]

$$\begin{cases} N \geq n_{\min} / n, \\ N \geq N_{\min} = \left\lceil \dfrac{(3Y\sqrt{\alpha 1(1-\alpha 1)} + \sqrt{9Y^2\alpha 1(1-\alpha 1) + 4(1-\alpha 1Y)N_{\text{тр}}})^2}{4(1-\alpha 1Y)^2} \right\rceil, \end{cases}$$

где $n_{\min}$ – минимальная длина последовательности ε для тестов набора № 1;

$N_{\min}$ – минимальное количество сгенерированных СП, которое обеспечит требуемое количество $N_{\text{тр}}$ СП со свойствами РРСП после успешного прохождения всех этапов тестирования;

$\alpha 1$ – уровень значимости для тестов наборов № 1 и № 2.

4. Формирование непрерывной битовой последовательности ε путем побитной записи сгенерированных СП в поток данных.

5. Тестирование последовательности ε по тестам набора № 1, в результате которого получается массив значений $P_T : \{p_{Ti}\}$, где p_{Ti} – вероятность превышения статистикой теста T_{1i} значения, полученного экспериментально, $i = \overline{1, X}$.

6. Оценка результатов тестирования в соответствии с этапом 5. Если хотя бы один тест набора № 1 не пройден, т. е. не выполняется логическое условие $p_{Ti} \geq \alpha 1$ при всех $i = \overline{1, X}$, то осуществляется переход к этапу 3. Если выполняется условие $p_{Ti} \geq \alpha 1$ для всех $i = \overline{1, X}$, исследование продолжается.

7. Тестирование каждой СП по тестам набора № 2, в результате которого получается массив $\{p_{Tkj}\}$ значений вероятности P_T, где p_{Tkj} – вероятность превышения статистикой теста T_{2j} значения, полученного экспериментально при тестировании *k*-й СП, $k = \overline{1, N}$, $j = \overline{1, Y}$.

8. Проверка соответствия эмпирических распределений значений $\{p_{Tkj}\}$ теоретическим распределениям с применением критерия согласия «хи-квадрат». Для каждого теста T_{2j} рассчитывается значение p_{0j} вероятности P_0, характеризующей степень соответствия эмпирического распределения значений $\{p_{Tkj}\}$ теоретическому распределению. При выполнении логического условия $p_{0j} \geq \alpha 2$, где $\alpha 2$ – уровень значимости, для всех $j = \overline{1, Y}$, выполняется переход к следующему этапу. В противном случае выполняется переход к этапу 3.

9. Формирование массива СП, успешно прошедших все тесты набора № 2.

На рисунке 1 представлена блок-схема алгоритма, реализующего предложенную методику статистического тестирования ГСЧ ЭПК, в которой в основу наборов № 1 и № 2 легла система тестов NIST. Алгоритм реализован в виде файл-программы в системе MATLAB.

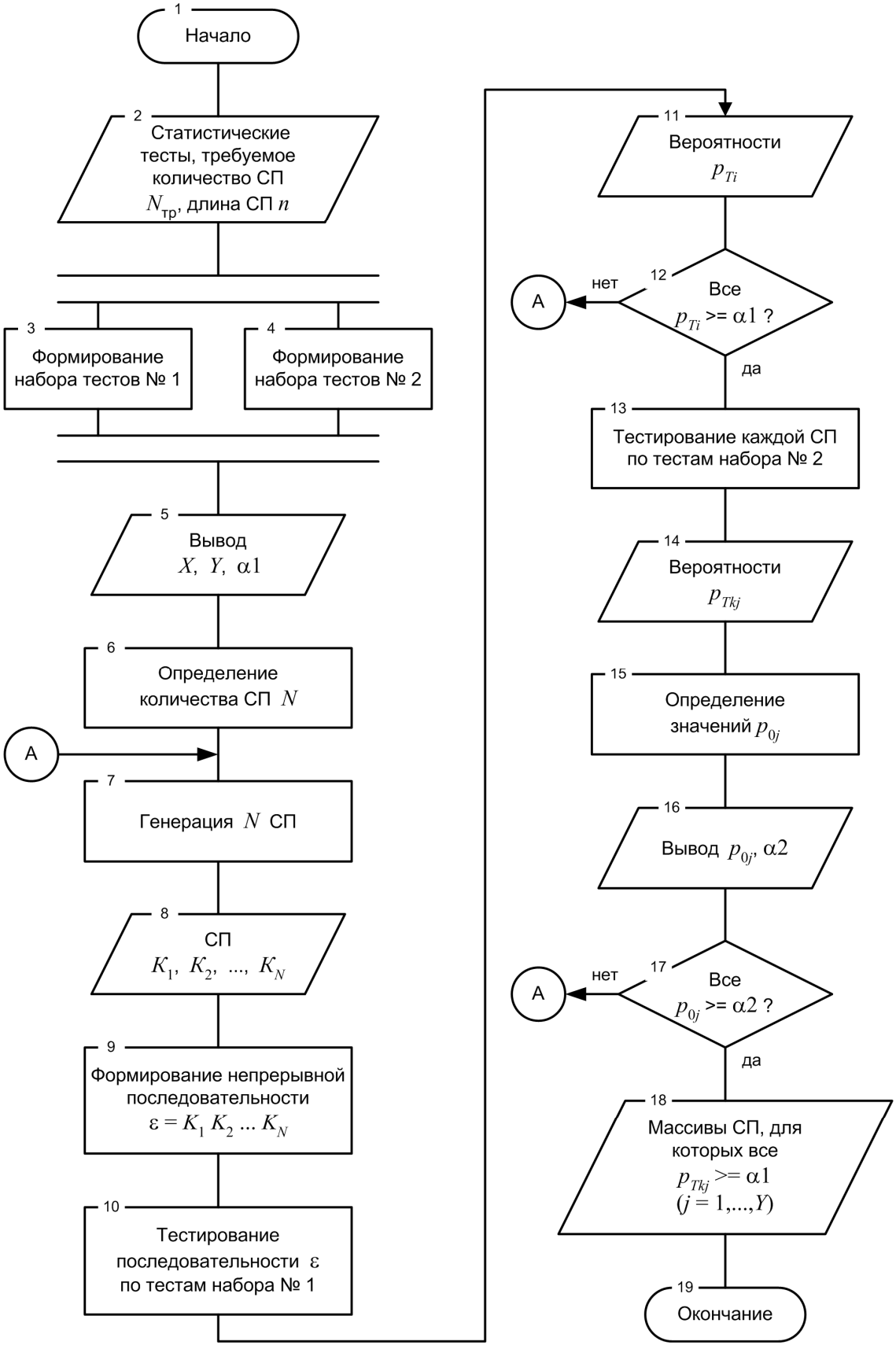


Рисунок 1. – Блок-схема алгоритма, реализующего методику статистического тестирования ГСЧ ЭПК

Установлено, что одна из статистик теста серий системы NIST эквивалентна статистике теста аппроксимированной энтропии при стремлении длины последовательности к бесконечности [2]. Эквивалентность подтверждается теоретически при сопоставлении статистики теста серий

$$\nabla\psi^2_{m1} = \psi^2_{m1} - \psi^2_{m1-1} = \frac{2^{m1}}{n}\sum_{k=0}^{2^{m1}-1} w_k^2 - \frac{2^{m1-1}}{n}\sum_{i=0}^{2^{m1-1}-1} v_i^2, \qquad (1)$$

где $m1$ и $(m1-1)$ – длины пересекающихся битовых серий;

w_k – число появлений в последовательности серии k-го вида длиной $m1$;

v_i – число появлений в последовательности серии i-го вида длиной $(m1-1)$,

со статистикой теста аппроксимированной энтропии с параметром $m = m1-1$:

$$\chi^2 = 2n(\ln 2 - \varphi^{(m)} + \varphi^{(m+1)}) = 2n(\ln 2 - \varphi^{(m1-1)} + \varphi^{(m1)}), \qquad (2)$$

где $\varphi^{(m1-1)} = \sum_{i=0}^{2^{m1-1}-1} \frac{v_i}{n}\ln\left(\frac{v_i}{n}\right)$, $\varphi^{(m1)} = \sum_{k=0}^{2^{m1}-1} \frac{w_k}{n}\ln\left(\frac{w_k}{n}\right)$.

После замены в (2) величин $\varphi^{(m1-1)}$ и $\varphi^{(m1)}$ эквивалентными при $n \to \infty$ соотношениями $\varphi^{(m1-1)} \sim -(m1-1)\ln 2 + \frac{2^{m1-1}}{2n}\sum_{i=0}^{2^{m1-1}-1} Z_i^2$ и $\varphi^{(m1)} \sim -m1\cdot\ln 2 + \frac{2^{m1}}{2n}\sum_{k=0}^{2^{m1}-1} Y_k^2$,

где $Z_i = \sqrt{n}\left(\frac{v_i}{n} - \frac{1}{2^{m1-1}}\right)$, $Y_k = \sqrt{n}\left(\frac{w_k}{n} - \frac{1}{2^{m1}}\right)$, получаем

$$\chi^2 = 2n\left(\ln 2 + (m1-1)\ln 2 - \frac{2^{m1-1}}{2n}\sum_{i=0}^{2^{m1-1}-1} Z_i^2 - m1\cdot\ln 2 + \frac{2^{m1}}{2n}\sum_{k=0}^{2^{m1}-1} Y_k^2\right) =$$

$$= \frac{2^{m1}}{n}\sum_{k=0}^{2^{m1}-1} w_k{}^2 - \frac{2^{m1-1}}{n}\sum_{i=0}^{2^{m1-1}-1} v_i{}^2 = \nabla\psi^2_{m1}.$$

Так как для обоих тестов статистики имеют распределение «хи-квадрат» с одинаковым числом степеней свободы, получаем равные значения вероятностей P_T. Поскольку тест серий предусматривает вычисление помимо статистики (1) еще одной статистики, то он поглощает тест аппроксимированной энтропии.

Полученные результаты позволяют исключить тест аппроксимированной энтропии из набора тестов № 1. Результаты не являются достаточными в отношении тестов набора № 2, поэтому в нем данный тест сохранен.

Исходя из требований к минимальной длине проверяемой последовательности, в набор № 1 включены все тесты системы, за исключением теста аппроксимированной энтропии, а в набор № 2 – семь тестов системы NIST, для которых минимальная длина СП не превышает 100 бит. Оба набора реализованы в файл-программе Statistical_testing в системе MATLAB, что позволяет проводить исследования, задавая параметры тестирования по

требованию. Дополнительно файл-программа Statistical_testing позволяет проводить исследования с использованием статистических тестов FIPS 140-2.

При совместном использовании метода формирования массивов данных для тестирования ГСЧ ЭПК и системы MATLAB со встроенной файл-программой Statistical_testing создано АПС статистического тестирования ГСЧ ЭПК. Структурная схема АПС представлена на рисунке 2.

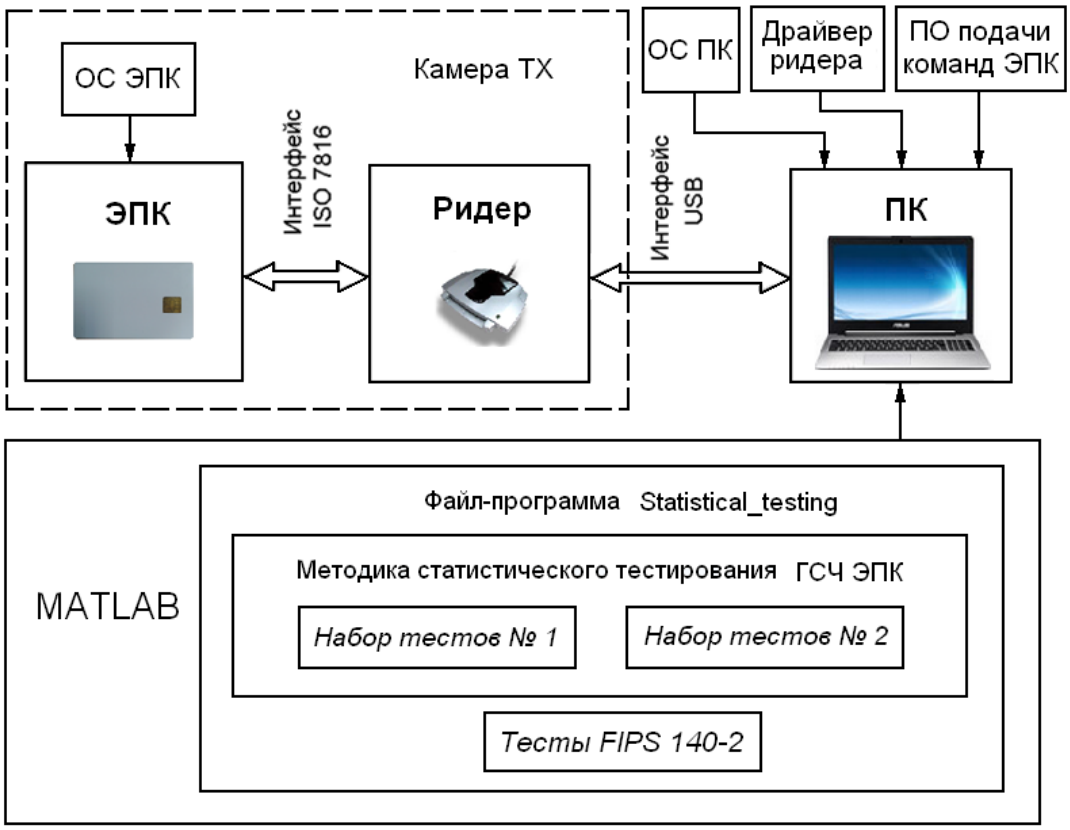


Рисунок 2. – Структурная схема АПС статистического тестирования ГСЧ ЭПК

При формировании массивов данных для тестирования ГСЧ ЭПК в диапазоне рабочих температур используется ЭПК, ридер, персональный компьютер (ПК), содержащий программное обеспечение (ПО) подачи команд ЭПК, и камера ТХ (тепло – холод) для обеспечения требуемой температуры работы ЭПК. Камера ТХ не используется при комнатной температуре.

В **третьей главе** показано, что применение равномерного распределения в качестве теоретического распределения значений P_T при двухуровневом тестировании СП длиной 128 и 256 бит по частотному тесту, частотному тесту в подпоследовательностях, тесту на подпоследовательности одинаковых бит, тесту на самые длинные подпоследовательности единиц в блоках, тесту серий, тесту аппроксимированной энтропии и тесту кумулятивных сумм может привести к неверным выводам о качестве работы ГСЧ ЭПК. Найдены теоретические распределения тестовых статистик S вышеперечисленных семи

тестов и вероятностей P_T превышения возможных значений статистик в соответствии с алгоритмом, представленном на рисунке 3.

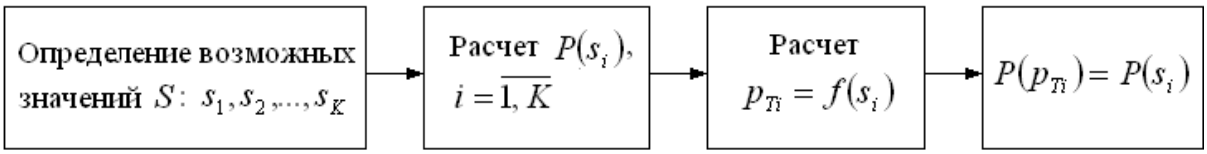


Рисунок 3. – Алгоритм нахождения теоретических распределений тестовых статистик и вероятностей превышения их возможных значений

В частотном тесте рассчитывается статистика $S = |S_n| / \sqrt{n}$, где S_n – разность числа элементов «1» и числа элементов «0», n – длина СП. Возможные значения S: $s_1 = 0$, $s_2 = 2/\sqrt{n}$, $s_3 = 4/\sqrt{n}\,4$, …, $s_{n/2+1} = \sqrt{n}$. Получены выражения для расчета вероятностей $P(p_{Ti}) = P(s_i)$ [3]:

$$P(p_{T1}) = \frac{n!}{(n/2)!\cdot(n/2)!\cdot 2^n},\ P(p_{Ti}) = \frac{n!}{(n/2-1+i)!\cdot(n/2+1-i)!\cdot 2^{n-1}},$$

где $i = \overline{2, n/2+1}$.

В частотном тесте в подпоследовательностях рассчитывается тестовая статистика $\chi^2 = 4M\sum_{k=1}^{N}(\pi_k - 1/2)^2$, где M – длина подпоследовательности, N – число подпоследовательностей, π_k – доля элементов «1» в k-й подпоследовательности. Для всевозможных комбинаций $\pi_k^{(j)}$, где j – номер комбинации значений π_k, рассчитываются значения статистики χ_j^2 и определяются ее возможные значения s_i. Получено выражение для расчета вероятностей значений величины P_T [3]:

$$P(p_{Ti}) = \sum_j \frac{(M!)^N}{2^{M\cdot N}\prod_{k=1}^{N}((\pi_k^{(j)}M)!(M-\pi_k^{(j)}M)!)},$$

где суммирование осуществляется для комбинаций $\pi_k^{(j)}$, для которых $\chi_j^2 = s_i$.

В тесте на подпоследовательности одинаковых бит тестовой статистикой является количество r непрерывных подпоследовательностей одинаковых бит. Для всевозможных комбинаций значений r_j непрерывных подпоследовательностей бит и количества $n1_j$ элементов «1» в СП, где j – номер комбинации, рассчитываются значения вероятности P_T и определяются ее возможные значения p_{Ti}. Выражение для расчета значений $P(p_{Ti})$ имеет вид [3]

$$P(p_{Ti}) = \sum_j P(n1_j, r_j),$$

где суммирование осуществляется для комбинаций r_j и $n1_j$, для которых значение P_T равно p_{Ti}, а

$$P(n1_j, r_j) = 2\binom{n1_j - 1}{r_j/2 - 1}\binom{n - n1_j - 1}{r_j/2 - 1}/2^n, \text{ если } r_j - \text{четное число;}$$

$$P(n1_j, r_j) = \left[\binom{n1_j - 1}{(r_j - 1)/2}\binom{n - n1_j - 1}{(r_j - 3)/2} + \binom{n1_j - 1}{(r_j - 3)/2}\binom{n - n1_j - 1}{(r_j - 1)/2}\right]/2^n,$$

если r_j – нечетное число.

В тесте на самые длинные подпоследовательности единиц в блоках последовательность разбивается на N подпоследовательностей (блоков), каждый из блоков относится к одной из четырех категорий в зависимости от длины самой длинной подпоследовательности элементов «1» и рассчитывается статистика $\chi^2 = \sum_{k=0}^{3}(v_k - N\pi_k)^2 / N\pi_k$, где v_k – количество блоков, отнесенных к $(k+1)$-й категории; π_k – вероятность отнесения блока к $(k+1)$-й категории. Значения v_k могут быть целыми числами от 0 до N. Для всевозможных комбинаций $v_k^{(j)}$, где j – номер комбинации, рассчитаны значения χ_j^2 статистики χ^2 и сформирован массив $S = \{s_i\}$ возможных значений величины χ^2, которым соответствуют значения p_{Ti} вероятности P_T превышения статистикой χ^2 возможных значений. Получено выражение для расчета значений $P(p_{Ti})$ [5]:

$$P(p_{Ti}) = \sum_j \left(\frac{\pi_0^{v_0^{(j)}} \cdot (1-\pi_0)^{N-v_0^{(j)}} N!}{(v_0^{(j)})! \cdot (N - v_0^{(j)})!} \cdot \frac{\left(\frac{\pi_1}{(1-\pi_0)}\right)^{v_1^{(j)}} \cdot \left(1 - \frac{\pi_1}{(1-\pi_0)}\right)^{N - v_0^{(j)} - v_1^{(j)}} \cdot (N - v_0^{(j)})!}{(N - v_0^{(j)} - v_1^{(j)})! \cdot (v_1^{(j)})!} \times \right.$$

$$\left. \times \frac{\left(\frac{\pi_2}{(1-\pi_0-\pi_1)}\right)^{v_2^{(j)}} \cdot \left(1 - \frac{\pi_2}{(1-\pi_0-\pi_1)}\right)^{N - v_0^{(j)} - v_1^{(j)} - v_2^{(j)}} \cdot (N - v_0^{(j)} - v_1^{(j)})!}{(N - v_0^{(j)} - v_1^{(j)} - v_2^{(j)})! \cdot (v_2^{(j)})!} \right),$$

где суммирование осуществляется для $v_k^{(j)}$ $(k = \overline{0,3})$, для которых $\chi_j^2 = s_i$.

В тестах серий и аппроксимированной энтропии в СП подсчитываются пересекающиеся серии w_k длиной $m1$ и серии v_i длиной $(m1-1)$, $k = \overline{0,2^{m1} - 1}$, $i = \overline{0,2^{m1-1} - 1}$. При $m1 = 2$ подсчитывается количество w_0 серий «00», количество w_1 серий «01», количество w_2 серий «10», количество w_3 серий «11», количества v_0 и v_1 элементов «0» и «1» соответственно. Далее рассчитываются статистика $\nabla\psi_2^2 = (4/n)\sum_{k=0}^{3}(w_k)^2 - (2/n)\sum_{i=0}^{1}(v_i)^2$ теста серий и

статистика $\chi^2 = 2n(\ln 2 - \varphi^{(1)} + \varphi^{(2)})$ теста аппроксимированной энтропии, где $\varphi^{(1)} = \sum_{i=0}^{1}(v_i/n)\ln(v_i/n)$, $\varphi^{(2)} = \sum_{k=0}^{3}(w_k/n)\ln(w_k/n)$. Количества пересекающихся серий связаны со значениями $n1$ и r: $w_1 = w_2 = r/2$, $w_3 = n1 - r/2$, если r – четное число; $w_1 = w_2 = (r-1)/2$, $w_3 = n1 - (r-1)/2$, если r – нечетное число; $w_0 = n - (2w_1 + w_3)$. При нахождении теоретических распределений тестовых статистик для всевозможных комбинаций $n1$ и r рассчитываются вероятности $P(n1, r)$ и соответствующие значения статистик $\nabla\psi_2^2$ и χ^2. Вероятности полученных значений $\nabla\psi_2^2$ и χ^2 определяются по рассчитанным значениям $P(n1, r)$ [19, 20].

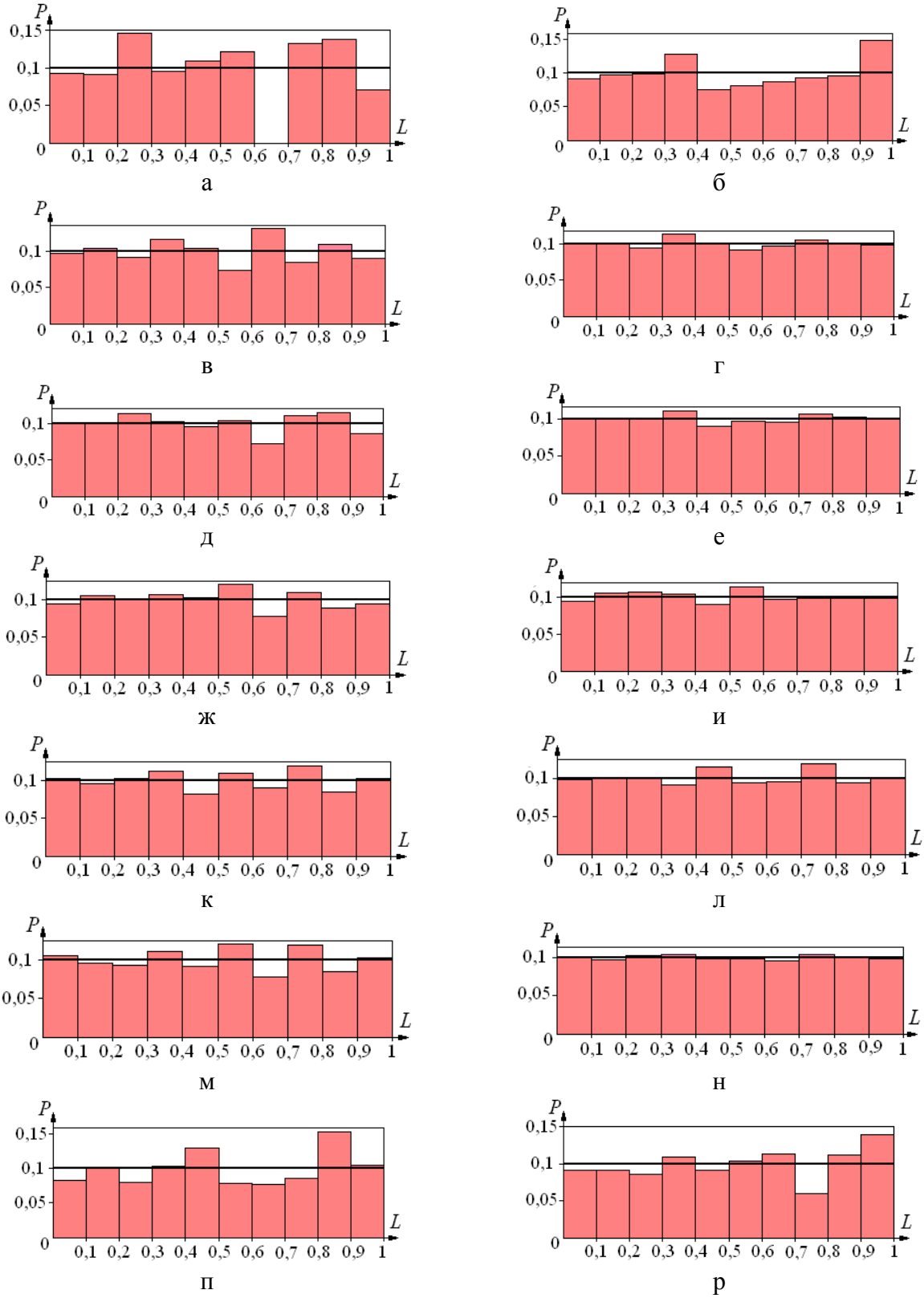
В тесте кумулятивных сумм рассчитываются две статистики z_1 и z_2 для последовательности $x = x_1 x_2 ... x_n$, которая получается из исходной СП путем преобразования элементов «0» в элементы «– 1». Статистики $z_1 = \max\limits_{k=1,n}\left|\sum_{i=1}^{k} x_i\right|$ и $z_2 = \max\limits_{k=1,n}\left|\sum_{i=n-k+1}^{k} x_i\right|$ имеют одинаковые теоретические распределения, так как элементы «1» и «– 1» в СП x имеют одинаковые вероятности. Величины z_1 и z_2 могут принимать целые значения от 1 до n. Пусть z_1^n – статистика z_1 для СП длиной n бит, $z_1^n(k)$ – значение статистики z_1^n для k-й СП упорядоченного полного набора СП, где $k = \overline{1,2^n}$. Получена система уравнений, позволяющая при известных значениях z_1^{n-2} рассчитать значения z_1^n [18]:

$$\begin{cases} z_1^n(1) = n, \\ z_1^n(k) = z_1^{n-2}(k - 2^y), & \text{если} \quad z_1^{n-2}(k-2^y) \geq n - y - 1, \\ z_1^n(k) = n - y - 1, & \text{если} \quad z_1^{n-2}(k-2^y) < n - y - 1, \\ z_1^n(2^n - k + 1) = z_1^n(k), \end{cases} \tag{3}$$

где $k = \overline{2^y + 1, 2^{y+1}}$, $y = \overline{0, n-2}$.

Для определения вероятностей $P(z_1^n)$ количество каждого значения z_1^n делится на число 2^n СП в полном наборе. Получены распределения тестовой статистики z_1 при длинах СП 128 и 256 бит по следующему алгоритму: вычислены значения статистики z_1^6 для полного набора СП длиной 6 бит, по известным значениям z_1^6 вычислены значения z_1^8 в соответствии с системой (3), далее по известным значениям z_1^8 определены значения z_1^{10} и т. д.

Гистограммы, соответствующие полученным распределениям при длинах СП 128 и 256 бит, показаны на рисунке 4, где P – вероятность попадания значений величины P_T в интервал L.



а, в, д, ж, к, м, п – при n = 128 бит; б, г, е, и, л, н, р – при n = 256 бит;
а, б – для частотного теста; в, г – для частотного теста в подпоследовательностях;
д, е – для теста на подпоследовательности одинаковых бит;
ж, и – для теста на самые длинные подпоследовательности единиц в блоках;
к, л – для теста серий; м, н – для теста аппроксимированной энтропии;
п, р – для теста кумулятивных сумм

Рисунок 4. – Гистограммы вероятностей P

Полученные значения P использованы при двухуровневом тестировании СП длиной 128 и 256 бит.

В **четвертой главе** с использованием разработанного АПС статистического тестирования ГСЧ ЭПК выполнена оценка качества работы ГСЧ пяти ЭПК с микроконтроллером К5004 ВЕ2. Для этого из каждой из пяти ЭПК извлечено по 8 тыс. СП длиной 128 бит и по 4 тыс. СП длиной 256 бит. Общий объем извлеченных данных составил 10,24 млн бит. После реализации процедур, предусмотренных методикой статистического тестирования ГСЧ ЭПК, было получено 38 419 СП длиной 128 бит и 19 151 СП длиной 256 бит, статистические свойства которых соответствуют свойствам РРСП.

Также экспериментально проверено качество работы ГСЧ двух ЭПК при температурах 0, 20 и 50 ˚С из диапазона рабочих температур от 0 ˚С до 50 ˚С по тестам стандарта FIPS 140-2. Установлено, что 18 последовательностей (по три СП длиной 20 тыс. бит для каждой температуры для двух ЭПК) прошли все тесты стандарта FIPS 140-2, при этом все значения величин, полученные по результатам тестирования, попадают в диапазон допустимых значений. Приведены соответствующие таблицы результатов.

Дополнительно выполнены проверка распределения единиц в байтах вырабатываемых СП и тесты системы NIST, за исключением теста аппроксимированной энтропии, для ГСЧ двух ЭПК при 0, 20 и 50 ˚С. Для СП длиной 1,024 млн бит для каждой из температур при проверке распределения единиц в байтах получены значения вероятности P_T в диапазоне от 0,0815 до 0,8791 при уровне значимости 0,01, а при проверке по тестам NIST значения вероятности P_T попали в диапазон от 0,0218 до 0,9875 при уровне значимости 0,01. Это свидетельствует о высоком качестве исследованных ГСЧ.

В **приложениях** представлены результаты исследований СП различной длины, полученных из ЭПК, листинг фрагмента файл-программы Statistical_testing, реализованной в среде MATLAB, акты внедрения и использования результатов диссертационной работы.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложена и обоснована методика статистического тестирования генераторов случайных чисел электронных пластиковых карт, включающая:

– тестирование последовательности, составленной из всех сгенерированных случайных последовательностей, которое позволяет оценить качество работы генератора с использованием любого статистического теста;

– двухуровневое тестирование случайных последовательностей, что позволяет оценить статистические свойства каждой сгенерированной последовательности, предназначенной для использования в качестве криптографического ключа, и проверить равновероятность вырабатываемых генератором случайных последовательностей,

отличающаяся использованием двухуровневого тестирования случайных последовательностей с длинами, равными длинам практически используемых ключей [4, 23].

2. Теоретически доказано, что одна из статистик теста серий эквивалентна статистике теста аппроксимированной энтропии при стремлении длины проверяемой последовательности к бесконечности, и на примере ГСЧ ЭПК с микроконтроллером К5004 ВЕ2 показано, что тест аппроксимированной энтропии может быть исключен при использовании теста серий при длинах последовательностей от 1 млн бит [2].

3. Получены теоретические распределения тестовых статистик и вероятностей превышения возможных значений статистик для частотного теста, частотного теста в подпоследовательностях, теста на подпоследовательности одинаковых бит, теста на самые длинные подпоследовательности единиц в блоках, теста серий, теста аппроксимированной энтропии и теста кумулятивных сумм при длинах СП 128 и 256 бит, что позволяет выполнить двухуровневое тестирование СП указанных длин [3, 5, 6, 17–20].

4. Разработано аппаратно-программное средство статистического тестирования ГСЧ ЭПК, основанное на предложенной методике, позволяющее оценивать качество работы ГСЧ ЭПК в диапазоне рабочих температур и формировать массивы ключей, свойства которых соответствуют равномерно распределенным случайным последовательностям [1, 7–16, 21, 22, 24, 25].

Рекомендации по практическому использованию результатов

1. Предложенная методика статистического тестирования ГСЧ ЭПК может быть использована для оценки качества работы различных ГСЧ и формирования массивов СП, свойства которых соответствуют РРСП (приложение Ж).

2. Разработанное аппаратно-программное средство статистического тестирования ГСЧ ЭПК можно использовать для оценки качества работы различных ГСЧ и получения от них массивов СП со свойствами, соответствующими свойствам РРСП (приложение Ж).

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в рецензируемых научных журналах

1. Киевец, Н. Г. Аппаратно-программный комплекс для исследования генераторов случайных чисел электронных пластиковых карт / Н. Г. Киевец, А. И. Корзун // ЭЛЕКТРОНИКА инфо. – 2013. – № 6 (96). – С. 158–160.

2. Киевец, Н. Г. Сравнение статистик тестов серий и аппроксимированной энтропии / Н. Г. Киевец, А. И. Корзун // Доклады БГУИР. – 2014. – № 3 (81). – С. 12–17.

3. Киевец, Н. Г. Методика нахождения эталонных законов распределения вероятностей, получаемых при статистическом тестировании последовательностей ключей / Н. Г. Киевец, А. И. Корзун // Доклады БГУИР. – 2014. – № 5 (83). – С. 38–43.

4. Киевец, Н. Г. Методика получения доверительного набора криптографических ключей / Н. Г. Киевец, А. И. Корзун // Веснік сувязі. – 2014. – № 4 (124). – С. 33–37.

5. Киевец, Н. Г. Двухуровневое тестирование случайных последовательностей длиной 128 и 256 бит / Н. Г. Киевец, А. И. Корзун // Доклады БГУИР. – 2017. – № 3 (105). – С. 78–83.

6. Киевец, Н. Г. Оценка качества работы генераторов случайных чисел на основе двухуровневого тестирования / Н. Г. Киевец // Проблемы инфокоммуникаций. – 2017. – № 1 (5). – С. 19–23.

Статьи в сборниках материалов научных трудов

7. Киевец, Н. Г. Применение системы статистических тестов NIST для исследования генераторов случайных чисел электронных пластиковых карт / Н. Г. Киевец // Инфокоммуникационные технологии: Техника. Экономика. Образование : сб. науч. тр. профессорско-преподавательского состава, посвященный 20-летию УО ВГКС / Высш. гос. колледж связи. – Минск, 2013. – С. 30–33.

Статьи в сборниках материалов научных конференций и семинаров

8. Капля, П. Б. Некоторые особенности работы с криптографическими электронными пластиковыми картами / П. Б. Капля, Н. Г. Киевец, А. И. Корзун // Современные средства связи : материалы XV Междунар. науч.-техн. конф., Минск, 28–30 сентября 2010 г. / Высш. гос. колледж связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2010. – С. 62.

9. Киевец, Н. Г. Некоторые особенности обработки массивов случайных чисел, извлекаемых из электронных пластиковых карт / Н. Г. Киевец,

А. И. Корзун // Современные средства связи : материалы XVI Междунар. науч.-техн. конф., Минск, 27–29 сентября 2011 г. / Высш. гос. колледж связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2011. – С. 97.

10. Корзун, А. И. Аппаратно-программное средство исследования датчиков случайных чисел электронных пластиковых карт / А. И. Корзун, Н. Г. Киевец // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы междунар. науч.-техн. семинара, Минск, 2011 г. / Белорус. гос. ун-т информатики и радиоэлектроники. – Минск, 2011. – С. 83–88.

11. Киевец, Н. Г. Система статистического тестирования генераторов случайных чисел электронных пластиковых карт / Н. Г. Киевец, А. И. Корзун // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы междунар. науч.-техн. семинара, Минск, 2012 г. / Белорус. гос. ун-т информатики и радиоэлектроники. – Минск, 2012. – С. 65–69.

12. Киевец, Н. Г. Корреляция публикаций об исследованиях генераторов случайных чисел (ГСЧ) с количеством пользователей Интернета и результаты исследования ГСЧ электронной пластиковой карты по FIPS 140-1 / Н. Г. Киевец, А. И. Корзун, Г. И. Мельянец // Современные средства связи : материалы XVII Междунар. науч.-техн. конф., Минск, 16–18 октября 2012 г. / Высш. гос. колледж связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2012. – С. 217.

13. Киевец, Н. Г. Тестирование генераторов случайных чисел электронных пластиковых карт по системе NIST / Н. Г. Киевец // Современные средства связи : материалы XVIII Междунар. науч.-техн. конф., Минск, 15–16 октября 2013 г. / Высш. гос. колледж связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2013. – С. 203.

14. Ярук, А. М. Системы статистического тестирования генераторов случайных чисел / А. М. Ярук, Н. Г. Киевец // Современные средства связи : материалы XIX Междунар. науч.-техн. конф., Минск, 14–15 октября 2014 г. / Высш. гос. колледж связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2014. – С. 154–155.

15. Ярук, А. М. Исследование генераторов случайных чисел электронных пластиковых карт по системе NIST / А. М. Ярук, Н. Г. Киевец // Современные средства связи : материалы XX Междунар. науч.-техн. конф., Минск, 14–15 октября 2015 г. / Высш. гос. колледж связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2015. – С. 154–155.

16. Киевец, Н. Г. Классификация статистических тестов для оценки качества работы генераторов случайных чисел / Н. Г. Киевец // Современные

средства связи : материалы XXI Междунар. науч.-техн. конф., Минск, 20–21 октября 2016 г. / Белорус. гос. акад. связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2016. – С. 231.

17. Киевец, Н. Г. Теоретические распределения тестовой статистики теста серий / Н. Г. Киевец, А. М. Ярук // Современные средства связи : материалы XXII Междунар. науч.-техн. конф., Минск, 19–20 октября 2017 г. / Белорус. гос. акад. связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2017. – С. 301–302.

18. Киевец, Н. Г. Двухуровневое тестирование последовательностей по тесту кумулятивных сумм / Н. Г. Киевец // Современные средства связи: материалы XXII Междунар. науч.-техн. конф., Минск, 19–20 октября 2017 г. / Белорус. гос. акад. связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2017. – С. 302–303.

19. Киевец, Н. Г. Нахождение теоретических распределений статистики теста аппроксимированной энтропии / Н. Г. Киевец, А. М. Ярук // Информационные технологии и системы 2017 (ИТС 2017) : материалы междунар. науч. конф., Минск, 25 октября 2017 г. / Белорус. гос. ун-т информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин (гл. ред.) [и др.]. – Минск, 2017. – С. 190–191.

20. Киевец, Н. Г. Статистическое тестирование генераторов случайных чисел электронных пластиковых карт / Н. Г. Киевец // Математические методы в технике и технологиях : сб. тр. Междунар. науч. конф., Санкт-Петербург, 30 мая – 02 июня 2017 г., Минск, 24–27 октября 2017 г., Самара, 31 октября – 02 ноября 2017 г. : в 12 т. / под общ. ред. А. А. Большакова. – СПб., 2017. – Т. 12 : в 3 ч. – Ч. 2. – С. 19–22.

Тезисы докладов на научных конференциях

21. Киевец, Н. Г. Датчик случайных чисел на основе электронных пластиковых карт / Н. Г. Киевец, П. Б. Капля, А. И. Корзун // Технические средства защиты информации : тез. докл. VIII Белорус.-рос. науч.-техн. конф., Браслав, 24–28 мая 2010 г. / Белорус. гос. ун-т информатики и радиоэлектроники ; редкол.: Л. М. Лыньков [и др.]. – Минск, 2010. – С. 62–63.

22. Киевец, Н. Г. Тестирование генераторов случайных чисел электронных пластиковых карт по методологии NIST / Н. Г. Киевец // Технические средства защиты информации : тез. докл. XI Белорус.-рос. науч.-техн. конф., Минск, 5–6 июня 2013 г. / Белорус. гос. ун-т информатики и радиоэлектроники ; редкол.: Л. М. Лыньков [и др.]. – Минск, 2013. – С. 41.

23. Киевец, Н. Г. Методика тестирования последовательностей криптографических ключей / Н. Г. Киевец // Технические средства защиты информации : тез. докл. XI Белорус.-рос. науч.-техн. конф., Минск, 28–29 мая

2014 г. / Белорус. гос. ун-т информатики и радиоэлектроники ; редкол.: Л. М. Лыньков [и др.]. – Минск, 2014. – С. 26–27.

24. Ярук, А. М. Проверка качества работы генератора случайных чисел / А. М. Ярук, Н. Г. Киевец, А. И. Корзун // Технические средства защиты информации : тез. докл. XIII Белорус.-рос. науч.-техн. конф., Минск, 4–5 июня 2015 г. / Белорус. гос. ун-т информатики и радиоэлектроники ; редкол.: Л. М. Лыньков [и др.]. – Минск, 2015. – С. 50–51.

25. Проверка качества работы генераторов случайных чисел электронных пластиковых карт в диапазоне рабочих температур / А. М. Ярук, Н. Г. Киевец, А. В. Босак, Э. В. Машкович // Технические средства защиты информации : тез. докл. XIV Белорус.-рос. науч.-техн. конф., Минск, 25–26 мая 2016 г. / Белорус. гос. ун-т информатики и радиоэлектроники ; редкол.: Л. М. Лыньков [и др.]. – Минск, 2016. – С. 44.

РЭЗЮМЭ

Кіевец Наталля Рыгораўна

Апаратна-праграмны сродак статыстычнага тэсціравання генератараў выпадковых лікаў электронных пластыкавых карт

Ключавыя словы: выпадковая паслядоўнасць, генератар выпадковых лікаў, статыстычнае тэсціраванне.

Мэта работы заключаецца ў распрацоўцы апаратна-праграмнага сродку статыстычнага тэсціравання генератараў выпадковых лікаў электронных пластыкавых карт для адзнакі якасці іх работы і фармавання масіваў выпадковых паслядоўнасцяў, уласцівасці якіх адпавядаюць уласцівасцям раўнамерна размеркаваных выпадковых паслядоўнасцяў.

Метады даследавання і апаратура: вынікі дысертацыйнай работы атрыманы з выкарыстаннем метадаў тэорыі верагоднасцяў, матэматычнай статыстыкі і эксперыментальных даследаванняў выпадковых паслядоўнасцеў, атрыманых з электронных пластыкавых карт; у якасці апаратных сродкаў выкарыстоўваюцца персанальны камп’ютар, электронныя пластыкавыя карты і рыдар.

Атрыманыя вынікі і іх навізна: распрацаваны апаратна-праграмны сродак статыстычнага тэсціравання генератараў выпадковых лікаў электронных пластыкавых карт, якое рэалізуе прапанаваную методыку статыстычнага тэсціравання; даказана, што адна са статыстык тэста серый і статыстыка тэста апраксімаванай энтрапіі эквівалентныя пры імкненні даўжыні паслядоўнасці да бясконцасці; атрыманы тэарэтычныя размеркаванні тэставых статыстык і верагоднасцяў перавышэння магчымых значэнняў тэставых статыстык чашчыннага тэста, чашчыннага тэста ў падпаслядоўнасцях, тэста на падпаслядоўнасці аднолькавых біт, тэста на самыя доўгія падпаслядоўнасці адзінак у блоках, тэста серый, тэста апраксімаванай энтрапіі і тэста кумулятыўных сум пры даўжынях выпадковых паслядоўнасцяў 128 і 256 біт.

Ступень выкарыстання: атрыманыя у рабоце вынікі выкарыстоўваюцца на прадпрыемствах ЗАТ «Цэнтр новых інтэлектуальных інтэграваных сістэм», ЗАТ «НТЦ Кантакт» і ў навучальным працэсе УА «БДУІР».

Вобласць ужывання: інфармацыйная бяспека.

РЕЗЮМЕ

Киевец Наталья Григорьевна

Аппаратно-программное средство статистического тестирования генераторов случайных чисел электронных пластиковых карт

Ключевые слова: случайная последовательность, генератор случайных чисел, статистическое тестирование.

Цель работы состоит в разработке аппаратно-программного средства статистического тестирования генераторов случайных чисел электронных пластиковых карт для оценки качества их работы и формирования массивов случайных последовательностей, свойства которых соответствуют свойствам равномерно распределенных случайных последовательностей.

Методы исследования и аппаратура: результаты диссертационной работы получены с использованием методов теории вероятностей, математической статистики и экспериментальных исследований случайных последовательностей, полученных из электронных пластиковых карт; в качестве аппаратных средств используются персональный компьютер, электронные пластиковые карты и ридер.

Полученные результаты и их новизна: разработано аппаратно-программное средство статистического тестирования генераторов случайных чисел электронных пластиковых карт, реализующее предложенную методику статистического тестирования; доказано, что одна из статистик теста серий и статистика теста аппроксимированной энтропии эквивалентны при стремлении длины последовательности к бесконечности; получены теоретические распределения тестовых статистик и вероятностей превышения возможных значений тестовых статистик частотного теста, частотного теста в подпоследовательностях, теста на подпоследовательности одинаковых бит, теста на самые длинные подпоследовательности единиц в блоках, теста серий, теста аппроксимированной энтропии и теста кумулятивных сумм при длинах случайных последовательностей 128 и 256 бит.

Степень использования: полученные в работе результаты внедрены в ЗАО «Центр новых интеллектуальных интегрированных систем», ЗАО «НТЦ Контакт» и в учебный процесс УО «БГУИР».

Область применения: информационная безопасность.

SUMMARY

Kiyevets Natallia Grigoryevna

Hardware-software means of statistical testing of electronic plastic card random number generators

Keywords: random sequence, random number generator, statistical testing.

Aim of the work is to develope hardware-software means of statistical testing of electronic plastic card random number generators for estimation of their quality and formation of random sequences files with properties of uniform random sequences.

Research methods and equipment: working data are received by means of methods of the probability theory, the mathematical statistics and experimental researches of the random sequences received from electronic plastic cards; personal computer, electronic plastic cards and reader are used as hardware.

Final results and their novelty: the hardware-software means of statistical testing of electronic plastic card random number generators are developed that realise a technique of statistical testing; it is proved that one of serial test statistics and approximation entropy test statistic are equal when sequence length goes to infinity; the theoretical distributions of the test statistics and probabilities of the exceeding of possible values were obtained for frequency test, frequency test within a block, runs test, test for longest run of ones in a block, serial test, approximate entropy test and cumulative sums test when the length of random sequence was equal to 128 and 256 bits.

Extend of usage: the results were used in closed companies «Center of the new intellectual integrated systems» and «Scientific and technical centre Contact», in the educational process of the BSUIR.

Scope: information security.

Научное издание

Киевец Наталья Григорьевна

АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Подписано в печать	Формат 60×84 $^{1}/_{16}$	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л.
Уч.-изд. л. 1,4	Тираж 60 экз.	Заказ .

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 1/238 от 24.04.2014,
№ 2/113 от 07.04.2014, № 3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск