Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056:519.254

КИЕВЕЦ
Наталья Григорьевна

АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

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

Минск 2016

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: **Конопелько Валерий Константинович**, доктор технических наук, профессор, заведующий кафедрой сетей и устройств телекоммуникаций учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Половеня Сергей Иванович, кандидат технических наук, заведующий кафедрой телекоммуникационных систем учреждения образования «Белорусская государственная академия связи»

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

Защита состоится « 9 » июня 2016 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 « 6 » мая 2016 г.

Ученый секретарь
совета по защите диссертаций,
доктор технических наук А.А. Борискевич

КРАТКОЕ ВВЕДЕНИЕ

Практически любая современная технология передачи данных, использующая сети общего пользования, предусматривает шифрование передаваемых сообщений. При этом предполагается использование криптографических ключей, в качестве которых применяют равномерно распределенные случайные последовательности. Наиболее предпочтительным источником ключей является физический генератор случайных чисел (ГСЧ).

Одним из устройств, содержащих физические ГСЧ, является электронная пластиковая карта (ЭПК). ЭПК обладает рядом достоинств: защищенная от внешнего вмешательства компоновка карты; при работе с ЭПК используются стандартные команды; сгенерированные данные могут храниться в области энергонезависимой памяти, недоступной для чтения. Вместе с тем физические ГСЧ могут быть подвержены изменению в связи со старением элементов и из-за условий эксплуатации, чем обусловлена необходимость оперативного контроля каждой вырабатываемой ими случайной последовательности (СП). В связи с этим необходимо исследование СП, генерируемых ГСЧ ЭПК, с целью оперативного контроля его параметров методами статистического тестирования.

Особенностью ГСЧ ЭПК является выработка СП только фиксированных длин, определяемых производителями ЭПК и, как правило, связанных с длинами криптографических ключей, используемых операционной системой и программными приложениями карт. Однако методы тестирования требуют выработки на порядки более длинных последовательностей, для получения которых сгенерированные СП объединяют в непрерывный битовый поток требуемой длины. Это приводит к большим затратам времени на формирование СП для тестирования. Поэтому существует объективная необходимость проработки вопроса оценки качества ГСЧ, не прибегая к формированию больших массивов данных.

Возникает задача разработки аппаратно-программного средства, позволяющего оперативно оценить качество работы ГСЧ ЭПК на основе эффективного тестирования относительно коротких последовательностей длиной от 1 млн бит с использованием двухуровневых тестов. Для этого требуется разработка методики тестирования с применением статистического контроля каждой сгенерированной СП, предназначенной для использования в качестве ключа; двухуровневых тестов для повышения мощности тестирования без увеличения длины СП.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами и темами

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по теме «Программно-аппаратный комплекс «Подсистема криптографической защиты информации электронной системы реализации лотерейной продукции» в части корректировки библиотеки функций генерации ключевой информации CNIISGen (РБ.ЦИЕС.00002-01).

Результаты диссертации соответствуют пункту 3.2 Паспорта специальности 05.13.19 (технические науки) – «Разработка новых и повышение эффективности существующих аппаратных, программных и аппаратно-программных средств криптографической защиты информации (шифрования, электронной цифровой подписи, управления доступом, контроля целостности, генерации ключевой документации)».

Цель и задачи исследования

Целью диссертационной работы является разработка аппаратно-программного средства тестирования СП для оперативной оценки качества работы ГСЧ и формирования массивов СП, пригодных для использования в ключевых документах.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать методы статистического тестирования СП, позволяющих без увеличения длины СП повысить мощность тестирования и таким образом проверить качество работы ГСЧ при экономии времени на генерацию данных.
2. Разработать методику формирования массивов СП для криптографических приложений, позволяющую одновременно оценить качество работы ГСЧ.
3. Создать аппаратно-программное средство тестирования СП, реализующее методику формирования массивов СП.
4. Сформировать массивы СП различных длин для ключевых документов с использованием разработанного аппаратно-программного средства тестирования СП на примере ГСЧ электронных пластиковых карт.

Научная новизна

1. Для частотного теста, частотного теста в подпоследовательностях, теста на подпоследовательности одинаковых бит, теста на самые длинные

подпоследовательности единиц в блоках системы американского Национального института стандартов и технологий (NIST) при длинах последовательностей 128 и 256 бит найдены теоретические распределения вероятностей превышения статистиками значений, получаемых экспериментально, что позволяет выполнить процедуру двухуровневого тестирования последовательности, применяя тест к ее отрезкам указанных длин.

2. Теоретически и экспериментально доказано, что одна из статистик теста серий системы NIST эквивалентна статистике теста аппроксимированной энтропии системы NIST при стремлении длины последовательности к бесконечности, что позволяет при использовании теста серий не применять тест аппроксимированной энтропии при длинах последовательностей более 1 млн бит.

Положения, выносимые на защиту

1. Методика формирования массивов случайных последовательностей, позволяющая оперативно оценить качество работы ГСЧ и получить последовательности с проверенными статистическими свойствами для применения в ключевых документах, отличающаяся использованием процедуры двухуровневого тестирования для повышения мощности тестов без увеличения объема генерируемых данных.

2. Методика комплексной оценки результатов тестирования случайных последовательностей, основанная на проверке соответствия эмпирических распределений вероятностей превышения тестовой статистикой значений, получаемых экспериментально, теоретическим распределениям, отличающаяся использованием вместо равномерного распределения теоретических распределений, которые находятся при заданных длинах последовательностей.

3. Математические выражения для нахождения теоретических распределений вероятностей превышения тестовой статистикой значений, получаемых при проверке случайных последовательностей по тестам системы NIST: частотному, частотному в подпоследовательностях, на подпоследовательности одинаковых бит и на самые длинные подпоследовательности единиц в блоках.

4. Аппаратно-программное средство тестирования случайных последовательностей, позволяющее оценивать качество работы ГСЧ и получать массивы последовательностей для ключевых документов в соответствии с предложенными методиками.

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 формирования массивов случайных последовательностей и методики комплексной оценки результатов тестирования случайных последовательностей; разработка аппаратно-программного средства тестирования случайных последовательностей, реализующего предлагаемые методики. Определение целей и задач исследований, обсуждение и анализ полученных результатов осуществлялись с научным руководителем кандидатом технических наук А.И. Корзуном, который является соавтором публикаций.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях и семинарах: 88-я, 11-я, 12-я Белорусско-российские научно-технические конференции «Технические средства защиты информации» (Браслав, 2010 г., Минск, 2013, 2014 гг.); 16-я, 17-я, 18-я международные научно-технические конференции «Современные средства связи» (Минск, 2011, 2012, 2013 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.).

Опубликование результатов диссертации

Результаты исследований представлены в 13 опубликованных работах, в том числе 4 статьи в рецензируемых научных журналах Республики Беларусь объемом 1,25 авторского листа, 3 статьи в материалах семинаров и научных трудов, тезисы 6 докладов в сборниках материалов научно-технических конференций.

Структура и объем диссертации

Работа состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников и приложений. Общий объем диссертационной работы составляет 178 страниц, из них 104 страницы текста, 29

рисунков на 18 страницах, 26 таблиц на 11 страницах, библиографический список из 120 наименований, включая 13 собственных публикаций автора, на 12 страницах, 5 приложений на 33 страницах.

ОСНОВНАЯ ЧАСТЬ

Во **введении** определены основные направления исследования и показана актуальность разработки аппаратно-программного средства тестирования СП для оперативной оценки качества работы ГСЧ.

В **первой главе** проведен анализ методов получения СП и методов их статистического тестирования, по результатам которого принимается решение о целесообразности использования последовательностей в качестве криптографических ключей. Обоснован выбор ГСЧ ЭПК в качестве источника СП.

Анализ методов статистического тестирования показал, что на сегодняшний день существует множество систем тестирования. Полнота ни одной из систем не доказана, что объясняется неограниченностью отклонений от свойств истинно случайной последовательности, поэтому представляет интерес выбор системы тестирования, которая предназначена для ГСЧ, используемых в криптографических приложениях.

Во **второй главе** разработано аппаратно-программное средство, позволяющее извлекать из ЭПК СП заданной длины, осуществлять их тестирование для оценки качества работы ГСЧ и на его основе формировать массивы СП, которые по статистическим свойствам пригодны для использования в качестве криптографических ключей. Для создания данного средства был решен ряд задач:

- сформировано $АПС_1$ генерирования СП на примере ЭПК;
- разработана методика формирования массивов СП;
- выбрана система статистических тестов для оценки свойств СП;
- разработано $АПС_2$ для статистического тестирования СП.

$АПС_1$ включает в себя ЭПК, ридер и персональный компьютер (ПК), содержащий программное обеспечение (ПО) подачи команд ЭПК. $АПС_1$ позволяет извлекать из карт требуемое количество случайных последовательностей.

Предложена методика формирования массивов СП, позволяющая оперативно выполнить проверку качества работы ГСЧ за счет использования процедур двухуровневого тестирования и получить массивы СП, прошедших статистический контроль и признанных пригодными для использования в криптографических приложениях [4, 13]. Методика предусматривает выполнение следующих этапов:

1. Формирование набора тестов № 1 для исследования длинной битовой последовательности, составленной из всех сгенерированных СП: $T_{11}, T_{12}, \ldots, T_{1X}$, где X – количество тестов набора.

2. Формирование набора тестов № 2 для исследования отдельных СП: $T_{21}, T_{22}, \ldots, T_{1Y}$, где Y – количество тестов набора.

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

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

$$\begin{cases} N \geq n_{\min} / n, \\ N \geq N_{\min} = \left\lceil \dfrac{\left(3Y\sqrt{\alpha_1(1-\alpha_1)} + \sqrt{9Y^2\alpha_1(1-\alpha_1) + 4(1-\alpha_1 Y)N_{mp}}\right)^2}{4(1-\alpha_1 Y)^2} \right\rceil, \end{cases} \quad (1)$$

где $n_{\min}$ – минимальная длина последовательности для тестов набора № 1; $N_{\min}$ – минимальное количество сгенерированных СП, которое обеспечит требуемое количество N_{mp} СП в массиве после успешного прохождения всех этапов тестирования; Y – количество тестов в наборе № 2, выбирается из условия: $Y < 1/\alpha_1$; α_1 – уровень значимости для тестов наборов № 1 и № 2 ($0 < \alpha_1 < 1$).

4. Формирование непрерывной битовой последовательности длиной $N \times n$ путем побитной записи сгенерированных СП в поток данных.

5. Исследование сформированной битовой последовательности по тестам набора № 1, в результате которого получается массив значений вероятности P_T :($p_{T1}, p_{T2}, \ldots, p_{TX}$), где p_{Ti} – вероятность превышения статистикой теста T_{1i} значения, полученного экспериментально.

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 $i = \overline{1, X}$, сгенерированные СП отбрасываются и осуществляется переход к этапу 3. Если все тесты набора № 1 пройдены, т. е. выполняется логическое условие $p_{Ti} \geq \alpha_1$ при всех $i = \overline{1, X}$, исследование продолжается.

7. Исследование каждой СП по тестам набора № 2, в результате которого получается массив значений вероятности $P_T: \begin{pmatrix} p_{T11} & p_{T12} & \cdots & p_{T1Y} \\ \cdots & \cdots & \cdots & \cdots \\ p_{TN1} & p_{TN2} & \cdots & p_{TNY} \end{pmatrix}$, где p_{Tij} – вероятность, полученная при исследовании i-й СП по тесту T_{2j}.

8. Комплексная оценка результатов тестирования СП по каждому тесту T_{2j} ($j=\overline{1,Y}$) набора № 2 двумя способами.

Во-первых, проверяется соответствие эмпирических распределений вероятностей p_{Tij} теоретическим распределениям по критерию согласия Пирсона, для чего для каждого теста T_{2j} рассчитывается значение p_{cj} величины P_c – вероятности превышения случайной величиной χ^2 значения:

$$\chi^2 = \sum_{g=1}^{G} \left[\left(n_g - N p_g \right)^2 / \left(N p_g \right) \right], \qquad (2)$$

где G – количество интервалов разбиения диапазона значений p_{Tij} ($i=\overline{1,N}$); p_g – вероятность попадания значения p_{Tij} в g-й интервал; n_g – частота попадания значения p_{Tij} в g-й интервал.

Во-вторых, проверяется попадание доли d_j СП, прошедших тест T_{2j} ($j=\overline{1,Y}$), в заданный доверительный интервал:

$$l = [1-\alpha_1 - 3\sqrt{\alpha_1(1-\alpha_1)/N}; 1-\alpha_1 + 3\sqrt{\alpha_1(1-\alpha_1)/N}]. \qquad (3)$$

В случае положительного результата по всем проверкам, т. е. при выполнении условий $p_{cj} \geq \alpha_2$ (α_2 – уровень значимости) и $d_j \in l$ для всех $j=\overline{1,Y}$, осуществляется переход к следующему этапу. При отрицательном результате хотя бы по одной из проверок сгенерированные СП отбрасываются и осуществляется переход к этапу 3.

9. Формирование массива последовательностей из СП, прошедших все тесты набора № 2. Полученный массив будет состоять из последовательностей, которые по статистическим свойствам пригодны для использования в качестве ключей.

На рисунке 1 представлена блок-схема алгоритма, реализующего методику формирования массивов СП. Для реализации предложенной методики за основу наборов № 1 и № 2 взята система тестов NIST [6, 7, 11 ,12]. Данные тесты были реализованы в вычислительной системе MATLAB.

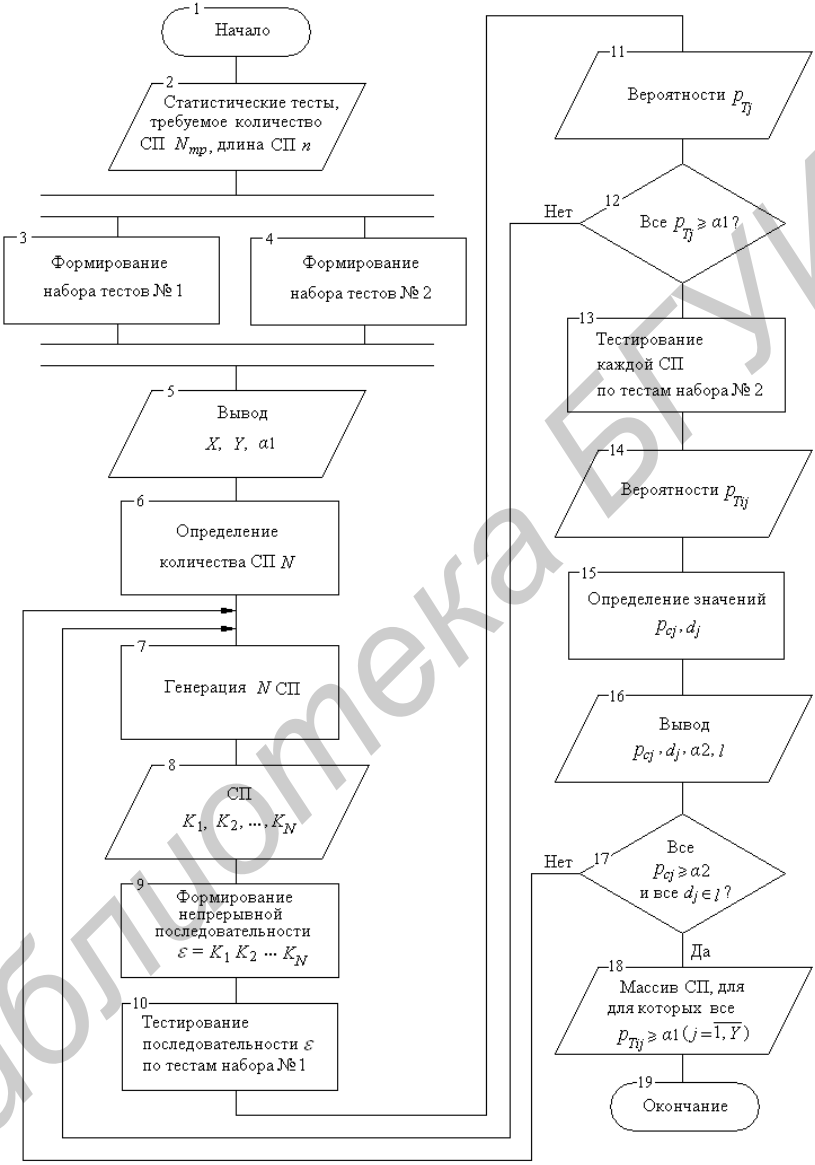


Рисунок 1. – Блок-схема алгоритма, реализующего методику формирования массивов СП

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 серий

$$\nabla\psi^2_{m1} = \psi^2_{m1} - \psi^2_{m1-1} = \frac{2^{m1}}{n}\sum_{k=0}^{2^{m1}-1} w_k^2 - \frac{2^{m1-1}}{n}\sum_{i=0}^{2^{m1-1}-1} v_i^2, \qquad (4)$$

где $m1$ и $(m1-1)$ – длины пересекающихся серий; w_k – число появлений в последовательности серии k-го вида длины $m1$; v_i – число появлений в последовательности серии i-го вида длины $(m1-1)$, со статистикой теста аппроксимированной энтропии с параметром $m2 = m1-1$:

$$\chi^2 = 2n(\ln 2 - \varphi^{(m2)} + \varphi^{(m2+1)}) = 2n(\ln 2 - \varphi^{m1-1} + \varphi^{m1}), \qquad (5)$$

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 (5) величин φ^{m1-1} и φ^{m1} эквивалентными при $n \to \infty$ соотношениями $\varphi^{m1-1} \sim -(m1-1)\cdot\ln 2 + \frac{2^{m1-1}}{2n}\sum_{i=0}^{2^{m1-1}-1} Z_i^2$ 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 $K = 2^{m1-1}$, получаем равные значения вероятностей P_T. Поскольку тест серий предусматривает вычисление помимо статистики (4) еще одной статистики, то он поглощает тест аппроксимированной энтропии и последний может быть исключен из системы.

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 было решено сохранить.

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. Данные наборы реализованы в файл-программе Statistical_testing системы вычислительной математики MATLAB для статистического тестирования СП, что позволяет проводить исследования, задавая параметры тестирования по требованию. Персональный компьютер с системой MATLAB и алгоритмами тестирования является $АПС_2$, позволяющим осуществлять проверку статистических свойств СП, получаемых не только из ГСЧ ЭПК, но также из других источников.

В результате объединения $АПС_1$ и $АПС_2$ получено АПС, позволяющее извлекать из ЭПК СП заданной длины, осуществлять их статистическое тестирование и формировать массивы последовательностей в соответствии с предложенной методикой [1, 5, 8, 9]. Структурная схема АПС представлена на рисунке 2.

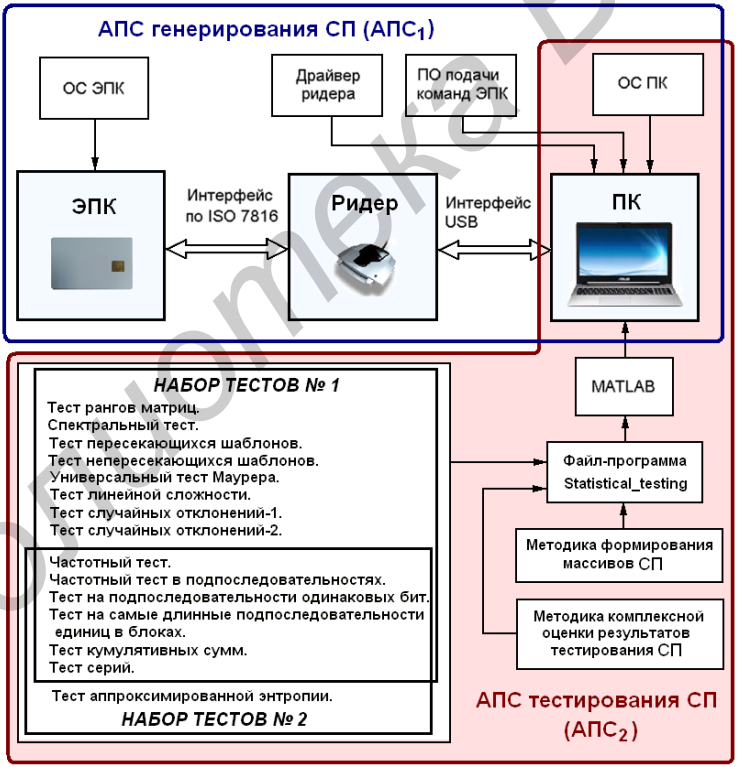


Рисунок 2. – Структурная схема АПС генерирования и тестирования случайных последовательностей

В **третьей главе** разработана методика комплексной оценки результатов тестирования СП, основанная на сравнении эмпирических распределений вероятностей P_T превышения статистиками значений, получаемых экспериментально, с теоретическими распределениями [3]. Методика отличается тем, что в качестве теоретического распределения вероятностей P_T вместо равномерного используется распределение, которое находится для теста при заданной длине последовательности. Основные этапы реализации методики оценки результатов тестирования СП:

1. Нахождение теоретического распределения вероятности P_T для данного теста при заданной длине СП.

2. Тестирование каждой СП и получение массива значений P_T .

3. Проверка соответствия эмпирического распределения вероятности P_T теоретическому распределению по критерию согласия Пирсона.

Первый этап методики требует анализа тестовой статистики и выполняется в соответствии с порядком, показанном на рисунке 3. Получены расчетные выражения и найдены распределения вероятностей для частотного теста, частотного теста в подпоследовательностях, теста на подпоследовательности одинаковых бит, теста на самые длинные подпоследовательности единиц в блоках при длинах СП 128 и 256 бит.

Рисунок 3. – Порядок нахождения распределений вероятностей P_T

Для *частотного теста* вероятности значений величины P_T определяются из выражений [3]

$$\begin{cases} P(p_{T1}) = \dfrac{n!}{(n/2)!(n/2)!2^n}, \\ P(p_{Ti}) = \dfrac{n!}{(n/2-1+i)!(n/2+1-i)!2^{n-1}}, \quad i = \overline{2,(n/2+1)}. \end{cases} \tag{6}$$

В случае *частотного теста в подпоследовательностях* вероятности значений величины P_T определяются из выражения [3]

$$P(p_{Ti}) = \sum_j \frac{(M!)^N}{2^{M\cdot N}\prod_{k=1}^{N}\left(\left(\pi_k^{(j)}M\right)\left(M-\pi_k^{(j)}M\right)\right)}, \qquad (7)$$

где j – номер комбинации долей единиц в N подпоследовательностях длиной M, суммирование осуществляется для комбинаций, при которых $P_T = p_{Ti}$; k – номер подпоследовательности; $\pi_k^{(j)}$ – доля единиц в k-й подпоследовательности из j-й комбинации.

Для *теста на подпоследовательности одинаковых бит* вероятности значений величины P_T определяются [3]

$$P(p_{Ti}) = \sum_j P(n1_j, r_j), \qquad (8)$$

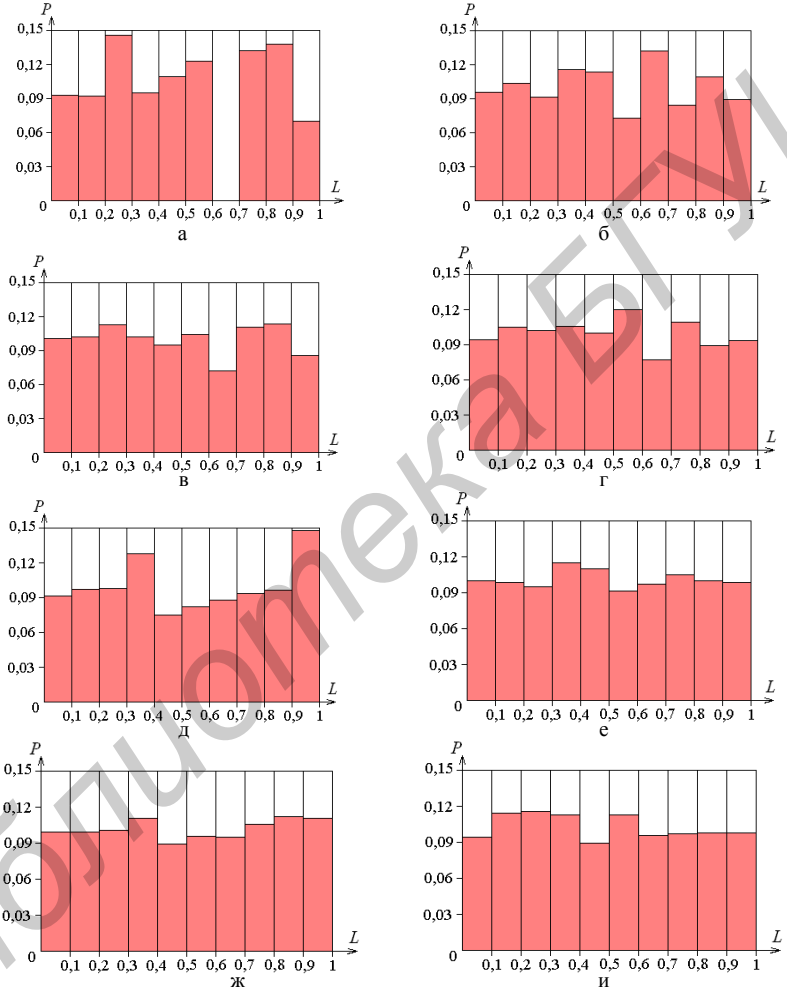
где j – номер комбинации количества r_j непрерывных подпоследовательностей бит и количества $n1_j$ единиц в подпоследовательности, суммирование осуществляется для комбинаций, при которых $P_T = p_{Ti}$; $P(n1_j, r_j) = 2\binom{n1_j - 1}{r_j/2 - 1}\binom{n - n1_j - 1}{r_j/2 - 1}/\left(2^n\right)$, если r_j – четное число; $P(n1_j, r_j) = \left[\binom{n1_j - 1}{(r_j - 1)/2}\binom{n - n1_j - 1}{(r_j - 3)/2} + \binom{n1_j - 1}{(r_j - 3)/2}\binom{n - n1_j - 1}{(r_j - 1)/2}\right]/\left(2^n\right)$, если r_j – четное число.

В случае *теста на самые длинные подпоследовательности единиц в блоках* значения $P(p_{Ti})$ вероятности $P(P_T)$ определяются [3]

$$P(p_{Ti}) = \sum_j \left(\frac{\pi_0^{v_0^{(j)}} \cdot \left(1-\pi_0\right)^{N-v_0^{(j)}} N!}{\left(v_0^{(j)}\right)!\left(N-v_0^{(j)}\right)!} \cdot \frac{\left(\frac{\pi_1}{(1-\pi_0)}\right)^{v_1^{(j)}} \cdot \left(1-\frac{\pi_1}{(1-\pi_0)}\right)^{N-v_0^{(j)}-v_1^{(j)}} \cdot \left(N-v_0^{(j)}\right)!}{\left(N-v_0^{(j)}-v_1^{(j)}\right)!\left(v_1^{(j)}\right)!} \times \right.$$
$$\left. \times \frac{\left(\frac{\pi_2}{(1-\pi_0-\pi_1)}\right)^{v_2^{(j)}} \cdot \left(1-\frac{\pi_2}{(1-\pi_0-\pi_1)}\right)^{N-v_0^{(j)}-v_1^{(j)}-v_2^{(j)}} \cdot \left(N-v_0^{(j)}-v_1^{(j)}\right)!}{\left(N-v_0^{(j)}-v_1^{(j)}-v_2^{(j)}\right)!\left(v_2^{(j)}\right)!} \right), \qquad (9)$$

где j – номер комбинации чисел элементов в четырех группах, к которым относят блоки последовательности в зависимости от значения максимальной длины непрерывной подпоследовательности единиц, суммирование осуществляется для комбинаций, при которых $P_T = p_{Ti}$; π_k – вероятность отнесения блока к k-й группе; $v_k^{(j)}$ – число блоков из j-й комбинации, принадлежащих k-й группе; N – количество блоков.

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. Полученные значения P использованы при комплексной оценке результатов тестирования СП длиной 128 и 256 бит.



а, б, в, г, - при длинах СП 128 бит; д, е, ж, и – при длинах СП 256 бит; а, д – для частотного теста; б, е – для частотного теста в подпоследовательностях; в, ж – для теста на подпоследовательности одинаковых бит; г, и – для теста на самые длинные подпоследовательности единиц в блоках

Рисунок 4. – Гистограммы вероятностей *P*

В таблице представлены результаты проверки соответствия найденных теоретических распределений вероятностей P_T равномерному распределению по критерию согласия «хи-квадрат». В таблице χ^2 – случайная величина, значения которой рассчитаны по формуле (2), и P_c – вероятность превышения величиной χ^2 значений, полученных экспериментально.

Таблица – Значения величин χ^2 и P_c

Название теста	n = 128 бит		n = 256 бит	
	χ^2	P_c	χ^2	P_c
Частотный тест	$2{,}1398 \cdot 10^{37}$	0	$5{,}1082 \cdot 10^{75}$	0
Частотный тест в подпоследовательностях	$0{,}8614 \cdot 10^{37}$	0	$0{,}3857 \cdot 10^{75}$	0
Тест на подпоследовательности одинаковых бит	$0{,}5160 \cdot 10^{37}$	0	$0{,}3460 \cdot 10^{75}$	0
Тест на самые длинные подпоследовательности единиц в блоках	$0{,}4309 \cdot 10^{37}$	0	$0{,}4583 \cdot 10^{75}$	0

Таблица показывает, что найденные теоретические распределения не совпадают с равномерным распределением, т. к. все значения $P_c = 0$, что меньше уровня значимости $\alpha 2 = 0{,}0001$. Полученные результаты свидетельствуют о необходимости использования выражений (6)-(9) при комплексной оценке результатов тестирования последовательностей длиной до 256 бит.

С учетом найденных распределений произведена корректировка программного обеспечения АПС тестирования СП. В качестве тестов набора № 2 взяты тесты системы NIST: частотный, частотный в подпоследовательностях, тест на подпоследовательности одинаковых бит, тест на самые длинные подпоследовательности единиц в блоках; при комплексной оценке используются полученные теоретические распределения.

Произведен расчет временных затрат на проверку ГСЧ ЭПК в соответствии с методикой формирования массивов СП и методикой комплексной оценки результатов тестирования СП. Показано, что АПС позволяет оперативно оценить качество работы ГСЧ ЭПК при объеме данных от 1 млн бит.

В **четвертой главе** АПС тестирования СП апробировано путем множества экспериментальных исследований [7, 10, 11, 12]. С использованием АПС проведены исследования по оценке качества работы ГСЧ ЭПК при температурах 0 ˚С, 20 ˚С и 50 ˚С и сформированы массивы

последовательностей длиной 128, 256 и 1024 бит, которые могут быть использованы в качестве ключей.

В **приложениях** представлены результаты исследований СП различной длины, полученных из ЭПК, алгоритмы тестирования СП в среде MATLAB, акты внедрения и использования результатов диссертационной работы.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложена и обоснована методика формирования массивов СП, позволяющая оперативно оценивать качество работы ГСЧ и получать СП для ключевых документов. Методика отличается использованием процедур двухуровневого тестирования для повышения мощности тестов без увеличения длины последовательности, что приводит к экономии времени на генерацию данных [4, 13].

2. Теоретически и экспериментально доказано, что одна из статистик теста серий эквивалентна статистике теста аппроксимированной энтропии при стремлении длины проверяемой последовательности к бесконечности, что позволяет исключить тест аппроксимированной энтропии из системы тестирования при длинах последовательностей от 1 млн бит [2].

3. Разработана методика комплексной оценки результатов тестирования СП, которая предусматривает нахождение теоретических распределений вероятностей превышения тестовыми статистиками экспериментальных значений, что позволяет использовать двухуровневые тесты при относительно коротких длинах СП до 256 бит. Найдены теоретические распределения вероятностей превышения тестовыми статистиками значений, получаемых экспериментально, по частотному тесту, частотному тесту в подпоследовательностях, тесту на подпоследовательности одинаковых бит, тесту на самые длинные подпоследовательности единиц в блоках при длинах СП 128 и 256 бит [3].

4. Разработано аппаратно-программное средство тестирования СП, основанное на методике формирования массивов СП и методике комплексной оценки результатов тестирования СП, позволяющее оперативно осуществлять статистическое тестирование ГСЧ и получать массивы СП, пригодные для использования в качестве криптографических ключей [1, 5, 8].

Рекомендации по практическому использованию результатов

1. Предложенная методика формирования массивов случайных последовательностей может быть использована для оперативной оценки качества работы ГСЧ и получения случайных последовательностей, предназначенных для криптографических приложений.

2. Предложенная методика комплексной оценки результатов тестирования, основанная на проверке соответствия эмпирических распределений вероятностей превышения тестовыми статистиками экспериментальных значений теоретическим распределениям, которые требуется находить при заданной длине последовательности, может быть использована в любой из существующих систем тестирования.

3. Разработанное аппаратно-программное средство тестирования случайных последовательностей может применяться в качестве средства для оперативной оценки качества ГСЧ и формирования массивов случайных последовательностей для ключевых документов.

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 // Вестник связи. – 2014. – № 4 (124). – С. 33–37.

Статьи в сборниках материалов семинаров и научных трудов

5. 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 международного науч.-техн. семинара, Минск, 2011 г. / БГУИР. – Минск, 2011. – С. 83–88.

6. 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 международного науч.-техн. семинара, Минск, 2012 г. / БГУИР. – Минск, 2012. – С. 65–69.

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 / УО ВГКС. – Минск, 2013. – С. 30–33.

Тезисы докладов на научных конференциях

8. Киевец, Н.Г. Датчик случайных чисел на основе электронных пластиковых карт // Технические средства защиты информации: тез. докл. VIII Белорусско-российской науч.-техн. конф., Браслав, 24–28 мая 2010 г. / БГУИР. – Минск, 2010. – С. 62–63.

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 Международной науч.-техн. конф. Минск, 27–29 сентября 2011 г. / ВГКС. – Минск, 2011. – С. 97.

10. 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 Международной науч.-техн. конф. Минск, 16 октября–8 октября 2012 г. / ВГКС. – Минск, 2012. – С. 217.

11. Киевец, Н.Г. Тестирование генераторов случайных чисел электронных пластиковых карт по методологии NIST / Н.Г. Киевец // Технические средства защиты информации: тез. докл. XI Белорусско-российской науч.-техн. конф., Минск, 5–6 июня 2013 г. / БГУИР. – Минск, 2013. – С. 41.

12. Киевец, Н.Г. Тестирование генераторов случайных чисел электронных пластиковых карт по системе NIST / Н.Г. Киевец // Современные средства связи: материалы XVIII Международной науч.-техн. конф. Минск, 15 октября – 16 октября 2013 г. / ВГКС. Минск, 2013. – С. 203.

13. Киевец, Н.Г. Методика тестирования последовательностей криптографических ключей / Н.Г. Киевец // Технические средства защиты информации: тез. докл. XI Белорусско-российской науч.-техн. конф., Минск, 28–29 мая 2014 г. / БГУИР. – Минск, 2014. – С. 26–27.

РЭЗЮМЭ

Кіевец Наталля Рыгораўна

Апаратна-праграмны сродак тэсціравання выпадковых паслядоўнасцеў для ключавых дакументаў

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

Мэта работы заключаецца ў даследаванні метадаў статыстычнага тэсціравання выпадковых паслядоўнасцеў і распрацоўцы апаратна-праграмнага сродку, прызначанага для фарміравання масіваў выпадковых паслядоўнасцеў для ключавых дакументаў.

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'ютэр, электронныя пластыкавыя карты і рыдар.

Атрыманыя вынікі і іх навізна: распрацаваны апаратна-праграмны сродак, які дазваляе рэалізаваць методыку фарміравання масіваў паслядоўнасцеў для ключавых дакументаў на аснове іх статыстычнага тэсціравання; даказана, што адна са статыстык тэста серый і статыстыка тэста апраксімаванай энтрапіі эквівалентныя пры імкненні даўжыні паслядоўнасці да бясконцасці; распрацавана методыка комплекснай ацэнкі вынікаў тэсціравання выпадковых паслядоўнасцеў, якая дазваляе за кошт выкарыстання працэдур двухузроўневага тэсціравання павялічыць магутнасць тэстаў без павелічэння колькасці элементаў паслядоўнасцеў.

Ступень выкарыстання: распрацаваны апаратна-праграмны сродак тэсціравання выпадковых паслядоўнасцеў ужываўся ў ЗАТ "Цэнтр новых інтэлектуальных інтэграваных сістэм" і ЗАТ «НТЦ Кантакт»пры фарміраванні масіваў крыптаграфічных ключоў; методыка комплекснай ацэнкі вынікаў тэсціравання выпадковых паслядоўнасцеў укараненая ў навучальны працэс установы адукацыі "Беларускі дзяржаўны ўніверсітэт інфарматыкі і радыеэлектронікі".

Вобласць ужывання: інфармацыйная бяспека.

РЕЗЮМЕ

Киевец Наталья Григорьевна

Аппаратно-программное средство тестирования случайных последовательностей для ключевых документов

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

Цель работы состоит в разработке аппаратно-программного средства тестирования случайных последовательностей для оперативной оценки качества работы генераторов случайных чисел и формирования массивов случайных последовательностей для ключевых документов.

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, позволяющее реализовать методику формирования массивов случайных последовательностей для ключевых документов на основе их статистического тестирования; доказано, что одна из статистик теста серий и статистика теста аппроксимированной энтропии эквивалентны при стремлении длины последовательности к бесконечности; разработана методика комплексной оценки результатов тестирования случайных последовательностей, позволяющая за счет использования процедур двухуровневого тестирования повысить мощность тестов без увеличения количества элементов последовательностей.

Степень использования: разработанное аппаратно-программное средство тестирования случайных последовательностей применялось в ЗАО «Центр новых интеллектуальных интегрированных систем» и ЗАО «НТЦ Контакт» при формировании массивов криптографических ключей; методика комплексной оценки результатов тестирования случайных последовательностей внедрена в учебный процесс учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Область применения: информационная безопасность.

SUMMARY

Kiyevets Natallia Grigoryevna

Hardware-software means of testing of random sequences for key documents

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

Aim of the work is to study the methods of statistical testing of binary sequences and working out of the hardware-software means intended for formation of random sequences files for key documents.

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 are developed that allowed to realise a technique of formation of sequence files for key documents based on statistical testing; it is proved that one of serial test statistics and approximation entropy test statistic are equivalent at aspiration of sequence length to infinity; the technique of the interpretation of empirical testing results has been developed, that allow to increase the power of tests due to two-level testing without increase in the sequence length.

Extend of usage: the developed hardware-software means of testing of random sequences was applied in closed companies «Center of the new intellectual integrated systems» and « Scientific and technical centre Contact» at formation of cryptographic key files; the technique of the interpretation of empirical testing results is introduced in educational process of education establishment «Belarussian state university of informatics and radioelectronics».

Scope: information security.

Научное издание

Киевец Наталья Григорьевна

АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ

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.	Тираж 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.
ЛП № 02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6.