Література: ***1.*** *А. Ю. Ільніцький, В. В. Шорошев, І. Л. Близнюк. Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" (шифр "Торсіон-1"). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді програмного продукту "Торсіон-1". – К.: Видавництво НАВСУ, 2003 р. – 316 с.* ***2.*** *Шорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно европейским "Критериям оценки безопасности информационных технологий ITSEC" (Information Technology Security Evaluation Criteria). Журнал "Бизнес и безопасность" № 3, 1998 г.* ***3.*** *Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 1 1999г. Рекомендации по основам информационной безопасности согласно Единых критериев CCITSE (Common Criteria for Information Technology Security Evaluation), 1996-1997 г.г.* ***4.*** *Стандарт ISO/IEC 17799: 2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.* ***5.*** *Стандарт ISO/1EC 15408: 2000. Information technology - Security techniques -Evaluation criteria for IT security. - Part 1: Introduction and general model.* ***6.*** *Стандарт ISO/IEC 15408: 2000. Information technology - Security techniques Evaluation criteria for IT security. - Part 2: Security functional requirements.* ***7.*** *Стандарт ISO/IEC 15408: 2000. Information technology - Security techniques -Evaluation criteria for IT security. - Part 3: Security assurance requirements.* ***8.*** *Шорошев В. В. Модель угроз для локальних вычислительных сетей по рекомендаціям Конвенции Сонета Европы о кибеопреступности. Науково-виробничий журнал Державної адміністрації зв'язку та інформатизації України "Зв'язок" № 4, 2005. С. 37-42.* ***9.*** *Шорошев В. В., Близнюк И. Л., Балина С. Н. Классификация угроз для компьютерніх данных и систем по рекомендациям Конвенции о киберпреступности Сонета Европы. Бизнес и безопасность № 1, 2005. С. 36-39.* ***10.*** *Шорошев В. В., Близнюк І. Л. Моделі загроз комп'ютерним даним і системам за Конвенцією Ради Європи про кіберзлочинність. // Науковий вісник НАВСУ. – К., 2005. - № 6.- С. 119-128.*

УДК 681.3.06

МНОГОМЕРНЫЙ СТАТИСТИЧЕСКИЙ ТЕСТ ДЛЯ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Михаил Савчук, Виталий Шарапов
Физико-технический институт Национального технического университета Украины "КПИ"

Аннотация: **Строится многомерный статистический критерий проверки качества случайных последовательностей. С использованием слабой сходимости векторных случайных процессов находятся асимптотические распределения статистик. Приводятся формулы, облегчающие практическое использование критерия. Даются рекомендации по выбору параметров.**
Summary: **The multidimensional statistical criterion of quality check of casual sequences is constructed. Weak convergence of vector casual processes is used for research of asymptotic statistics distributions. Formulas facilitating practical use of criterion and recommendations for parameters selection are presented.**
Ключевые слова: **Многомерный случайны процесс, неравновероятные последовательности, сходимость случайных процессов, случайные и псевдослучайные последовательности, статистический критерий.**

I Постановка задачи

Пусть задана последовательность $\varepsilon = \varepsilon_1\varepsilon_2\ldots\varepsilon_s$, $\varepsilon_i \in \{0,1\}$, $i = 1,\ldots,s$, которую рассматриваем как реализацию некоторого случайного дискретного процесса. Необходимо проверить гипотезу H_0 о том, что последовательность ε является реализацией последовательности независимых двоичных знаков, которые с вероятностью p, $0 < p < 1,$ принимают значение 1, иначе говоря, случайные величины ε_i независимы в совокупности и $\forall i = 1,\ldots,s \;\; P(\varepsilon_i = 1) = 1 - P(\varepsilon_i = 0) = p$.

II Построение случайного процесса

Пусть $s = nN$. Введем случайные процессы на интервале $[0,1]$:

$$Y_N^i(t)=\sum_{l=1}^{[Nt]}\delta(i,\sum_{m=0}^{n-1}\varepsilon_{mN+l}),\ i=0,...,n,\ t\in[0,1],\ \sum_{i=0}^{n}Y_N^i(t)=[Nt], \tag{1}$$

где $[x]$ – целая часть вещественного числа x, $\delta(i,j)$ – символ Кронекера, равный 1 при $i=j$ и равный 0 при $i\neq j$;

$$\mu_N^i(t)=N^{-1/2}(Y_N^i(t)-MY_N^i(t)),\ i=0,...,n,\ t\in[0,1]. \tag{2}$$

Таким образом, $\mu_N^i(t)$ – центрированный случайный процесс с математическим ожиданием $M\mu_N^i(t)=0$.

Построение случайного процесса (1) по случайной последовательностью $\varepsilon=\varepsilon_1\varepsilon_2\ldots\varepsilon_s$, $\varepsilon_i\in\{0,1\}$, $i=1,\ldots,s$, $s=nN$, удобно описать следующим образом. Записываем последовательность по строкам в $(n\times N)$ - матрицу: то есть первая строка матрицы – $\varepsilon_1\varepsilon_2\ldots\varepsilon_N$, вторая строка – $\varepsilon_{N+1}\varepsilon_{N+2}\ldots\varepsilon_{2N}$ и т. д. до *n*-ой строки – $\varepsilon_{(n-1)N+1}\varepsilon_{(n-1)N+2}\ldots\varepsilon_{nN}$. Случайный процесс $Y_N^i(t)$ – это число столбцов от первого до столбца с номером $[Nt]$ таких, которые содержат ровно i единиц, $0\le t\le 1$.

III Слабая сходимость векторных случайных процессов

Теорема 1. Когда $N\to\infty$, $n=const\ge 1$ последовательность случайных процессов

$$\mu_N(t)=(\mu_N^1(t),\mu_N^2(t),\ldots,\mu_N^n(t)), \tag{3}$$

слабо сходится в *n*-мерном пространстве D^n функций без разрыва 2-го рода с топологией Скорохода к непрерывному с вероятностью 1 гауссовскому диффузионному процессу с нулевым математическим ожиданием и матрицей корреляционных функций

$$K(t,s)=\left\|k_{ij}(t,s)\right\|_1^n,\ k_{ij}(t,s)=b_i(n,p)(\delta_{ij}-b_j(n,p))\min\{t,s\},$$

$$b_i(n,p)=C_n^i p^i(1-p)^{n-i}.$$

Доказательство. Будем использовать метод доказательства слабой сходимости векторных случайных процессов, описанный в работе [1, гл. 7]. Обозначим $t_{Nk}=k/N, k=0,1,...,N$. $\mu_{Nk}=\mu_N(t_{Nk})$. Последовательность серий случайных векторов

$$\mu_{N0},\ \mu_{N1},\mu_{N2},...,\mu_{NN},\ N=1,2,3,... \tag{4}$$

связана в каждой серии в цепь Маркова и $P(\mu_{N0}=0)=1$. Обозначим $\Delta t_{Nk}=t_{N,k+1}-t_{Nk}$, $\Delta Y_{Nk}^i=Y_{N,k+1}^i-Y_{Nk}^i$, $\Delta\mu_{Nk}=\mu_{N,k+1}-\mu_{Nk}$. Найдутся борелевские функции $a_{Nk}(x)=(a_{Nk}^1(x),...,a_{Nk}^n(x))\in R^n$, $B_{Nk}^2(x)=\left\|b_{Nk}^{ij}(x)\right\|_1^n\in R^{n\times n}$, $x=(x_1,...,x_n)$, такие, что $\alpha_{Nk}=a_{Nk}(\mu_{Nk})$, $\beta_{Nk}=B_{Nk}^2(\mu_{Nk})$ и $\Delta\mu_{Nk}=\alpha_{Nk}\Delta t_{Nk}+\beta_{Nk}\Delta\psi_{Nk}$ где $\Delta\psi_{Nk}=\beta_{Nk}^{-1}(\Delta\mu_{Nk}-\alpha_{Nk}\Delta t_{Nk})$.

При условии, что $\varepsilon=\varepsilon_1\varepsilon_2\ldots\varepsilon_s$ является последовательностью независимых знаков и $P(\varepsilon_i=1)=p$ (т. е. при условии справедливости гипотезы H_0), a_{Nk}^i и b_{Nk}^{ij} не зависят от $\mu_{Nk}=\mu_N(t_{Nk})$ и поэтому находим для любых $k=0,1,\ldots,N-1$, $i,j=1,2,\ldots,n$ следующие выражения:

$$M\Delta Y_{Nk}^i=b_i(n,p),\ \text{где}\ b_i(n,p)=C_n^i p^i(1-p)^{n-i},$$

$$MY_{Nk}^i=kb_i(n,p),\ MY_N^i(t)=\sum_{l=1}^{[Nt]}\delta(i,\sum_{m=0}^{n-1}\varepsilon_{mN+l})=[Nt]b_i(n,p),$$

$$a_{Nk}^i=N\,M\Delta\mu_{Nk}^i=\sqrt{N}\,M(\Delta Y_{Nk}^i-M\Delta Y_{Nk}^i)=0,$$

$$b_{Nk}^{ii}=D\Delta Y_{Nk}^i=M(\Delta Y_{Nk}^i)^2-(M\Delta Y_{Nk}^i)^2=b_i(n,p)(1-b_i(n,p)),$$

$$b_{Nk}^{ij} = \mathrm{cov}(\Delta Y_{Nk}^{i}, \Delta Y_{Nk}^{j}) = M\Delta Y_{Nk}^{i}\Delta Y_{Nk}^{j} - M\Delta Y_{Nk}^{i} M\Delta Y_{Nk}^{j} = -b_i(n,p)b_j(n,p), \text{ при } i \neq j.$$

Обозначим $a_N(t,x) = a_{Nk}(x)$ и $B_N(t,x) = B_{Nk}(x)$, когда $t \in [t_{Nk}, t_{N,k+1})$, $k = 0,1,..., N-1$. Таким образом, $a_N(t,x) = (0,...,0) \in R^n$, $B_N^2(t,x) = \left\| b_{ij} \right\|_1^n$, где $b_{ij} = b_i(n,p)(\delta_{ij} - b_j(n,p))$, не зависят от N, t, x; δ_{ij} – символ Кронекера. Пусть $a\ (t,x) = (0,...,0) \in R^n$, $B^2(t,x) = \left\| b_{ij} \right\|_1^n$, $b_{ij} = b_i(n,p)(\delta_{ij} - b_j(n,p))$.

Тогда для последовательностей серий случайных векторов (4), неслучайных моментов t_{Nk} и функций $a_N(t,x)$, $B\ (t,x) = \sqrt{B^2(t,x)}$ будут выполняться условия леммы 1 параграфа 7.1 из [1]. Таким образом, последовательность случайных процессов (3) слабо сходится в *n*-мерном пространстве D^n функций без разрыва 2-го рода с топологией Скорохода к решению стохастического дифференциального уравнения

$$d\mu(t) = Bdw(t), \quad \mu(0) = (0,...,0) \in R^n, \tag{5}$$

где $w(t)$ – стандартный *n*-мерный винеровский случайный процесс. Предельный диффузионный процесс $\mu(t)$ имеет нулевой вектор сноса и оператор диффузии $B^2 = \left\| b_{ij} \right\|_1^n$, $b_{ij} = b_i(n,p)(\delta_{ij} - b_j(n,p))$. Фундаментальная матрица решений уравнения (5) $\Phi(t,s) = E$ является единичной матрицей, потому что $\frac{\partial \Phi(t,0)}{\partial t} = 0$, $\Phi(0,0) = E$, $\Phi^{-1}(t,0) = \Phi(0,t)$. Согласно лемме 2 параграфа 7.1 из [1] решением уравнения (5) является непрерывный с вероятностью 1 гауссовский диффузионный процесс с нулевым математическим ожиданием и корреляционной функцией $K(t,s) = B^2 \min\{t,s\}$. Теорема доказана.

Таким образом, для любого фиксированного t, $0 < t \leq 1$, асимптотическое распределение случайного вектора $\mu_N(t) = (\mu_N^1(t), \mu_N^2(t), \ldots, \mu_N^n(t))$, который построен по последовательности независимых бит ε с вероятностью p, $0 < p < 1$, появления 1 (гипотеза H_0), согласно теореме 1 является невырожденным гауссовским распределением с нулевым математическим ожиданием и корреляционной матрицей $K(t) = B^2 t$. Существует невырожденная матрица $A(t)$ такая, что $A(t)A'(t) = K(t)$ и $\mu(t) = A(t)\eta(t)$, где $\mu(t)$ и $\eta(t)$ – векторы-столбцы, $A'(t)$ транспонированная матрица, а $\eta(t) = (\eta_1(t), \eta_2(t), ..., \eta_n(t))$ – случайный вектор, который имеет стандартное n-мерное гауссовское распределение. То есть, координатные случайные величины $\eta_i(t), i = 1,..,n,$ независимые и имеют нормальное распределение с параметрами (0; 1) [2]. Известно, что случайная величина $\xi(t) = \eta_1^2(t) + \eta_2^2(t) + ... + \eta_n^2(t)$ имеет χ^2- распределение с n степенями свободы, а случайная величина $\sqrt{\xi}$ имеет χ- распределение с n степенями свободы. Существует обратная матрица $A^{-1}(t)$ и вектор $\eta(t)$ можно записать в виде $\eta(t) = A^{-1}(t)\mu(t)$.

IV Статистический критерий

1. Пусть задана последовательность $\varepsilon' = \varepsilon_1\varepsilon_2\ldots\varepsilon_v$.

   Выбираются параметры алгоритма:

   $n, N, s \in \mathbf{N}$ так, что $n = \left[\frac{v}{N}\right]$, $s = nN$;

   k моментов времени $0 < t_1 < t_2 < ... < t_k \leq 1$;

   уровень значимости критерия согласия α, $0 < \alpha < 1$.

   Дальше будем рассматриваем последовательность $\varepsilon = \varepsilon_1\varepsilon_2\ldots\varepsilon_s$.

2. По последовательности $\varepsilon = \varepsilon_1\varepsilon_2\ldots\varepsilon_s$ строим случайные величины и векторы:

$$Y_N^i(t_j) = \sum_{l=1}^{[Nt_j]} \delta(i, \sum_{m=0}^{n-1} \varepsilon_{mN+l}),$$

$$\mu_N^i(t_j) = N^{-1/2}(Y_N^i(t_j) - MY_N^i(t_j)),\ i = 1,...,n,\quad j = 1,2,...,k,$$

$$\mu_N(t_j) = (\mu_N^1(t_j), \mu_N^2(t_j), ..., \mu_N^n(t_j)),\quad j = 1,2,...,k,$$

$$\mu_N(t_1,...,t_k) = (\mu_N(t_1), \mu_N(t_2), ..., \mu_N(t_k)).$$

Последний nk-мерный вектор имеет асимптотически $(nk \times nk)$ - матрицу ковариаций $\sum = \|K(t_l, t_m)\|$, $l, m = 1,2,...,k$, которая образованна k^2 блоками, каждый блок соответственной $n \times n$-матрицей. Так l-й сверху и *m*-й слева блок образованы матрицей $K(t_l, t_m)$ в соответствии с теоремой 1.

3. Находим $(nk \times nk)$ - матрицу A такую, что $AA' = \sum$, и обратную матрицу A^{-1}.

Находим выборочное значение гауссовского вектора со стандартным nk-мерным распределением $\eta(t_1,...,t_k) = A^{-1}\mu_N(t_1,...,t_k)$.

4. Подсчитываем значение статистики $\xi(t_1,...,t_k) = \eta_1^2 + \eta_2^2 + ... + \eta_{nk}^2$, где η_i, $i = 1,...,nk$, координаты вектора $\eta(t_1,...,t_k)$. Находим квантиль $Z_{1-\alpha}$ уровня $1-\alpha$ χ^2-распределения с nk степенями свободы.

5. Если значение статистики $\xi(t_1,...,t_k) > Z_{1-\alpha}$, то гипотеза H_0 о том, что последовательность ε является реализацией последовательности независимых двоичных знаков, которые с вероятностью p, $0 < p < 1$, принимают значение 1, отклоняется с уровнем значимости α. Значение $Z_{1-\alpha}$ определяет эллипсоид концентрации многомерного распределения.

Если значение статистики $\xi(1) \le Z_{1-\alpha}$, то гипотеза H_0 принимается с уровнем значимости α, как не противоречащая данной последовательности ε. Т. е. последовательность ε считается реализацией дискретного случайного процесса, который генерирует независимые знаки $\varepsilon_i \in \{0,1\}$ и $P(\varepsilon_i = 1) = p$.

V Вычисление матрицы A

Матрица A, которая удовлетворяет выражению $AA' = \sum$, является нижней треугольной матрицей. Пусть $A = \|a_{ij}\|_1^{nk}$, $\Sigma = \|\sigma_{ij}\|_1^{nk}$, тогда $\sigma_{ij} = \sum_{l=1}^{nk} a_{il}a_{jl}$. С учетом того, что $a_{ij} = 0$ для $i < j$, можно записать, что

$$\sigma_{ij} = \begin{cases} \sum_{v=1}^{j} a_{iv}a_{jv}, & j \le i \le nk; \\ 0, & i < j. \end{cases}$$

Отсюда получаем следующую систему уравнений:

$$\begin{cases} \sigma_{11} = a_{11}^2 \\ \sigma_{21} = a_{11}a_{21} + a_{21}a_{22} \\ \sigma_{22} = a_{21}^2 + a_{22}^2 \\ \sigma_{31} = a_{11}a_{31} \\ \sigma_{32} = a_{21}a_{31} + a_{22}a_{32} \\ \sigma_{33} = a_{31}^2 + a_{32}^2 + a_{33}^2 \\ \dots \quad \dots\dots\dots\dots \end{cases}$$

Для произвольного $w = \overline{1, nk}$ можно записать

$$\begin{cases} \sigma_{w1} = a_{11}a_{w1} \\ \sigma_{w2} = a_{11}a_{w1} + a_{22}a_{w2} \\ \sigma_{w3} = a_{31}a_{w1} + a_{32}a_{w2} + a_{33}a_{w3} \\ \dots \quad \dots\dots\dots\dots \\ \sigma_{wm} = a_{m1}a_{w1} + a_{m2}a_{w2} + \dots + a_{mm}a_{wm}, m < w \\ \dots \quad \dots\dots\dots\dots \\ \sigma_{ww} = a_{w1}^2 + a_{w2}^2 + \dots + a_{ww}^2 \end{cases} \tag{6}$$

Из системы (6) можно вывести общее рекуррентное соотношение для элементов матрицы A:

$$\begin{cases} a_{ww} = \sqrt{\sigma_{ww} - \sum_{j=1}^{w-1} a_{wj}^2}, \quad 1 \le w \le nk \\ a_{iw} = \dfrac{\sigma_{iw} - \sum_{j=1}^{w-1} a_{ij}a_{wj}}{a_{ww}}, \quad w < i \le nk \end{cases} \tag{7}$$

Матрица $\sum$ блочная и ее элементы выражаются через элементы матрицы $K(s,t)$ как $\sigma_{i,j} = b_{i \bmod n, j \bmod n} \min\{t_{\lceil i/n \rceil}, t_{\lceil j/n \rceil}\}$, где $x \bmod n \in \{1,2,\dots,n\}$. Таким образом

$$\sigma_{ij} = \begin{cases} (C_n^{i'} p^{i'}(1-p)^{n-i'} - (C_n^{i'} p^{i'}(1-p)^{n-i'})^2) t_{\lceil i/n \rceil}, & i = j; \\ -C_n^{i'} C_n^{j'} p^{i'+j'}(1-p)^{2n-i'-j'} t_{\lceil i/n \rceil}, & i \ne j; \end{cases} \tag{8}$$

где $i' = i \bmod n$, $j' = j \bmod n$, $i \bmod n \in \{1,2,\dots,n\}$.

Широко распространенным является случай равновероятности бит, то есть когда $p = 1/2$, в этом случае формула (8) принимает более простой вид:

$$\sigma_{ij} = \begin{cases} \dfrac{1}{2^n} C_n^{i'} (1 - \dfrac{1}{2^n} C_n^{i'}) t_{\lceil i/n \rceil}, & i = j; \\ -\dfrac{1}{2^{2n}} C_n^{i'} C_n^{j'} t_{\lceil i/n \rceil}, & i \ne j; \end{cases} \tag{9}$$

Матрица A, может быть легко обращена с помощью метода исключения Гаусса [3]. Необходимо отметить, что при обращении по этому алгоритму нет необходимости выполнять прямой проход, так как матрица изначально треугольная.

VI Экспериментальные исследования

Приведенный выше критерий был апробирован с помощью статистического моделирования на ЭВМ с большим количеством экспериментов. Описываемые в данном разделе эксперименты, относятся к равновероятным последовательностям с независимыми знаками, у которых вероятность p появления единицы (и, соответственного нуля) равна $\dfrac{1}{2}$.

В качестве экспериментального материала использовались следующие двоичные последовательности:

- выходная последовательность блочного шифратора RC6, полученная в режиме счетчика;
- последовательность, сгенерированная с использованием криптографического алгоритма шифрования ГОСТ 28147—89 в соответствии с дополнением А национального стандарта Украины ДСТУ 4145–2002 [4];

- двоичная запись алгебраических чисел $\sqrt{2}$, $\sqrt{13}$ с точностью до 800 миллионов знаков после запятой;
- двоичная запись трансцендентных чисел π, e, $\sqrt{\pi}$, $\sqrt{e}$ с точностью до 400 миллионов знаков после запятой.

Известно, что эти последовательности хорошо моделируют выход дискретного источника с равновероятными независимыми двоичными знаками.

Анализ параметров статистического критерия n и N. При $k=1$, $t_1=1$ для экспериментов выбрано ряд значений для параметров n и N: $n \in \{n_1, n_2, \dots n_c\}$, $N \in \{N_1, N_2, \dots N_d\}$. Необходимо установить какие из сочетаний n_i и N_j, $i=\overline{1,c}$, $j=\overline{1,d}$ будут наиболее предпочтительными в качестве параметров алгоритма, т. е. каким образом лучше разбивать исходную последовательность на блоки.

Пусть для статистического эксперимента взята последовательность $\varepsilon = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$, причем $s \geq (\max\limits_i n_i)(\max\limits_j N_j)Q$, где Q это количество испытаний для одной пары (n_i, N_j). Тогда для каждой пары (i,j), $i=\overline{1,c}$, $j=\overline{1,d}$ строится вариационный ряд $X(i,j)$ из значений статистики $\xi(1)$ ($X = X_{(1)}, X_{(2)}, \dots X_{(Q)}$). Полученные вариационные ряды сравниваются с квантилями распределения χ^2 с n_i степенями свободы. Каждый из полученных вариационных рядов отображался в виде графика путем откладывания на координатной плоскости точек $(\frac{l}{Q}, X_{(l)})$ где $l=\overline{1,Q}$. На той же координатной плоскости стоилась функция $Z(\alpha)$ – функция квантилей уровня α для распределения χ^2 с n_i степенями свободы. Примеры таких графиков приведены на рис. 1 и 2; сплошной линией изображен график функции $Z(\alpha)$, а пунктирной – график вариационного ряда; при построении этих графиков Q бралось 10^5.

Анализ параметров времени $t_1, t_2, \dots, t_k$, k. Пусть уже выбраны и зафиксированы параметры n и N. Тогда можно построить вариационные ряды $X(k, t_1, \dots, t_k)$ для различных k и комбинаций $t_1, t_2, \dots, t_k$ из значений статистики $\xi(t_1, t_2, \dots t_k)$. На практике были проведены эксперименты для случаев $k = 2, \dots, 5$. Временной параметр t_k брался всегда равным 1, а параметры $t_1, t_2, \dots, t_{k-1}$ рассматривались по всем возможным вариантам с шагом 0.1 для $k \in \{2,3\}$ и 0.2 для $k \in \{4,5\}$. Такие эксперименты были поставлены для всех пар n и N, таких что $n \in \{5,10,15,20,25\}$ и $N \in \{64,128,256,512,1024\}$. Количество испытаний Q бралось 10^3. Сравнение вариационных рядов выполнялось точно такжекак и для параметров n и N с единственной оговоркой, что функция $Z(\alpha)$ – это функция квантилей уровня α для распределения χ^2 с $n_i k$ степенями свободы.

VII Выбор параметров

С помощью вышеописанных экспериментов было изучено поведение вероятностных характеристик критерия при различных параметрах алгоритма, что позволяет привести ряд рекомендаций по выбору этих параметров с учетом точности аппроксимации предельными распределениями.

Для проверки качества отдельно взятых последовательностей рекомендуется использовать один временной параметр $k=1$, $t_1=1$. Параметры n, N выбирать исходя из длины последовательности согласно табл. 1. Проверку осуществлять с уровнем значимости не превосходящим 0.8: $0 < \alpha \leq 0.8$.

Несколько временных параметров $k>1$ рекомендуется использовать в случае, когда:

– необходимо проверить не отдельно взятую последовательность, а генератор двоичных последовательностей;

– необходимо проверить длинную, более 30 тысяч бит, последовательность.

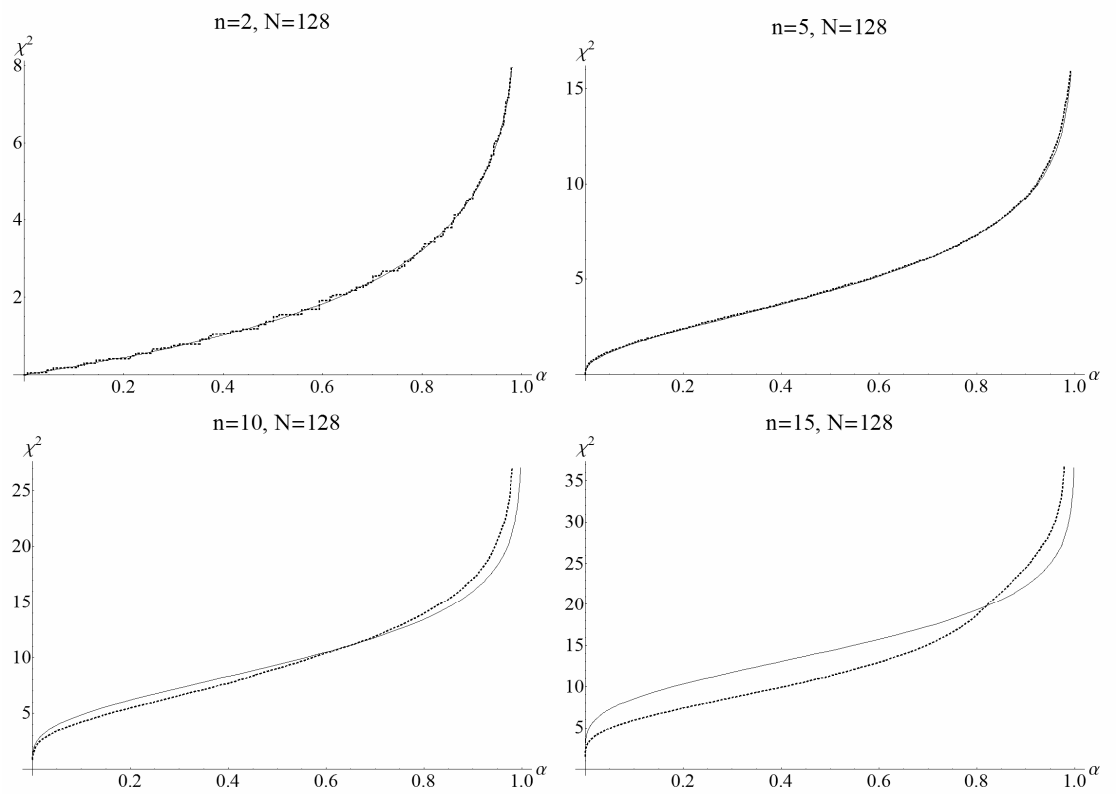

Рисунок 1 – Зависимость теоретического и экспериментального значения квантиля от уровня значимости критерия α для различных n при $N=128,\ k=1,\ t_1=1$

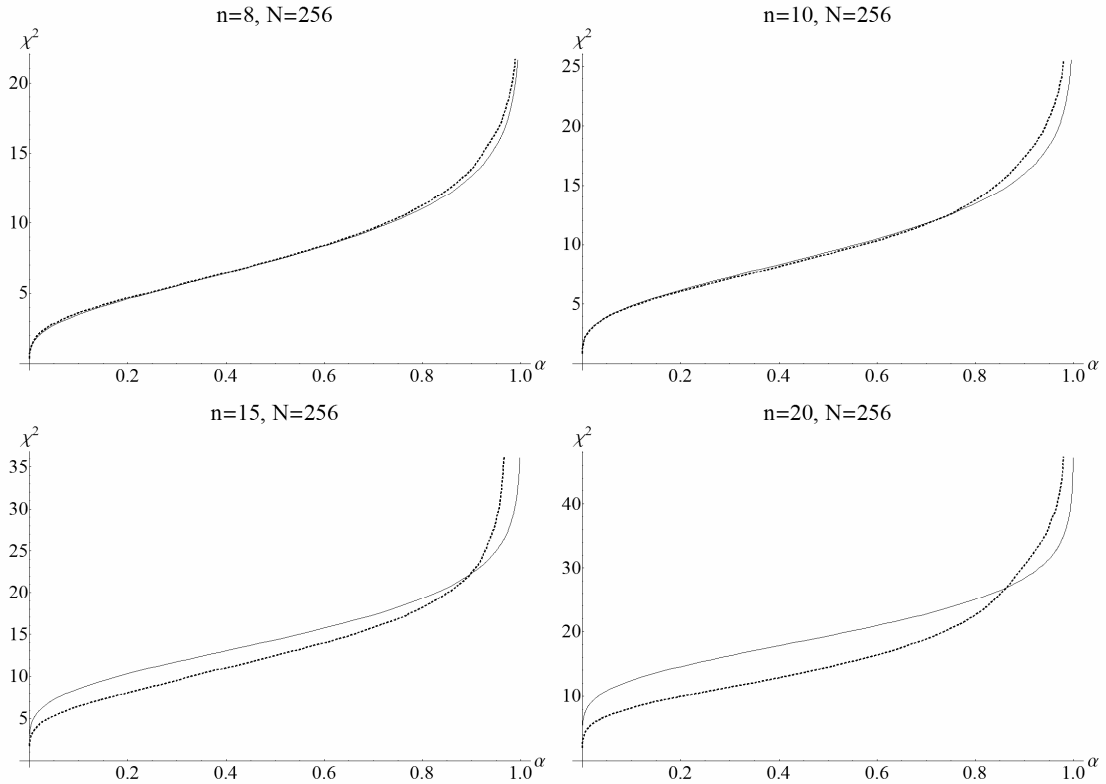

Рисунок 2 – Зависимость теоретического и экспериментального значения квантиля от уровня значимости критерия α для различных n при $N=256,\ k=1,\ t_1=1$

Рекомендуется использовать четное количество временных параметров, так чтобы один из них был равен **1**, а остальные были симметричны относительно **0.5**. Например, $\{0.2,0.5,0.8,1\}$ $(0.2 = 0.5 - 0.3, 0.8 = 0.5 + 0.3)$.

Таблица – Рекомендуемое сочетание параметров n и N

N	Размерность n. Рекомендуемый интервал	Наилучшее значение n	Длины последовательностей, бит
768 – 1024	15 – 25	$N/50$	115200 – 25600
324 – 767	10 – 20	$N/35$	3240 – 15340
196 – 323	5 – 15	$N/30$	980 – 4845
96 – 195	2 – 10	$N/20$	192 – 1950
32 – 95	2 – 8	$N/10$	64 – 760

VIII Выводы

Приведенный статистический тест, основанный на использовании многомерных случайных процессов, позволяет эффективно анализировать случайные и псевдослучайные битовые последовательности. Данный тест ориентирован на работу с короткими и средними последовательностями и позволяет также тестировать очень короткие последовательности. Тест дает возможность анализировать неравновероятные битовые последовательности.

Литература: ***1.*** *Коваленко И. Н., Левитская А. А., Савчук М. Н. Избранные задачи вероятностной комбинаторики. – К.: Наук. думка, 1986, - 224с.* ***2.*** *Афифи А., Эйзен С. Статистический анализ. Поход с использованием ЭВМ. – М.: Мир, 1982. – 488с.* ***3.*** *Турчак Л. И. Основы численных методов: Учеб. пособие. – М.: Наука. Гл. ред. физ-мат. лит., 1987. – 320 с.* ***4.*** *ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння.*

УДК 681.3:621.396

СПЕЦИАЛЬНЫЕ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ В ТЕЛЕКОММУНИКАЦИЯХ И КРИТЕРИИ ОЦЕНКИ ИХ ЭФФЕКТИВНОСТИ

Геннадий Максименко
Национальная Комиссия по вопросам регулирования связи Украины, Киев

Аннотация: **Изложены общетеоретические и концептуальные подходы к построению специальных систем поддержки принятия решений, используемых в телекоммуникационных сетях для выявления и анализа критических событий с целью устранения преднамеренных или непреднамеренных негативных воздействий на сеть. Приведены критерии оценки эффективности функционирования таких систем**.

Summary: **This article deals with theoretical and conceptual ideas to crate special intellectual expert systems for detection and analysis critical anomaly events in telecommunication networks. The aim of this expert systems to prevent network negative influences. In article gives performance criteria's of this expert systems.**

Ключевые слова: **Система поддержки принятия решений, мониторинг, аномалия сети, прогнозирование**.

I Введение

Одной из наиболее важных задач в системе государственного управления является создание систем оценки кризисных ситуаций и негативных явлений в сетях связи, их комплексная оценка, анализ и прогнозирование наиболее вероятных сценариев развития, а также оценка рисков и выработка мер по минимизации последствий.