Литература

1. Трубей А.И., Палуха В.Ю., Пирштук И.К., Мальцев М.В., Ращеня Н.А. *Методика тестирования случайных последовательностей на основе статистического расстояния и закона повторного логарифма* // Проблемы защиты информации. Сборник научных статей. 2020. № 16. С. 64–94.

2. Волошко В.А., Вечерко Е.В. *Новые верхние границы для функции нецентрального хи-квадрат распределения* // Журнал Белорусского государственного университета. Математика. Информатика. 2020. № 1. С. 70–74.

О ПРИМЕНЕНИИ ТЕСТА МОНОБИТ ДЛЯ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ КОРОТКИХ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.Н. Гайдук

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь gaidukan@bsu.by

В работе [1] предлагается два подхода к оценке результатов тестирования случайных и псевдослучайных последовательностей: определение доли последовательностей с p-значением, превышающим определенную границу, и распределение p-значений на отрезке [0,1]. Для проверки распределения p-значений на отрезке [0,1] используется тест хи-квадрат, который разбивает отрезок [0,1] на 10 одинаковых частей с вероятностью попадания p-значения в любой подинтервал равной 0.1.

При тестировании коротких последовательностей возникают две основные проблемы. Первая заключается в том, что согласно [2] аппроксимирующие распределения не могут быть применены, и должны быть заменены на точные значения распределений, которые трудно найти. Вторая проблема заключается в том, что вероятность попадания p-значения в подинтервал не одинакова для всех подинтервалов. Это следует из того факта, что рассматриваются дискретные случайные величины, а не их аппроксимации непрерывными случайными величинами. Для решения этих проблем в работе [2] предложен альтернативный подход, который предполагает использовать исходное распределение p-значений. Затем, для каждого теста вычисляется вероятность попадания p-значения в каждый подинтервал. Обозначим $p_i = P(\frac{i}{10} \leq p\text{-}value \leq \frac{i+1}{10})$ для $i = 0, \ldots 9$.

В работе [2] рассмотрены значения длин последовательности $n = 128, 160, 256$. В таблице 1 представлены теоретическое распределение p-значений в зависимости от длины последовательности $n = 192, 512, 1024$ для теста монобит.

Литература

1. Rukhin, A., A statisticaltest suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 Revision 1a (2010) / A. Rukhin // `http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf`.

2. Sulak, F. *Evaluation of Randomness Test Results for Short Sequences* // Sequences and Their Applications – SETA 2010. – 2010. – Springer. – 309–319 P.

Таблица 1: Теоретическое распределение p-значений в зависимости от длины последовательности n для теста монобит

Интервал	Frequency test		
	$n = 192$	$n = 512$	$n = 1024$
[0.0,0.1)	0.096683	0.101917	0.097623
[0.1,0.2)	0.123088	0.098008	0.102459
[0.2,0.3)	0.059210	0.109480	0.102339
[0.3,0.4)	0.148373	0.091700	0.096399
[0.4,0.5)	0.088755	0.106320	0.112863
[0.5,0.6)	0.097438	0.119488	0.083584
[0.6,0.7)	0.104772	0.063943	0.089312
[0.7,0.8)	0.110345	0.134285	0.093956
[0.8,0.9)	0.113829	0.069399	0.097311
[0.9,1.0)	0.057507	0.105460	0.124154

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ПЛЕНОЧНЫМИ ЭКРАНЫМИ ОТ ВОЗДЕЙСТВИЯ УЗКИХ ПУЧКОВ ЭЛЕКТРОМАГНИТНЫХ ВОЛН

Ерофеенко В.Т.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь bsu_erofeenko@tut.by

Введение. Разработана методика аналитического моделирования побочных электромагнитных излучений (ПЭМИ) в виде узких пучков монохроматических электромагнитных волн $\vec{E}_{\text{уз.п.}}, \vec{H}_{\text{уз.п.}}$, обобщающих гауссовы пучки волн [1]. Используются другие типы пучков волн [2]. Решена краевая задача экранирования узких пучков электромагнитных волн плоским экраном из магнитодиэлектрических материалов в случае ортогонального распространения пучка к экрану.

Краевая задача. При заданном первичном монохроматическом электромагнитном поле $\vec{E}_{\text{уз.п.}}, \vec{H}_{\text{уз.п.}}$ требуется определить поле $\vec{E}_2, \vec{H}_2$, прошедшее в область $D_2(z > \Delta)$ за экраном $D(0 < z < \Delta)$ и поле $\vec{E}_1', \vec{H}_1'$, отраженное от экрана в области $D_1(z < 0)$. Выполнены уравнения

$$\text{rot}\vec{E} = i\omega\mu\vec{H},\ \text{rot}\vec{H} = -i\omega\varepsilon\vec{E},\ \text{в } D, \tag{1}$$

$$\text{rot}\vec{E}_j = i\omega\mu_0\vec{H}_j,\ \text{rot}\vec{H}_j = -i\omega\varepsilon_0\vec{E}_j,\ \text{в } D_j, \tag{2}$$

где $\vec{E}_1 = \vec{E}_{\text{уз.п.}} + \vec{E}_1'$ — суммарное поле в области D_1; граничные условия на плоскостях экрана $\Gamma_1(z = 0)$, $\Gamma_2(z = 0)$

$$\left(\vec{E}_{1\tau} - \vec{E}_\tau\right)\Big|_{\Gamma_1} = 0, \left(\vec{H}_{1\tau} - \vec{H}_\tau\right)\Big|_{\Gamma_1} = 0, \left(\vec{E}_{2\tau} - \vec{E}_\tau\right)\Big|_{\Gamma_2} = 0, \left(\vec{H}_{2\tau} - \vec{H}_\tau\right)\Big|_{\Gamma_2} = 0, \tag{3}$$

и условия излучения на бесконечности в областях D_j.

Для аналитического решения задачи (1)–(3) используются двухсторонние граничные условия, связывающие электромагнитные поля по обе стороны экрана D. Поле пучка излучается плоскостью $\Gamma(z = -h)$, на которой сформировано касательное электрическое поле, сконцентрированное в окрестности точки $(0, 0, -h)$:

$$\vec{E}\Big|_{z=-h} = \left(f_1(\rho)\vec{e}_\rho + f_2(\rho)\vec{e}_\varphi\right)\Phi_m,$$