УДК 519.233.32

**МОЩНОСТЬ КРИТЕРИЯ, ОСНОВАННОГО НА
ОДНОВРЕМЕННОМ ПРИМЕНЕНИИ «MONOBIT TEST»,
«FREQUENCY TEST WITHIN A BLOCK» И ОБОБЩЕНИЯ
КРИТЕРИЯ «APPROXIMATE ENTROPY TEST»**

М. П. Савелов

*МГУ им. М.В. Ломоносова, Ленинские горы, д.1,
119991, г. Москва, Россия, savelovmp@gmail.com*

Представлено предельное совместное распределение статистики критерия приближенной ϕ -энтропии и статистик критериев пакета NIST «Monobit Test» и «Frequency Test within a Block» в ситуации, когда исследуемая последовательность «близка» к последовательности независимых случайных величин, имеющих распределение Бернулли с параметром $\frac{1}{2}$. Будет предъявлено предельное значение мощности критерия, основанного на одновременном применении данных трех статистик.

Ключевые слова: совместное распределение статистик, пакет критериев NIST, мощность, критерий приближенной энтропии, критерий приближенной ϕ -энтропии, критерий частот, критерий частот в блоках, критерий подпоследовательностей фиксированной длины, цепи Маркова, критерии согласия.

**POWER OF THE TEST BASED ON JOINT APPLICATION OF
«MONOBIT TEST», «FREQUENCY TEST WITHIN A BLOCK» AND
A GENERALIZATION OF «APPROXIMATE ENTROPY TEST»**

M. P. Savelov

*Lomonosov Moscow State University, Leninskie Gory, 1,
119991, Moscow, Russian Federation, savelovmp@gmail.com*

We will present the limit joint distribution of the statistic of «Approximate ϕ -Entropy Test» and statistics of the NIST package tests «Monobit Test» and «Frequency Test within a Block», in case when the tested sequence is «close» to a sequence of independent Bernoulli trials with parameter $\frac{1}{2}$. The limiting value of the power of the test based on the simultaneous use of these three statistics is obtained.

Keywords: joint distribution of statistics, NIST package, power, «Approximate Entropy Test», «Approximate ϕ -Entropy Test», «Monobit Test», «Frequency Test within a Block», «Serial Test», Markov chains, goodness of fit test.

Критерий приближенной ϕ -энтропии является обобщением критериев «Approximate Entropy Test» и «Serial Test» пакета NIST. В докладе будет представлено предельное совместное распределение статистики критерия приближенной ϕ -энтропии и статистик T_{mon} и T_{fr} критериев пакета NIST «Monobit Test» и «Frequency Test within a Block» соответственно в ситуации, когда исследуемая последовательность «близка» к последовательности независимых случайных величин, имеющих распределение Бернулли с параметром $\frac{1}{2}$. Также будет выписано предельное значение мощности критерия, основанного на одновременном применении данных трех статистик, и предельное совместное распределение статистик T_{mon} , T_{fr} статистик критериев «Approximate Entropy Test» и «Serial Test». Будут рассмотрены результаты работ [2, 3] и их обобщения.

Библиографические ссылки

1. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., Vo S. A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22 Revision 1a, ed. L. E. Bassham III, NIST, April 2010.
2. Савелов М. П. Мощность критерия, основанного на одновременном применении «Monobit Test», «Frequency Test within a Block» и «Serial Test» // Дискрет. матем. 2023. Т. 35, № 4. С. 79–114.
3. Савелов М. П. Мощность критерия, основанного на одновременном применении «Monobit Test», «Frequency Test within a Block» и обобщения критерия «Approximate Entropy Test» // Дискрет. матем. 2024. Т. 36, № 1. С. 67–102.