

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе
**«Построение вероятностной модели
физических генераторов случайных чисел
и тестирование их выходных последовательностей»**

Доманин Владислав Эдуардович

Научный руководитель – ДОЦЕНТ КАФЕДРЫ ММАД Пирштук И.К.

2017

АННОТАЦИЯ

Дипломная работа, 56 ст., 5 рис., 19 табл, 10 источников.

Ключевые слова: ФИЗИЧЕСКИЕ ГЕНЕРАТОРЫ СЛУЧАЙНЫХ ЧИСЕЛ, ВЕРОЯТНОСТНАЯ МОДЕЛЬ, СЛУЧАЙНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ.

Объектом исследования является построение вероятностной модели физического генератора случайных чисел и методы статистического тестирования его выходных последовательностей.

Цели работы:

1. Провести обзор существующих физических генераторов случайных чисел.
2. Рассмотреть методы построения вероятностной модели физических генераторов случайных чисел.
3. Изучить методы статистического тестирования выходных последовательностей физических генераторов.
4. Создать программы для проведения статистического тестирования случайных последовательностей.
5. Провести статистическое тестирование выходных последовательностей физического генератора с помощью реализованных программ.

Результаты работы: алгоритмы, программные инструменты и отчет по проведенным исследованиям.

Область применения: системы защиты информации, системы анализа выходных последовательностей физических генераторов случайных чисел.

Практическая значимость: построение вероятностной модели физического генератора и статистическое тестирование выходных последовательностей повышает защищенность криптографической системы, в которой он применяется.

ABSTRACT

Diploma thesis, 56 p., 5 fig., 19 tab., 10 sources.

PHYSICAL RANDOM NUMBER GENERATOR, PROBABILISTIC MODEL, RANDOM SEQUENCE, STATISTICAL TESTING.

Object of research – construction of a probabilistic model of a physical random number generator and methods of statistical testing of its output sequences.

Purpose of research:

1. Review existing physical random number generators.
2. Consider methods for constructing a probabilistic model of physical random number generators.
3. Study methods of statistical testing of output sequences of physical generators.
4. Create programs for statistical testing of random sequences.
5. Carry out statistical testing of the output sequences of the physical generator with the help of implemented programs.

Results of work: algorithms, software tools and report on the conducted research.

Scope: information security systems, analysis systems of output sequences of physical random number generators.

Practical significance: the construction of a probability model of a physical generator and statistical testing of output sequences increases the security of the cryptographic system in which it is applied.