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

МИЛЬГУНОВ Евгений Вадимович

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Дипломная работа

Научный руководитель:
ст. преподаватель,
М.А. Казловский

Допущена к защите
«__»_____2025 г.
Зав. кафедрой математического
моделирования и анализа данных
доктор экономических наук,
профессор В.И. Малюгин

Минск, 2025

Аннотация

Дипломная работа включает 62 страницы, 22 рисунка, 3 таблицы, 9 источников.

Ключевые слова: C++, ГЕНЕРАТОРЫ СЛУЧАЙНЫХ ЧИСЕЛ, СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ТЕСТИРОВАНИЕ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, БАТАРЕИ ТЕСТОВ.

Объект исследования – методика тестирования выходных последовательностей генераторов случайных чисел МИ.10127.10.03.

Цель работы – разработка и экспериментальное применение программного комплекса реализующего алгоритмы тестирования методики МИ.10127.10.03.

Методы исследования – изучение литературы, посвящённой батареям тестов выходных последовательностей ГСЧ, проектирование архитектуры и разработка программного комплекса, проверка работоспособности полученного таким образом программного комплекса.

Полученные результаты и их новизна – получен полноценно функционирующий программный комплекс статистического тестирования выходных последовательностей ГСЧ.

Достоверность материалов и результатов дипломной работы. Результаты работы получены реализацией методики МИ.10127.10.03, разработанной НИИ ППМИ, в процессе разработки работа алгоритмов сверялась с эталонной реализацией, достоверность подтверждена реалистичными показателями результатов работы программного комплекса.

Область применения – оценка качества числовых последовательностей, генерируемых ГСЧ.

Анатацыя

Дыпломная работа ўключае 62 старонкі, 22 малюнка, 3 табліцы, 9 крыніц.

Ключавыя словы: C++, ГЕНЕРАТАРЫ ВЫПАДКОВЫХ ЛІКАЎ, СРОДКІ КРЫПТАГРАФІЧНАЙ АБАРОНЫ ІНФАРМАЦЫІ, ТЭСТАВАННЕ ВЫПАДКОВЫХ НАСЛЕДЧАСЦЯЎ, БАТАРЭІ ТЭСТАЎ.

Аб'ект даследавання – методыка тэставання выходных паслядоўнасцяў ФГСЧ МИ.10127.10.03.

Мэта работы – распрацоўка і эксперыментальнае прымяненне праграмнага комплексу які рэалізуе алгарытмы тэсціравання методыкі «МИ.10127.10.03».

Метады даследавання – вывучэнне літаратуры, прысвечанай батарэям тэстаў выходных паслядоўнасцяў ГСЧ, праектаванне архітэктуры і распрацоўка праграмнага комплексу, праверка працаздольнасці атрыманага такім чынам праграмнага комплексу.

Атрыманыя вынікі і іх навізна – атрыманы паўнавартасна які функцыянуе праграмны комплекс статыстычнага тэставання выходных паслядоўнасцяў ГСЧ.

Дакладнасць матэрыялаў і вынікаў дыпломнай працы. Вынікі працы атрыманы рэалізацыяй методыкі «МИ.10127.10.03», распрацаванай НДІ ППМИ, у працэсе распрацоўкі праца алгарытмаў спраўджвалася з эталоннай рэалізацыяй, дакладнасць пацверджана рэалістычнымі паказчыкамі вынікаў працы праграмнага комплексу.

Вобласць прымянення – ацэнка якасці лікавых паслядоўнасцяў, якія генерыруюцца ГСЧ.

Annotaion

The thesis includes 62 pages, 22 images, 3 tables, 9 sources.

Keywords – C++, RANDOM NUMBER GENERATORS, CRYPTOGRAPHIC INFORMATION PROTECTION MEANS, RANDOM SEQUENCE TESTING, TEST BATTERIES.

Object of research – the methodology for testing the output sequences of the physical random number generators «МИ.10127.10.03».

Purpose of the work – development and experimental application of a software package implementing the testing algorithms of the «МИ.10127.10.03»methodology.

Research methods – study of the literature devoted to the RNG output sequence test batteries, architecture design and software package development, testing the operability of the resulting software package.

The results obtained and their novelty – a fully functioning software package for statistical testing of RNG output sequences.

Reliability of materials and results of the thesis. The results of the work were obtained by implementing the «МИ.10127.10.03» methodology developed by the Research Institute of applied problems of mathematics and computer science, during the development process, the algorithms were compared with the reference implementation, reliability is confirmed by realistic indicators of the results of the software.

Scope – assessment of the quality of numerical sequences generated by the random number generators.