БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет радиофизики и компьютерных технологий
Кафедра интеллектуальных систем

Аннотация к дипломной работе

«Криптографический генератор псевдослучайных последовательностей на основе детерминированного хаоса»

Гореликов Юрий Николаевич

Научный руководитель: профессор кафедры интеллектуальных систем, кандидат технических наук, доцент В.С. Садов

2017

РЕФЕРАТ

Дипломная работа: 50 страниц, 3 рисунка, 17 источников, 2 приложения.

КРИПТОГРАФИЧЕСКИЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ДЕТЕРМИНИРОВАННОГО ХАОСА

Объект исследования – последовательность получаемая от генератора псевдослучайных последовательностей.

Цель работы – анализ технических решений по повышению криптостойкости.

В результате выполнения работы проверена последовательность с помощью статистических тестов «DIEHARD». Проверены некоторые последовательности получение от генератора в ручную. Выданы рекомендации по повышению криптостойкости генератора. Программная реализация генератора выполнена в системе компьютерной математики MATLAB.

РЕФЕРАТ

Дыпломная праца: 50 старонак, 3 малюнка, 17 крыніц, 2 прыкладанні.

КРЫПТАГРАФИЧНЫ ГЕНЕРАТАР ПСЕЎДАВЫПАДКОВЫХ ПАСЛЯДОЎНАСТЕЙ НА АСНОВЕ ДЭТЭРМІНАВАНАГА ХАОСУ.

Аб'ект даследавання - паслядоўнасць якая атрымліваецца ад генератара псеўдавыпадковых паслядоўнасцяў.

Мэта работы -- аналіз тэхнічных рашэнняў па критикестойкости.

У выніку выканання работы праверана паслядоўнасць з дапамогай статыстычных тэстаў «DIEHARD». Праверaны некаторыя паслядоўнасці атрыманне ад генератара ў ручную. Выдадзены рэкамендацыі па павышэнні крыптаўстойлівасці генератара. Праграмная рэалізацыя генератара выканана ў сістэме камп'ютэрнай матэматыкі MATLAB.

ABSTRACT

Thesis: 50 pages, 3 figures, 17 sources, 2 applications.

CRYPTOGRAPHIC GENERATOR OF PSEUDO-SILENT SEQUENCES BASED ON DETERMINATED CHAOS

Object of research - analysis of technical solutions for criticality.

Objective - to increase the cryptographic strength of the pseudo-random sequence generator.

As a result of the work, the sequence was checked using the statistical tests "DIEHARD". Some sequences of obtaining from the generator in the manual are checked. Recommendations are given on increasing the cryptographic strength of the generator. The software implementation of the generator is performed in the computer mathematics system MATLAB.