

ОТЗЫВ

на автореферат диссертационной работы «Модель и программный комплекс генератора псевдослучайных чисел, основанного на нечеткой логике», представленной Альнаджар Халед Хасан на соискание ученой степени кандидата технических наук по специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ

Анализ структуры и содержания автореферата показывает, что в нем содержится новая научная информация по специальности 05.13.18.

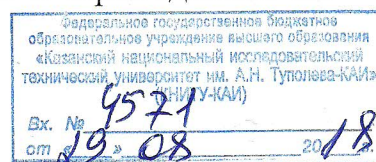
К числу важнейших результатов диссертации, обладающих научной новизной и выносимых на защиту относятся: новый метод математического моделирования процесса генерации псевдослучайных чисел, использующего нечеткую логику и линейные регистры сдвига с обратной связью с целью получения псевдослучайных последовательностей, которые близки к случайным по статистическим характеристикам; разработка архитектуры генератора псевдослучайных чисел, основанного на нечеткой логике, и исследование параметров предложенной модели, которые используются для анализа статистических свойств выходов применяемых регистров сдвига с обратной линейной связью, что позволяет выполнить тюнинг данных параметров, осуществляя поиск лучших из них, тем самым повышая безопасность предлагаемого генератора против корреляционных атак, и обеспечивая решение задач генерации криптографических ключей, реализации протоколов аутентификации, создания имитационных моделей; разработка и программная реализация численного метода нахождения характеристических примитивных полиномов для предлагаемого генератора, в основе которого заложен выбор вида полиномов и уменьшение вычислительной сложности процедуры тестирования их на простоту, что влияет на снижение временной сложности формирования множества характеристических полиномов с экспоненциальной до степенной; создание подхода к тестированию предлагаемого генератора, в основу которого положен метод анализа иерархий, что значительно сокращает продолжительность исследования параметров модели построенного генератора псевдослучайных чисел.

Замечания по автореферату:

1) В автореферате отображены результаты тестирования ПСП, производимом только на одной ПЭВМ с процессором INTEL Core i7 1.8 ГГц? Проводились ли тестирования на других ПЭВМ?

2) Если тестирование проводилось на разных ПЭВМ, то какие были получены результаты?

3) В автореферате указано, что при проведении сравнения НГПСЧ с ГПСЧ Matlab rand методом Монте-Карло были получены результаты, подтвердившие высокое качество разработанного НГПСЧ. Проводилось ли



аналогичное сравнение с ГПСЧ других математических пакетов? Если проводилось, то какие были получены результаты?

Содержательная сторона основных результатов обладающих новизной, а также квалификационный вклад соискателя состоит в исследовании способов генерации случайных чисел в ГПСЧ, основанных на регистрах сдвига с линейной обратной связью, повышении качества ПСП предлагаемого генератора посредством введения нелинейной комбинационной функции, основанной на использовании аппарата теории нечетких множеств, и формировании характеристических примитивных полиномов для НГПСЧ с целью снижения вычислительной трудоемкости. Это позволяет оценить диссертационную работу положительно.

Диссертационная работа Альнаджар Халед Хасан «Модель и программный комплекс генератора псевдослучайных чисел, основанного на нечеткой логике» представляет собой завершённое исследование, отвечает требованиям действующего Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а также ее автор - Альнаджар Халед Хасан – заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ.

Доктор технических наук,
профессор, декан факультета
управления и информатики
в технологических системах
ФГБОУ ВО «Воронежский
государственный университет
инженерных технологий»

Скрыпников Алексей Васильевич

Кандидат технических наук,
доцент кафедры высшей математики и
информационных технологий
ФГБОУ ВО «Воронежский
государственный университет
инженерных технологий»

Сафонова Юлия Александровна

Адрес организации: 394036, г. Воронеж, пр. Революции, д.19, тел. (473)255-65-11

Адрес Скрыпникова А.В.: 394000, г. Воронеж, ул. Морозова, д.29а, кв. 59 тел. (473)255-65-11, email: skrypnikovsafe@mail.ru

Адрес Сафоновой Ю.А.: 394000, г. Воронеж, ул. Тимирязева, д.27а, кв. 298 тел. 89601024304, email: kulakova7@yandex.ru

