ОТЗЫВ
на автореферат диссертации Альнаджара Халеда Хасана "Модель и программный комплекс генератора псевдослучайных чисел, основанного на нечеткой логике", представленной на соискание ученой степени кандидата технических наук по специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ»

Проблема разработки генераторов случайных чисел актуальна при проведении научных исследований в различных прикладных областях – в веб-безопасности, криптографии, в области машинного обучения, при имитационном моделировании и реализации эвристических алгоритмов, в области искусственного интеллекта и т.д..

Встроенные средства реализации последовательностей псевдослучайных чисел далеко не всегда позволяют решить поставленную задачу с требуемым качеством и скоростью получения результата. Это связано с такими причинами, как предсказуемость зависимости получения чисел и инициализации генератора, а также его зацикливанием из-за недостаточной длины периода генерируемой последовательности.

Диссертационная работа Альнаджара Халеда Хасана посвящена вопросам устранения уязвимостей ГПСЧ, что определяет, безусловно, актуальность данного исследования.

Автором поставлена задача повышения качества решения - случайности генерации последовательностей псевдослучайных величин, и в результате исследования этой проблемы разработана модель и реализован программный комплекс генерации двоичных псевдослучайных последовательностей и чисел, близких по статистическим свойствам к случайным. Особенностями предложенной модели является ее адаптивность, возможность конфигурирования параметров модели с целью повышения качества сгенерированных псевдослучайных последовательностей и чисел. Предложенный автором подход к тестированию генератора псевдослучайных чисел, основанный на выборе наиболее важных тестов с помощью метода анализа иерархий, позволяет сократить время исследования параметров предложенной модели более, чем в 15 раз. Использование полученных в диссертации результатов дает мощный инструмент разработчикам для исследований качества используемых ГПСЧ.

Есть замечания по автореферату:

1. В автореферате перечислены авторы, которые исследовали аппарат теории нечетких множеств для введения нелинейности при проектировании ГПСП. При этом не ясно, какие задачи остались нерешенными и на основании чего сделан вывод, что «вопросы применения данного математического аппарата при проектировании ГПСЧ остаются не до конца исследованными». Что не исследовано? В каких задачах? По каким критериям качества?

2. Автор часто использует слово «подходящий» в разных формулировках:

- «походящих … полиномов» (стр. 1, 2), «подходящих параметров модели» (на стр. 2, в пункте 1 новизны, в теоретической значимости, на стр. 17 в заключении).

В научных исследованиях слово «подходящий» не применимо, так же как и слова «лучше», «хуже», «больше», «меньше». Нужен критерий оценки, численное выражение результата.

3. Есть ошибки в тексте автореферата, связанные со склонением слов, например, во фразах:

- п.2. новизны «основанного на выборе …. и сокращени***я***» (стр.2), но если «основанного на выборе ….», то и, очевидно, «основанного на …. сокращени***и***»;
- «используются две лингвистически***х*** переменны***х***» (стр.5), но «используются…», винительный падеж, вопрос «что?», «используются две лингвистически***е*** переменны***е***»;
- «можно использовать следующи***х*** два примитивных полинома» (стр.7), правильно «можно использовать следующи***е*** два примитивных полинома» и т.д.

Перечисленные замечания не влияют на теоретическую и практическую значимость диссертационной работы. Диссертационная работа Альнаджара Х.Х. полностью соответствует требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, имеет прикладную и теоретическую значимость. Считаю, что автор работы Альнаджар Халед Хасан заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ».

Заведующая кафедрой
Информатики и систем управления
ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева»
доктор технических наук, профессор /Э.С. Соколова/

Докторская диссертация защищена по специальности 05.13.01 – «Системный анализ, управление и обработка информации»

Соколова Элеонора Станиславовна
603950, Нижний Новгород, ул. Минина, д.24
Телефон: (831) 436-83-44
E-mail: essokolowa@gmail.com

Министерство науки и высшего образования Российской Федерации ... Нижний Новгород Нижегородская область
Отдел кадров № 1
Сотрудник ОК
заверяю
2018 г.