О Т З Ы В

на автореферат диссертации **Кукарцева Анатолия Михайловича**
«Эффективные алгоритмы анализа джевонс-эквивалентности данных»,
представленной на соискание учёной степени
кандидата физико-математических наук
по специальности 05.13.17 – Теоретические основы информатики

Работа Анатолия Михайловича посвящена проблеме анализа Джевонс-эквивалентности данных. Отличительной особенностью такого рода данных является то обстоятельство, что они соответствуют определённым булевым функциям (БФ), множество инвертирований и перестановок аргументов которых образуют группу Джевонса. Автором отмечается, что работы в этой области ведутся по различным прикладным областям с начала XX века, однако проблема эффективного анализа Джевонс-эквивалентности данных, включая проблему поиска элементов группы Джевонса, связывающих эти данные, по прежнему не решена до конца. Обобщив результаты предшествующих исследований Анатолий Михайлович сформулировал основную научную проблему, цель и задачи, а также методы исследования.

В результате проведённых исследований автором предложена модель канонического представления элемента группы Джевонса и разработан алгоритм решения уравнения действия элемента группы Джевонса над БФ. Полученные экспериментальные результаты позволяют судить об эффективности данного алгоритма, в сравнении с тривиальным, который является экспоненциально сложным. Особенностью разработанного алгоритма является частотный анализ промежуточных джевонс-эквивалентных данных, который, при определённых условиях, позволяет существенно повысить скорость нахождения решений. Это обстоятельство говорит, в том числе, и о практической значимости исследования. Например, в области криптографии, нелинейные блоки преобразования информации могут порождать выходные данные, которые связаны Джевонс-эквивалентностью с входными. Это обстоятельство может связать проблему поиска элементов группы Джевонса с прикладными задачами в области криптоанализа.

По автореферату имеются следующие замечания:

– В экспериментальной части работы, автором даётся утверждение, что «для формирования статистики случайные бинарные вектора распределены равномерно, потому, что при обработке реальных данных, в общем случае, будет такое же распределение», из автореферата работы остаётся не ясным, почему реальные данные носят случайный характер с равномерным

распределением. Кроме того, остаётся не ясным, каким образом были получены эти бинарные вектора;

– В автореферате автором приводится количественная оценка эффективности предложенного алгоритма относительно тривиального (в 750 раз эффективней) для бинарных векторов длиной 2^5, при этом остаётся не ясным, влияет ли длина вычисляемого бинарного вектора на данный показатель.

Указанные недостатки безусловно не снижают значимость данного диссертационного исследования, в котором автором получены новые теоретические результаты в области разработки и исследования моделей и алгоритмов анализа данных. Полученные соискателем результаты были опубликованы в различных изданиях, а также неоднократно докладывались на конференциях различного уровня. Автореферат диссертации написан ясным научным языком, а его содержание свидетельствует о завершённом научном исследовании.

Считаю, что диссертационная работа Кукарцева Анатолия Михайловича «Эффективные алгоритмы анализа джевонс-эквивалентности данных» соответствует требованиям Положения о присуждении учёных степеней, утверждённого постановлением Правительства РФ от 24 сентября 2016 № 842, а её автор, Кукарцев Анатолий Михайлович, заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 05.13.17 – Теоретические основы информатики.

Руководитель научно-учебной
лаборатории «Информационной
безопасности» каф. прикладной
математики и компьютерной
безопасности ФГАОУ ВО
«Сибирский Федеральный
Университет», канд. техн. наук _____/ А.Н. Шниперов /

Шниперов Алексей Николаевич
Почтовый адрес: 660074, г. Красноярск,
ул. Киренского, 26ж.
Тел.: +7 (391) 206-27-43
e-mail: Ashniperov@sfu-kras.ru

ФГАОУ ВО СФУ
Подпись заверяю
Начальник общего отдела
«29» 03 2017 г.