ОТЗЫВ

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

Автор исследует представления данных в виде булевых функций. Над аргументами таких функций выполняются отрицания и/или перестановки. Отрицания и/или перестановки описываются конечной группой Джевонса, которая действует на множестве булевых функций. Такие действия задают отношение эквивалентности на множестве булевых функций и, как следствие, соответствующих им данным. Целью исследования является вычисление отрицаний и/или перестановок, которые могут связывать два фрагмента данных.

Указанные преобразования данных (преобразования Джевонса) находят своё применение в задачах защиты информации в криптографии и криптологии. Это связано с тем, что вычисление отрицаний и/или перестановок, преобразующих фрагменты данных, имеет экспоненциальную временную сложность, что позволяет использовать преобразования Джевонса для защиты информации на уровне представления. Полученные автором результаты ценны тем, что объективно налагают ограничения на применение преобразований Джевонса без дополнительной модификации как метода защиты. Отдельные результаты по генерации информационных сообщений с одинаковыми частотными (энтропийными) характеристиками во всех их допустимых алфавитах позволяют подготавливать исходные данные дня энтропийного анализа средств защиты информации.

Научные положения и результаты исследования, выносимые на защиту, обоснованы и доказаны, а также полностью опубликованы в 4 изданиях из списка рекомендованных ВАК, в 8 других изданиях. Имеется 2 свидетельства о регистрации программ, зарегистрированных в Российском реестре программ для ЭВМ. Разработанные программы для ЭВМ позволяют непосредственно исследовать вопросы применения полученных результатов для задач защиты информации.

При чтении автореферата возникли следующие замечания:

1. В автореферате присутствует избыточная информация, уже представленная в научных источниках (определения понятий алфавита, символа алфавита, частоты символа, слова и т.д.). Автореферат перегружен математическими обозначениями и определениями, что затрудняет восприятие материала.
2. Не показано использование полученных решений в смежных отраслях науки и народного хозяйства. Отсутствуют указания на конкретные прикладные задачи, в которых применяются джевонс-эквивалентные данные. Целесообразно было указать в автореферате конкретное применение джевонс-эквивалентных данных в области обработки и защиты информации.

Указанные замечания не влияют на общую положительную оценку научных результатов исследования, её теоретическую и практическую ценность. Представленные материалы удовлетворяют п. 9 «Положения о порядке присуждения учёных степеней» постановления Правительства Российской Федерации от 24.09.13 г. № 842, а её автор Кукарцев Анатолий Михайлович заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 05.13.17 – Теоретические основы информатики.

Д-р техн. наук, профессор
профессор кафедры
Безопасности информационных технологий
ФГАОУ ВО Южный федеральный университет Бабенко Людмила Климентьевна

Подпись Бабенко Л. К.

Федеральное государственное автономное
образовательное учреждение высшего образования
Южный федеральный университет
344006 г. Ростов-на-Дону, ул. Б. Садовая, 105/42
Телефон: 8-(8634)-312-018
E-mail: blk@tsure.ru

ДИРЕКТОР ИНСТИТУТА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТА ЮФУ

Т.Е. ВЕСЕЛОВ

2012 г.