ОТЗЫВ

об автореферате диссертации Игоря Владимировича Чередника
«Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований», представленной
на соискание ученой степени кандидата физико-математических наук
по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки)

В диссертации И.В. Чередника предлагается способ построения классов блочных преобразований, функциональная схема которых является сетью постоянной ширины и определяет класс преобразований, функциональные элементы определяются выбором базисной бинарной операции из заранее заданного множества бинарных операций. Такие классы преобразований обобщают известные схемы обратимых преобразований (например, схемы Фейстеля) и представляют интерес для практики ввиду относительной простоты структуры, допускающей различные варианты реализации.

Автором разработан новый метод исследования свойств таких преобразований, основанный на так называемых разметках функциональных сетей. Этот метод позволяет описывать структуру сетей рассматриваемых классов, которые при любой допустимой базисной операции реализуют только обратимые блочные преобразования, что является необходимым для ряда применений в устройствах защиты информации.

В диссертации получены удобные критерии кратной транзитивности для класса преобразований, реализуемого сетью постоянной ширины. Предложено несколько способов построения широких классов таких сетей, реализующих кратно транзитивные классы преобразований.

Таким образом, в диссертации Чередника И. В. предложены и обоснованы новые способы построения кратно транзитивных классов блочных преобразований, которые представляют как теоретический, так и практический интерес.

Судя по автореферату, результаты диссертационной работы И.В. Чередника «Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований» являются новыми, получены автором самостоятельно и достаточно полно опубликованы. На мой взгляд, эта диссертация отвечает всем требованиям к кандидатским диссертациям,

изложенным в «Положении о присуждении ученых степеней в Московском государственном университете имени М. В. Ломоносова», а ее автор И.В. Чередник заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Заведующий Отделом дискретной математики
ФГБУН Математический институт им.В.А.Стеклова
Российской академии наук,
доктор физико-математических наук А. М. Зубков

18 ноября 2021 г.

Контактные данные:
тел. +7 (499) 941-01-84, 36-31 e-mail: zubkov@mi-ras.ru
Адрес места работы:
119991, Москва, ул. Губкина, 8

Подпись А. М. Зубкова удостоверяю
Ученый секретарь МИАН С.А.Поликарпов