МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени М.В. ЛОМОНОСОВА

Механико-математический **ФАКУЛЬТЕТ**

ОТЗЫВ НА НАУЧНО-КВАЛИФИКАЦИОННУЮ РАБОТУ

аспиранта _4_ года обучения *Царегородцева Кирилла Денисовича*
(Фамилия и инициалы)

Кафедра *Высшей алгебры*

Научный руководитель-*доцент Панкратьев Антон Евгеньевич*

Тема *Алгебраические свойства квазигрупп, порожденных правильными семействами булевых функций*
(печатными буквами)

Тема на английском языке *Algebraic properties of quasigroups generated with the use of proper families of Boolean functions*
(печатными буквами)

Научно-квалификационная работа К.Д. Царегородцева посвящена изучению алгебраических свойств квазигрупп, задаваемых правильными семействами булевых функций, а также изучению свойств самих правильных семейств функций.

Актуальность работы определяется растущим в последнее время интересом к использованию преобразований, основанных на некоммутативных и неассоциативных алгебраических структурах (в частности, квазигруппах), как в теоретических исследованиях, так и в построении практических криптосистем. В частности, квазигрупповые системы предлагались в качестве кандидатов на конкурсах NIST по выбору новых криптографических стандартов. Изучаемый К.Д.Царегородцевым подход к построению квазигрупп, основанный на использовании правильных семейств булевых функций, был изначально предложен в работах В.А. Носова.

Работа состоит их введения, включающего краткое содержание работы, трёх глав, и списка литературы, включающего 86 наименований. Первая глава посвящена правильным семействам функций и их свойствам, вторая — алгебраическим свойствам квазигрупп, третья — применению квазигрупп в криптографии и теории кодирования.

К.Д. Царегородцевым получены важные собственные результаты, а именно, установлено взаимно-однозначное соответствие между правильными семействами булевых функций и одностоковыми ориентациями графов булевых кубов, доказано, что количество неподвижных точек отображения, задаваемого правильным семейством булевых функций, всегда чётно, предложены оценки количества правильных семейств булевых функций и доли треугольных семейств среди всех правильных семейств булевых функций. Также предложен новый алгоритм шифрования, основанный на квазигрупповых операциях.

В целом работа выполнено на высоком научном уровне, все утверждения строго доказаны, автор вполне овладел методами алгебры и дискретной математики.

Считаю, что работа К.Д. Царегородцева «Алгебраические свойства квазигрупп, порождённых правильными семействами булевых функций» удовлетворяет всем требованиям, предъявляемым к научно-квалификационным работам, и заслуживает оценки «ОТЛИЧНО».

Научный руководитель,

доцент А.Е. Панкратьев