ОТЗЫВ

на автореферат диссертационной работы Пудовкиной Марины Александровны **«Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации»**, представленной на соискание ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

В современном технологическом обществе острота проблем защиты информации постоянно нарастает. Составные части многих систем защиты информации моделируются итерационными криптографическими функциями. В большинстве случаев анализ таких систем основывается на присутствие в них определённых уязвимостей, которые, как правило, задаются в виде функциональных зависимостей между прообразами и образами, а возможно также ключами, моделируемой итерационной криптографической функции. Для развития и совершенствования современных систем защиты информации актуальны исследования, направленные на изучение структур итерационных функций для оценки стойкости систем защиты, составные части которых моделируются такими функциями, а также на разработку необходимого для этого универсального математического аппарата. Диссертационная работа Пудовкиной М. А. посвящена решению этой актуальной научной проблемы.

В диссертации Пудовкиной М. А. рассмотрен широкий спектр задач, результатом решения которых является общий комбинаторно-алгебраический способ описания и исследования структурных свойств итерационных криптографических функций, основанный на понятии p_G-структуры, и на свойствах преобразований, составляющих итерационные криптографические функции.

Все основные результаты, полученные в диссертационной работе Пудовкиной М. А., являются новыми, теоретически и практически значимыми. Они создают математическую основу для разработки новых и обобщения известных методов криптоанализа, для создания новых и совершенствование существующих систем защиты информации.

В частности, в диссертационной работе Пудовкиной М. А. получен ряд новых результатов, относящихся к теории графов. В диссертации исследованы графы, метрики которых являются подметриками метрики Хемминга, а их группы автоморфизмов – надгруппы группы Джевонса. В диссертации выполнена классификация подметрик метрики Хемминга, описаны группы ав-

томорфизмов для всех графов установленных подметрик, определены идентификационные признаки дистанционно-транзитивных графов.

В целом по результатам диссертационного исследования автором опубликовано 51 работа, из которых 14 статей в рецензируемых научных изданиях из списка, рекомендованного ВАК РФ, и входящих в международные базы научного цитирования Web of Science и Scopus, 18 статей в других рецензируемых научных журналах и приложениям к ним. Результаты диссертационного исследования докладывались в 2007 – 2016 гг. на многочисленных всероссийских и международных семинарах и конференциях, тематика которых полностью отвечает направлению диссертационного исследования.

Автореферат Пудовкиной М. А. содержит все обязательные разделы в соответствии с требованиями ВАК и обладает внутренним единством. Автореферат полностью отвечает содержанию диссертации. Достоверность и обоснованность представленных в автореферате основных научных результатов обеспечивается четкими математическими определениями, формулировками теорем и утверждений, и строгими доказательствами теорем и утверждений, приведенными в тексте диссертации.

Замечания к автореферату.

1. В автореферате не указаны границы практической применимости основных теоретических результатов диссертационной работы.

2. Имеются опечатки и стилистические неточности.

Общее заключение. Диссертация Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» представляет собой завершенную научно-квалификационную работу, содержащую теоретические положения по решению актуальной научной проблемы в области информационной безопасности: разработка общего комбинаторно-алгебраического способа описания и исследования структур итерационных криптографических функций. Рассмотренная и решенная в диссертации научная проблема соответствует п. 54 Перечня научно-технических проблем обеспечения информационной безопасности РФ «Разработка фундаментальных проблем теоретической криптографии и смежных с ней областей математики»

Диссертационная работа Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» соответствует областям исследования специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность по следующим пунктам:

- п. 9 «Модели и методы защищенности информации и информационной безопасности объекта»,
- п. 13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Считаю, что диссертация Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» полностью отвечает критериям «Положения о присуждении ученых степеней» ВАК РФ, предъявляемым к докторским диссертациям, а ее автор, Пудовкина Марина Александровна, заслуживает присуждения ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Профессор кафедры Высшей и прикладной математики
Федерального государственного автономного
образовательного учреждения высшего образования
«Сибирский федеральный университет»,
доктор физико-математических наук, доцент
(специальность 05.13.17 – Теоретические основы
информатики)

Быкова Валентина
Владимировна

24 марта 2017 г.
E-mail: bykvalen@rrari.ru

ФГАОУ ВО СФУ
Подпись Быкова заверяю
Начальник общего отдела
«24» 03 2017 г.

Адрес: 660041, г. Красноярск, пр. Свободный, д. 79/10,
Федеральное государственное автономное образовательное учреждение
высшего образования «Сибирский федеральный университет»
Сайт: http://www.sfu-kras.ru, Тел: +7 (391) 206-21-48, E-mail: office@sfu-kras.ru