Утверждаю

Проректор по НИР
ФГБОУ ВО «Саратовский национальный
исследовательский государственный
университет имени Н.Г.Чернышевского»
доктор физ.-мат. наук, профессор
А.А.Короновский

«____» марта 2017 г.

# ОТЗЫВ

ведущей организации о диссертации М.А.Пудовкиной
«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 большинстве современных алгоритмов шифрования функции, преобразующие открытый текст в соответствующую криптограмму, строятся на основе итерационного метода. Для исследования свойств итерационных криптографических функций широко используются алгебраические и комбинаторные конструкции. Алгебраическое направление связано в основном с групповыми свойствами криптографических функций. Например, много работ посвящено исследованию группы, порожденной раундовыми функциями, для различных алгоритмов блочного шифрования. Комбинаторные методы всегда широко применялись в криптографии.

Большое внимание здесь уделяется, в частности, графам. Значительный вклад в упомянутые направления криптографии внесли отечественные математики М.М.Глухов, Ю.Н.Горчинский, Б.А.Погорелов, В.Н.Сачков, В.Е.Степанов и другие.

При исследовании криптографических функций естественно возникают некоторые производные структуры, с помощью которых в ряде случаев удается найти новые подходы в криптоанализе, в частности, блочных шифров.

В диссертации рассматриваются так называемые $p_G$-структуры. Если $X$ – заданный алфавит и $S(X)$ симметрическая группа на нем, то для фиксированного подмножества $G$ из $S(X)$ и разбиений $R$ и $R'$ декартовой степени $X^t$ формулируются условия, означающие, что $G$ имеет $p_G$-структуру $(R, R')$ размерности $t$ (в работе $t$ принимает значения 1 или 2). Автор приводит многочисленные примеры $p_G$-структур, встречающихся в криптографической практике.

Выделим основные, на наш взгляд, результаты работы, тема которой представляется актуальной как с точки зрения теоретических, так и прикладных разделов современной криптографии.

В первой главе диссертации исследуются $p_G$-структуры, задаваемые разбиениями множества $X$ с равномощными блоками. Показано, что группа автоморфизмов ряда таких $p_G$-структур является сплетением групп подстановок (утверждение 1.2.1). Изучается вопрос о возможных расстояниях Хемминга от подстановок из $S(X)$ до подстановок из (импримитивной) группы $IG_W$ (максимальная группа подстановок, сохраняющая разбиение $W$). В теореме 1.3.4 найдено минимальное значение этой величины (порядок $W$-примитивности подстановки). Большой интерес в криптографии представляют функции, максимально далекие от множества всех аффинных функций (бент-функции). Автор характеризует подстановки, максимально далекие от группы $IG_W$ (утверждение 1.3.5), их можно считать аналогом бент-функций.

Показано, как эти построения можно применить для оценки расстояний в алгоритме шифрования SMS4, иллюстрируется их полезность в некоторых методах криптоанализа.

Вторая глава посвящена связи между двумерными $p_G$-структурами и некоторыми специальными метриками, в частности натуральными (к таковым относится, например, метрика связного графа, заданная расстоянием между вершинами). Показано, что группа изометрий натуральной метрики, определенной на $X^2$ классом двумерных $p_G$-структур, задаваемых симметричным бинарным отношением $R$, совпадает с группой автоморфизмов графа с отношением смежности $R$ (утверждение 2.3.2). Получено (утверждения 2.6.2-2.6.10) полное описание натуральных метрик, инвариантных относительно группы Джевонса (они являются натуральными метриками графов орбиталов для надгрупп этой группы).

В третьей главе исследуются групповые свойства двумерных $p_G$-структур. В теоремах 3.2.1 и 3.2.17 дается полная классификация групп автоморфизмов графов орбиталов надгрупп группы Джевонса. Это дает возможность классифицировать дистанционно транзитивные графы орбиталов надгрупп группы Джевонса (теорема 3.3.2), среди них выявляются двудольные и антиподальные графы (утверждение 3.3.4). В теореме 3.4.1 приводятся некоторые характеристики и свойства указанных графов в зависимости от их диаметров. Показано, как эти результаты могут быть применены в криптографии. В частности, скорректировано полученное ранее другими авторами описание группы инерций всех двоичных корреляционно-иммунных функций заданного порядка.

В главе 4 рассматриваются свойства графов орбиталов группы $C_n(g)$ для приводимой матрицы $g$ из $GL_n$ и описываются натуральные метрики этих орбиталов. Найдены условия связности графов орбиталов (утверждения 4.2.4 и 4.2.6), их изоморфности (утверждение 4.2.7). В разделе 4.3 приводятся условия, равносильные дистанционной транзитивности и дистанционной регулярности. Характеристики графов орбиталов группы $C_n(g)$ представлены

для конкретных матриц $g$, используемых в некоторых алгоритмах блочного шифрования. В разделе 4.6 предлагается модификация разностного метода криптоанализа для марковского *XSL*-алгоритма блочного шифрования с приводимым линейным преобразованием. Преимущества предложенного подхода иллюстрируются на примере шифра ISEBERG.

Специальным криптографическим приложениям $p_G$-структур посвящена глава 5. Для некоторого семейства алгоритмов шифрования, связанных с обобщенным алгоритмом Фейстеля второго типа, обнаружены $p_G$-структуры, являющиеся одновременно инвариантными и невозможными (утверждения 5.2.1 и 5.2.2). Это позволяет отличить раундовую функцию зашифрования от случайной подстановки при любом числе раундов. Выделяется особый класс итерационных марковских алгоритмов блочного шифрования. Указана связь между такими алгоритмами и существованием двумерных $p_G$-структур, а также наличием для алгоритма в ряде случаев нетривиального подстановочного гомоморфизма (теорема 5.5.1).

Приведенный обзор основных результатов диссертации позволяет сделать вывод о том, что их совокупность можно квалифицировать как научное достижение, как весомый вклад в математические методы современной криптографии. Для изучения комбинаторно-алгебраических свойств преобразований, составляющих итерационную криптографическую функцию, привлекаются так называемые $p_G$-структуры, что позволяет автору создать новую идеологию для трактовки классических проблем криптографии, добиться существенных продвижений в анализе ряда алгоритмов блочного шифрования. Отметим, что в Приложении к работе имеются три акта о внедрении ее результатов.

Принципиальных замечаний по работе нет. Она хорошо структурирована, доказательства проведены с достаточной полнотой. Отметим лишь некоторую перегруженность текста второстепенными деталями. И одно замечание общего характера: новым, в особенности перспективным понятиям следует присваивать имена, являющиеся словами естественного

языка или похожими на них по форме (как, например, произносить ключевые термины «$p_G$-структура» или «$\otimes_W$-марковский»?)

Основные положения диссертации довольно полно изложены в 51 публикациях автора, 14 из которых осуществлены в изданиях, рекомендованных ВАК. Автореферат правильно отражает содержание работы.

Считаем, что диссертационная работа «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» удовлетворяет требованиям пп. 9-11, 13, 14 «Положения о присуждении ученых степеней», а ее автор Марина Александровна Пудовкина заслуживает присуждения ей ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв заслушан и обсужден на заседании кафедры теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета им. Н.Г.Чернышевского 6 марта 2017 г., протокол № 13.

Зав. кафедрой
теоретических основ компьютерной безопасности
и криптографии СГУ
кандидат физ.-мат. наук, профессор

Вячеслав Николаевич Салий

Подпись В.Н.Салия заверяю

Ученый секретарь СГУ
доцент

И.В.Федусенко

06.03.2017

Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовский национальный исследовательский государственный университет имени Н.Г.Чернышевского»,
410012 Саратов, ул. Астраханская, 83,
Тел.: (8452) 26-16-96, e-mail: rector@sgu.ru