ОТЗЫВ

официального оппонента на диссертацию Пудовкиной Марины Александровны "Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации", представленную на соискание ученой степени доктора физико-математических наук по специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" (физико-математические науки)

Диссертационная работа М.А. Пудовкиной посвящена новому направлению в исследовании систем защиты информации — использованию для разработки и исследования эффективности методов, средств и систем защиты информации классического математического аппарата комбинаторных схем и алгебры.

В последние годы интерес к построению итерационных блочных преобразований с хорошими свойствами значительно возрос. Этому способствовало значительное число публикаций (включая монографии и многочисленные доклады на международных конференциях), посвященных изучению свойств и описанию все новых и новых классов таких преобразований, обладающих хорошими параметрами. С другой стороны, многие новые способы анализа таких преобразований, основанные на исследовании внутренних закономерностей и выделении свойств, влияющих на защищенность, позволили найти слабости для многих из построенных классов преобразований. В диссертации изложен новый общий подход к изучению таких свойств, позволяющий с единых позиций взглянуть на многие известные, а также наметить новые подходы к выявлению возможных слабостей существующих систем.

Комбинаторно-алгебраические структуры возникают в силу специфики построения итерационных преобразований, применяемых в системах защиты, работающих по блочному принципу, когда преобразование информации осуществляется не побитно, а сразу большими блоками. Характер реализованных в них операций обуславливает возможные типы алгебраических структур, применяемых для моделирования их работы. В сочетании с современным математическим аппаратом, разработанным в рамках комбинаторно-алгебраического направления и основанным на анализе закономерностей в терминах инвариантных структур, в диссертационной работе систематично и последовательно излагается конкретный конструктивный подход, позволя-

ющий с единых позиций исследовать конструктивные особенности применяемых систем защиты. Как показано в диссертации, наличие таких структур позволяет конечном итоге уменьшить сложность преодоления защиты и, тем самым, улучшить оценки трудоемкости для многих известных методов анализа таких систем. Это говорит об **актуальности** темы диссертации.

В работе выделен и описан **новый** класс потенциальных уязвимостей, вызванных наличием определенных метрических и комбинаторно-вероятностных закономерностей. Для их описания автором введено новое понятие p_G-структуры и проведена классификация конечнозначных метрик, характеризующих близость к множеству преобразований, сохраняющих некоторое разбиение. Развитый в диссертационной работе аппарат позволяет охватить и описать с единых позиций как многие выявленные ранее слабости, так и обнаружить новые потенциальные уязвимости для исследованных ранее систем, влияющие на надежность построенных на их основе средств защиты информационных и телекоммуникационных систем.

Диссертация состоит из введения, пяти глав и заключения.

Во **введении** вводится определение p_G-структуры, основного изучаемого в диссертации объекта, которая в общем виде задаётся парой разбиений множества всех t-грамм алфавита текстов, и формулируется суть предлагаемого подхода к исследованию свойств блочных преобразований на основе описания групп, графов и метрик, определяемых p_G-структурами.

В **главе 1** устанавливается связь p_G-структуры с операцией сплетения групп подстановок в терминах величины χ_G, характеризующей расстояние Хемминга от изучаемого преобразования g до ближайшей подстановки из импримитивной группы IG_W, строение которой описывается операцией сплетения. Описано множество подстановок максимально удаленных от группы IG_W и найдено их число. Эти подстановки выступают как аналог бент-функций (двоичных функций максимально удалённых от множества всех аффинных функций), однако в отличие от последних автору удалось получить исчерпывающее описание всех таких подстановок.

Применительно к преобразованиям g, описываемых широко применяемыми в системах защиты информации XSL-алгоритмами, найдены верхние оценки величины χ_G для преобразований S-слоя и частичных раундовых функций. Для этого рассмотрены разбиения W, инвариантные относительно преобразований X- и L-слоев. Вводится понятие L-факторструктуры подстановки g, обобщающее известное понятие «линейной структуры» преобразования

и гарантирующее наличие p_G-структуры с группой автоморфизмов, являющейся сплетением симметрических групп. Показана связь задачи оценки величины χ_G с проблемой оценки параметров ряда известных методов, используемых при анализе систем защиты информации.

Глава 2 посвящена описанию натуральных конечно-значных метрик, связанных с изучаемыми классами p_G-структур и обобщающих метрику Хемминга. Автором разработана оригинальная техника, позволяющая в общем виде описывать возможные метрики и связанные с ними инвариантные разбиения, основанная на исследовании графов орбиталов группы и ее надгрупп. На основе результатов Б.А. Погорелова по описанию нагрупп группы Джевонса и результатов М.Е. Музычука по классификации подсхем схемы Хемминга получено полная классификация метрик графов орбиталов надгрупп группы Джевонса. Обобщения метрики Хемминга позволяют расширить классы множеств «оптимальных» или «слабых» преобразований относительно некоторых типов уязвимостей, что позволяет расширить область применения известных методов анализа систем защиты информации.

Глава 3 содержит полную классификацию групп изометрий натуральных метрик графов орбиталов надгрупп группы Джевонса и описание их свойств. Показано, как классификация групп автоморфизмов графов орбиталов может быть использована в математических методах анализа систем защиты информации. В частности, с ее помощью исправлены ошибки в описании группы инерции множества корреляционно-иммунных двоичных функций фиксированного порядка, полученном ранее в работе У.Мейера и О. Стафлбаха.

В **главе 4** приводится характеризация графов орбиталов для группы, порожденной преобразованиями X- и L-слоев для применяемых на практике XSL-алгоритмов. Исследуется зависимость свойств таких преобразований, обуславливающих возможность применения методов анализа, от групповых свойств преобразования L-слоя. Обобщается введенное ранее понятие марковости алгоритма: вместо рассмотрения последовательностей разностных характеристик между блоками изучаются последовательности смежных классов инвариантного подпространства линейного преобразования.

В **главе 5** подробно разбираются отдельные приложения разработанной техники. Явно указаны p_G-структура для одной модификации схемы Фейстеля, наличие которой позволяет обосновать невыполнение условия 2-транзитивности и найти большое число "запретных" (т.е. появление которых невоз-

можно) разностей, что указывает на слабость данной схемы, а также p_G-структура, соответствующая $\otimes_W$–марковским алгоритмам. Вводится понятие $\otimes_W$-марковости для XSL-алгоритмов, исследуются их инвариантные подмножества и устанавливается связь с наличием гомоморфизмов. Показано, что в общем случае свойство $\otimes_W$-марковости алгоритма не является эквивалентным существованию гомоморфизма. Для известного блочного преобразования SAFER, применяемого в системах защиты беспроводной связи и основанного на операциях экспоненцирования и логарифмирования в кольце вычетов и поле Галуа, указаны соответствующие разбиения W. также изучается свойство $\otimes_W$-марковости для широко известных в математических методах защиты информации APN-преобразований, считающихся оптимальными при использовании в качестве s-боксов с целью «противодействия» разностному методу. Показано, что для каждого элемента g группы автоморфизмов орграфа, соответствующего APN-преобразованию b, множество всех орбит элемента g однозначно задает такое разбиение W, что b является $\otimes_W$-марковским преобразованием.

В качестве основных результатов сформулированы 8 положений, излагающих суть преложенного автором общего подхода к изучению алгебраических и комбинаторных свойств итерационных преобразований блочных криптографических систем. Предложенный подход проиллюстрирован на примерах конкретных криптографических алгоритмов.

В качестве недостатков можно отметить следующее. На взгляд оппонента, не совсем удачен термин "инвариантная $p(G, \mathbf{R}, \mathbf{R}')$ структура" на стр. 13 (определение 2), так как термин "инвариантность" означает неизменность, а в данном случае имеется ввиду отображение одного разбиения $\mathbf{R}$ на другое разбиение $\mathbf{R}'$.

Так на стр. 48 при описании алгоритма SMS4 упоминаются s-боксы, но не указано как они применяются в алгоритме.

Некоторые обозначения неудачны. Так стр. 65 обозначение A_i используется как для подмножества, состоящего из пар, так и для подмножества, состоящего из самих элементов. Затрудняет чтение также то, что многие обозначения вводятся не по тексту, а только в общем списке обозначений и сокращений, приводимом в конце диссертации.

Имеются неточности в написании отдельных формул.

На стр. 64 в формулировке теоремы 2.2.1 следует указывать интервал $\nu_1 + 1 \leq r \leq \nu_d$ вместо включения в неточно описанное множество

$r \in \{\nu_1 + 1, \ldots, \nu_d\}$.

На стр. 80 в формулировке теоремы 2.5.2 вместо

$$\chi_{n,\{\beta_1,\ldots,\beta_t\}}(\alpha, \alpha') =$$

$$= \begin{cases} \chi_{n,\{\beta_1,\ldots,\beta_{t-1}\}}(\alpha, \alpha'), & \text{если } \alpha \oplus \alpha' \in \langle \beta_1, \ldots, \beta_{t-1} \rangle \setminus \langle \beta_1, \ldots, \beta_{t-2} \rangle, \\ \chi_{n,\{\beta_1,\ldots,\beta_{t-1}\}}(\alpha, \alpha' \oplus \beta_t) + 2^{t-1}, & \text{если } \alpha \oplus \alpha' \in \langle \beta_1, \ldots, \beta_{t-1} \rangle \setminus \langle \beta_1, \ldots, \beta_{t-2} \rangle, \end{cases}$$

должно быть

$$\chi_{n,\{\beta_1,\ldots,\beta_t\}}(\alpha, \alpha') =$$

$$= \begin{cases} \chi_{n,\{\beta_1,\ldots,\beta_{t-1}\}}(\alpha, \alpha'), & \text{если } \alpha \oplus \alpha' \in \langle \beta_1, \ldots, \beta_{t-1} \rangle, \\ \chi_{n,\{\beta_1,\ldots,\beta_{t-1}\}}(\alpha, \alpha' \oplus \beta_t) + 2^{t-1}, & \text{если } \alpha \oplus \alpha' \in \langle \beta_1, \ldots, \beta_{t-1} \rangle \setminus \langle \beta_1, \ldots, \beta_{t-2} \rangle, \end{cases}$$

На стр. 86 строки 6,7 сказано "Если же $B^{(m,s)} = \emptyset$, то $||s|| \notin \{2^{m-1} - 2^{m/2-1}, 2^{m-1} + 2^{m/2-1}\}$", что неверно, так как в этом случае s — произвольная функция от m переменных.

На стр. 123 некорректно выписаны представители классов эквивалентности квадратичных форм $q_{n,1}$ и $q_{n,2}$, соответствующие двум неизоморфным типам ортогональных групп $O_n^{(1)}$ и $O_n^{(2)}$, так как при $n = 4t$ эти формы оказываются эквивалентными относительно группы GL_n.

На стр. 176 в промежуточных выражениях, входящих в цепочку равенств $\langle \alpha, \beta^h \rangle = \ldots = \langle \alpha^{th}, \beta \rangle$, пропущены скобки.

Перечисленные недостатки относятся, в основном, к оформлению диссертации и не снижают научной и практической значимости полученных в диссертации результатов.

Диссертация написана формальным математическим языком на современном уровне. Результаты диссертации являются новыми, они с достаточной полнотой обоснованы и изложены с необходимой степенью подробности. Обоснованность и достоверность положений диссертации обеспечивается их строгим математическим доказательством.

Основные результаты получены автором лично, они с достаточной полнотой опубликованы в 51 работе в научных изданиях, из которых 14 статей опубликованы в рецензируемых научных изданиях, указанных в перечне ВАК, и апробированы на международных научных конференциях и семинарах.

Работа содержит изложение математических принципов и решений, способствующих созданию новых и совершенствованию существующих средств

защиты информации и обеспечению информационной безопасности. Поэтому диссертация соответствует специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" (физико-математические науки).

Автореферат отражает содержание диссертации.

Вывод.

Диссертационная работа Пудовкиной М.А. вносит существенный вклад в решение научной проблемы, связанной с разработкой общего алгебраического и комбинаторного подхода к описанию структурных свойств итерационных преобразований, влияющих на качество построенных на их основе криптографических схем, имеющей существенной значение для разработки надежных систем защиты информации. По новизне и уровню научной проработки полученных результатов представленная работа соответствует специальности и требованиям ВАК, предъявляемым к докторским диссертациям, а ее автор, Пудовкина Марина Александровна, заслуживает присвоения ей ученой степени доктора физико-математических наук.

Официальный оппонент
доктор физико-математических наук, профессор,
специальность 20.03.04
(информация о наименовании специальности закрыта),
член-корреспондент Академии криптографии РФ,
научный консультант ФГУП «НИИ «Квант»

Черемушкин Александр Васильевич

24 апреля 2017 г.

Подпись Черемушкина Александра Васильевича заверяю

Федеральное государственное унитарное предприятие
«Научно-исследовательский институт «Квант» (ФГУП «НИИ «Квант»)
125438, г. Москва, 4-й Лихачёвский переулок, 15
Тел. +7 (499) 745-73-02
www.rdi-kvant.ru