ОТЗЫВ

на автореферат диссертации **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 (физико-математические науки)

Интенсивное развитие компьютерных средств и информационных технологий приводит к необходимости своевременного совершенствования имеющихся средств защиты информации, а также и разработки новых, с целью противодействия появляющимся новым методам анализа. Для этого необходимо постоянно осуществлять анализ средств защиты информации для выявления возможных уязвимостей, которые могут потенциально привести к возникновению новых подходов к анализу. Криптографические средства являются основой современных средств защиты информации в компьютерных системах и сетях.

При разработке средств защиты информации часто придерживаются итерационного принципа, который осуществляется итерационными функциями. Примером этого служат функции шифрования большинства современных блочно-итерационных алгоритмов, которые представимы в виде последовательного применения фиксированного числа относительно «несложных» итерационных преобразований, отличающихся между собой только зависимостью от конкретных цикловых ключей. Анализ такого средства защиты информации часто сводится к выявлению специфических свойств преобразований соответствующей итерационной функции, позволяющих описать некоторую структуру всей функции. Нахождение такой структуры может привести к возможности обнаружения потенциальных уязвимостей в средстве защиты информации. При этом возникает необходимость развития общей математической теории для описания и исследования таких специфических структур итерационных

функций, включающих и функции шифрования блочно-итерационных алгоритмов. Диссертации М.А. Пудовкиной как раз и посвящена разработке такой теории, основанной, в первую очередь, на методах теории групп подстановок и алгебраической теории графов.

Согласно автореферату диссертация состоит из введения, пяти глав, заключения и приложения. Во введении показана актуальность темы диссертации, определены цели и задачи проведённых исследований, дано краткое изложение диссертации по главам. Вводятся p_G-структуры итерационных криптографических функций, которые исследуются в диссертации. Первая глава посвящена p_G-структурам, задающихся разбиениями алфавита текстов с равномощными блоками. Указана их связь с особым классом групп, называемым сплетением симметрических групп подстановок. Описаны подстановки, которые максимально удалены от фиксированного представителя G этого класса. Соискателем отмечено, что такие подстановки по отношению к группе G выступают как аналог бент-функций по отношению к множеству всех аффинных функций. Вторая глава посвящена свойствам p_G-структур, задающихся конечными метриками на алфавите текстов. Исследован класс метрик, комбинаторно-групповые свойства которых в некотором роде схожи с соответствующими свойствами метрики Хемминга (например, их группы изометрий – надгруппы группы изометрий метрики Хемминга). Для этого сначала получено полное описание таких метрик. После этого в третьей главе проведена классификация их групп изометрий, а также характеризованы графы, задаваемые этими метриками (кратчайшее расстояние между вершинами в соответствующем графе). В завершение главы 3 дан пример, применения полученной классификации групп изометрий, для нахождения группы инерции корреляционно-иммунных функций. Эти результаты представляют несомненный математический и прикладной интерес. Четвертая глава посвящена исследованию влияния приводимости матрицы линейного преобразования XSL-алгоритма на свойства p_G-структур. Рассмотрение

криптографических приложений p_G-структур продолжено в пятой главе. Сначала для модификации алгоритма Фейстеля 2-го типа с 4m-битными блоками описываются p_G-структуры, использование которых позволяет отличить этот алгоритм для любого числа итераций от подстановки, равновероятно выбираемой из множества всех 4m-битных подстановок. Безусловно, этот результат представляет прикладной интерес. Оставшаяся часть главы 5 посвящена свойствам марковских блочно-итерационных алгоритмов и их обобщений. Несомненно, полученные здесь результаты имеют теоретический интерес для получения оценок защищённости информации.

В автореферате имеются незначительные стилистические погрешности (например, стр. 4, 7). Представляется интересным перенести результаты главы 4 (§4.6) и главы 5 (§5.5, §5.6) для алгоритмов Фейстеля.

Диссертация соответствует требованиям паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность по следующим областям исследований:

9. Модели и методы оценки защищённости информации и информационной безопасности объекта.

13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечению информационной безопасности.

Результаты диссертационных исследований докладывались на международных и всероссийских научных семинарах и конференциях. Автореферат правильно отражает содержание диссертации.

Считаю, что представленная диссертация «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» удовлетворяет всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации,

информационная безопасность, а её автор, Марина Александровна Пудовкина, несомненно заслуживает присуждения ученой степени доктора физико-математических наук.

Ведущий научный сотрудник ФГНБУ «РИСИ»,
доктор технических наук, старший научный сотрудник
(специальность 05.13.01 – системный анализ, управление и
обработка информации (в отраслях информатики,
вычислительной техники и автоматизации))

Абаев Лев Черменович

29 марта 2017 года
Email: abaev_lev@mail.ru

Подпись Л.Ч. Абаева заверяю

Ученый секретарь РИСИ,
начальник отдела научного
планирования и развития, к.э.н. Е.А Шарова

125413, г. Москва, ул. Флотская, дом 15Б, Федеральное государственное научное бюджетное учреждение «Российский институт стратегических исследований» («РИСИ»),
E-mail: mail@riss.ru
Эл. адрес сайта: http://riss.ru
Тел. (495) 454-92-64