ОТЗЫВ

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

В связи с интенсивным развитием электронного документооборота проблемам защиты конфиденциальной информации в современном мире уделяется с каждым годом всё большее внимание. Поэтому необходимо улучшение существующих и разработка новых средств защиты информации, что невозможно без глубокого математического исследования свойств примитивов, лежащих в основе этих средств. Одним из таких примитивов является итерационная функция. Во многих случаях поиск потенциальных уязвимостей в системе защиты информации, использующей такую функцию, может быть сведён к анализу ей структур, задаваемых соотношениями между её образами и прообразами. Поэтому тема, выбранная автором диссертации для исследования, представляет, несомненно, научный и практический интерес. Данное научное направление исследования относится к областям исследований пп. 9, 13 паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

К наиболее значимым результатам, отражённым в автореферате диссертации, относятся следующие.

1. Предложен единый метод задания и выявления структур, прежде всего, вызванных алгебраическими и комбинаторными свойствами «базовых» преобразований, составляющих итерационную функцию. В качестве базовых преобразований, рассматриваемых в диссертации, выступают S-блоки блочно-итерационных алгоритмов, линейные преобразования, преобразования-сдвиги векторного пространства и т.д.

2. Приведена классификация надгрупп группы Джевонса на $\{0,1\}^n$, из которой следует описание группы инерции множества всех корреляционно-иммунных функций порядка m при любом $m \in \{1, \dots, n\}$. Таким образом, исправлена ошибка в «классической» работе Meier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // EuroCrypt'89. Lect. Notes Comp. Sci. – 1989. – V. 434. – P. 549 – 562.

3. Описана структура блочно-итерационного алгоритма, предложенного в работе Zhang L., Zhang W., Wu W. Proposition of two cipher

structures // InsCrypt'2009. Lect. Notes Comp. Sci.– 2010. – V.6151. – P. 215 – 229. Применение такой структуры делает возможным для любого числа итераций отличить блочный алгоритм от множества независимых и равновероятно выбираемых подстановок, что, несомненно, вызовет уязвимость систем защиты информации, использующих этот алгоритм.

Из автореферата следует, что результаты диссертации были использованы в исследованиях Академии криптографии РФ, а также в ООО «СТЦ», АО «МакроСистемы» и в учебном процессе на кафедре ИУ8 МГТУ им. Н.Э. Баумана, что говорит о теоретической и практической значимости проделанной работы и полученных в ней результатов.

В качестве замечаний по автореферату следует отметить имеющиеся в нём стилистические погрешности (стр. 7, 20).

В целом, диссертация Пудовкиной М. А. «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» является научно-квалификационной работой, выполненной на высоком научном уровне и соответствующей требованиям «Положения о присуждении учёных степеней» ВАК, предъявляемым к докторским диссертациям. Считаю, что автор диссертации – Пудовкина Марина Александровна – заслуживает присуждения учёной степени доктора физико-математических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

И.О. зав. кафедрой «Комплексная защита
информации» ИИНТБ РГГУ,
старший научный сотрудник,
доктор технических наук,
(05.13.19 – «Методы и системы защиты информации, информационная безопасность)

Казарин Олег Викторович

117534, г. Москва, ул. Кировоградская, 25, корп. 2, Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гуманитарный университет», Институт информационных наук и технологии безопасности (ИИНТБ РГГУ),

e-mail: okaz2005@yandex.ru,
телефон: (495)250-62-57
адрес сайта: http://www.rsuh.ru/iintb/

Подпись О.В. Казарина
заверяю
зам. начальника
Управления кадров
Т.Н. Ананьева
15.03.2017