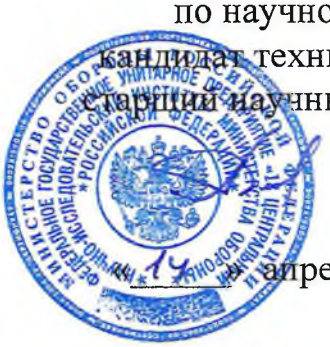
«УТВЕРЖДАЮ»
Заместитель руководителя
ФГУП "18 ЦНИИ" МО РФ
по научной работе
кандидат технических наук
старший научный сотрудник



В.П.Галах

14 апреля 2017 г.

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** (физико-математические науки)

В современном мире исключительно большое значение в разных областях приобрели вопросы обеспечения защиты конфиденциальной информации от несанкционированного доступа, в том числе и от ознакомления, воровства, модификации и подмены. При решении этих вопросов значительное место уделяется средствам криптографической защиты информации (СКЗИ). В теоретическом плане принцип, лежащий в основе большинства СКЗИ и предложенный К. Шенноном, состоит в построении стойкой криптосистемы путём последовательного применения относительно «простых» преобразований. Поэтому итерационные алгоритмы блочного шифрования являются наиболее распространённым типом среди реально существующих или теоретически предложенных, что объясняется простотой их программной реализацией, так и возможностью моделирования с помощью интегральных схем. В свою очередь каждый такой алгоритм моделируется итерационной функцией (функцией шифрования), которая основывается на многократном применении

преобразований, зависящих от ключа. Большинство слабостей итерационного алгоритма блочного шифрования вызвано наличием у соответствующей функции шифрования структур, часто задающихся отношениями между частями открытых, промежуточных, шифрованных текстов и ключа.

Разработка универсальных математических методов описания подобных структур, является актуальной проблемой.

Диссертационная работа Пудовкиной М.А. посвящена проблеме исследования структур итерационных криптографических функций, предназначенных для обнаружения возможных слабостей СКЗИ, использующих такие функции, и обусловленных алгебраическими и комбинаторными свойствами их компонент. Для этого соискателем выделены изучаемые в работе структуры, связанные с множеством преобразований G итерационной криптографической функции и названные p_G – структурами, которые позволили, в том числе, осуществить интерпретацию вариаций метода гомоморфизмов и различных обобщений линейного и разностного методов.

В диссертационной работе исследование p_G – структур множества G проводилось по следующим направлениям:

1) описание способов построения p_G – структур для множества G;

2) оценивание степени сохранения p_G – структуры множеством G;

3) нахождение расстояний относительно некоторой метрики на алфавите текстов, в том числе и метрики Хэмминга, между преобразованиями из множества G и множеством всех преобразований, сохраняющих p_G – структуру.

Один из основополагающих способов построения p_G – структур, рассматриваемых соискателем, заключается в сопоставлении им некоторой целочисленной метрики на алфавите текстов. Поэтому в диссертационной работе большое внимание уделено свойствам целочисленных метрик, в

том числе и схожих с метрикой Хэмминга. С учётом этого осуществлена классификация всех подметрик метрики Хэмминга и их групп изометрий.

В качестве приложений p_G – структур рассмотрена модель итерационных алгоритмов блочного шифрования с независимыми и равновероятно выбираемыми ключами для каждой итерации и алфавитом текстов X. Указаны условия, обеспечивающие сохранения марковости при укрупнении цепи Маркова с множеством состояний X^2, соответствующей биграммам промежуточных текстов. Описаны свойства рассматриваемых марковских алгоритмов и преобразований укрупнения, указана их связь с p_G – структурами. В качестве следствия получены известные в открытом криптографическом сообществе результаты работы "Lai X., Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis // EuroCrypt'91. Lect. Notes Comp. Sci.– 1991.– V. 547. – P. 17 – 38". Это подтверждает высокий научный уровень диссертационной работы.

Материалы диссертационного исследования внедрены в ООО «Специальный Технологический Центр» и в АО «МакроСистемы», а также на кафедре информационной безопасности МТГУ имени Н.Э. Баумана (национальный исследовательский университет). Следует также отметить, что значительная доля результатов получена при выполнении различных открытых тем Академии криптографии Российской Федерации в 2005 – 2016 гг. Всё это свидетельствует о высоком теоретическом уровне диссертационной работы.

В положительную сторону также следует отметить высокий уровень апробации результатов работы на научных конференциях и семинарах. Однако не ясно сколько из них входят в издания, включенные в перечень ВАК.

Вместе с тем, диссертационная работа Пудовкиной М.А. не лишена недостатков:

1. Судя по разделу "Актуальность темы" в автореферате слабо вскрыта проблемная ситуация и, как следствие, нечётко поставлена научная проблема, решаемая в диссертации.

2. В §1.4 приведен пример нахождения параметра $\chi_{\mathbf{W}}$ для алгоритма блочного шифрования SMS4. Представляет интерес найти параметр $\chi_{\mathbf{W}}$ для других алгоритмов, например, AES, Klein, ARIA, PRESENT, а также провести сравнение этих алгоритмов относительно значений параметра $\chi_{\mathbf{W}}$.

3. Из автореферата не ясно каким образом параметр $\chi_{\mathbf{W}}$ связан с характеристиками метода вероятностных гомоморфизмов?

4. В разделе автореферата "Внедрение..." не указано в каких именно образцах техники предприятий СТЦ и "МакроСистемы" внедрены результаты диссертационных исследований и что это внедрение дало.

5. Раздел автореферата "Личный вклад соискателя" требует уточнения.

Большинство отмеченных недостатков, скорее всего, объясняются ограниченным объёмом автореферата и не влияют на положительную оценку диссертационной работы.

Вывод. Диссертационная работа Пудовкиной М. А. является законченной научно-исследовательской работой, посвященной актуальной научной проблеме разработки и развития методов исследования комбинаторно-алгебраических структур итерационных функций, применяемых в системах защиты информации, отличающаяся научной новизной и практической значимостью полученных результатов.

Диссертация соответствует критериям, установленным «Положением о присуждении ученых степеней», утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013 г. №842, и удовлетворяет требованиям, предъявляемым к диссертациям на соискание ученой степени доктора физико-математических наук по специальности

05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки), а сама Пудовкина Марина Александровна заслуживает присуждения ей ученой степени доктора физико-математических наук по данной специальности.

Начальник отдела
кандидат технических наук
(специальность 05.13.01 – Системный анализ,
управление и обработка информации)

Александр Юрьевич Романенко

« 12 » апреля 2017 г.

Главный научный сотрудник ФГУП «18 ЦНИИ» МО РФ
доктор технических наук,
старший научный сотрудник
(специальность 20.02.14 – Вооружение и военная техника)

Игорь Леонидович Гатилов

« 12 » апреля 2017 г.

111123, г. Москва, Свободный проспект, д. 4, Федеральное государственное унитарное предприятие «18 Центральный научно-исследовательский институт» Министерства обороны Российской Федерации.
телефон: (495)-303-43-78

Подписи кандидата технических наук Александра Юрьевича Романенко, доктора технических наук Игоря Леонидовича Гатилова удостоверяю.

Начальник ОКиС
ФГУП «18 ЦНИИ» МО РФ Л.Ю.Чернова

М.П.