СВЕДЕНИЯ О РЕЗУЛЬТАТАХ ПУБЛИЧНОЙ ЗАЩИТЫ ДИССЕРТАЦИИ

Диссертационный совет Д 212.267.22, созданный на базе федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет», извещает о результатах состоявшейся 17 мая 2017 года публичной защиты диссертации Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность на соискание ученой степени доктора физико-математических наук.

На заседании присутствовали 16 из 19 членов диссертационного совета, в том числе 9 докторов наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, физико-математические науки:

1. Майер Г.В., доктор физико-математических наук, 05.13.19 (физ.-мат. науки) председатель диссертационного совета
2. Агибалов Г.П., доктор технических наук, 05.13.19 (техн. науки) заместитель председателя диссертационного совета
3. Тренькаев В.Н., кандидат технических наук, 05.13.19 (техн. науки) ученый секретарь диссертационного совета
4. Васильев В.А., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
5. Вернигоров Н.С., доктор технических наук, 05.13.19 (техн. науки)
6. Воробейчиков С.Э., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
7. Демкин В.П., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
8. Дмитренко А.Г., доктор физико-математических наук, 05.13.19 (техн. науки)
9. Дмитриев Ю.Г., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
10. Калайда В.Т., доктор технических наук, 05.13.19 (техн. науки)
11. Конев В.В., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
12. Костюк Ю.Л., доктор технических наук, 05.13.19 (техн. науки)
13. Кошкин Г.М., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
14. Крылов П.А., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
15. Старченко А.В., доктор физико-математических наук, 05.13.19 (физ.-мат. науки)
16. Сущенко С.П., доктор технических наук, 05.13.19 (техн. науки)

Заседание провёл председатель диссертационного совета доктор физико-математических наук, профессор Майер Георгий Владимирович.

По результатам защиты диссертации тайным голосованием (результаты голосования: за присуждение ученой степени – 16, против – нет, недействительных бюллетеней – нет) диссертационный совет принял решение присудить М.А. Пудовкиной ученую степень доктора физико-математических наук.

Заключение диссертационного совета Д 212.267.22
на базе федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский Томский государственный университет»
Министерства образования и науки Российской Федерации
по диссертации на соискание ученой степени доктора наук

аттестационное дело № _____

решение диссертационного совета от 17.05.2017, № 8

О присуждении **Пудовкиной Марине Александровне**, гражданину Российской Федерации, ученой степени доктора физико-математических наук.

Диссертация **«Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации»** по специальности **05.13.19** – Методы и системы защиты информации, информационная безопасность принята к защите 30.01.2017 г., протокол № 7, диссертационным советом **Д 212.267.22** на базе федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет» Министерства образования и науки Российской Федерации (634050, г. Томск, пр. Ленина, 36, приказ о создании диссертационного совета № 75/нк от 15.02.2013).

Соискатель **Пудовкина Марина Александровна**, 1976 года рождения.

Диссертацию на соискание ученой степени кандидата физико-математических наук «Свойства программно реализуемых поточных шифров (на примере RC4, GI, Веста)» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность защитила в 2004 г. в совете ДМ 212.130.08, созданном на базе Московского инженерно-физического института (государственного университета).

Работает в должности доцента кафедры «Криптология и кибербезопасность» в федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский ядерный университет «МИФИ» Министерства образования и науки Российской Федерации; по совместительству – в должности доцента кафедры «Информационная

безопасность» в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)» Министерства образования и науки Российской Федерации.

Диссертация выполнена на кафедре «Информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» Министерства образования и науки Российской Федерации.

Научный консультант – действительный член Академии криптографии Российской Федерации, доктор физико-математических наук, профессор **Погорелов Борис Александрович** (информация о занимаемой должности закрыта).

Официальные оппоненты:

Черёмушкин Александр Васильевич, член-корреспондент Академии криптографии Российской Федерации, доктор физико-математических наук, профессор, федеральное государственное унитарное предприятие «Научно-исследовательский институт «Квант», научный консультант

Бабаш Александр Владимирович, доктор физико-математических наук, профессор, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики», кафедра информационной безопасности, профессор

Титов Сергей Сергеевич, доктор физико-математических наук, профессор, федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщений», кафедра «Информационные технологии и защита информации», главный научный сотрудник

дали положительные отзывы на диссертацию.

Ведущая организация – федеральное государственное бюджетное образовательное учреждение высшего образования **«Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского»**, г. Саратов, в своем положительном отзыве, подписанном **Салием Вячеславом Николаевичем** (кандидат физико-математических наук, профессор, кафедра

теоретических основ компьютерной безопасности и криптографии, заведующий кафедрой), отметила, что 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. Комбинаторные методы всегда широко применялись в криптографии. Большое внимание здесь уделяется, в частности, графам. При исследовании криптографических функций естественно возникают некоторые производные структуры, с помощью которых в ряде случаев удается найти новые подходы в анализе, в частности, блочных шифров. Тема работы представляется актуальной как с точки зрения теоретических, так и прикладных разделов 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. К основным результатам диссертации относятся: характеризация подстановок, максимально далеких от импримитивной группы IG_W (максимальной группы, сохраняющей разбиение W), которых можно считать аналогом бент-функций; полное описание натуральных метрик, инвариантных относительно группы Джевонса (они являются натуральными метриками графов орбиталов для надгрупп этой группы); полная классификация групп автоморфизмов графов орбиталов надгрупп группы Джевонса; классификация дистанционно транзитивные графы орбиталов надгрупп группы Джевонса; корректировка полученного ранее другими авторами описания группы инерции всех двоичных корреляционно-иммунных функций заданного порядка; модификация разностного метода криптоанализа для марковского XSL-алгоритма с приводимым линейным преобразованием; выделение особого класса итерационных марковских алгоритмов и указание связи между такими алгоритмами и существованием двумерных p_G-структур, а также указанием

наличия для алгоритма в ряде случаев нетривиального подстановочного гомоморфизма. Совокупность полученных результатов можно квалифицировать как весомый вклад в развитие математических методов современной криптографии.

Соискатель имеет 96 опубликованных работ, в том числе по теме диссертации 51 работу, опубликованных в рецензируемых научных изданиях – 32 (из них 4 статьи в российском журнале, переводные версии которого индексируются Web of Science), публикации в сборниках материалов международных и всероссийских научных конференций и семинаров – 19 (из них 8 статей в сборниках материалов зарубежных конференций, в том числе 2 зарубежные конференции, сборники материалов которых индексируются Scopus). Общий объём публикаций – 63,04 п.л., авторский вклад – 41,32 п.л.

Наиболее значительные научные работы по теме диссертации, опубликованные в журналах, включенных в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора наук:

1. **Пудовкина М. А.** Невозможные разности XSL алгоритмов шифрования Фейстеля / М. А. Пудовкина // Системы высокой доступности. – 2011. – Вып. 2. – С. 28–33. – 0,66 п.л.

2. Погорелов Б. А. Натуральные метрики и их свойства. Ч. 2. Метрики типа Хемминга / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2012. – Т. 3, вып. 1. – С. 71–95. – 2,75 / 1,83 п.л.

3. Погорелов Б. А. Факторструктуры преобразований / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2012. – Т. 3, вып. 3. – С. 81–104. – 2,64 / 1,76 п.л.

4. **Пудовкина М. А.** О классах слабых ключей обобщенной шифрсистемы PRINT / М. А. Пудовкина, Г. И. Хоруженко // Математические вопросы криптографии. – 2013. – Т. 4, вып. 2. – С. 113–125. – 1,43 / 0,72 п.л.

5. Погорелов Б. А. Комбинаторная характеризация XL-слоев / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии.– 2013. – Т. 4, вып. 3. – С. 99–129. – 3,41 / 2,73 п.л.

6. **Пудовкина М. А.** Об оценке числа раундов с невозможными разностями в обобщённых алгоритмах шифрования Фейстеля / М. А. Пудовкина, А. В. Токтарев// Прикладная дискретная математика. – 2015. – № 1 (27). – С. 37–51. – 1,65 / 0,82 п.л.

7. Погорелов Б. А. О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности / Б. А. Погорелов, **М. А. Пудовкина** // Дискретная математика. – 2013. – Т. 25, вып. 3. – С. 78–95. – 1,98 / 1,32 п.л.

в переводной версии журнала:

Pogorelov B. On the distance from permutations to the imprimitive groups with fixed parameters of imprimitivity systems/ B. Pogorelov, **M. Pudovkina** // Discrete Mathematics and Applications. – 2014. – Vol. 24, is. 2. – P. 95–108. – DOI: 10.4213/dm1249. (*Web of Science*)

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации.

На автореферат поступило 16 положительных отзывов. Отзывы представили:
1. **А. А. Молдовян**, д-р техн. наук, проф., начальник научно-исследовательского отдела проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации РАН, **И. В. Котенко**, д-р техн. наук, проф., заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, *с замечаниями*: не представлено исследование комбинаторно-алгебраических свойств множества подстановок, задаваемых управляемыми подстановочно перестановочными сетями, в отношении существования нетривиальных структур; представляет интерес провести анализ блочных шифров на основе управляемых операций на наличие рассматриваемых в диссертации структур, например, для семейства блочных шифров SPECTR, COBRA и DDP; не ясно, проведена ли оценка трудоемкости взлома блочного шифра ISEBERG на базе структуры, предложенной в диссертации. 2. **А. В. Лакеев**, д-р физ.-мат. наук, ведущий научный сотрудник Института динамики систем и теории управления им. В.М. Матросова СО РАН, г. Иркутск, *с замечаниями*: автору следовало бы более четко выделить сильные стороны предлагаемых в диссертации методов в сравнении с известными

подходами к анализу биграмм; в предложении «Примерами $+_W$ -марковских преобразований...», по всей видимости, допущена опечатка и должно быть: «Примерами $\otimes_W$ - марковских преобразований...». 3. **А. Н. Скиба**, д-р физ.-мат. наук, проф., профессор кафедры алгебры и геометрии Гомельского государственного университета имени Франциска Скорины, Республика Беларусь, *с замечаниями*: интересно классифицировать надгруппы группы экспоненцирования $S_2 \uparrow S_n$ при $q > 3$; интересно идентифицировать графы, задаваемые подметриками метрики Хемминга, которые не являются дистанционно-транзитивными. 4. **Е. А. Голубев**, д-р техн. наук, проф., советник руководителя 18-го Центрального научно-исследовательского института Минобороны России, г. Москва, **А. С. Островский**, канд. техн. наук, старший научный сотрудник 18-го Центрального научно-исследовательского института Минобороны России, г. Москва, **Д. С. Кононов**, канд. техн. наук, начальник лаборатории 18-го Центрального научно-исследовательского института Минобороны России, г. Москва, *с замечаниями*: несколько раз используются утверждения о потенциальной возможности без указания чётких параметров и примеров реализации, что не позволяет критически оценить следующие выводы автора: «существование такой отличимости может привести к применению «фундаментальной» атаки различением» (стр. 13); «наличие группы IG_W...может означать возможность применения метода гомоморфизмов» (стр. 14); «существование $p_{C_n(h)}$-структуры у группы $C_n(h)$ ... может влиять на криптографические свойства всего алгоритма» (стр. 21) и т.д.; автор указывает, что полученные научные результаты позволяют «предлагать новые методы криптоанализа, и обобщать известные» (стр. 10), при этом не приведено ни конкретных примеров таких методов, ни сравнение их с существующими методами криптоанализа; утверждение диссертанта «приведённый подход в ряде случаев эффективнее по сравнению со способом нахождения вероятностей «классических» разностных характеристик» (стр. 22) не подтверждено; не раскрыто понятие эффективности; не ясно, какова эффективность данного подхода по сравнению с методами, использующими отличные от «классических» разностные характеристики; неправильно оформлены отсылки к

библиографическим записям в затекстовой ссылке, кроме того, для некоторых источников не указаны сведения о местоположении объекта ссылки в документе: «атаки различением (см. [36])»; «понятие «преобладающей» метрики [34]» и т.д.; на странице 24 вместо термина «$\otimes_W$-марковских» используется «$+_W$-марковских». 5. **И. Л. Гатилов**, д-р техн. наук, ст. науч. сотр., главный научный сотрудник 18-го Центрального научно-исследовательского института Минобороны России, г. Москва, **А. Ю. Романенко**, канд. техн. наук, начальник отдела 18-го Центрального научно-исследовательского института Минобороны России, г. Москва, *с замечаниями*: слабо вскрыта проблемная ситуация и нечётко поставлена научная проблема, решаемая в диссертации; в § 1.4 приведен пример нахождения параметра χ_W для алгоритма блочного шифрования SMS4, представляет интерес найти параметр χ_W для других алгоритмов, например, AES, Klein, ARIA, PRESENT, а также провести сравнение этих алгоритмов относительно значений параметра χ_W; из автореферата не ясно каким образом параметр χ_W связан с характеристиками метода вероятностных гомоморфизмов; в разделе автореферата "Внедрение..." не указано, в каких именно образцах техники предприятий СТЦ и "Макросистемы" внедрены результаты диссертационных исследований и что это внедрение дало; раздел автореферата «Личный вклад соискателя» требует уточнения. 6. **В. В. Быкова**, д-р физ.-мат. наук, доц., профессор кафедры высшей и прикладной математики Сибирского федерального университета, г. Красноярск, *с замечаниями*: не указаны границы практической применимости основных теоретических результатов диссертационной работы; имеются опечатки и стилистические неточности. 7. **В. Н. Товчигречко**, д-р техн. наук, главный научный сотрудник ЦБС Центрального научно-исследовательского института химии и механики, г. Москва, **И. Ю. Коркин**, канд. техн. наук, старший научный сотрудник 908 научно-исследовательского отдела центра прикладных разработок Центрального научно-исследовательского института химии и механики, г. Москва, **К. В. Малёваный**, канд. техн. наук, начальник центра прикладных разработок – заместитель генерального директора Центрального научно-исследовательского института химии и механики, г. Москва, *без замечаний*. 8. **И. И. Левин**, д-р техн. наук, проф., директор Научно-исследовательского центра

супер-ЭВМ и нейрокомпьютеров, г. Таганрог, *с замечаниями*: автором доказано существование, но не приведено описание p_G-структур алгоритмов блочного шифрования PRINTcipher, Robin, iSCREAM, Zorro; не прослеживается связь между свойствами орбитальных производных и p_G-структур. 9. **Л. К. Бабенко**, д-р техн. наук, проф., профессор кафедры «Безопасность информационных технологий» Южного федерального университета, г. Таганрог, *с замечаниями*: полезно получить информацию по области граничной применимости разработанных способов построения структур для современных итерационных криптографических функций; хотелось бы увидеть развернутое представление практического использования разработанных способов поиска и построения p_G-структур для задач анализа надежности семейств XLS-алгоритмов шифрования. 10. **Л. Ч. Абаев**, д-р техн. наук, ст. науч. сотр., ведущий научный сотрудник Российского института стратегических исследований, г. Москва, *без замечаний*. 11. **М. Н. Чесноков**, д-р техн. наук, заместитель начальника отдела связи Специального технологического центра, г. Санкт-Петербург, *с замечаниями*: обоснованию актуальности темы диссертации и истории вопроса вместе со списком известных источников отведено 8 страниц, что ограничило возможность автора по изложению сути решенных задач; к сожалению, в автореферате не приведены сведения, показывающие результаты применения разработанных p_G-структур к известным алгоритмам блочного шифрования; в автореферате отсутствуют количественные характеристики разработанного способа анализа XSL-алгоритмов блочного шифрования в сравнении с разностным методом. 12. **О. В. Казарин**, д-р техн. наук, ст. науч. сотр., исполняющий обязанности заведующего кафедрой «Комплексная защита информации» Российского государственного гуманитарного университета, г. Москва, *с замечанием*: следует отметить имеющиеся в автореферате стилистические погрешности (стр. 7, 20). 13. **Р. В. Мещеряков**, д-р техн. наук, проф., проректор по научной работе и инновациям, заведующий кафедрой безопасности информационных систем Томского государственного университета систем управления и радиоэлектроники, *с замечаниями*: неясно, какая связь существует между APN-подстановками и p_G-структурами; на странице 24 автореферата имеется опечатка в фразе о s-боксах алгоритма SAFER; пункт 6

научной новизны, сформулированный на странице 9 автореферата, не отражен в тексте автореферата. 14. **Ф. К. Алиев**, д-р физ.-мат. наук, ведущий советник Главного управления развития информационных и телекоммуникационных технологий Минобороны России, г. Москва, *с замечанием*: можно отметить отдельные стилистические погрешности (например, на стр. 4). 15. **Ю. С. Харин**, д-р физ.-мат. наук, проф., член-корреспондент НАН Беларуси, директор НИИ прикладных проблем математики и информатики Белорусского государственного университета, г. Минск, Республика Беларусь, *с замечаниями*: вопросы выраженности p_G-структуры произвольной криптосистемы и времени на проверку действия подстановок на ней, которые определяют вероятность успеха атак по распознаванию/и их сложность, не освещены; не ясно, какие из результатов диссертации внедрены в Академии криптографии РФ, ООО «СТЦ» и АО «Макросистемы». 16. **Малюгин С.А.**, д-р физ.-мат. наук, ведущий научный сотрудник лаборатории дискретного анализа Института математики им. С.Л. Соболева СО РАН, г. Новосибирск, **Токарева Н. Н.,** канд. физ.-мат. наук, старший научный сотрудник лаборатории дискретного анализа Института математики им. С.Л. Соболева СО РАН, г. Новосибирск, *без замечаний*.

Авторы отзывов отмечают, что разработка и создание доверенных отечественных технологий и средств защиты информации, отвечающих российским стандартам и требованиям информационной безопасности, относится к первоочередному направлению обеспечения национальной безопасности России. Диссертационная работа М.А. Пудовкиной нацелена на разработку теоретического обеспечения для решения этой актуальной проблемы. Автор исследует структуры итерационных функций в связи с математическими задачами, возникающими при поиске уязвимостей в системах защиты информации, в том числе и в криптографических примитивах. В теоретико-вероятностных терминах автор вводит строгое математическое определение структуры дискретного отображения, исследует способы описания структур. Описание и исследование структур проводится с использованием комбинаторно-алгебраических методов, активно применяется теоретико-групповой подход. Такие структуры задаются разными комбинаторными объектами, например, метриками, графами и разбиениями

конечных множеств, а группами автоморфизмов этих структур выступают соответственно группы изометрий метрик, группы автоморфизмов графов, и группы, сохраняющие разбиения. При этом охватывается широкий круг фундаментальных математических задач – от классификации графов надгрупп группы Джевонса до приложения теории цепей Маркова к описанию свойств алгоритмов блочного шифрования. Диссертационное исследование М.А. Пудовкиной вносит существенный вклад в развитие научно-методического аппарата оценки уязвимостей систем защиты информации. Результаты работы будут интересны специалистам в области дискретной математики, алгебры, теоретической криптографии и могут быть применены для обеспечения выполнения необходимых требований при разработке отечественных средств защиты информации.

Выбор официальных оппонентов и ведущей организации обоснован тем, что **А. В. Черёмушкин** является высококвалифицированным специалистом в области дискретной математики и систем защиты информации; **А. В. Бабаш** – высококвалифицированным специалистом в области конечно-автоматных методов и систем защиты информации; **С. С. Титов** – высококвалифицированным специалистом в области алгебраических методов и систем защиты информации; **Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского** является одним из ведущих отечественных научных центров в области дискретной математики и ее приложений к защите информации и компьютерной безопасности.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований получены следующие новые научные результаты:

впервые введено понятие p_G-структуры множества подстановок G через разбиения множества X^t и показано, что оно является одним из естественных способов описания структур итерационных криптографических функций, в том числе и итерационных алгоритмов блочного шифрования; описаны классы разбиений, задающие p_G-структуры, их алгебраические, комбинаторные и криптографические свойства;

впервые введена величина $\chi_W(g)$, характеризующая удаленность произвольного преобразования от сплетения групп подстановок, сохраняющего p_G-структуру; и *получены* верхние и нижние оценки $\chi_W(g)$;

получено полное описание подстановок, максимально далеких от сплетения групп подстановок при заданной системе импримитивности;

полностью классифицированы подметрики метрики Хемминга на n-мерном векторном пространстве и их группы изометрий;

полностью классифицированы дистанционно транзитивные графы орбиталов надгрупп группы Джевонса;

впервые описаны свойства графов орбиталов группы $C_n(g)$, порождённой преобразованиями X- и L-слоёв XSL-алгоритма; *получены* условия, при которых графы орбиталов группы $C_n(g)$ принадлежат к таким важным для алгебраической комбинаторики классам графов как дистанционно транзитивные и дистанционно регулярные;

впервые введены понятия $\otimes_W$-марковских преобразований и $\otimes_W$-алгоритмов блочного шифрования и *описаны* их свойства, в том числе условия на разбиение W множества X, при которых имеет место $\otimes_W$-марковость;

получено описание группы инерции множества всех двоичных корреляционно-иммунных функций фиксированного порядка;

впервые введено понятие L-факторструктуры и описана её группа автоморфизмов.

Теоретическая значимость исследования обоснована тем, что:

разработан общий способ поиска и построения p_G-структур, обусловленных комбинаторно-алгебраическими свойствами преобразований, составляющих итерационную криптографическую функцию, позволяющий предлагать новые методы анализа, и обобщать известные;

описаны подстановочные и комбинаторные свойств групп, порождённых преобразованиями, составляющими итерационную криптографическую функцию, в том числе преобразованиями X- и L- слоёв функции зашифрования, а также характеризация свойств соответствующих графов орбиталов и их метрик;

описано влияние свойств отдельных преобразований, составляющих функцию зашифрования, на существование различных потенциально опасных p_G-структур; определено влияние приводимости преобразования линейного слоя на стойкость XSL-алгоритмов;

выявлена связь конечных целочисленных метрик, p_G-структур и метрик, инвариантных относительно преобразования линейного слоя, в том числе метрик типа Хемминга; в связи с этим описаны свойства метрик, инвариантных относительно группы сдвига пространства $V_n(2)$, а также полностью классифицированы метрики типа Хемминга, группа изометрий которых является надгруппой группы Джевонса, а также их группы изометрий;

разработан способ анализа XSL-алгоритмов, использующего инвариантные подпространства линейного преобразования и обобщающего разностный метод.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

Результаты исследования включены в отчеты по темам НИР Академии криптографии РФ в 2005–2016 гг.

Результаты работы внедрены в ООО «Специальный технологический центр» (в рамках выполнения научно-исследовательских работ по государственным контрактам № 665/ЕГН/Р/2015 от 27.02.2015, № 2194/ЕГН/Р/2016 от 24.03.2016) при анализе систем закрытия данных, в которых используется XSL-алгоритмы, в частности AES, для анализа возможных уязвимостей; в АО «МакроСистемы» (в рамках выполнения научно-исследовательских работ: НИР «Атлас-2014» (исх. №107с м/с от 17.11.2014), НИР «Алгол-2015» (исх. №132с м/с от 09.11.2015)). Внедрение результатов позволило значительно повысить уровень научной обоснованности проектирования и совершенствования программно-аппаратных средств по комплексной безопасности информационных систем предприятий.

Результаты работы использованы на кафедре «Информационная безопасность» Московского государственного технического университета им. Н.Э. Баумана при составлении курсов обучения дисциплинам специальности «Компьютерная безопасность», а также курсов обучения «Алгебраический криптоанализ», «Современные методы криптоанализа».

Рекомендации об использовании результатов диссертационного исследования. Полученные результаты могут быть использованы для систематизации известных методов синтеза и анализа систем защиты информации,

основанных на итерационных алгоритмах блочного шифрования, а также могут быть применены при анализе систем защиты информации, в которых используются итерационные алгоритмы блочного шифрования, для поиска возможных уязвимостей, основанных на наличии различных нетривиальных потенциально опасных p_G-структур, в частности, для обеспечения выполнения необходимых требований при разработке отечественных средств защиты информации и анализе зарубежных.

Результаты работы могут быть использованы в учебном процессе по направлениям подготовки 10.05.01 – Компьютерная безопасность (профиль подготовки «Математические методы защиты информации»), 10.03.01 – Информационная безопасность (профиль подготовки «Безопасность автоматизированных системы»), 10.04.01 – Информационная безопасность (профиль подготовки «Криптографические методы обеспечения кибербезопасности»).

Оценка достоверности результатов исследования выявила:

корректность выводов и доказательств утверждений и теорем;

совпадение полученных результатов в частных случаях с известными результатами других авторов;

обобщение и исправление известных ранее результатов других авторов.

согласие полученных результатов с результатами, представленными в независимых источниках.

Личный вклад автора состоит в: постановке цели диссертационной работы и решении задач для ее достижения; в получении лично соискателем всех основных изложенных в диссертации результатов (включая: классификацию подметрик метрики Хемминга и их групп изометрий, классификацию дистанционно транзитивных графов орбиталов надгрупп группы Джевонса, описание группы инерции множества корреляционно-иммунных функций, описание свойств инвариантных относительно группы сдвигов пространства $V_n(2)$ метрик, описание свойств $\otimes_W$-марковских преобразования и $\otimes_W$-марковских алгоритмов, описание подстановок, максимально далеких от группы $S_w \wr S_r$ при фиксированной системе импримитивности, оценки величины $\chi_W(g)$, разработку для

XSL-алгоритмов способа построения обобщённой разностной характеристики, основанной на смежных классах инвариантного подпространства линейного преобразования, описание p_G-структуры обобщений алгоритма Фейстеля 2-го типа); в введении понятий p_G-структура, L-факторструктура, $\otimes_W$-марковские преобразования и $\otimes_W$-алгоритмы блочного шифрования; в написании по полученным результатам статей (в соавторстве); в сделанных докладах на научных конференциях и семинарах.

Диссертация отвечает критериям, установленным Положением о присуждении ученых степеней для диссертаций на соискание ученой степени доктора наук, и, в соответствии с пунктом 9 Положения, является научно-квалификационной работой, в которой на основании выполненных автором исследований решена актуальная научная проблема разработки и описания общих комбинаторно-алгебраических структур преобразований и групп подстановок, порожденных составляющими итерационных криптографических функций, имеющая важное значение для разработки методов оценки защищенности действующих и перспективных средств защиты информации, а также для создания надежных систем защиты информации.

На заседании 17.05.2017 диссертационный совет принял решение присудить **Пудовкиной М.А.** ученую степень доктора физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 9 докторов наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, физико-математические науки, из 19 человек, входящих в состав совета, проголосовал: за – 16, против – нет, недействительных бюллетеней – нет.

Председатель
диссертационного совета Майер Георгий Владимирович

Ученый секретарь
диссертационного совета Тренькаев Вадим Николаевич

17 мая 2017 г.