ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА МГУ.05.01 ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ ДОКТОРА НАУК

Решение диссертационного совета от 25 декабря 2019 г. № 18

О присуждении Логачеву Олегу Алексеевичу, гражданину Российской Федерации, ученой степени доктора физико-математических наук.

Диссертация «Построение и анализ эффективности алгоритмов обращения дискретных функций в математических моделях информационной безопасности» по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность (физико-математические науки) принята к защите диссертационным советом 02 октября 2019 года, протокол № 14.

Соискатель **Логачев Олег Алексеевич,** 1950 года рождения,

в 1972 году окончил Технический факультет Высшей школы КГБ СССР по специальности «Прикладная математика» с присвоением квалификации «инженер-математик» (диплом специалиста Щ № 058615);

в 1977 году окончил очную аспирантуру Высшей школы КГБ СССР;

в 1980 году защитил диссертацию по спецтеме на соискание ученой степени кандидата физико-математических наук по закрытой специальности (диплом кандидата наук ФМ № 012773).

в 1988 году соискателю присвоено ученое звание старший научный сотрудник по специальности «Математическая кибернетика» (аттестат старшего научного сотрудника СН № 055298).

Соискатель **с 2000 года по настоящее время** работает в Московском государственном университете имени М.В. Ломоносова в Институте проблем информационной безопасности факультета вычислительной математики и кибернетики (Москва, Мичуринский проспект, д. 1, офис 10). **С 2004 года по настоящее время** соискатель состоит в должности заведующего отделом математических проблем информационной безопасности.

Диссертация выполнена в ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра информационной безопасности.

Научный консультант — нет.

Официальные оппоненты:

Алиев Физули Камилович, доктор физико-математических наук, доцент, консультант отдела Департамента информационных систем Министерства обороны РФ,

Никонов Владимир Глебович, доктор технических наук, профессор, член-корреспондент Академии криптографии,

Фомичев Владимир Михайлович, доктор физико-математических наук, профессор, профессор кафедры информационной безопасности ФГБОУ ВО «Финансовый университет при правительстве Российской Федерации»

дали **положительные отзывы** на диссертацию.

Соискатель имеет 65 опубликованных работ, в том числе по теме диссертации 26 работ, из них **17 статей, опубликованных в рецензируемых научных изданиях, индексируемых Web of Science, Scopus или RSCI**, либо в иных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность (физико-математические науки).

1. Логачев О.А., Проскурин Г.В., Ященко В.В. Локальное обращение конечного автомата с помощью автоматов. // Дискр. математика, том7, вып. 2, 1995, с. 19-33 (импакт-фактор Scopus 0,325).
2. Логачев О.А., Сальников А.А., Ященко В.В. Бент-функции на конечной абелевой группе. // Дискр. математика, том 9, вып. 4, 1997, с.3-20 (импакт-фактор Scopus 0,325).
3. Логачев О.А., Ященко В.В. Коды типа Рида-Маллера на конечной абелевой группе. // Пробл. передачи информации, том 34, вып. 2, 1998, с.32-46 (импакт-фактор Web of Science 0,557).
4. Логачев О.А., Сальников А.А., Ященко В.В. Спаривание конечных модулей, дуальность линейных кодов и тождества Мак-Вильямс. // Пробл. передачи информации, том.34, вып. 3, 1998, с. 50-59 (импакт-фактор Web of Science 0,557).
5. Логачев О.А., Сальников А.А., Ященко В.В. О свойствах сумм Вейля на конечных полях и конечных абелевых группах. // Дискр. математика, том 11, вып. 2, 1999, с. 66-85 (импакт- фактор Scopus 0,325).
6. Логачев О.А., Сальников А.А., Ященко В.В. Невырожденная нормальная форма булевых функций. // Докл. РАН, том 373, № 2, 2000, с.164-167 (импакт-фактор Web of Science 0,625).
7. Логачев О.А., Сальников А.А., Ященко В.В. Об одном свойстве ассоциированных представлений группы GL(n,k). // Дискр. математика, том 12, вып. 2, 2000, с.154-159 (импакт-фактор Scopus 0,325).
8. Логачев О.А., Сальников А.А., Ященко В.В. Некоторые характеристики «нелинейности» групповых отображений. // Дискр. анализ и иссл. операций, серия 1,том 8, № 1, 2001, с. 40-54 (импакт-фактор Scopus 0,247).
9. Логачев О.А., Сальников А.А., Ященко В.В. О наследовании свойств при сужении булевых функций. // Дискр. математика, том 14, вып. 2, 2002, с. 9-19 (импакт-фактор Scopus 0,325).
10. Буряков М.Л., Логачев О.А. Об уровне аффинности булевых функций. // Дискр. математика, том 17, вып. 4, 2005, с. 98-107 (импакт-фактор Scopus 0,325).
11. Логачев О.А. Нижняя граница уровня аффинности для почти всех булевых функций. // Дискр. математика, том 20, вып. 4, 2008, с. 85-88 (импакт-фактор Scopus 0,325)
12. Логачев О.А. О значениях уровня аффинности для почти всех булевых функций. // Прикл. дискр. математика, № 3, 2010, с. 17-21 (импакт-фактор Scopus 0,265).
13. Логачев О.А. Критерий совершенной уравновешенности сдвиг-композиции функций над конечным алфавитом. // Дискр. математика, том 29,

вып. 4, 2017, с. 59-65 (импакт-фактор Scopus 0,325).

14. Логачев О.А. О локальной обратимости конечных автоматов без потери информации. // Прикл. дискр. математика, № 39, 2018, с. 78-93 (импакт-фактор Scopus 0,265).

15. Логачев О.А. Теоретико-информационная характеризация совершенно уравновешенных функций. // Информатика и ее применения, том 12, вып.4, 2018, с.70-74 (импакт-фактор Scopus 0,279).

16. Логачев О.А., Федоров С.Н., Ященко В.В. Булевы функции как точки на гиперсфере в евклидовом пространстве. // Дискр. математика, том 30, вып. 1, 2018, с. 39-55 (импакт-фактор Scopus 0,325).

17. Логачев О.А., Федоров С.Н., Ященко В.В. О Δ — эквивалентности булевых функций. // Дискр. математика, том 30, вып. 4, 2018, с.29-40 (импакт-фактор Scopus 0,325).

На автореферат **поступило 2 отзыва, оба отзыва — положительные**.

Выбор официальных оппонентов обусловлен тем обстоятельством, что они являются специалистами в области методов и систем защиты информации, а также имеют работы, близкие к теме диссертации соискателя.

Диссертационный совет отмечает, что **диссертация** О.А.Логачева, представленная на соискание ученой степени доктора физико-математических наук, **является научно-квалификационной работой,** в которой на основании выполненных автором исследований описываются **решения трудных и, в ряде случаев, давно поставленных задач. В диссертационном исследовании разработаны теоретические положения, совокупность которых представляет собой крупное научное достижение.**

Диссертация посвящена **проблеме обращения дискретных функций, ассоциированных со средствами обеспечения информационной безопасности(ИБ)**. Методы анализа средств обеспечения ИБ имеют математическую природу и используются в рамках математических моделей, описывающих процессы функционирования таких средств, действия противника, а также возможные угрозы ИБ. Параметры методов и алгоритмов обращения дискретных функций существенным образом определяют итоговую оценку уровня защиты информации. Поскольку значительное число задач обращения дискретных функций относится к условному сложностному классу трудно решаемых задач, в ходе анализа математических моделей средств обеспечения ИБ необходимо исследовать и разрабатывать новые подходы к их совершенствованию, развивать методы обращения дискретных функций и получать новые результаты исследования свойств таких функций, что обуславливает актуальность тематики диссертации.

Диссертация представляет собой **самостоятельное законченное исследование,** обладающее внутренним единством.

Положения, выносимые на защиту, содержат обоснование актуальности темы, её теоретической новизны и практической значимости, а также полученных в ходе диссертационного исследования следующих новых научных результатов, которые свидетельствуют о **личном вкладе автора в науку**:

1. впервые для семейства групповых функций, определенных на произвольных конечных абелевых группах, предложена и обоснована математическая модель, обобщающая семейство двоичных полиномиальных кодов Рида-Маллера, и найдены необходимые и достаточные условия принадлежности любой групповой функции некоторому обобщенному коду Рида-Маллера;
2. впервые для семейств групповых функций, определенных на произвольных конечных абелевых группах, предложено и обосновано обобщение понятия булевой бент-функции и исследованы спектральные и алгебраические свойства бент-функций на произвольной конечной абелевой группе;
3. впервые для семейств групповых функций, определенных на произвольных конечных абелевых группах, исследовано представление групповой функции, обобщающее понятие аффинного расщепления булева отображения, доказаны новые соотношения, связывающие параметры этого представления и необходимые для расчета эффективности методов обращения групповых функций;
4. впервые для кодов на конечных модулях введено понятие дуальности и доказаны соотношения, связывающие ρ-характеристики дуальных кодов на конечных модулях и обобщающие известное тождество Мак-Вильямс для весовых функций дуальных блочных кодов над конечными полями;
5. доказана на основе использования нового понятия циклотомически приведенного полинома над конечным полем приведенная оценка Вейля для модуля суммы аддитивных характеров конечного поля, используемая при оценке эффективности методов обращения групповых функций;
6. впервые для Фурье-кластеризации булевых функций на гиперсфере евклидова пространства с использованием понятия линейного транслятора булевой функции описан класс пустых секций этой кластеризации;
7. впервые исследованы алгебраические свойства класса невырожденных булевых функций и доказано, что любая булева функция RM-эквивалентна некоторой невырожденной булевой форме;
8. получены новые свойства обобщенной лавинной характеристики для пар булевых функций;
9. впервые для изучения наследования спектральных и комбинаторных свойств булевых фукнкций их подфункциями введено понятие стабильности, определяемое аффинным подпространством, доказан критерий стабильности, разработан алгоритм для построения семейства аффинных подпространств, относительно которых данная булева функция является стабильной, а также с использованием свойства стабильности доказан новый критерий корреляционной иммунности булевых функций;
10. для уровня аффинности булевой функции-минимального числа переменных, фиксация которых переводит исходную функцию в аффинную функцию, и обобщенного уровня аффинности-минимальной

возможной коразмерности локальных аффинностей функции доказаны асимптотические верхние оценки, выполняющиеся для почти всех булевых функций;

11. впервые предложена аффинная нормальная форма (АффНФ) булевой функции, определяемой относительно разбиения пространства Хэмминга на ее локальные аффинности, получен общий вид спектрального коэффициента Уолша-Адамара булевой функции, использующий параметры ее АффНФ, описан новый класс бент-функций, разработан новый метод решения систем булевых уравнений, использующий особенности аффинных нормальных форм уравнений;
12. для булевых платовидных функций доказана верхняя граница размерностей их локальных аффинностей, определяемая числом переменных и порядками платовидности функций;
13. впервые предложена и обоснована теоретико-автоматная модель частичного обращения дискретных функций, реализуемых конечными автоматами, для функций, реализуемых автоматами без потери информации, разработан метод их частичного обращения и расчитаны его параметры;
14. впервые предложена и обоснована теоретико-автоматная модель локального обращения дискретных функций, реализуемых конечными автоматами, доказано, что приведенный автомат без потери информации обладаетсвойством локальной обратимости тогда и только тогда, когда ассоциированный с ним автомат без выхода синхронизуем, описаны новые классы двоичных неавтономных регистров сдвига с фильтрующими булевыми функциями, обладающие свойством локальной обратимости;
15. разработан метод синтеза совершенно уравновешенных функций над конечным алфавитом, не являющихся перестановочными по крайним переменным, доказан критерий совершенной уравновешенности сдвиг - композиции пары булевых функций;
16. доказан новый теоретико-информационный критерий совершенной уравновешенности функции над конечным алфавитом.

Достоверность результатов исследования гарантируется следующими факторами:

- все результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами;
- установлено, что все результаты диссертации являются новыми, а результаты других авторов, упомянутые в диссертации, отмечены соответствующими ссылками;
- результаты диссертации прошли апробацию на всероссийских и международных конференциях и семинарах.

При решении задач, представленных в диссертации, автором были разработаны: метод частичного обращения конечных автоматов без потери информации, метод локального обращения конечных автоматов без потери информации, метод решения систем булевых уравнений, использующий

особенности аффинных нормальных форм уравнений, метод синтеза совершенно уравновешенных функций над конечным алфавитом, не являющихся перестановочными по крайним переменным.

На заседании 25 декабря 2019 года диссертационный совет принял решение присудить Логачеву О.А. ученую степень доктора физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве __22__ человек, из них _5__ докторов наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность, участвовавших в заседании, из __29__ человек, входящих в состав совета, проголосовали: за __22__, против __0__, недействительных бюллетеней __0__.

Зам. председателя
диссертационного совета,
доктор физико-математических наук,
профессор Васенин Валерий Александрович

Учёный секретарь
диссертационного совета, кандидат
физико-математических наук Кривчиков Максим Александрович

25 декабря 2019 года