Заключение диссертационного совета МГУ.012.3
по диссертации на соискание ученой степени кандидата наук

Решение диссертационного совета от «18» декабря 2024 г. №14
о присуждении Карелиной Екатерине Константиновне, гражданке РФ,
ученой степени кандидата физико-математических наук.

Диссертация «Методы синтеза корреляционно-иммунных функций на основе минимальных функций» по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность принята к защите диссертационным советом 30.10.2024, протокол № 12.

Соискатель **Карелина Екатерина Константиновна**, 1993 года рождения, в 2015 году с отличием окончила специалитет факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова на кафедре информационной безопасности. В 2019 году окончила очную аспирантуру факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова по направлению «Информационная безопасность».

Соискатель работает в должности математика на кафедре информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова.

Диссертация выполнена на кафедре информационной безопасности факультета вычислительной математики и кибернетики ФГБОУ ВО «МГУ имени М.В. Ломоносова».

Научный руководитель — Логачев Олег Алексеевич, доктор физико-математических наук, доцент, доцент кафедры информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Официальные оппоненты:

- **Селезнева Светлана Николаевна** – доктор физико-математических наук, доцент, профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова;
- **Таранников Юрий Валерьевич** – доктор физико-математических наук, доцент кафедры дискретной математики механико-математического факультета Московского государственного университета имени М.В. Ломоносова;

- **Алиев Физули Камилович** – доктор физико-математических наук, доцент, консультант Департамента информационных систем Министерства обороны Российской Федерации;

дали положительные отзывы на диссертацию.

Соискатель имеет 5 опубликованных работ, в том числе 5 публикаций по теме диссертации, 4 из которых опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Результат диссертационной работы опубликованы в открытой печати.

Основные публикации по теме диссертации:

1. Алексеев Е. К., Карелина Е. К. Классификация корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций от 4 и 5 переменных // Дискретная математика. — 2015. — Т.27, №1. — С.22-33. DOI: https://doi.org/10.4213/dm1312 (1.39 п.л. / авторский вклад - 1.39 п.л. Входит в перечень ВАК РФ, RSCI, ИФ РИНЦ: 0,220). \ Соавтор верифицировал полученные результаты.\

   Перевод:

   Alekseev E. K., Karelina E. K. Classification of correlation-immune and minimal correlation-immune Boolean functions of 4 and 5 variables // Discrete Mathematics and Applications. — 2015. — Т.25, №4. — С.193-202. DOI: https://doi.org/10.1515/dma-2015-0019 (1.04 п.л. / авторский вклад - 1.04 п.л. Web of Science, Scopus, SJR — 0.177).
2. Alekseev E. K., Karelina E. K., Logachev O. A. On construction of correlation-immune functions via minimal functions // Математические вопросы криптографии. — 2018 — Т.9, №2. — С. 7-22 DOI: https://doi.org/10.4213/mvk251 (1.85 п.л. / авторский вклад - 0.45 п.л. Входит в перечень ВАК РФ, RSCI, ИФ РИНЦ: 0,143). Работа опубликована в открытой печати. \ Соавторам принадлежит формулирование метода построения CI-функций, основанного на переборе CI-функций в некотором подпространстве. Базис для этого пространства может быть построен с помощью метода, предложенного автором настоящей диссертации (раздел 4.1 по тексту статьи). Карелиной Е.К. получены практические результаты использования метода, предложенного соавторами (раздел 6 по тексту).
3. Карелина Е. К. Об одном методе синтеза корреляционно-иммунных булевых функций // Дискретная математика. — 2018. — Т.30, №4. — С.12-28. DOI: https://doi.org/10.4213/dm1524 (1.96 п.л. Входит в перечень ВАК РФ, RSCI, ИФ РИНЦ: 0,220).

Перевод:

Karelina E. K. On a method of synthesis of correlation-immune Boolean functions // Discrete Mathematics and Applications. — 2020. — Т.30, №2. — С.79-91. DOI: https://doi.org/10.1515/dma-2020-0008 (1.39 п.л. Web of Science, Scopus, SJR — 0.177).

4. Карелина Е. К. Мощностные оценки множества корреляционно-иммунных булевых функций // Дискретная математика. — 2021. — Т.33, №1. — С.12-19 DOI: https://doi.org/10.4213/dm1628 (0.92 п.л. Входит в перечень ВАК РФ, RSCI, ИФ РИНЦ: 0,220).

   Перевод:

   Karelina E. K. Some cardinality estimates for the set of correlation-immune Boolean functions // Discrete Mathematics and Applications. — 2022. — Т.32, №2. — С. 91-96. DOI: https://doi.org/10.1515/dma-2022-0008 (0.58 п.л. Web of Science, Scopus, SJR — 0.177).

На автореферат диссертации поступило 2 **дополнительных отзыва, оба положительные**.

Выбор официальных оппонентов обоснован их высокой профессиональной квалификацией, наличием научных публикаций по направлениям, тесно связанным с темой диссертации автора, а также их соответствием критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

Диссертационный совет отмечает, что **представленная диссертация** на соискание учёной степени кандидата физико-математических наук **является научно-квалификационной работой**, в которой на основании выполненных автором исследований содержатся решения актуальных задач построения CI-функций от большого числа переменных, получения мощностных оценок множеств CI-функций, а также исследования свойств минимальных CI-функций.

Диссертация представляет собой **самостоятельное законченное исследование, обладающее внутренним единством**. Положения, выносимые на защиту, содержат новые научные результаты и свидетельствуют **о личном вкладе автора** в науку:

1. Метод построения CI-функций и минимальных CI-функций, основанный на комбинации рекурсивного и переборного методов, в основе которого лежит введенное в работе отображение для наращивания числа переменных. Данный метод использует известные CI-функции и минимальные CI-функции от малого числа переменных и позволяет строить CI-функции и минимальные CI-функции соответственно уже от большего числа переменных.

2. Классификация относительно группы Джевонса минимальных CI-функций от 4, 5, 6 переменных.
3. Построение устойчивых функций от 7, 8, 9, 10, 11 переменных с помощью предложенного метода.
4. Оценка мощности множеств CI-функций и минимальных CI-функций, получаемых с помощью данного метода.
5. Доказательство верхней оценки веса минимальных CI-функций. Доказательство, что минимальные CI-функции существенно зависят от всех своих переменных. Формулировка и доказательство критерия минимальности и достаточного условия существования минимальных CI-функций.
6. Доказательство асимптотической оценки мощности множества CI(n, w) – множества корреляционно-иммунных функций от n переменных веса w. Доказательство асимптотической оценки мощности множества BCI(n, w) – множества корреляционно-иммунных функций от n переменных веса w, в таблицах истинности которых нет взаимообратных наборов. Доказательство верхней оценки мощности множества CI(n, w).

В рамках исследований применялся математический аппарат алгебры, теории булевых функций и комбинаторики, а также вычислительная техника для построения CI-функций и их классификаций. Все результаты являются чётко сформулированными, а их достоверность обеспечивается строгими математическими доказательствами.

Все результаты диссертации являются новыми. Результаты других авторов, упомянутые в диссертации, отмечены соответствующими ссылками. Результаты диссертации прошли апробацию на конференциях и научно-исследовательских семинарах. Основные результаты опубликованы в научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Сформулированные в диссертации положения доказаны автором самостоятельно, **они теоретически и практически значимы, являются существенным продвижением в решении важной в теоретическом плане и практическом отношении проблемы** синтеза CI-функций от большого числа переменных.

На заседании 18 декабря 2024 года диссертационный совет принял решение присудить Карелиной Е.К. ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 4 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за - 19, против - 0, недействительных бюллетеней - 0.

Заместитель председателя
диссертационного совета МГУ.012.3,
доктор физико-математических наук, профессор В.А. Васенин

Ученый секретарь
диссертационного совета МГУ.012.3,
кандидат физико-математических наук А.В. Галатенко

«18» декабря 2024 г.