Сведения об официальных оппонентах
по диссертации *Карелиной Екатерины Константиновны*
«*Методы синтеза корреляционно-иммунных функций на основе минимальных функций***»**

1. Ф.И.О.: Селезнева Светлана Николаевна
Ученая степень: доктор физико-математических наук
Ученое звание: доцент
Научная специальность: 01.01.09 – «Дискретная математика и математическая кибернетика»
Должность: профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова
Место работы: кафедра математической кибернетики факультета вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова»
Адрес места работы: 119991, Москва, ГСП-1, Ленинские горы, МГУ имени М.В. Ломоносова, 2-й учебный корпус
Тел.: +7 (495) 939-53-92
E-mail: selezn@cs.msu.ru

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет:

1. Селезнева С.Н. «О проверке мультиаффинности многочленов над конечным полем», Дискретная математика. 2023. Т. 35, № 2. С. 109-124. DOI:10.4213/dm1743
   Перевод: Selezneva S.N. Deciding multiaffinity of polynomials over a finite field, Discrete Mathematics and Applications. 2024. V.34, N 4. P. 233-244. DOI: 10.1515/dma-2024-0020
2. Селезнева С.Н. «О сложности поиска периодов функций, заданных многочленами над конечным простым полем», Дискретный анализ и исследование операций. 2022. Т. 29, № 1. С. 56–73. DOI: 10.33048/daio.2022.29.727
   Перевод: Selezneva S.N. On complexity of search for the periods of functions given by polynomials over a prime field, Journal of Applied and Industrial Mathematics. 2022. V. 16, N 1. P. 136–147. DOI: 10.1134/S1990478922010136
3. Селезнева С.Н. «О проверке мультиаффинности функций алгебры логики по их многочленам Жегалкина», Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2022. № 1. С. 42–49.
   Перевод: Selezneva S.N. Multiaffinity testing of Boolean functions using their Zhegalkin polynomials // Moscow University Computational Mathematics and Cybernetics. V. 46, N 1. P. 42–49. DOI: 10.3103/S027864192201006X

4. Селезнева С.Н. «О поиске периодов многочленов Жегалкина», Дискретная математика. 2021. Т. 33, № 3. С. 107–120. DOI: 10.4213/dm1658
   Перевод: Selezneva S.N. Finding periods of Zhegalkin polynomials // Discrete Mathematics and Applications. 2022. V. 32, N 3. P.129–138. DOI: 10.1515/dma-2022-0012
5. Селезнева С.Н. «О мультиаффинных многочленах над конечным полем», Дискретная математика. 2020. Т. 32, № 3. С. 85–97. DOI: 10.4213/dm1608
   Перевод: Selezneva S.N. Multiaffine polynomials over a finite field // Discrete Mathematics and Applications. 2021. V. 31, N 6. P. 421–430. DOI: 10.1515/dma-2021-0038

2. Ф.И.О.: Таранников Юрий Валерьевич
Ученая степень: доктор физико-математических наук
Ученое звание:
Научная специальность: 2.3.6 – «Методы и системы защиты информации, информационная безопасность»
Должность: доцент кафедры дискретной математики механико-математического факультета МГУ имени М. В. Ломоносова
Место работы: кафедра дискретной математики механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова»
Адрес места работы: 119991, ГСП-1, Москва, Ленинские горы, МГУ, д.1, Главное здание, механико-математический факультет
Тел.: +7 (495) 939-42-68
E-mail: yutarann@gmail.com

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет:

1. Баксова И.П., Таранников Ю.В., «Об одной конструкции бент-функций», Обозрение прикладной и промышленной математики, 27:1(2020), 64-66
2. Потапов В. Н., Тараненко А. А., Таранников Ю. В., «An asymptotic lower bound on the number of bent functions», Designs, Codes, and Cryptography, 92:3 (2024), 639-651
3. Баксова И.П., Таранников Ю.В., «Оценки числа разбиений векторного пространства над конечным полем на аффинные подпространства одинаковой размерности», Прикладная дискретная математика. Приложение, 16 (2023), 5-8
4. Tarannikov Yu V., « On the existence of Agievich-primitive partitions», Journal of Applied and Industrial Mathematics, 16:4 (2022), 809-820

3. Ф.И.О.: Алиев Физули Камилович
Ученая степень: доктор физико-математических наук
Ученое звание: доцент
Научная(ые) специальность(и): 5.13.19 – «Методы и системы защиты информации, информационная безопасность»
Должность: консультант Департамента информационных систем Министерства обороны Российской Федерации
Место работы: Министерство обороны Российской Федерации
Адрес места работы: 119160, г. Москва, ул. Знаменка, д. 19
E-mail: alievfk@mail.ru

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет:

1. Алиев Ф.К., Баранов А.П., Ивахин А.В., Корольков А.В., Рудской В.И, «Теоретические основы создания квантового фотонного вычислителя», Системы высокой доступности, 20:2(2024), 5-27
2. Алиев Ф.К., Баранов А.П., Ивахин А.В., Корольков А.В., Рудской В.И, «Математические основы применения квантовой фотонной компьютерной технологии решения сложных вычислительных задач систем высокой доступности», Системы высокой доступности, 19:1(2023), 14-27
3. Алиев Ф. К., Корольков А. В., Матвеев Е. А., «Класс квантовых криптографических систем АКМ2021 на основе использования синглетных состояний многокубитовых квантовых систем», Системы высокой доступности, 18:3 (2022), 5-22
4. Алиев Ф. К., Букин Е. Г., Корольков А. В., Матвеев Е. А., «Квантовая фотонная компьютерная технология решения сложных вычислительных задач систем высокой доступности», Системы высокой доступности, 17:4 (2021), 34-54
5. Алиев Ф. К., Корольков А. В., Матвеев Е. А., Шеремет И. А., «О чувствительности гаммы квантовой криптографической системы АКМ2017 к изменениям сеансового ключа», Программная инженерия, 12:4 (2021), 179-188

Ученый секретарь
диссертационного совета МГУ.012.3,
А. В. Галатенко