Сведения об официальных оппонентах
по диссертации *Давыдова Степана Андреевича*
«*Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах***»**

1. Ф.И.О.: Фомичёв Владимир Михайлович
Ученая степень: доктор физико-математических наук
Ученое звание: профессор
Научная(ые) специальность(и): 05.13.19. Методы и системы защиты информации, информационная безопасность
Место работы: Российский университет дружбы народов имени Патриса Лумумбы
Должность: профессор кафедры теории вероятностей и кибербезопасности Института компьютерных наук и телекоммуникаций факультета физико-математических и естественных наук Российского университета дружбы народов имени Патриса Лумумбы
Адрес места работы: 117198, Москва, ул. Миклухо-Маклая, 6.
Тел.: +7(495)955-0999 (доб. 3999)
E-mail: fomichev_vm@rudn.ru

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет: *(указывается от 3 до 5)*

1. В. М. Фомичёв, “О сложности метода последовательного опробования”, *Дискретный анализ и исследование операций*, 31:2 (2024), 144–154; *Journal of Applied and Industrial Mathematics*, 18:2 (2024), 227–233.
2. Fomichev, V. Estimation of the maximum order of substitutions. *Journal of Computer Virology and Hacking Techniques*, 21:13 (2025).
3. В. М. Фомичёв, В. М. Бобров, “О ⟨2⟩-экспонентах орграфов нелинейности регистровых преобразований”, *Прикладная дискретная математика*, 2022, № 55, 77–87.
4. В. М. Фомичёв, “О степени нелинейности координатных полиномов произведения преобразований двоичного векторного пространства”, *Дискретный анализ и исследование операций*, 28:2 (2021), 74–91; *Journal of Applied and Industrial Mathematics*, 15:2 (2021), 212–222.
5. В. М. Фомичёв, “О наибольшем порядке подстановок заданной степени”, *Прикладная дискретная математика. Приложение*, 2021, № 14, 32–36.

2. Ф.И.О.: Камловский Олег Витальевич
Ученая степень: доктор физико-математических наук
Ученое звание: доцент
Научная(ые) специальность(и): 6.4.4. Теоретическая криптография
Место работы: МИРЭА — Российский технологический университет
Должность: профессор кафедры 252 Института искусственного интеллекта МИРЭА — Российского технологического университета
Адрес места работы: 119454, г. Москва, проспект Вернадского, д. 78
Второе место работы: Московский технический университет связи и информатики

Должность: профессор кафедры теория вероятностей и прикладной математики Московского технического университета связи и информатики
Адрес места работы: 111024, ул. Авиамоторная, д. 8а
Тел.: +7 (495) 957-77-31
E-mail: o.v.kamlovskij@mtuci.ru

Третье место работы: Академия криптографии Российской Федерации
Должность: главный научный сотрудник Академии криптографии Российской Федерации
Адрес места работы: 119331, г. Москва, а/я 100

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет: *(указывается от 3 до 5)*

1. Камловский О.В., Мизеров В.В. Распределение элементов в последовательностях, вырабатываемых алгоритмом поточного шифрования GEA-1 // *Математические вопросы криптографии*, 2024. - № 3 – С. 67-82.
2. Камловский О.В., Бугров А.Д. Свойства классов булевых функций, построенных из нескольких линейных рекуррент над кольцом Z_{2^n} // *Математические вопросы криптографии*, 2024. - № 4 – С. 9-22.
3. Камловский О.В., Панков К.Н. Класс дискретных функций, построенных по нескольким линейным рекуррентам над примарным кольцом вычетов // *Дискретная математика*, 2025. - № 1 – С. 9-21.
4. Камловский О.В., Пензяков Р.В. Оценки линейных характеристик некоторых классов функций над кольцами Галуа // *Дискретная математика*, 2025. - № 3 – С. 77-93.

3. Ф.И.О.: Таранников Юрий Валерьевич
Ученая степень: доктор физико-математических наук
Ученое звание:
Научная(ые) специальность(и): 2.3.6. Методы и системы защиты информации, информационная безопасность
Место работы: кафедра дискретной математики механико-математического факультета Московского государственного университета имени М. В. Ломоносова
Должность: профессор кафедры дискретной математики механико-математического факультета Московского государственного университета 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

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

1. Ю. В. Таранников, «О числе разбиений гиперкуба $(Z_q)^n$ на большие подкубы», *Сибирские электронные математические известия*, 21:2 (2024), 1503–1521.
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. Ю. В. Таранников, “О существовании разбиений, примитивных по Агиевичу”, *Дискретный анализ и исследование операций*, 29:4 (2022), 104–123; *Journal of Applied and Industrial Mathematics*, 16:4 (2022), 809–820.
5. Баксова И.П., Таранников Ю.В., «Оценки числа разбиений пространства $(F_2)^m$ на аффинные подпространства размерности k», *Вестник Московского университета. Серия 1: Математика. Механика*, № 3 (2022), 21-25.

Ученый секретарь
диссертационного совета МГУ.012.3-1,
А.В. Галатенко

_____
Подпись, печать