

Сведения об оппоненте

по диссертационной работе **Лелюка Евгения Андреевича**
на тему «Синтез постквантовой схемы инкапсуляции сеансового ключа»,
представленной на соискание ученой степени кандидата технических наук
по специальности 2.3.6 – «Методы и системы защиты информации, информационная
безопасность», технические науки

Фамилия, имя, отчество оппонента	Малыгина Екатерина Сергеевна
Гражданство	Российская Федерация
Ученая степень и отрасль науки	Кандидат физико-математических наук
Шифр и наименование специальностей, по которым защищена диссертация	01.01.06 «Математическая логика, алгебра и теория чисел»
Ученое звание	–
Полное наименование организации, являющейся основным местом работы оппонента	Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики», г. Москва
Занимаемая должность	Доцент департамента «Прикладная математика»
Почтовый индекс, адрес организации	123458, г. Москва, ул. Таллинская, 34, НИУ ВШЭ, МИЭМ
Телефон	+7 (495) 916-88-29
Адрес электронной почты, веб- сайт	miem@hse.ru https://miem.hse.ru
Список основных публикаций официального оппонента, соответствующих научной специальности диссертации, в ведущих рецензируемых научных изданиях за последние 5 лет (от 5 до 15 публикаций)	
1. Современные парадигмы построения схем цифровой подписи на решётках / А. Г. Леевик, Е. С. Малыгина, Е. М. Мельничук, Д. А. Набоков // Прикладная дискретная математика. – 2025. – № 67. – С. 36-69. – DOI 10.17223/20710410/67/2. (ВАК, К1, RSCI)	
2. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на изогениях и кодах, исправляющих ошибки / Е. С. Малыгина, А. В. Куценко, С. А. Новоселов, Н. С. Колесников, А. О. Бахарев, И. С. Хильчук, А. С. Шапоренко, Н. Н. Токарева // Дискретный анализ и исследование операций. – 2024. – Т. 31, № 1(159). – С. 52-84. – DOI 10.33048/daio.2024.31.772. (Post-Quantum Cryptosystems: Open Problems and Current Solutions. Isogeny-Based and Code-Based Cryptosystems / E. S. Malygina, A. V. Kutsenko, S. A. Novoselov, N. S. Kolesnikov, A. O. Bakharev, I. S. Khilchuk, A. S. Shaporenko, N. N. Tokareva // Journal of Applied and Industrial Mathematics. – 2024. – Vol. 18, No. 1. – P. 103-121. – DOI 10.1134/S1990478924010101) (Scopus, Q3, RSCI)	
3. Кунинец, А. А. Вычисление пар, исправляющих ошибок для алгеброгеометрического кода / А. А. Кунинец, Е. С. Малыгина // Прикладная дискретная математика. – 2024. – № 63. – С. 65-90. – DOI 10.17223/20710410/63/4. (ВАК, К1, RSCI)	
4. Кунинец, А. А. Построение квазициклических альтернативных кодов и их приложение в кодовых криптосистемах / А. А. Кунинец, Е. С. Малыгина // Прикладная дискретная математика. – 2024. – № 65. – С. 84-109. – DOI 10.17223/20710410/65/5. (ВАК, К1, RSCI)	
5. Kirshanova, E. Construction-D lattice from Garcia–Stichtenoth tower code / E. Kirshanova, E. Malygina // Designs, Codes and Cryptography. – 2023. – DOI 10.1007/s10623-023-01333-2. (Scopus, Q1)	
6. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на решётках / Е. С. Малыгина, А. В. Куценко, С. А. Новоселов, Н. С. Колесников, А. О. Бахарев, И. С. Хильчук, А. С. Шапоренко, Н. Н. Токарева // Дискретный анализ и исследование операций. – 2023. – Т. 30, № 4(158). – С. 46-90. – DOI	

- 10.33048/daio.2023.30.771. (Post-Quantum Cryptosystems: Open Problems and Solutions. Lattice-Based Cryptosystems / E. S. Malygina, A. V. Kutsenko, S. A. Novoselov, N. S. Kolesnikov, A. O. Bakharev, I. S. Khilchuk, A. S. Shaporenko, N. N. Tokareva // Journal of Applied and Industrial Mathematics. – 2023. – Vol. 17, No. 4. – P. 767-790. – DOI 10.1134/s1990478923040087.) (Scopus, Q3, RSCI)
7. Mathematical problems and solutions of the Ninth International Olympiad in Cryptography NSUCRYPTO / V. A. Idrisova, N. N. Tokareva, A. A. Gorodilova, I. I. Beterov, T. A. Bonich, E. A. Ishchukova, N. A. Kolomeec, A. V. Kutsenko, E. S. Malygina, I. A. Pankratova, M. A. Pudovkina, A. N. Udovenko // Applied Discrete Mathematics. – 2023. – No. 62. – P. 29-54. – DOI 10.17223/20710410/62/4. (BAK, K1, RSCI)
8. Алгеброгеометрические коды и декодирование на основе пар, исправляющих ошибки / Е. С. Малыгина, А. А. Кунинец, В. Л. Раточка, А. Г. Дупленко, Д. Я. Нейман // Прикладная дискретная математика. – 2023. – № 62. – С. 83-105. – DOI 10.17223/20710410/62/7. (BAK, K1, RSCI)
9. An overview of the eight International Olympiad in cryptography “non-Stop university CRYPTO” / A. A. Gorodilova, N. N. Tokareva, S. V. Agievich, I. I. Beterov, T. Beyne, L. Budaghyan, C. Carlet, V. A. Idrisova, S. Dhooghe, N. A. Kolomeec, A. V. Kutsenko, E. S. Malygina, N. Mouha, M. A. Pudovkina, F. Sica, A. N. Udovenko // Siberian Electronic Mathematical Reports. – 2022. – Vol. 19, No. 1. – P. 412-440. – DOI 10.33048/semi.2022.19.023. (Scopus, Q3)
10. Малыгина, Е. С. Исследование группы автоморфизмов кода, ассоциированного с оптимальной кривой рода три / Е. С. Малыгина // Прикладная дискретная математика. – 2022. – № 56. – С. 5-16. – DOI 10.17223/20710410/56/1. (BAK, K1, RSCI)
11. Малыгина, Е. С. Анализ минимального расстояния АГ-кода, ассоциированного с максимальной кривой рода три / Е. С. Малыгина, А. А. Кунинец // Прикладная дискретная математика. – 2022. – № 58. – С. 5-14. – DOI 10.17223/20710410/58/1. (BAK, K1, RSCI)
12. Алгоритм вычисления идеала Штикельбергера для мультикватратичных полей / Е. А. Кирианова, Е. С. Малыгина, С. А. Новоселов, Д. О. Олефиренко // Прикладная дискретная математика. – 2021. – № 51. – С. 9-30. – DOI 10.17223/20710410/51/1. (BAK, K1, RSCI)

Официальный оппонент: кандидат физико-математических наук,
доцент департамента «Прикладная математика»,

Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет «Высшая школа экономики», г. Москва

кандидат физико-математических наук



Е. С. Малыгина

Согласен на обработку персональных данных
кандидат физико-математических наук



Е. С. Малыгина

Подпись Е. С. Малыгиной заверяю.



Подпись заверяю
СПЕЦИАЛИСТ ПО КАДРОВОМУ ДЕЛОПРОИЗВОДСТВУ
ЦЕНТРА ПО КАДРОВОМУ АДМИНИСТРИРОВАНИЮ
УПРАВЛЕНИЯ ПЕРСОНАЛА
Е. Ю. САРКИСОВА

