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

Решение диссертационного совета от «26» ноября 2025 г. № 24 о присуждении Высоцкой Виктории Владимировне, гражданке Российской Федерации, ученой степени кандидата физико-математических наук.

Диссертация «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки» по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность принята к защите диссертационным советом «24» сентября 2025 г., протокол № 20.

Соискатель **Высоцкая Виктория Владимировна**, 1995 года рождения, в 2022 году окончила очную аспирантуру факультета Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова по направлению 10.06.01 «Информационная безопасность».

Соискатель работает в должности математика на кафедре информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Диссертация выполнена на кафедре информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Научный руководитель - Чижов Иван Владимирович, кандидат физико-математических наук, доцент кафедры информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Официальные оппоненты:

- **Вороненко Андрей Анатольевич**, доктор физико-математических наук, профессор, профессор кафедры математической кибернетики факультета Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова;
- **Кабатянский Григорий Анатольевич**, доктор физико-математических наук, вице-президент по науке и академическому сотрудничеству Сколковского института науки и технологий;
- **Гашков Сергей Борисович**, доктор физико-математических наук, профессор, профессор кафедры дискретной математики механико-математического факультета МГУ имени М.В. Ломоносова;

дали положительные отзывы на диссертацию.

Выбор официальных оппонентов обосновывался тем, что оппоненты являются известными специалистами по кодовым криптосистемам и алгебраической теории кодирования и имеют работы, близкие к теме диссертационного исследования, в центральных математических журналах.

Соискатель имеет 11 опубликованных работ, в том числе по теме диссертации 5 работ, из них 4 работы 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). Результаты диссертационной работы опубликованы в открытой печати.

Основные публикации по теме диссертации:

1. Vysotskaya V. «Characteristics of Hadamard Square of Special Reed – Muller Subcodes» // Прикладная дискретная математика. 2021. № 53. С. 75-88. (Scopus, RSCI, импакт-фактор 0.11 (JCI), 0.88 п.л.). EDN: TEDEFN.

2. Высоцкая В. В., Высоцкий Л. И. «Обратимые матрицы над некоторыми факторкольцами: идентификация, построение и анализ» // Дискретная математика. 2021. Т. 33. № 2. С. 46-65 (RSCI, импакт-фактор 0.39 (РИНЦ), 1.25 п.л.). EDN: VASNIG.
Соавтору принадлежит алгоритм приведения матрицы над факторкольцом кольца многочленов к верхнетреугольному виду (Алгоритм 1 по тексту статьи), остальные результаты статьи получены Высоцкой В. В. (1.06 п.л., 90%).
На англ. языке: Vysotskaya V., Vysotsky L. «Invertible matrices over some quotient rings: identification, generation, and analysis» // Discrete Mathematics and Applications. 2022. 32(4). pp. 263-278 (Scopus, WoS, импакт-фактор 0.22 (JCI), 1 п.л., вклад автора 90%, 0.94 п.л.). EDN: EDHYGI.

3. Высоцкая В. В. «О структурных особенностях пространства ключей криптосистемы Мак-Элиса – Сидельникова на обобщенных кодах Рида – Соломона» // Дискретная математика. 2024. Т. 36. № 4. С. 28-43 (RSCI, импакт-фактор 0.39 (РИНЦ), 1 п.л.). EDN: IBRMIU.

4. Vysotskaya V., Chizhov I. «The security of the code-based signature scheme based on the Stern identification protocol» // Прикладная дискретная

математика. 2022. № 57. С. 67-90 (Scopus, RSCI, импакт-фактор 0.11 (JCI), 1.56 п.л.). EDN: FFRFUH.

Соавтору принадлежит постановка задачи и верификация результатов, остальные результаты статьи получены Высоцкой В. В. (1.56 п.л., 95%).

5. Vysotskaya V. «New estimates for dimension of Reed – Muller subcodes with maximum Hadamard square» // Прикладная дискретная математика. Приложение. 2020. № 13. С. 98-100 (ВАК, импакт-фактор 0.06 (РИНЦ), 0.19 п.л.). EDN: TCYZCI.

Дополнительно поступило 5 отзывов на автореферат диссертации, все положительные.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени кандидата физико-математических наук является научно-квалификационной работой, в которой содержатся следующие результаты: описаны структурные свойства подкодов кода Рида – Маллера RM(r, m), устойчивых к атакам, применимым к исходному коду, получена оценка доли стойких подкодов кода RM(r, m) с ростом параметра m; разработаны эффективные алгоритмы генерации квазициклических невырожденных матриц с равномерным распределением на множестве всех таких невырожденных матриц заданного размера; получена оценка снизу на мощность множества открытых ключей схемы подписи CFS, построенной на основе конструкции В.М. Сидельникова, описана структура классов эквивалентности секретных ключей схемы через группы автоморфизмов линейного кода и его квадрата, выделены три класса ключей схемы подписи на основе обобщенных кодов Рида – Соломона, такие что квадрат кода, задающего открытый ключ, не раскладывается в прямое произведение квадратов базовых кодов; построена схема электронной подписи на основе протокола идентификации Штерна, доказана теорема о стойкости подписи к экзистенциальной подделке при атаке с выбором сообщения (модель EUF-CMA).

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:

- Метод описания структурных свойств подкодов кода Рида – Маллера, схема подписи CFS на которых является стойкой к известному типу атак. Способы построения таких подкодов и метод оценки их доли.
- Два эффективных алгоритма построения невырожденных квазициклических матриц, необходимых для эффективной реализации схемы подписи CFS на квазициклических кодах.
- Метод получения нижней оценки мощности множества открытых ключей схемы подписи CFS, построенной на основе конструкции Сидельникова. Описание структуры множества секретных ключей на кодах общего вида и обобщенных кодах Рида – Соломона, схема подписи на которых подвержена атакам, разделяющим копии кода. Метод построения секретных ключей подписи CFS с использованием обобщенных кодов Рида – Соломона, позволяющий избежать известных атак.
- Схема электронной подписи, стойкость которой не зависит от сложности задач на известном классе кодов. Обоснование стойкости построенной подписи.

В диссертации используются методы теории кодирования, комбинаторной теории вероятностей, теории алгоритмов, теории сложности вычислений и теории графов.

Результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами, являются новыми, прошли апробацию на международных конференциях и научных семинарах. Основные результаты диссертационной работы изложены в 5 работах, 4 из которых опубликованы в научных изданиях, индексируемых в базах данных WoS, Scopus, RSCI и рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

На заседании 26.11.2025 диссертационный совет принял решение присудить Высоцкой В.В. 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 нет.

Заместитель председателя
диссертационного совета,
д.ф.-м.н., профессор **Васенин В.А.**

Ученый секретарь
диссертационного совета,
к.ф.-м.н. **Галатенко А.В.**

Дата 26.11.2025

Печать структурного подразделения МГУ