

ОТЗЫВ

на автореферат диссертации Высоцкой Виктории Владимировны
на тему «Анализ постквантовых схем электронной подписи, построенных на
кодах, исправляющих ошибки»
на соискание учёной степени кандидата физико-математических наук
по специальности 2.3.6. Методы и системы защиты информации,
информационная безопасность

Согласно автореферату, в диссертации Высоцкой В.В. исследуются свойства кодов, исправляющих ошибки, значимые с точки зрения синтеза схем цифровой подписи. Теория кодов, исправляющих ошибки, является одной из областей математики, достижения которых представляются перспективными для использования при построении постквантовых криптографических механизмов. В связи с этим исследование соответствующих свойств кодов представляет актуальнейшую задачу с точки зрения развития математических основ создания новых средств защиты информации. Значительный вклад в решение этой задачи вносит коллектив под руководством Чиждова И.В. Заметное место в этом вкладе занимают результаты диссертационной работы Высоцкой В.В.

Особенностью результатов диссертации является введение автором новых практико-ориентированных математических понятий (например, стабильные и нестабильные подкоды, коды с разложимым и неразложимым квадратом), что приближает науку к решению практических задач в области информационной безопасности. Работа имеет авторитетную публикационную библиографию и хорошую апробацию, что, в свою очередь, даёт основания полагать, что все выносимые на защиту результаты являются новыми и достоверными.

К тексту автореферата можно сделать некоторые замечания, подобные следующим.

1. В тексте автореферата синонимично используются термины «схема электронной подписи», «алгоритм электронной подписи», «схема цифровой подписи», «схема подписи», «электронная подпись», «подпись».

2. В разделе «Общая характеристика работы» некоторые тезисы приводятся в излишне свободной форме, что может допустить их некорректную интерпретацию (например, «задача атакована», «доказательства сводились к сложности», «задачи эквивалентны по сложности, таким образом схемы на них эквивалентны по уровню стойкости», «выросло время алгоритма», «атака на код»). При этом считаю важным отметить, что раздел «Основное содержание работы», где описаны результаты диссертации, лишён данного недостатка.

3. В некоторых случаях утверждается об «эффективности» того или иного алгоритма, при этом оценки его вычислительной сложности не приводятся (хотя в диссертации они есть).

4. Нумерация теорем в тексте автореферата не соответствует оной в тексте диссертации, что усложняет их совместное использование.

Указанные замечания, несомненно, снижают качество автореферата, однако не имеют отношения к результатам диссертации, не снижают их теоретической и практической значимости и не мешают сделать вывод о том, что, судя по автореферату, диссертация Высоцкой В.В. «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки» является научно-квалификационной работой, в которой решается задача, имеющая значение для развития методов и систем защиты информации, а её автор, Высоцкая Виктория Владимировна, заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кяжин Сергей Николаевич
кандидат физико-математических наук,
доцент кафедры криптологии и кибербезопасности
ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ»

(подпись) 21.11.2025
(дата)

Подпись Кяжина С.Н. заверяю: