ОТЗЫВ

на автореферат диссертации Лелюка Евгения Андреевича, выполненной на тему «Синтез постквантовой схемы инкапсуляции сеансового ключа» и представленной на соискание учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертационного исследования не вызывает сомнений в свете современных вызовов, связанных с развитием квантовых вычислений. Угроза применения алгоритма Шора к широко используемым асимметричным криптосистемам делает переход к постквантовой криптографии одной из ключевых задач в области информационной безопасности. Международные инициативы, такие как конкурс NIST PQC, а также активная работа российских технических комитетов, подтверждают высокую значимость исследований в этом направлении. В данном контексте кодовая криптография, и, в частности, развитие схем типа Мак-Элиса, представляет собой один из наиболее перспективных и фундаментально стойких подходов.

Проведенное исследование демонстрирует комплексный подход к решению поставленной задачи. Автором получен ряд весомых теоретических и прикладных результатов, направленных на создание новой кодовой криптосистемы на основе D-кодов. Разработаны алгоритмы гарантированного и вероятностного декодирования, предложен метод анализа стойкости системы с использованием свойств произведения Шура-Адамара, а также синтезирована новая криптографическая схема, демонстрирующая улучшенное соотношение между стойкостью и размером открытого ключа по сравнению с классическими аналогами. Все результаты имеют строгое теоретическое обоснование и подтверждены вычислительными экспериментами.

Теоретическая значимость работы заключается в углубленном изучении свойств D-кодов и разработке новых методов их декодирования, что вносит вклад в теорию кодирования и криптографии. Практическая ценность подтверждается программной реализацией предложенных алгоритмов, а также внедрением результатов в деятельность профильных организаций, что свидетельствует о востребованности и применимости разработки.

Автореферат написан научным языком, выдержанным в соответствии с требованиями к диссертационным работам. Структура документа логична: постановка задачи, анализ существующих решений, изложение

предложенного подхода, описание результатов и заключение. Материал изложен последовательно, с достаточной детализацией, позволяющей оценить научную и практическую значимость работы.

В качестве замечания к работе стоит отметить, что анализ структурной стойкости предложенной криптосистемы в основном сосредоточен на классе атак с использованием произведения Шура-Адамара, недостаточно исследована устойчивость к другим известным структурным атакам.

Данное замечание не влияет на общую положительную оценку автореферата и диссертационной работы.

Диссертация Лелюка Евгения Андреевича «Синтез постквантовой схемы инкапсуляции сеансового ключа» отвечает требованиям, установленным Положением «О присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в действующей редакции) и предъявленным к диссертациям на соискание учёной степени кандидата наук, а автор, Лелюк Евгений Андреевич, заслуживает присвоения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Мкртичян Вячеслав Виталиевич,
кандидат технических наук (специальность 05.13.19 – методы и системы защиты информации, информационная безопасность),
заведующий лабораторией телекоммуникационных технологий,
Федеральное государственное автономное научное учреждение "Научно-исследовательский институт "Специализированные вычислительные устройства защиты и автоматика",
Юридический адрес:344003, г. Ростов-на-Дону, ул. Города Волос, 6,
Почтовый адрес: 344002, г.Ростов-на-Дону, а/я 167,
Тел.: +7(863) 201-28-17,
e-mail: info@niisva.org.

"16" апреля 2026 г. / В. В. Мкртичян /

Подпись В. В. Мкртичяна заверяю

ФГАНУ НИИ «Спецвузавтоматика»
Директор (подпись) Р.А. Хади