Экз. № 1

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 обусловлена глобальным вызовом, связанным с развитием квантовых вычислений. Доказанная уязвимость широко распространенных асимметричных криптосистем, основанных на задачах факторизации и дискретного логарифмирования, перед алгоритмом Шора делает переход к постквантовой криптографии одной из наиболее приоритетных задач в области информационной безопасности. Международные усилия по стандартизации, такие как конкурс NIST PQC, а также национальные инициативы, включая работу российских технических комитетов, подчеркивают высокую востребованность и своевременность исследований в данном направлении. В этом контексте кодовая криптография, и, в частности, развитие схем типа Мак-Элиса, представляет собой один из наиболее перспективных и фундаментально стойких подходов, что и определяет высокую значимость представленной работы.

Представленная работа характеризуется системным решением актуальной научной проблемы. Автором получены существенные результаты, вносящие вклад в развитие кодовой криптографии. Теоретическая значимость исследования подтверждается созданными алгоритмическими моделями и глубоким анализом криптографических свойств исследуемых кодов. Практическая ценность работы демонстрируется подобранными параметрами криптосистемы, обеспечивающими конкурентные характеристики по сравнению с существующими аналогами. Все результаты имеют строгое обоснование и подтверждены соответствующими вычислительными экспериментами и аналитическими выкладками.

Автореферат диссертационного исследования составлен в соответствии с действующими нормативными требованиями. Документ обладает чёткой структурой, включающей все необходимые компоненты. Материал изложен последовательно, с достаточной детализацией, позволяющей оценить научную и практическую значимость работы.

Вместе с тем, в ходе ознакомления с авторефератом можно выделить отдельные аспекты, требующие дополнительного внимания:

1. Основные преимущества предложенной криптосистемы, в частности, сокращение размера открытого ключа, достигаются только для сценария одноразового использования, тогда как при многоразовом использовании система уступает по данному параметру классическим аналогам.
2. В работе заявлено, что теоретико-графовый подход к декодированию может применяться в системах связи для защиты от помех. Однако этот потенциал не раскрыт и не проанализирован.

Отмеченные замечания носят характер пожеланий по дальнейшему развитию исследования и не влияют на положительную оценку автореферата и диссертационной работы.

Диссертационная работа 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.

Сотрудник Академии ФСО России
доктор технических наук, доцент Козачок Александр Васильевич

«21» ноября 2025 г.

Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России)
Тел.: +7(4862) 54-94-99
E-mail: a.kozachok@academ.msk.rsnet.ru
Адрес: Россия, 302015, г. Орел, ул. Приборостроительная, д. 35

Подпись сотрудника Академии ФСО России доктора технических наук, доцента Козачка Александра Васильевича ЗАВЕРЯЮ.

Руководитель кадрового аппарата Академии ФСО России А.Б. Семибратов