

Отзыв

на выпускную квалификационную работу

Воронина Юрия Игоревича

На тему «Система электронной подписи»

Системы цифровой электронной подписи являются основой криптографии с публичным ключом. Используемые в настоящее время на практике системы являются не стойкими по отношению к атакам с помощью квантового компьютера. Хотя квантовый компьютер пока технологически далек от создания, изучение возможностей построения систем цифровой подписи, устойчивых к атакам с помощью квантового компьютера представляет, как теоретический, так и прикладной интерес. Поэтому тема работы Ю.И. Воронина, посвященной изучению систем построения цифровой подписи на основе цифровых решеток, является актуальной.

Перед Ю.И. Ворониным были поставлены следующие задачи:

1. Изучить известные системы цифровой подписи
2. Реализовать систему, основанную на числовой решетке

Ю. И. Воронин успешно решил эти задачи, проявив самостоятельность и инициативность.

Считаю, что выпускная работа Ю.И. Воронина соответствует требованиям, предъявляемым ГАК к выпускным работам, и заслуживает оценки «отлично», а автор работы заслуживает присвоения квалификации «бакалавр» по направлению «Математическое обеспечение и администрирование информационных систем».

Научный рук. работы

д.т.н. профессор



Е.А. Крук