

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
10.05.03 – Информационная безопасность автоматизированных систем

Аннотация рабочей программы
дисциплины «Квантовые вычисления»

Общая трудоемкость дисциплины составляет 3 зач. единиц, 108 часов, форма промежуточной аттестации – зачет с оценкой.

Программой дисциплины предусмотрены следующие виды занятий: лекционные – 18 часов, лабораторные – 36 часов, самостоятельная работа обучающегося составляет 54 часа.

Дисциплина подразумевает изучение следующих основных разделов:

Вычисление как процесс. Виды вычислителей. Особенности квантового вычисления. Принципы построения квантовых вычислителей и квантовых компьютеров.

Понятие кубита, эволюции состояний. Физические основы: парадокс ЭПР, неравенства Белла, квантовый параллелизм и квантовая телепортация.

Квантовые схемы и алгоритмы: понятия квантовой схемы и квантового алгоритма, простейшие квантовые алгоритмы, универсальные квантовые элементы.

Особенности задач, решаемых квантовыми компьютерами. Задача о скрытой подгруппе и ее связь с системами обеспечения информационной безопасности. Открытые вопросы развития криптосистем, связанные с появлением квантовых компьютеров.

Квантовый криптоанализ алгоритма RSA. Алгоритмы факторизации и дискретного логарифмирования: алгоритм Шора и его вариации. Сложность и точность вычислений в алгоритмах факторизации и дискретного логарифмирования.