УДК 519.688

МОДЕРНИЗАЦИЯ КЛАССИЧЕСКОЙ ЧАСТИ КВАНТОВОГО АЛГОРИТМА П.ШОРА

Авторы:

Разумов Павел Владимирович – студент 5-го кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: therazumov@gmail.com

Смирнов Иван Андреевич – студент 5-го кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: terran.doatk@mail.ru

Черкесова Лариса Владимировна – доцент, д.ф.-м.н., и профессор кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: chia2002@inbox.ru

Короченцев Денис Александрович – доцент, к.т.н., и заведующий кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: mytelefon@mail.ru

Поркшеян Виталий Маркосович – доцент, к.ф.-м.н., декан факультета «Информатика и вычислительная техника» Донского государственного технического университета, Ростов-на-Дону, e-mail: spu-40@donstu.ru

Научный руководитель – доцент, д.ф.-м.н., и профессор кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: chia2002@inbox.ru

Введение. В предлагаемой работе рассмотрен и проанализирован квантовый алгоритм факторизации Питера Шора и алгоритм факторизации ρ – метода Джона Полларда. Рассматриваемый квантовый алгоритм состоит из двух частей – классической и квантовой. В классической части, для нахождения наибольшего общего делителя чисел (НОД) предлагается использовать алгоритм Евклида. Но существует большое количество алгоритмов нахождения наибольшего общего делителя чисел.

Цель работы. Как известно, алгоритм Шора имеет квантовую и классическую части, что позволяет увеличить скорость вычисления алгоритма в целом, максимально модернизировав и упростив классическую часть.

Базовые положения исследования. В классической части для нахождения НОД предлагается использовать алгоритм Евклида, но, более того, существует достаточно большое количество алгоритмов нахождения наибольшего общего делителя пары чисел. В качестве исследуемых отобраны восемь наиболее распространенных алгоритмов нахождения НОД и произведена проверка их скорости вычисления на числах разной сложности.

Промежуточные результаты. Наиболее рациональным является выбор алгоритма gcd 8 (бинарный алгоритм итерационный со сдвигом), причиной чему служит то, что он предназначен для решения весьма трудоёмких задач.

Вывод. Результаты исследования показывают преимущество квантовых алгоритмов вычислений перед традиционными не квантовыми алгоритмами, вычислительная мощность которых значительно меньше. Оба рассмотренных алгоритма (стандартный и модифицированный) отличаются своей высокой производительностью. Благодаря усовершенствованию квантового алгоритма Шора, эффективность полученного алгоритма оказалось выше, чем у стандартного алгоритма за счет усовершенствования классической части.