

Разработка методики построения квантовой системы с использованием аппаратных средств оптимизации*

В. С. Потапов, С. М. Гушанский

Южный федеральный университет, г. Таганрог, Россия

Аннотация. В работе разработано и промоделировано аппаратное вычислительное ядро, являющееся основной частью ускорителя на базе программируемых логических интегральных схем с системой автоматизированного проектирования Altera Quartus. С учётом полученной временной зависимости количества тактов, необходимых для воздействия однокубитового квантового вентиля на квантовый регистр от количества кубитов и параллельных арифметико-логических устройств в аппаратном вычислительном ядре при моделировании квантовых вычислений разработана методика определения оценки увеличения производительности аппаратной части и предложены пути повышения производительности ускорителя на основе аппаратного вычислительного ядра на базе программируемых логических интегральных схем. Также выполнен сравнительный анализ методики оптимизации моделирования квантовых вычислений и математического моделирования.

Ключевые слова: квантовый алгоритм, квантовый бит, запутанность, квантовая схема, регистр, гейт, параллелизм, квантовый компьютер.

DOI 10.14357/20718632220103

Введение

В настоящее время активно развивается теория квантовых вычислений [1]. Квантовое вычислительное устройство имеет ряд преимуществ перед классическими компьютерами, главным из которых является квантовый параллелизм вычислительного процесса. Данный квантовый эффект предлагает одновременное вычисление с набором разных исходных данных. Актуальность темы квантовых компьютеров подтверждается тем, что уже сейчас банковские системы, криптография и шифрование

информации, требуют колоссальных ресурсов вычислительных систем, это только некоторые примеры, но наиболее важные и яркие, которые касаются повседневной жизни огромной части населения планеты. На всех этапах развития информационных технологий уделялось и уделяется в настоящее время большое внимание вопросам моделирования функционирующих специализированных высокопроизводительных вычислительных систем, позволяющих обеспечивать необходимые показатели по быстродействию в сочетании с минимизированными затратами программных ресурсов и потребляе-

* Работа выполнена при финансовой поддержке РФФИ, грант №20-07-00916.

мой энергии. Разработанная специализированная вычислительная система позволит наглядно увидеть сильные и слабые стороны разрабатываемого квантового вычислительного устройства, доказать преимущества его использования. Разрабатываемая моделирующая система является наглядным пособием для понимания основных методов взаимодействия информационных процессов и цифровой обработки информации в рамках новых технологий. Ряд важнейших задач не может быть решен с помощью классических вычислительных машин, в том числе, классических суперкомпьютеров, за разумное время. Разработка теоретических основ создания программных систем и конструирование алгоритмов для новых информационных технологий и специализированных вычислительных систем является динамичной областью, о чем свидетельствует количество существующих работ в данном направлении. Разработанные алгоритмы для различных задач классов сложности могут дать существенный выигрыш по эффективности в сравнении с существующими классическими и обеспечить решение ряда сложных математических и криптографических задач. Интерес к квантовым вычислениям возрос после того, как канадская компания D-Wave Systems объявила о продаже первого в мире коммерческого квантового компьютера «Орион» мощностью 16 кубитов. Компания Google создала свою квантовую вычислительную систему для моделирования работы квантовых алгоритмов. Кроме Google из известных частных компаний свои лаборатории по созданию квантового устройства сделали IBM и Microsoft.

1. Математический аппарат квантовых вычислений

Квантовый компьютер [2] – это вычислительное устройство, которое используется для вычисления явлений квантовой механики [3]. Квантовый вычислительный процесс характеризуется наличием особой формой представления данных и информации в целом. Кубит, как квантовая единица и вид информации в квантовой моделирующей системе [4], расширяет понятие классического бита. Главным отличием от классических компьютеров

является то, что квантовые алгоритмы функционируют с величинами вероятностного характера и использующие принципы квантового параллелизма [5], суперпозиции состояний квантовых частиц и квантовую запутанность [6], позволяющую выполнять вычисления на сторонних принципах и производить решение новых классов задач за малое время. Квантовый вычислитель оперирует, как было описано выше, с квантовыми битами, которые имеют два базисных состояния $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ и $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Состояние кубита $|0\rangle$ соответствует состоянию спина электрона в атоме «спин вверх», состояние «спин вниз» соответствует $|1\rangle$, а смешанное состояние (суперпозиция состояний) соответствует промежуточному положению спина. Спин [7] – это собственный момент импульса элементарных частиц, но спин не связан с движением в пространстве, это собственное число квантовой частицы, которое нельзя объяснить с позиции классической механики. В общем случае состояние кубита описывается волновой функцией (или вектором состояния): $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, где α_0 и α_1 – комплексные амплитуды вероятности чтения $|0\rangle$ или $|1\rangle$. Дело в том, что при измерении квантового бита в стандартном базисе с вероятностью $|\alpha|^2$ будет получен $|0\rangle$, а с вероятностью $|\alpha|^2 - |\alpha|^2$ – $|1\rangle$. При этом кубит перейдет в состояние квантового нуля или единицы. Эффект квантового смешанного состояния существует только до момента измерения кубита, то есть при чтении мы приводим кубит в одно из базисных состояний, а в какое именно – зависит от вероятности, полученной при вычислениях. Данное явление представлено графически на Рис. 1.

Один раз, измерив, квантовый бит, мы получим всего один бит информации, несмотря на то, что в состоянии суперпозиции в нем хранится гораздо больше. Операции над кубитами можно отобразить с помощью квантовых схем. Квантовая схема [8] – это последовательность физических преобразований из конечного набора базисных элементарных преобразований –

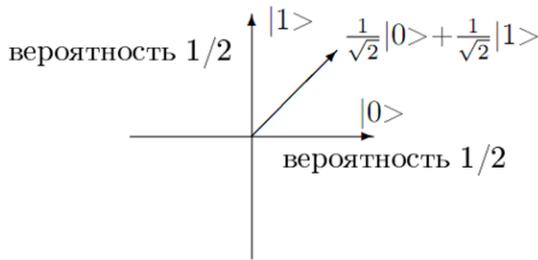


Рис. 1. Состояние кубита и вероятности измерения нуля и единицы

гейтов. На вход квантовой схемы подаются квантовые биты, а на выходе получают ее вероятностный результат работы. Вследствие того, что при измерении квантовых битов они переходят в состояния «0» или «1», то для получения точного результата можно использовать квантовую схему несколько раз для одинаковых входных данных.

Физически можно реализовать только те операции, которые сохраняют постоянной сумму квадратов коэффициентов над небольшой группой кубитов. Исходя из этого, можно заключить, что любое преобразование над k квантовыми битами задается в виде матрицы $2^k \times 2^k$. В общем случае, квантовый регистр описывается как $|\psi\rangle = |\psi_1, \psi_2, \dots, \psi_n\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$, где $\psi_i, i=1\dots n$ волновые функции отдельных кубитов, а n – общее количество кубитов в моделируемой квантовой системе.

2. Методика оптимизации квантового процесса с помощью квантовых гейтов и операций

Рассмотрим методику оптимизации квантового вычислительного процесса (Рис. 2), позволяющую уменьшить трудозатраты на выполнение квантовых вычислений и алгоритмов. Данная методика может быть применена в программных ядрах различных типов, а также в системах, состоящих из нескольких процессоров, для уменьшения количества итераций работы.

Описанная на Рис. 2 матрица состоит из подавляющего количества нулевых элементов, не играющих никакой роли в вычислительном процессе (Рис. 3). Задача методики – это вывод двумерной матрицы, перемножения ее на вектор состояния квантовой вычислительной системы с помощью конкретной последовательности шагов.

Пусть имеем 3 кубита, тогда описанная выше последовательность будет соответствовать приведенной на Рис. 4. Представим последовательность шагов, которая позволит увеличить производительность квантовой системы для операций с кубитами.

Для реализации первых этапов методики необходимо инициализировать начальное квантовое состояние и квантовый регистр. В рамках этого процесса устанавливается амплитуда для начального значения регистра. Затем просчитывается бинарный индекс кубита. Данный тип

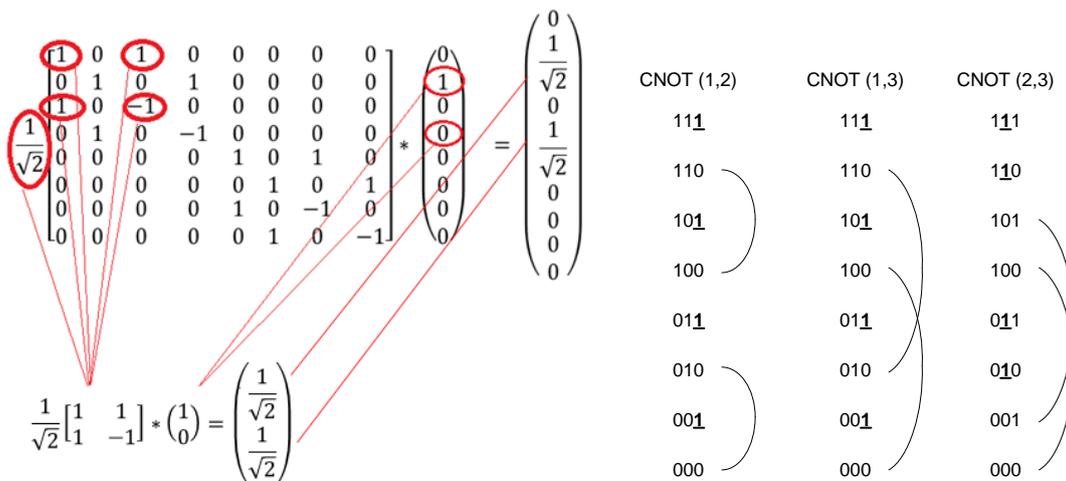


Рис. 2. Методика оптимизации квантового вычислительного процесса. Последовательность изменения состояний в зависимости от контролирующего и контролируемого кубита гейта CNOT

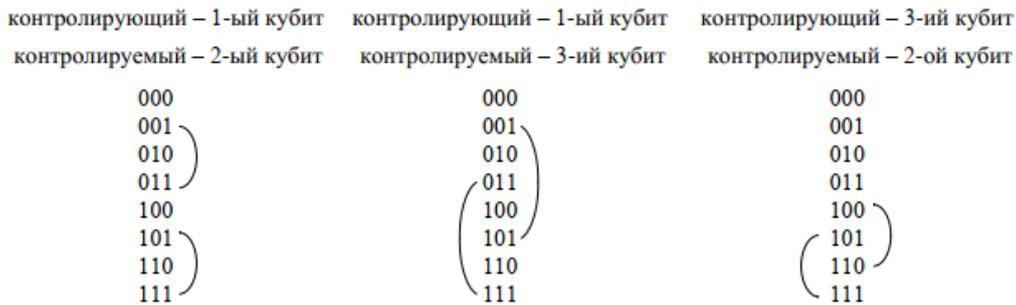


Рис. 3. Пример выборки состояний для двухкубитового универсального контролируемого вентиля

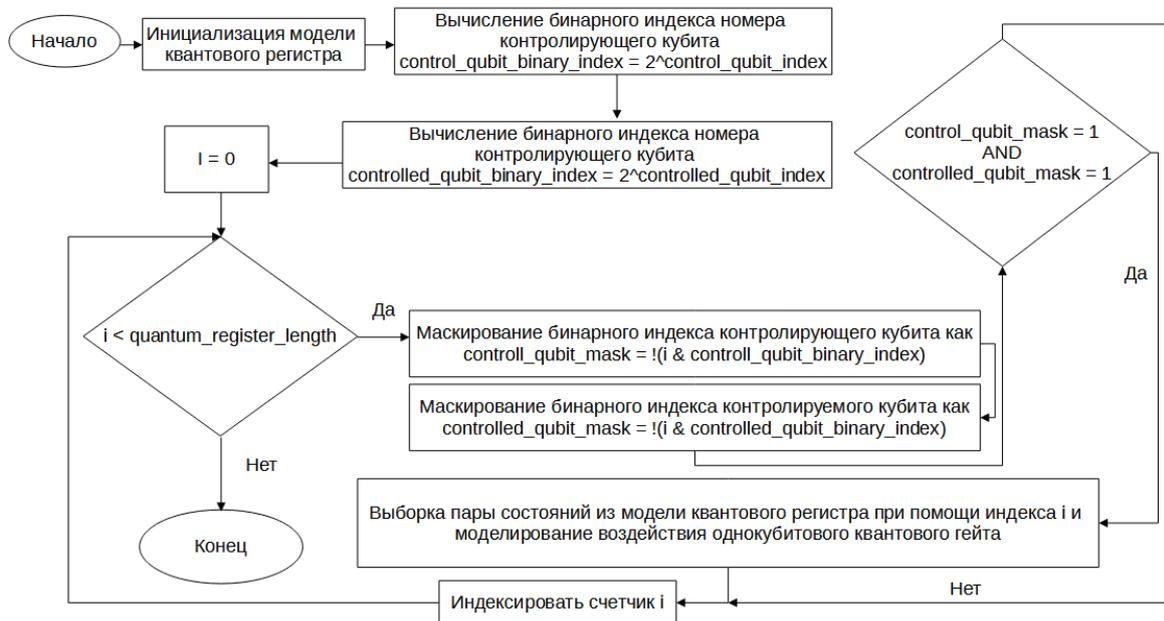


Рис. 4. Блок-схема методики оптимизации квантового вычислительного процесса

индекса в методике отражает числовое значение, в которое устанавливаются единицы в разрядной ячейке, соответствующей порядковому номеру кубита при взаимодействии с ним. Необходимым условием продолжения алгоритма является цикл, в котором выполняется полный перебор всех состояний квантового регистра, а также вывод пары состояний, осуществляющей работу с вентилем. Получение единственно истинного результата вычислительного процесса из набора амплитуд требует использования переменной маски, которая необходима для фильтрации наборов индексов состояния для соблюдения последовательности получения пар состояний. Алгоритм оканчивается после перебора всех квантовых состояний.

Как видно из блок-схемы на Рис. 4, в случае двухкубитового контролируемого квантового вентиля [9] (гейта) имеем две переменные, хранящие бинарные индексы контролирующего и контролируемого кубитов. При обходе состояний квантового регистра так же, как и в случае с однокубитовыми квантовыми вентилями, выбираются пары состояний. За правильность выборки отвечают две переменные, которые устанавливаются при помощи операции конъюнкции между текущим индексом состояния и бинарным индексом одного из кубитов, участвующих в преобразовании. Также можно проследить отличие алгоритма воздействия двухкубитового вентиля в количестве переменных масок. Остальные части алгоритма, которые

осуществляют непосредственную выборку по сформированным индексам состояний из модели квантового регистра и осуществление преобразования, остаются неизменными.

3. Сравнительный анализ методики оптимизации моделирования квантовых вычислений и математического моделирования

В работе предложен оптимизационный алгоритм, позволяющий исключать произведение тензорной природы во время процесса моделирования. Алгоритм применяется в ядрах программ, приложений и в многопроцессорных информационных системах с целью уменьшения количества операций, которые взаимодействуют с тензорным произведением, абсолютным удалением преобразовательных матриц. Проверим эффективность оптимизационного алгоритма при помощи программ сравнения результатов процесса моделирования, далее сравниваем реализацию алгоритма с помощью программы или ускорителя. При математическом моделировании квантового вычислительного процесса требуется совершить операцию умножения тензорного и матричного типов. Оптимизационный алгоритм наиболее предпочтителен с точки зрения сложности вычислений и объема памяти. Для сравнения программной реализации алгоритма оптимизации и его аппаратной версией для однокубитовых квантовых вентилях, имея модель системы автоматизированного проектирования Quartus II на програм-

мируемых логических интегральных схемах Stratix III EP3S3E50F780 можно привести следующие расчеты. Количество тактов блока генерации пар состояний для однокубитовых вентилях составляет $q + 5 * 2^{n-1}$, где q – номер кубита, n – количество кубитов в квантовом регистре. q тратятся на сдвиги при инициализации и 2^{n-1} тактов на генерацию пар состояний, 5 тактов тратятся на вычисление следующего индекса состояния равного 24. Данное количество тактов получается при перемножении матрицы однокубитового квантового вентиля на пару значений из вектора состояний модели квантового регистра. Табл. 1 показывает результаты процесса моделирования одного воздействия квантового вентиля на квантовые регистры с разным количеством квантовых битов. Как видно из Табл. 1 использование алгоритма повышает эффективность процесса моделирования для однокубитовых вентилях, что делает его использование оправданным и необходимым при построении аппаратного симулятора. Получение выигрыша аппаратной реализации достигается за счет реализации матричного умножителя. При числе квантовых битов 5 или более аппаратное моделирование уступает программному.

Также стоит отметить, что частота процессора вычислительной машины заметно выше по сравнению с частотой программируемых логических интегральных схем. Без оптимизации мы вынуждены производить одно воздействие на квантовый регистр за время $O(2^{4n} + 2^{3n})$ и использовать $O(2^{2n} + 2^n)$ ячеек памяти,

Табл. 1. Результаты моделирования однокубитового вентиля на квантовый регистр с помощью программных средств

Число Кубитов	Скорость исполнения однокубитовой операции в математической модели, нс	Скорость исполнения однокубитовой операции в аппаратной модели, нс	Скорость исполнения однокубитовой операции с оптимизацией, нс
3	21025	4466	7446
4	46432	8932	10512
5	137545	17864	18397
6	539668	35728	30662
7	2049165	71456	54754
8	8273320	140912	102941
9	31202690	285824	204127

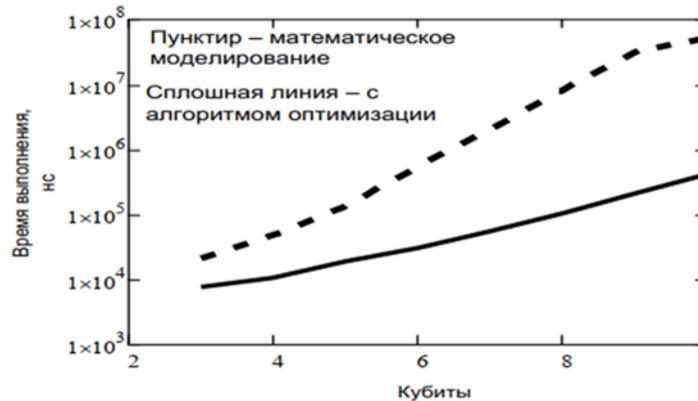


Рис. 5. Результаты моделирования

n – количество кубит. Данный алгоритм хотя и входит в класс NP-сложных алгоритмов, однако его использование предпочтительно. На Рис. 5 представлены результаты моделирования квантового вычислительного процесса с применением разработанного алгоритма оптимизации и математического моделирования.

Заключение

В результате исследования подходов и методик моделирования квантовых вычислений были выявлены их преимущества и недостатки, а также предложена оригинальная методика моделирования квантового вычислительного процесса с помощью аппаратного ускорителя. Методика оправдала себя в экспериментальной части, для создания которой были заимствованы алгоритмы программных симуляторов.

Однако программные симуляторы пока не способны производить вычисления с упрощенными типами данных. По этой причине в рамках анализа математических компонентов квантового вычислительного процесса был определен тип хранения амплитуд квантовых состояний. Это позволяет сократить часть расходов на ресурсы хранения в моделях квантовых вычислительных систем. Аппаратная составляющая позволяет создавать специальные операции, превышающие классические типы процессоров с точки зрения производительности. Если рассматривать программируемые логические интегральные схемы в качестве программно-аппаратной основы для будущего квантового ускорителя, то становится возмож-

ным выделить гибкости и универсальности методики, не нацеленной на моделирование конкретного количества квантовых битов. Перспектива дальнейших исследований состоит в нахождении и последующем исправлении слабых мест квантового вычислительного процесса: квантовые ошибки, декогеренция, вероятностный характер результатов вычислений. Также планируется исследование ускорения моделирования квантовых вычислений с применением распределенных вычислений.

Литература

1. Feynman, R.P. Simulating physics with computers // International Journal of Theoretical Physics. – 1982. – V. 21. – № 6. – P. 467-488.
2. Richter, M., Arnold, G., Trieu, B., Lippert, T. Massively Parallel Quantum Computer Simulations: Towards Realistic Systems. // John von Neumann Institute for Computing, NIC series. – 2007. – V. 38. – P. 61-68.
3. Khalid, A.U. FPGA Emulation of Quantum Circuits: master of Computer Engineering thesis: 31.10.2005 / Khalid Ahmed Usman; McGill University. – 2005. – 73 p.
4. Grover L.K. Quantum Mechanics Help in Searching for a Needle in a Haystack. / Phys. Rev. Lett. – 1997. – v.78 (2). – pp. 325-328.
5. Barends, R. et al., "Coherent Josephson Qubit Suitable for Scalable Quantum Integrated Circuits," Phys. Re. Lett., 111, (2013), doi:10.1103/PhysRevLett.111.080502, arXiv:1304:2322.
6. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. – 1997. – P. 1484 – 1509.
7. Guzik, V. Architecture and Software Implementation of a Quantum Computer Model / V. Guzik, S. Gushanskiy, M. Polenov, V. Potapov // 5th Computer Science On-line Conference 2016 (CSOS), Czech Republic, 2016. – P. 59 – 68.

8. Guzik, V. Development of Methodology for Entangled Quantum Calculations Modeling in the Area of Quantum Algorithms // 6th Computer Science On-line Conference 2017 (CSOS), Czech Republic, 2017. – P. 106 – 115.
9. Attractive photons in a quantum nonlinear medium. Ofer Firstenberg, Mikhail D. Lukin. Nature, vol. 502, October 2013.

Потапов Виктор Сергеевич. Ассистент, кафедра вычислительной техники, Южный федеральный университет г. Таганрог, Россия. E-mail: vpotapov@sfedu.ru

Гушанский Сергей Михайлович. Кандидат технических наук, доцент, кафедра вычислительной техники, Южный федеральный университет г. Таганрог, Россия. E-mail: smgushansky@sfedu.ru

Development of a Method for Constructing a Quantum System Using Optimization Hardware

V. S. Potapov, S. M. Gushansky

Southern Federal University, Taganrog, Russia

Abstract. The paper developed and simulated a hardware computing core, which is the main part of the accelerator based on field-programmable logic integrated circuits with the Altera Quartus computer-aided design system. Taking into account the obtained time dependence of the number of cycles required for the impact of a single-qubit quantum gate on a quantum register on the number of qubits and parallel arithmetic logic units in the hardware computing core, when simulating quantum computing, a method was developed to determine the estimate of the increase in hardware performance and ways to increase the performance of the accelerator based on hardware computing core based on programmable logic integrated circuits. A comparative analysis of the methodology for optimizing the simulation of quantum computing and mathematical modeling was also carried out.

Keywords: quantum algorithm, quantum bit, quantum circuit, entanglement, register, gate, parallelism, quantum computer.

DOI 10.14357/20718632220103

References

1. Feynman, R.P. Simulating physics with computers // International Journal of Theoretical Physics. – 1982. – V. 21. – № 6. – P. 467-488.
2. Richter, M., Arnold, G., Trieu, B., Lippert, T. Massively Parallel Quantum Computer Simulations: Towards Realistic Systems. // John von Neumann Institute for Computing, NIC series. – 2007. – V. 38. – P. 61-68.
3. Khalid, A.U. FPGA Emulation of Quantum Circuits: master of Computer Engineering thesis: 31.10.2005 / Khalid Ahmed Usman; McGill University. – 2005. – 73 p.
4. Grover L.K. Quantum Mechanics Help in Searching for a Needle in a Haystack. / Phys. Rev. Lett. – 1997. – v.78 (2). – pp. 325-328.
5. Barends, R. et al., "Coherent Josephson Qubit Suitable for Scalable Quantum Integrated Circuits," Phys. Re. Lett., 111, (2013), doi:10.1103/PhysRevLett.111. 080502, arXiv:1304:2322.
6. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. – 1997. – P. 1484 – 1509.
7. Guzik, V. Architecture and Software Implementation of a Quantum Computer Model / V. Guzik, S. Gushanskiy, M. Polenov, V. Potapov // 5th Computer Science On-line Conference 2016 (CSOS), Czech Republic, 2016. – P. 59 – 68.
8. Guzik, V. Development of Methodology for Entangled Quantum Calculations Modeling in the Area of Quantum Algorithms // 6th Computer Science On-line Conference 2017 (CSOS), Czech Republic, 2017. – P. 106 – 115.
9. Attractive photons in a quantum nonlinear medium. Ofer Firstenberg, Mikhail D. Lukin. Nature, vol. 502, October 2013.

Potapov V. S. Assistant, department of computer engineering, Southern Federal University, Taganrog, Engels str., 1, Russia.

Gushansky S. M. Candidate of technical sciences, associate professor, department of computer engineering, Southern Federal University, Taganrog, Engels str., 1, Russia.