Александр Дмитриевич Устюжанин родился в 1983 г. Бакалавр техники и технологии. Студент 2-го курса магистратуры МГТУ им. Н.Э. Баумана. Автор 6 научных работ в области систем управления летательными аппаратами.

A.D. Ustyuzhanin (b. 1983). Student of the Bauman Moscow State Technical University. Author of 6 publications in the field of control systems of flying vehicles.

Василий Дмитриевич Шашурин — д-р. техн. наук, профессор, зав. кафедрой "Технологии приборостроения" МГТУ им Н.Э. Баумана. Специализируется в области нанотехнологии в приборостроении, надежности технологических систем.

V.D. Shashurin — D. Sc. (Eng.), professor of "Technologies of Instrumental Engineering" department of the Bauman Moscow State Technical University. Specializes in the field of nano-technology in instrumental engineering, probability of technological systems.

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

УДК 004.27

П. Г. Ключарев

ОСНОВЫ КВАНТОВЫХ ВЫЧИСЛЕНИЙ И КВАНТОВОЙ КРИПТОГРАФИИ

Рассмотрены основные идеи теории квантовых вычислений и квантовой криптографии, активно развиваемые в настоящее время. Рассмотрены наиболее важные квантовые алгоритмы: алгоритм поиска Гровера, алгоритм квантового преобразования Фурье, алгоритм нахождения периода функции и алгоритм факторизации натуральных чисел Шора. В обзоре также рассмотрен квантово-криптографический протокол передачи данных.

Бóльшая часть литературы [1–12] предназначена для профессиональных физиков или профессиональных математиков. Избыток физической терминологии и использование сложных математических методов делает затруднительным понимание такой литературы программистами. Литература, понятная большинству программистов и в то же время достаточно полно отражающая основные идеи квантовых вычислений, практически отсутствует. Цель данного обзора состоит в том, чтобы восполнить этот пробел.

Не будем подробно рассматривать квантовую механику — заинтересованный читатель найдет подробное описание ее основ, например

в работе [7], воспользуемся только некоторыми фактами из квантовой механики, которые будут вводиться в виде постулатов по ходу изложения.

Квантовый компьютер способен изменить наши представления о вычислениях и их эффективности. Он принципиально отличается от обычного классического компьютера. Пока еще не полностью понятно, что может квантовый компьютер, однако, уже существует ряд квантовых алгоритмов, решающих некоторые задачи значительно более эффективно по сравнению с алгоритмами для классического компьютера.

Квантовые биты. Рассмотрим простейшую квантовую систему, имеющую два выделенных состояния (например, фотон может быть поляризован горизонтально или вертикально). Такую систему будем называть квантовым битом. Обозначим одно из его выделенных состояний $|0\rangle$, а другое $|1\rangle$. Состояние квантовой системы можно измерить. Квантовый бит может иметь такое состояние, что измерение может с некоторой вероятностью показать $|0\rangle$, а с некоторой другой вероятностью $|1\rangle$. Опишем состояние такой системы как линейную комбинацию выделенных состояний $(a\,|0\rangle + b\,|1\rangle)$, где a и b — комплексные числа, такие что $|a|^2 + |b|^2 = 1$. Тогда измерение состояния $(a\,|0\rangle + b\,|1\rangle)$ с вероятностью $|a|^2$ покажет состояние $|0\rangle$, а с вероятностью $|b|^2$ — состояние $|1\rangle$.

Рассмотрим теперь систему, состоящую из n квантовых битов. В дальнейшем такую систему будем называть квантовым регистром. Такой регистр имеет 2^n выделенных состояния, соответствующих n разрядным двоичным числам от $|00\ldots0\rangle$ до $|11\ldots1\rangle$.

Состояние квантового регистра записывается в виде линейной комбинации всех этих выделенных состояний (этот известный из квантовой механики факт примем в качестве постулата):

$$\sum_{x=0}^{2^n-1} a_x\,|x\rangle.$$

При этом выполняется условие нормировки

$$\sum_{i=0}^{2^n-1} |a_i|^2 = 1.$$

Коэффициенты a_x являются комплексными числами или амплитудами соответствующих состояний $|x\rangle$.

Таким образом, состояние системы, состоящей из n квантовых битов, описывается вектором единичной длины в 2^n-мерном комплексном евклидовом пространстве (скалярное произведение состояний

$|a\rangle = |a_1 \dots a_n\rangle$ и $|b\rangle = |b_1 \dots b_n\rangle$ обозначается как $\langle a|b\rangle$ и вводится обычным образом: $\langle a|b\rangle = \sum\limits_i a_i b_i$).

Отметим также, что умножение всего состояния на фазовый множитель $e^{i\varphi}$ приводит к неотличимому состоянию в том смысле, что невозможно поставить опыт, по результату которого можно определить значение параметра ϕ.

Одним из важнейших свойств квантового компьютера является тот факт, что с помощью системы, состоящей из n квантовых битов, можно представить различные значения n битов одновременно. Например, пусть наша система состоит из двух квантовых битов. Мы можем привести ее в состояние $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, которое представляет собой линейную комбинацию всех возможных значений двух битов.

Рассмотрим теперь квантовый регистр, состоящий из $n+m$ квантовых битов. В качестве очередного постулата отметим, что если привести первые его n битов в состояние $|z_1\rangle = a_1 |x_1\rangle + a_2 |x_2\rangle$, а остальные m битов — в состояние $|z_2\rangle = b_1 |y_1\rangle + b_2 |y_2\rangle$, то весь регистр приведется в состояние

$$|z_1\rangle |z_2\rangle = a_1 b_1 |x_1\rangle |y_1\rangle + a_1 b_2 |x_1\rangle |y_2\rangle + a_2 b_1 |x_2\rangle |y_1\rangle + a_2 b_2 |x_2\rangle |y_2\rangle . \quad (1)$$

Измерения. Чтобы извлечь из квантового регистра информацию, надо провести измерение. При этом измерить можно любой набор квантовых битов. Кроме того, поскольку квантовые состояния образуют евклидово пространство, измерения можно проводить в различных базисах. Однако, как это известно из квантовой механики, проведение измерения приводит к переходу системы в базисное состояние, соответствующее результатам измерения.

Рассмотрим процесс измерения в системе, состоящей из двух квантовых битов. Пусть система находится в состоянии

$$a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle .$$

Измерим первый квантовый бит в базисе $\{|0\rangle, |1\rangle\}$. В результате получим $|0\rangle$ с вероятностью $|a_0|^2 + |a_1|^2$. При этом квантовая система перейдет в состояние, у которого первый бит всегда равен нулю, а именно: $\frac{1}{\sqrt{|a_0|^2 + |a_1|^2}}(a_0 |00\rangle + a_1 |01\rangle)$. С другой стороны, мы получим $|1\rangle$ с вероятностью $|a_2|^2 + |a_3|^2$. В этом случае квантовая система перейдет в состояние $\frac{1}{\sqrt{|a_2|^2 + |a_3|^2}}(a_2 |10\rangle + a_3 |11\rangle)$.

Преобразования. Квантовым преобразованием будем называть отображение евклидова пространства, образуемого квантовой системой, в себя. Введем постулат: с квантовыми системами можно производить только линейные унитарные преобразования, причем любое линейное унитарное преобразование допустимо. Напомним, что унитарными преобразованиями называются преобразования, сохраняющие скалярное произведение, т.е. такие, для матрицы U которых выполняется

$$U^{-1} = (U^*)^{\mathrm{T}},$$

где знаком $*$ обозначено комплексное сопряжение.

Введем понятие булева оператора — булевым оператором называется система из m булевых функций, зависящих от n переменных. Заметим, что любому обратимому булеву оператору (т.е. подстановке) соответствует унитарное квантовое преобразование.

Например, обратимому булеву оператору $\{x, x \oplus y\}$ соответствует унитарное преобразование, превращающее состояние $(a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle)$ в состояние $(a_0|00\rangle + a_1|01\rangle + a_3|10\rangle + a_2|11\rangle)$. Такому преобразованию (его обычно называют Controlled-NOT) соответствует матрица

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

В силу линейности, квантовые преобразования полностью определяются их действием на базисные векторы.

Некоторые важнейшие элементарные преобразования (назовем их квантовыми вентилями) приведены в таблице.

Таблица

Название, обозначение и краткое описание квантового вентиля	Действие на базовые состояния	Матрица
Тождественное преобразование, I	$\|0\rangle \to \|0\rangle$ $\|1\rangle \to \|1\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Отрицание, X	$\|0\rangle \to \|1\rangle$ $\|1\rangle \to \|0\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Фазовый сдвиг, Z	$\|0\rangle \to \|0\rangle$ $\|1\rangle \to -\|1\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Фазовый сдвиг с отрицанием, Y	$\|0\rangle \to -\|1\rangle$ $\|1\rangle \to \|0\rangle$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Название, обозначение и краткое описание квантового вентиля	Действие на базовые состояния	Матрица
Controlled-NOT, CNOT, прибавляет ко второму биту первый по модулю 2	$\|00\rangle \to \|00\rangle$ $\|01\rangle \to \|01\rangle$ $\|10\rangle \to \|11\rangle$ $\|11\rangle \to \|10\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Controlled-Controlled NOT, вентиль Тофолли, прибавляет к третьему биту произведение двух первых (по модулю два).	$\|000\rangle \to \|000\rangle$ $\|001\rangle \to \|001\rangle$ $\|010\rangle \to \|010\rangle$ $\|011\rangle \to \|011\rangle$ $\|100\rangle \to \|100\rangle$ $\|101\rangle \to \|101\rangle$ $\|110\rangle \to \|111\rangle$ $\|111\rangle \to \|110\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
Преобразование Адамара, H:	$\|0\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\|1\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

В квантовых алгоритмах часто используется тот факт, что если применить преобразование Адамара по отдельности к каждому квантовому биту n-битного регистра, все биты которого обнулены, получим (учитывая свойство (1)) нормированную сумму всех базисных состояний:

$$H\left(|00\ldots0\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

Как показано в работе [11], с помощью квантовых вентилей X, Y, Z и CNOT можно вычислить любой обратимый булев оператор. Произвольный булев оператор f с m входами и k выходами можно вычислить с помощью квантового преобразования, отображающего состояние $|x\rangle\,|y\rangle$ в состояние $|x\rangle\,|y \oplus f(x)\rangle$, где x — m-мерный вектор, а y — k-мерный вектор.

Заметим, что в силу свойств унитарных преобразований, измерение квантового состояния в одном ортогональном базисе всегда может быть осуществлено путем некоторого квантового преобразования и измерения в другом ортогональном базисе.

Квантовые состояния нельзя копировать. Действительно, предположим, что P — это копирующее преобразование, такое что $P\left(|x\rangle\,|0\rangle\right) = |x\rangle\,|x\rangle$. Пусть $|x\rangle$ и $|y\rangle$ — некоторые ортогональные состояния. Рассмотрим состояние $|z\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + |y\rangle\right)$. Поскольку P —

копирующее преобразование, то должно выполняться (учитывая (1))

$$P\left(|z\rangle\,|0\rangle\right) = |z\rangle\,|z\rangle = \frac{1}{2}\left(|x\rangle\,|x\rangle + |x\rangle\,|y\rangle + |y\rangle\,|x\rangle + |y\rangle\,|y\rangle\right).$$

С другой стороны, в силу линейности,

$$P\left(|z\rangle\,|0\rangle\right) = \frac{1}{\sqrt{2}}\left(P\left(|x\rangle\,|0\rangle\right) + P\left(|y\rangle\,|0\rangle\right)\right) = \frac{1}{\sqrt{2}}\left(|x\rangle\,|x\rangle + |y\rangle\,|y\rangle\right).$$

Мы пришли к противоречию.

Таким образом, копирование неизвестных квантовых состояний в общем случае невозможно.

Алгоритм поиска Гровера. Поставим задачу следующим образом. Пусть имеется некоторая функция $f(x)$, где x — целое число в диапазоне $0 \leqslant x \leqslant 2^n - 1$. При некоторых значениях аргумента эта функция принимает значение 1, а при всех остальных — 0. Требуется найти хотя бы одно значение аргумента, при котором функция равна 1.

На классическом компьютере эта задача в общем случае может быть решена только методом полного перебора. Для этого требуется в среднем 2^{n-1} раз вычислить функцию $f(x)$ и произвести столько же сравнений.

На квантовом компьютере возможен следующий алгоритм:

1. Приводим квантовый регистр в состояние $\dfrac{1}{\sqrt{2^n}}\sum\limits_{x=0}^{2^n-1}|x\rangle$;

2. Вычисляем функцию f от этого регистра $\dfrac{1}{\sqrt{2^n}}\sum\limits_{x=0}^{2^n-1}|x\rangle\,|f(x)\rangle$;

3. Повторяем $\dfrac{\pi}{4}\sqrt{2^n}$ раз процедуру увеличения амплитуды всех x_i, для которых $f(x_i) = 1$. (Эта процедура описывается ниже);

4. Измеряем состояние регистра. Результат будет верным с вероятностью около 2^{-n}. Если результат все-таки оказался неверным, весь алгоритм следует повторить.

Процедура увеличения амплитуды состоит из двух этапов.

1. Изменение амплитуды с a_j на $-a_j$ для всех x_i, таких, что $f(x_i) = 1$. Эта операция представляет собой преобразование Z над последним квантовым битом регистра.

2. Инверсия относительно среднего. Это преобразование можно записать следующим образом:

$$\sum_i |x_i\rangle \to \sum_i \left(2a_{\text{ср}} - a_i\right)|x_i\rangle,$$

где $a_{\text{ср}}$ — средняя амплитуда.

Это преобразование можно представить в виде матрицы

$$D = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix}.$$

Как показал Гровер в работе [2], это преобразование может быть эффективно реализовано на квантовом компьютере, а сложность всего алгоритма оценивается как $O\left(\sqrt{2^n}\right)$.

Квантовое преобразование Фурье определяется так:

$$U_{QFT}\left(|x\rangle\right) = \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{\frac{2\pi i c x}{2^m}} |c\rangle.$$

Как показано в работе [10], такое преобразование можно построить, используя только $m(m+1)/2$ квантовых вентилей двух типов. Один из них представляет собой преобразование Адамара, примененное к j-му квантовому биту (обозначим его H_j). Другой вентиль реализует двухбитное преобразование вида

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\frac{\pi}{2^{k-j}}} \end{pmatrix}.$$

Согласно данным работы Шора [10], квантовое преобразование Фурье можно задать следующим образом:

$$U_{QFT} =$$

$$= H_0 S_{0,1} \ldots S_{0,m-1} H_1 \ldots H_{m-3} S_{m-3,m-2} S_{m-3,m-1} H_{m-2} S_{m-2,m-1} H_{m-1}.$$

Квантовый алгоритм нахождения периода функции. Пусть есть периодическая функция $f(x)$. Область определения и область значений этой функции — целые числа, причем $0 \leqslant x \leqslant 2^n - 1$ и $0 \leqslant f(x) \leqslant 2^m - 1$. Для того чтобы найти период этой функции, нужен квантовый регистр, состоящий из $n + m$ квантовых битов. Приведем его в состояние

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle.$$

Теперь вычислим от него функцию f так, чтобы у нас получилось состояние

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle.$$

Измерим последние m квантовых битов (т.е. квантовые биты, относящиеся к $f(x)$). Квантовый регистр перейдет в состояние

$$\sum_{x:f(x)=u} |x, u\rangle.$$

Проведем квантовое преобразование Фурье, в результате чего мы получим состояние

$$\sum_j c_j \left| j\frac{2^n}{r} \right\rangle,$$

где c_j равны нулю при всех j, не кратных $2^n/r$. Если период r не делит 2^n, преобразование выполняется не точно, причем большая амплитуда сосредоточена вблизи целых значений, кратных $[2^n/r]$.

Наконец, измерив полученное состояние, в результате получим число v.

Если период равняется степени двойки, то $v = j\dfrac{2^n}{r}$. А поскольку в большинстве случаев j и r — взаимно просты, то сокращение дроби $\dfrac{v}{2^n}$ даст дробь, знаменатель которой и есть период. В общем случае либо придется прогнать весь алгоритм несколько раз, пока мы не получим правильное значение периода (ему соответствует максимальная амплитуда, а следовательно, максимальная вероятность), либо воспользоваться известным из теории чисел разложением в бесконечную дробь (подробности см. работу [10]).

Алгоритм разложения числа на простые множители (алгоритм Шора). Поставим задачу следующим образом: у нас есть натуральное число N, имеющее ровно два простых делителя. Требуется найти эти делители.

Наилучший известный классический алгоритм решения этой задачи (так называемый алгоритм решета числового поля) имеет сверхполиномиальную сложность. На этом факте, в частности, основана стойкость криптосистемы RSA.

Однако существует квантовый алгоритм, решающий эту задачу за полиномиальное время. Действительно, предположим, что для некоторого числа a его порядок по модулю N (т.е. минимальное число r, такое, что $a^r = 1(\mathrm{mod}\, N)$) четен. Тогда выражение $a^r = 1(\mathrm{mod}\, N)$ можно записать в виде

$$\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right) = 0(\mathrm{mod} N).$$

Зная r, можно эффективно найти делители числа N. Учитывая, что порядок r фактически является периодом функции $a^x \bmod N$, r можно определить с помощью алгоритма нахождения периода функции. Число a можно взять случайным — если период функции окажется нечетным, то надо просто выбрать другое a и снова прогнать алгоритм.

Квантовая криптография. Обычные протоколы открытого распространения ключей, например протокол Диффи–Хеллмана, основаны на предположении о том, что используемая в них функция (например, возведение в степень по простому модулю) является однонаправленной. Однако на настоящий момент неизвестно действительно ли это так. Более того, многие из них не являются однонаправленными для квантового компьютера.

С помощью квантово-механических методов можно реализовать такое устройство для распределения ключей, что злоумышленник физически не сможет перехватить информацию. Более того, уже есть реальные устройства, обеспечивающие квантовую передачу ключей.

Итак, пусть у нас есть канал связи, по которому можно передавать квантовые биты. Два пользователя, A и B, хотят договориться об общем ключе для шифрования информации, передаваемой по открытому каналу.

Пользователь A может кодировать информацию в различных базисах. Определим два базиса: в первом 0 кодируется в $|0\rangle$, а 1 кодируется в $|1\rangle$, во втором базисе 0 кодируется в $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, а 1 — в $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Протокол квантового распространения ключей заключается в следующем.

1. A случайно выбирает битовую строку.

2. A случайно выбирает последовательность базисов длиной, равной длине битовой строки.

3. A кодирует битовую строку, используя соответствующие базисы, и передает закодированную битовую строку B.

4. B принимает квантовые биты от A и измеряет их, случайно выбирая базисы для измерения.

5. B сообщает A по открытому каналу свои базисы измерений.

6. A определяет, какие базисы, использованные B, совпадают с его собственными, и сообщает B по открытому каналу, какие биты он принял правильно.

7. B посылает пользователю A некоторые, выбранные наугад, биты по открытому каналу.

8. A сравнивает эти биты с посланными им. Если хотя бы один из них не совпадает, то кто-то пытается прослушивать канал связи, иначе он посылает B подтверждение.

9. A и B используют в качестве ключа биты, принятые B правильно, кроме тех, которые были переданы на седьмом шаге.

Предположим, что злоумышленник пытается перехватить информацию, передаваемую по квантовому каналу. Он может это сделать, только проводя измерения квантовых битов в каком-либо базисе, что изменяет состояние тех квантовых битов, для которых он не угадал базис (таких будет примерно половина). Такие биты пользователь B примет неправильно, что и выявится на шаге 8.

Такие системы уже существуют — они выпускаются, например, фирмой id Quantique. В качестве квантовых битов используются поляризованные фотоны. Состоянию $|0\rangle$ соответствуют фотоны с горизонтальной поляризацией, состоянию $|1\rangle$ — с вертикальной. Фотоны передаются по обычному оптоволоконному кабелю на расстояние до 67 км. Скорость передачи составляет от 100 до 4000 бит/с в зависимости от расстояния и применяемого оптоволокна.

Заключение. В настоящее время неясно, как сделать квантовый компьютер, состоящий хотя бы из нескольких десятков квантовых битов. Однако неизвестны какие-либо фундаментальные трудности для его создания. За рамками настоящей работы остались физические вопросы квантовых вычислений, а также большое число квантовых алгоритмов (например, эффективный алгоритм дискретного логарифмирования), теория квантового кодирования и другие интереснейшие вопросы. Подробное их освещение можно найти, например, в работе [12].

СПИСОК ЛИТЕРАТУРЫ

1. Браунштейн С. Л. Квантовые вычисления: Учебное руководство // Квантовые вычисления: за и против. – Ижевск: Удмуртский университет, 1999.
2. Гровер Л. К. Квантовая механика позволяет найти иголку в стоге сена // Квантовые вычисления: за и против. – Ижевск: Удмуртский университет, 1999.
3. Гровер Л. К. Польза суперпозиции // Квантовые вычисления: за и против. – Ижевск, Удмуртский университет, 1999.
4. Ди Винченцо Д. П. Квантовые вычисления // Квантовые вычисления: за и против. – Ижевск: Удмуртский университет, 1999.
5. Килин С. Я. Квантовая информация // Успехи физических наук. – Т. 169, № 5.
6. Прескилл Дж. Квантовые вычисления: за и против. // Квантовые вычисления: за и против. – Ижевск: Удмуртский университет, 1999.
7. Савельев И. В. Основы теоретической физики В 2 т. – М.: Наука. Физматлит, 1996. – Т. 2: Квантовая механика. – 432 с.

8. Ф е й н м а н Р. Квантовый компьютер и квантовые вычисления // Квантовый компьютер и квантовые вычисления. – Ижевск: Ижевская типография, 1999.

9. Ф е й н м а н Р. Моделирование физики на компьютерах // Квантовый компьютер и квантовые вычисления. – Ижевск: Ижевская типография, 1999.

10. Ш о р П. Полиномиальные по времени алгоритмы разложения числа на множители и нахождения дискретного логарифма для квантового компьютера // Квантовый компьютер и квантовые вычисления. – Ижевск: Ижевская типография, 1999.

11. B a r e n k o A., B e n n e t t C., C l e v e R., D i V i n c e n z o D., M a r g o l u s N., S h o p P., S l e a t o r T., S m o l i n J., W e i n f u r t e r H. Elementary gates for quantum computation // Physical Review A52, 5 – 1995.

12. P r e s k i l l J. Lecture Notes for Physics 229: Quantum Information and Computation.

13. S t e a n e A. Quantum computing // Rept. Prog. Phys. 61 (1998) 117–173.

Статья поступила в редакцию 14.11.2005

Петр Георгиевич Ключарев родился в 1980 г., окончил в 2004 г. МГТУ им. Н.Э. Баумана. Аспирант кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор 5 научных работ в области информационной безопасности.

P.G. Klyucharyov (b. 1980) graduated from the Bauman Moscow State Technical University in 2004. Post-graduate of “Information Semrity” department of the Bauman Moscow State Technical University. Author of 5 publications in the field of data safety.

УДК 65.016.4:658.5.012.1:338.92.001

М. В. П о п е н ч е н к о

АНАЛИЗ ФОРМИРОВАНИЯ УСТОЙЧИВОЙ КОНКУРЕНТОСПОСОБНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ОСНОВЕ РАЗВИТИЯ ПРОМЫШЛЕННЫХ КЛАСТЕРОВ

Рассмотрен один из аспектов формирования устойчивой конкурентоспособности информационных технологий на основе развития промышленных кластеров. Установлено, что многообразие форм проявления конкурентных преимуществ предопределяет необходимость комплексного рассмотрения критериев и параметров, определяющих конкурентоспособность объектов и субъектов экономической системы.

В ежегодном обзоре Всемирного экономического форума (WEF) “Доклад о мировой конкурентоспособности 2005–2006” [1] отмечено, что Россия продолжает медленно двигаться вниз в рейтинге конкурентоспособности стран мира. В настоящее время Россия занимает лишь