Отже, необхідність подолання сучасної кризової ситуації з комплектуванням бібліотек вимагає розробки теоретико – методологічних засад формування оптимальної системи документопостачання бібліотечних фондів в умовах інформатизації суспільства. Найважливішою складовою будь – якої теорії є закономірності розвитку досліджуваного явища, що відображають об'єктивні процеси дійсності і дозволяють розібратися в механізмах утворення нового, правильно оцінити масштаби, можливості і перспективи майбутніх змін.

Список використаних джерел

1. http://nootron.net.ua/ Help.htm? p=chapter3.1. html – Справка системы поддержки принятия решений (СППР) NooTron
2. www.diary.ru/ ~shamomist/p209503162. htm? oam – Комплектование библиотечного фонда, виды и этапы.
3. www.igmt.ru/index.php/component/k2/item/131-popolnenie-fonda-biblioteki – Пополнение фонда библиотеки

Vascheiykin K.S.
Student,
Faculty of information and Computer Technology,
NTUU "Igor Sikorsky Kyiv Polytechnic Institute"

QUANTUM COMPUTERS

Before the quantum in the course was the classical theory of electromagnetic radiation. In 1900 the German scientist Max Planck, who did not believe in quanta, considered them to be a fictitious and purely theoretical construction, was forced to admit that the energy of the heated body is radiated by portions-quanta; thus, the assumptions of the theory coincided with the experimental observations. And five years later the great Albert Einstein resorted to the same approach when explaining the photoelectric effect: when irradiating light in metals, an electric current appeared [1].

Quickly and effectively solving a lot of problems led to the development of electronic computers. A gradual decrease in their size and cost (in connection with mass production) paved the way for computers in every house. With the advent of the Internet, our dependence on computer systems, including communication, has become even stronger.

Dependence is growing, computational power is constantly growing, but it is time to recognize that, despite its impressive capabilities, computers have not been able to solve all the tasks that we are ready to put before them. One of the first to start talking about this was the famous physicist Richard Feynman: back in 1981, at the conference, he stated that it was impossible in principle to calculate accurately a real physical system on conventional computers [3]. The effects of the micro-scale are easily explained by quantum mechanics. Then, as an alternative, Feynman suggested using quantum computers to calculate physical systems.

If in normal computers this function is answered by bits – zeros and ones – then in quantum computers they are replaced by quantum bits (abbreviated – qubits). The qubit itself is a rather simple thing. It has two basic values (or states, as they like to say in quantum mechanics), which it can take: 0 and 1. However, thanks to the property of quantum objects called "superposition, "the qubit can take all values that are a combination of the basic ones. At the same time, its quantum nature allows it to be in all these states simultaneously [2].

In addition, to describe the exact state of the system, there is no need for huge computing power and RAM, because to calculate a system of 100 particles is enough for 100 qubits, and not trillions of trillions of bits. Moreover, with the increase in the number of particles (as in real complex systems), this difference becomes even more significant [4].

The most famous quantum algorithm is the Shore algorithm (invented in 1997 by the English mathematician Peter Shor.), which is aimed at solving the problem of factorization of numbers by prime factors (the factorization problem, the discrete logarithm). It would seem why do you need a quantum computer to solve such a problem? We all easily decompose into prime factors a number of the form 15 = 3 * 5, 55 = 5 * 11, 91 = 13 * 7, etc. But can you decompose into two prime factors the number 853, or 13297, or 99487? It's not so simple, is it? But if you write a program for a computer, it will quickly find the original multipliers by a simple search (or another, more complicated algorithm). And if the number does not have 5 characters, but, at least, 100? The most modern computers can’t cope with this task – this will take them from several tens to several million years, depending on the length of the number.

But quantum computers, performing Shore's algorithm, must cope with this task in a matter of seconds. At least in theory. In practice, it will be possible to verify only when the first full-fledged quantum computer will be created, operating with a pair of thousands of qubits. By the way, a couple of years ago, scientists performed the Shore algorithm on a quantum processor of 3 qubits.

Why is the problem of factoring numbers so important? The fact is that a lot of the modern protocols that provide secure data transmission (for example, when banking transactions) use the computational complexity of this task to generate a secret key that is used to encrypt / decrypt messages. With the creation of a quantum computer, these systems in the blink of an eye will cease to be as secret or safe.

Meanwhile, dozens of scientific groups and laboratories around the world began to engage in experimental studies of qubits and the possibilities of creating a quantum computer from them. After all, it is one thing – theoretically to come up with a qubit, and quite another – to make it a reality. To do this, it was necessary to find a suitable physical system with two quantum levels, which can be used as the basic states of a qubit – zero and one [4]. Feynman himself in his pioneer article suggested using photons twisted in different directions for these purposes, but in 1995 the first experimentally created qubits became ions trapped in special traps. The ions were followed by a lot of other physical realizations: atomic nuclei, electrons, photons, crystal defects, superconducting circuits – all of which met the requirements.

So, for the joy of cryptographers, a quantum computer is still a matter of the future. Although it is not as far back as it once seemed, because its creation is actively connected as the largest corporations like Intel, IBM and Google [1], as well as individual states for which the creation of a quantum computer is a matter of strategic importance.

References:

1. Quantum Mechanics. Available from: <https://en.wikipedia.org/wiki/Quantum_ mechanics>. [20 November 2017]

2. Inside the weird world of quantum computers. Available from: <http://www.wired.co.uk/ article/quantum-computing-explained>. [20 November 2017]

3. Physics World poll names Richard Feynmanone. Available from: <https://web.archive.org/ web/20120321043038/http://media.caltech.edu/press_releases/12019>. [20 November 2017]

4. The quantum computing quibit. Available from: <https://en.wikipedia.org/wiki/ Qubit>. [20 November 2017]