Security Threat Model Based on Analysis of Foreign National Quantum Programs

Alexei S. Petrenko [1], Sergei S. Petrenko [1], Krystina A. Makoveichuk [2], Alexander V. Olifirov[2], Hristo Krachunov [3]

[1] *Saint Petersburg Electrotechnical University "LETI", 5, Professor Popov Street, St. Petersburg, 197376, Russia*
[2] *V.I. Vernadsky Crimean Federal University, 4, Akademika Vernadsky Avenue, Simferopol, 295007, Crimea*
[3] *Technical University of Varna, Studentska 1, Varna, 9010, Bulgaria*

Abstract

Currently, 17 technologically developed countries of the world (USA, China, Russia, France, Germany, Great Britain, Israel, South Korea, Australia, Japan, etc.) are implementing national quantum programs to support exploratory research, R&D in the field of quantum technologies (Q). At the same time, in 12 countries, the mentioned programs are funded by the state, and leading scientific institutions, advanced research agencies for military intelligence and defense structures, as well as leading public and private universities in the field of natural sciences are involved in their implementation. Other countries of the world are actively participating in international programs for the development of quantum technologies. At the same time, national quantum programs are defined by the governments of these countries as critical for the national security and economic competitiveness of the state. Consider the national quantum programs of the United States and its partners in the NATO bloc to form a model of security threats to the critical information infrastructure of the Russian Federation.

Keywords

National quantum program, roadmap for the development of quantum technologies, quantum computing and computers, quantum and post-quantum cryptography, quantum cryptanalysis algorithms, quantum algorithms of Shor, Grover, and Simon, quantum Fourier transform, factorization and discrete logarithm problem.

1. Introduction

According to leading Russian political scientists [1, 3-5], the modern world is going through a period of profound changes, the essence of which is the formation of a polycentric international system:

- the world's potential for power and development is being dispersed and shifted to the Asia-Pacific region. The ability of the historic West to dominate the world economy and politics is shrinking;
- the contradictions arising from uneven world development, the widening of the gap between the welfare of States, the intensification of competition for resources, access to markets, and control of transport routes have become more pronounced. The desire of Western States to maintain their positions, including by imposing their views on global processes and by pursuing a policy of containing alternative centers of power, has led to increased instability in international relations, Increased turbulence at the global and regional levels. The struggle to dominate the formation of key principles for the organization of the future international system is becoming a major trend in the current stage of world development;

Proceedings of VI International Scientific and Practical Conference Distance Learning Technologies (DLT–2021), September 20-22, 2021, Yalta, Crimea
EMAIL: A.Petrenko1999@rambler.ru (A.1); s.petrenko@rambler.ru (A. 2); christin2003@yandex.ru (A. 3); alex.olifirov@gmail.com (A.4); euro_expert@abv.bg (A.5)
ORCID: 0000-0002-9954-4643 (A.1); 0000-0003-0644-1731 (A.2); 0000-0003-1258-0463 (A.3); 0000-0002-5288-2725 (A.4); 0000-0002-7044-9642 (A.5)
© 2021 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3057/paper2.pdf

- in the face of increasing political, social, economic divisions and instability in the world political and economic system, the role of force in international relations is becoming more important. The development and modernization of force capabilities and the development and deployment of new types of weapons undermine strategic stability and threaten the global security provided by the system of arms control treaties and agreements. While the risk of a large-scale war, including nuclear war, between the major States remains low, the risks of their being drawn into regional conflicts and crises are increasing;
- in addition to military power, important influences of States on international policy, such as economic, legal, technological, and information-related factors, have come to the fore. The pursuit of appropriate opportunities to pursue geopolitical interests is detrimental to the search for solutions to disputes and existing international problems through peaceful means based on international law;
- the use of instruments of «soft power», first of all, the possibilities of civil society, humanitarian and information-communication, and technologies to solve foreign policy problems, becomes an integral part of modern international policy, in addition to traditional diplomatic methods [2, 6, 7].

Western states, primarily the United States and NATO countries, are striving in every possible way to use technological superiority in the field of artificial intelligence (AI), quantum technologies (Q), collection and processing of big data (Big Data + ETL), high and ultra-high performance machine computing (up to 10 Exaflops) to dominate the information space. At the same time, it raises concern that information technologies are increasingly being used by these countries for military-political purposes, including for the implementation of actions aimed at undermining the sovereignty, political and social stability, and the territorial integrity of the Russian Federation.

For example, the National Quantum Initiative (2018) aims to maintain US technological leadership in quantum technology in the medium and long term. To this end, a series of (more than 80) dual-use research and development projects have been launched since 2019 under the United States National Security Agency (NSA), the Intelligence Advanced Research Projects Activity (IARPA), The Defense Advanced Research Projects Agency (DARPA), the United States National Science Foundation (NFS), the United States Department of Energy (DOE), etc. At the same time, the US budget for the development of quantum technologies in 2021 exceeded US $ 2.2 billion (for comparison, China's budget is US $ 2.5 billion, Russia's budget is the US $ 0,8 billion) (see Fig. 1). Let us consider the structure and content of the aforementioned US quantum initiative in more detail.

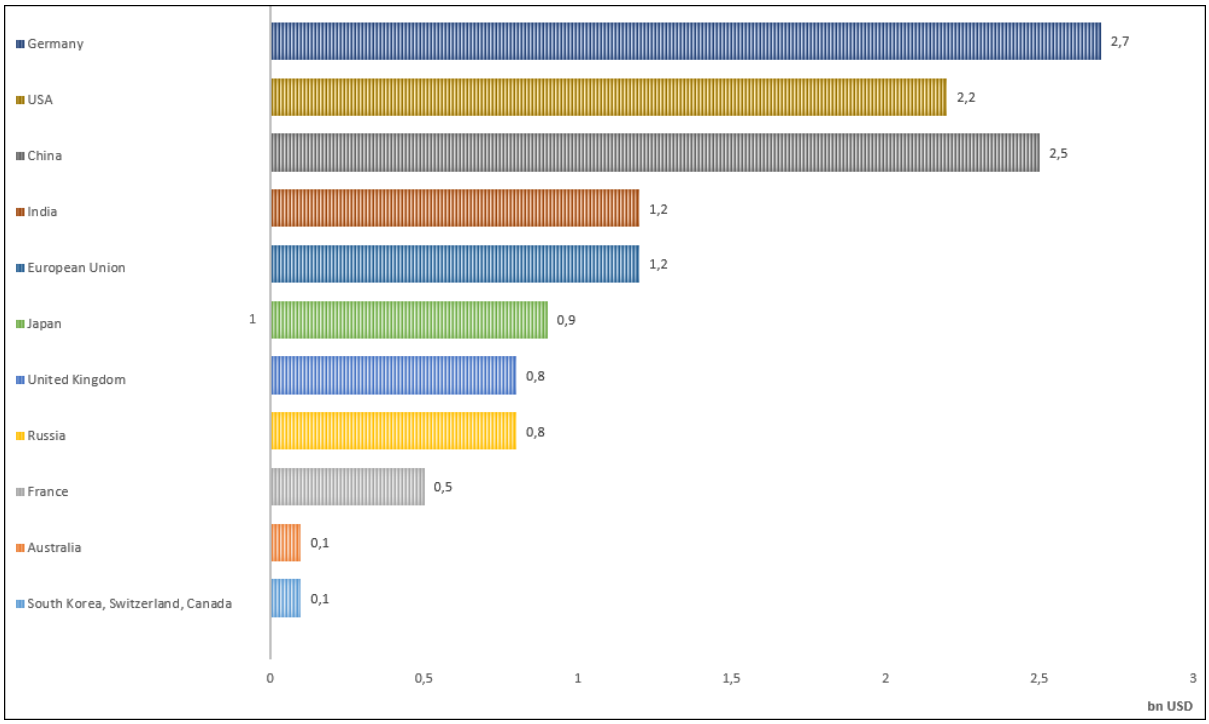

Figure 1: Open budgets of high-tech countries of the world for the development of quantum technologies (Q)

2. US Quantum Initiative 2018

Some specific steps by the United States military and political leadership and scientific community preceded the National Quantum Initiative (2018).

At the end of 2017, the issue became particularly pressing, as US political elites began to have serious fears of falling behind, mostly from China, in the global quantum computing race. On the instructions of the US Congress (one of the three highest federal government bodies of the US), the National Security Agency (NSA) has produced a series of classified reports assessing the military-technical capabilities of the United States and its opponents in the area of quantum technology.

In these documents, the following issues were presented in expanded form:

- structure and comparison of costs for national quantum initiatives of the US and NATO countries, as well as their opponents;
- the quantity and quality of previously conducted scientific and technical research;
- evaluation of the practical value of scientific results;
- assessment of the potential of an appropriate pilot framework;
- evaluation of the quality of training of military and civilian specialists in the field of quantum technology, etc.

Further, a Memorandum (2018) was developed on budgetary priorities of the US presidential administration in the field of dual-use R&D. At the same time, the following areas of promising research were identified: quantum technologies (Q), quantum communications, quantum computers, quantum computing, quantum, and post-quantum cryptography. The goal was to maintain the technological leadership of the United States in the field of quantum technologies in the medium and long term.

Finally, in 2018, the United States drafted the National Quantum Initiative Act, which plans to allocate substantial funds for the following developments:

- the US National Institute of Standards and Technology (NIST) of $ 400 billion (80 million per year) for the organization and conduct of scientific events on specified topics;
- the US National Science Foundation (NSF) of $ 250 million (50 million per year) for the creation and development of interdisciplinary research centers for exploratory research and training (Multidisciplinary Centers for Quantum Research and Education);
- the Coordination Office of the United States of $ 200 billion (40 million per year) for project management in the field of quantum technologies.

Further, during the discussion of budget items in the US House of Representatives, the US Department of Energy was allocated an additional $ 625 million ($ 125 million per year) for the creation of five leading research centers (National Quantum Information Science Research Centers).

As a result, the total amount of funding for the implementation of the US national quantum initiative amounted to the US $ 1.275 billion. On December 21, 2018, WE President Donald Trump approved this budget.

The US National Science Foundation (NSF) has two strategic projects planned for the period 2019-2025. The first is to create a "practical" quantum computer (Software-Tailored Architecture for Quantum co-design, STAQ). The main goals of this project were:

- –development of a promising architecture of a quantum computer with 64 and more qubits;
- –providing the required stability and noise immunity of the functioning of quantum computers in real operating conditions;
- –development of quantum algorithms, systems, and applied software for solving scientific and technical problems of dual-use.

The second project, «Enabling Quantum Leap: Convergent Accelerated Discovery Foundries for Quantum Materials Science, Engineering, and Information, Q-AMASE-i», was aimed at creating new samples of quantum materials. The total amount of financing for these projects was USD 25 million.

US Department of Energy 2019-2024 funded 85 promising quantum technology projects totaling the US $ 218 million. Including the project of the National Laboratory «Lawrence Berkeley National Laboratory» (LBNL / Berkeley Lab) to create a special test laboratory (Advanced Quantum Testbed, AQT). At the same time, the Lincoln Laboratory of the Massachusetts Institute of Technology (MIT-Lincoln Laboratory, MIT-LL) was involved to develop a program and testing methodology for various architectures of quantum computers.

Also in 2018, another major US bill, the Quantum Computing Research Act of 2018, was passed to support scientific and technological research for the interests of the US military.

In 2019, the Under Secretary of Defense for Research and Engineering prepared the "Advanced R&D Plan (for the period 2019-2025)" in the following areas:

- creation of new forms of weapons and equipment based on quantum technologies (Q);
- development of promising models and methods for collecting and processing big data (Big Data) based on quantum technologies (Q), methods of artificial intelligence (AI), and machine learning (ML) (national security data sets);
- development of quantum algorithms for solving military-technical problems of analysis and synthesis (including cryptanalysis problems);
- creation of trusted quantum communication systems, including the development of an appropriate component base and communication protocols;
- development of quantum computers for 100 or more logical qubits;
- development of mathematical and software for quantum computers;
- development of promising architectures of quantum systems and networks for performing quantum computations;
- development of models and methods of quantum and post-quantum cryptography, etc. [29, 30].

Starting in 2019, the R&D section of the US defense budget provides for annual funding for fundamental and applied research in the field of quantum technologies. For example, the US Army (feature 0601102A) and the US Navy (feature 0601153N) receive $ 5 million annually for related research.

It is interesting to note that the Defense Budget under Advanced Simulation and Computing has earmarked more than $ 700 million annually for the US Department of Energy, which is significantly higher than the Pentagon's "quantum" budget. This is due to the fundamental nature of the alleged exploratory research in the field of quantum technology.

Note that the number of Multidisciplinary University Research Initiative (MURI) for the needs of the US Department of Defense has grown from 12 projects in 2016 to 60 projects in 2021. One such project is the Tri-Service Quantum Science and Engineering Program (QSEP), an interdisciplinary university project.

Additionally, IARPA and DARPA have undertaken some dual-use R&D projects with the following objectives:

- overcoming the limitations of known quantum systems (Logical Qubits Program) (during 2020–2023);
- effective solution of optimization problems (Quantum Enhanced Optimization Program) (during 2020-2023);
- development of effective quantum cryptanalysis algorithms (Quantum Cryptanalysis) (during 2021-2024) (Table 1 and Table 2), etc. [9–18, 25-27, 31, 32].

Table 1

Assessment of the cryptographic strength of known encryption algorithms

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (up to 2010)	2TDEA, SKIPJACK	*L=1024 N=160*	*k=1024*	*f=160-223*
112 (up to 2030)	3TDEA	*L=2048 N=224*	*k=2048*	*f=224-255*
128 (after 2030)	AES-128	*L=3072 N=256*	*k=3072*	*f=256-383*
192	AES-192	*L=7680 N=384*	*k=7680*	*f=384-511*
256	AES-256	*L=15360 N=512*	*k=15360*	*f=512+*

Table 2

Resources Required for Quantum Solving of Factorization Problems and Key Finding of Known Symmetric Encryption Cryptosystems

Resources for Quantum Factorization and ECDLP						
Factorization			ECDLP			*Classic time*
n	Number of qubits	*Quantum time*	*n*	*Number of qubits*	*Quantum time*	
512	1024	$0.54*10^9$	*110*	*700*	$0.5*10^9$	$6.4*10^{16}$
1024	2048	$4.3*10^9$	*163*	*1000*	$1.6*10^9$	$3.0*10^{24}$
2048	4096	$34*10^9$	*224*	*1300*	$4.0*10^9$	$9.2*10^{33}$
3072	6114	$120*10^9$	*256*	*1500*	$6.0*10^9$	$6.0*10^{38}$
15360	30720	$1.5*10^{13}$	*512*	*2800*	$50*10^9$	$2.1*10^{77}$

Resources for a quantum solution to the problem of finding the key of a symmetric cryptosystem			
k	*Number of qubits*	*Quantum time*	*Classic time*
56	56	$2.1*10^8$	$7.2*10^{16}$
80	80	$8.6*10^{11}$	$1.2*10^{24}$
112	112	$5.7*10^{16}$	$5.2*10^{33}$
128	128	$1.4*10^{19}$	$3.4*10^{38}$
168	168	$1.5*10^{25}$	$3.7*10^{50}$
256	256	$2.7\text{-}10^{38}$	$1.2*10^{77}$

Leading public and private universities were involved to carry out the set R&D. For example, the University of Southern California has become a leader in a consortium of universities and private companies for five-year R&D (2017-2022) of IARPA with a budget of $ 45 million to develop the world's first 100-qubit quantum computer. This consortium also included: Lincoln Laboratory (MIT-LL), California Institute of Technology (Caltech, USA), Harvard University (Harvard, USA), University of California at Berkeley (UC Berkeley, USA), University College London (London, Britain), University of Waterloo (Waterloo, Canada), Saarland University (Saarland, Germany), Tokyo Institute of Technology (Tokyo, Japan), American companies Lockheed Martin and Northrop Grumman. Acceptance of the results of the mentioned R&D will be carried out by representatives of the Ames Research Center (NASA's Ames Research Center) and Texas A&M University (Texas A&M).

In 2021, the budget of the US National Quantum Initiative was revised upward (National Quantum Initiative Supplement to the President's FY 2021 Budget) (see Fig. 2). The total budget for the implementation of the US National Quantum Initiative exceeded the US $ 2.5 billion. At the same time, more than $ 50 million from this budget is planned for the development of quantum algorithms (including quantum cryptanalysis algorithms) (see Fig. 6) in the interests of the intelligence community and the armed forces of the United States and NATO countries [1, 6, 7, 12-18].

Thus, starting in 2018, research and development in the field of quantum technologies in the United States and NATO countries have been under the scrutiny of government and military structures. The strategic objective is to maintain technological leadership in this area in the medium and long term. The large public investment in quantum technology in the United States (over US $ 2.5 billion) is due to the strategic importance of these technologies for national security, including information domination.

Private investment from major USA IT manufacturers and service providers, including Amazon, Google, IBM, Intel, and Microsoft, also contributes to this goal. Other companies such as SpaceX, Lockheed Martin, and Boeing are already putting quantum technology into practice to solve specific technology challenges. In total, investments by private companies in the United States on quantum technologies have approached $ 1 billion per year. At the same time, private investment continues to grow, not only in the United States but also in other countries, for example, in China, Germany, Great Britain, France, Japan, and Singapore.

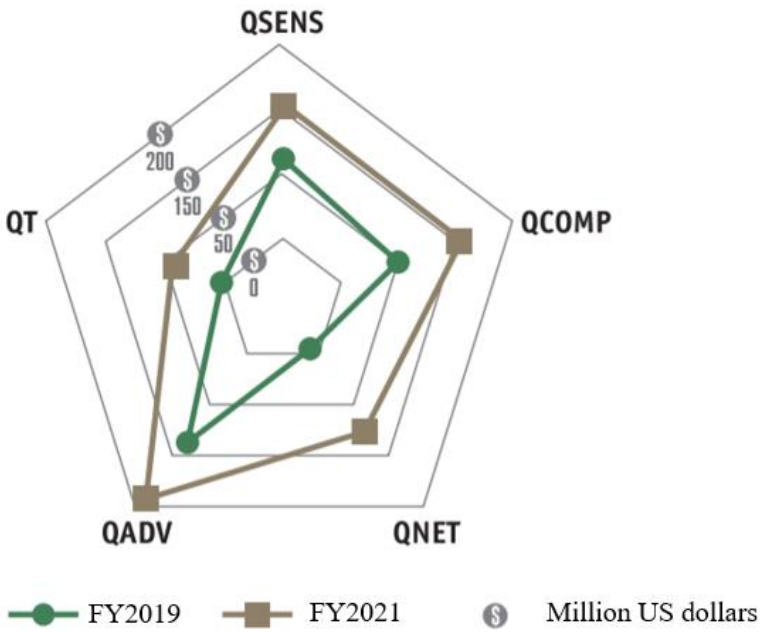

Figure 2: Priority for the development of quantum algorithms in the interests of the US Department of Defense

3. National Quantum Programs

The list of well-known national quantum programs is given in Table 3.

The main goals of national quantum programs are the cooperation of stakeholders in academia and industry to carry out promising dual-use R&D in the field of quantum technologies, as well as to promote the translation of exploratory research into a practical plane. An additional goal is the development of human capital (or resource). Some programs set clear medium-term goals, for example, by 2030 (or earlier) to develop a working industrial prototype of a "practical" quantum computer, as well as to develop scenarios for its use to create an ecosystem of quantum technologies [1, 6, 7, 12-18, 33-35].

The main tasks of the national quantum programs include:

- creation of scientific and technical centers of excellence in the field of quantum technologies;
- organization and conduct of promising dual-use R&D on a given topic;
- providing direct funding for special dual-use projects;
- provision of public investment or start-up capital to enterprises producing new quantum technologies.

The majority of national quantum programs have four main research areas [2-5, 12-18] (see Fig. 3):

- quantum computers and computing;
- quantum communications (near-term perspective).
- quantum cryptanalysis (near-term perspective);
- quantum cryptography.

So, in quantum cryptography [2-7, 9-18] the following key technologies are defined:

- quantum key distribution (QKD) and quantum encryption in fiber-optic communication channels and open space;
- quantum hashing and quantum digital signature;
- quantum cryptanalysis;
- quantum superdense coding of information using "entangled" and "hyper-entangled" particles (one quantum bit (qubit) can carry up to two ordinary bits), which allows increasing the bandwidth of the quantum communication channel;
- coding in systems of quantum information transfer, etc.

Table 3
List of well-known national quantum programs of technologically developed countries of the world*

Country	Name of the national quantum program	Budget and deadlines
USA	National Quantum Initiative (2018)	More than $ 2.5 billion, 2018–2023
China	Quantum technology R&D as a strategic industry in Five Year Plans and “Made in China 2025”	$ 15.3 billion (for the creation of an experimental center), 2020–2025
Germany	Quantum Technologies — From Basic Research to Market (2018)	$ 2.4 billion, 2018–2023
United Kingdom	National Quantum Technologies Programme (2013)	$ 1.23 billion, 2013–2022
France	National Strategy for Quantum Technologies (2021)	$ 1.2 billion, 2021–2024
India	National Mission on Quantum Technologies & Applications (2020)	$ 1.08 billion, 2020–2025
Netherlands	National Agenda for Quantum Technology: Quantum Delta NL (2019)	$ 850 million, 2019–2024
Russia	Quantum Technology Development Roadmap (2019)	$ 691 million (RUB 51.1 billion), 2019–2024
Israel	National Program for Quantum Science and Technology (2019)	$ 380 million, 2019–2025
Japan	Quantum Technology Innovation Strategy (2020)	$ 206 million, 2020–2025
Other EU countries	Quantum Technologies Flagship (2018)	$ 181 million, 2018–2021
Canada	Quantum Canada Strategy (in development since 2016)	$ 149.7 million, 2017–2022
Australia	«Growing Australia’s Quantum Technology Industry» (2020)	$ 98.6 million, 2020–2024
Singapore	Quantum Engineering Program (2018)	$ 90.9 million, 2018–2025
South Korea	Quantum Computing Technology Development Project (2019)	$ 40.9 million, 2019–2024

* Source: https://cifar.ca/cifarnews/2021/04/07/a-quantum-revolution-report-on-global-policies-for-quantum-technology/.

Note that in the problems of quantum cryptanalysis, it is taken into account that Shor's algorithm provides exponential acceleration of solving factorization problems, discrete logarithm (DLP), and discrete logarithm with an elliptic curve (ECDLP) (see Table 4), which are widely used in cryptographic applications in cyberspace. For example, the well-known protocols TLS, SSH, IPSec, etc. rely on Diffie-Hellman key agreements (which depend on the strength of DLP or ECDLP), digital signatures (DSA, ECDSA, or RSA-PSS signatures), or public key encryption (El Gamal, RSA-OAEP). As a result, Shor's quantum algorithm can potentially break most protocols and asymmetric encryption schemes (public-key cryptography) [8–18].

In general, all known quantum algorithms (see Table 5) can be conditionally divided into two groups: providing exponential gain (for example, Shor's algorithm) and providing quadratic gain (for example, Grover's algorithm) [1-6, 8-11]. Particular attention is paid to Shor's quantum algorithm and other polynomial algorithms capable of solving cryptanalysis problems with the required reliability and laboriousness in polynomial time [8-19].

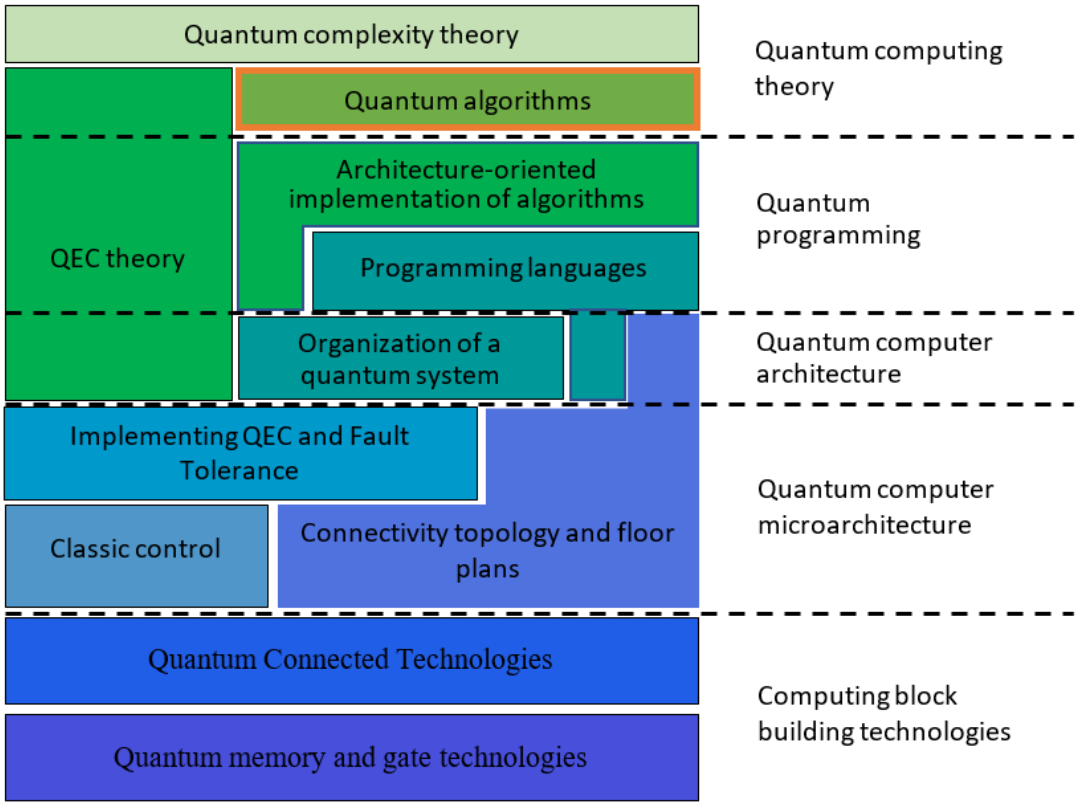

Figure 3: The main directions of development of quantum technologies in national quantum programs

Table 4
Estimate for the complexity of the decomposition of a large integer into prime factors

Classic exascale computer (1018 op / s) versus a quantum computer in the megahertz range (1 million op / s)			
Number of decimal places, k	$k = 250$	$k = 500$	$k = 1000$
The complexity of the classical algorithm	200 h	5 million years	$4*10^{17}$ years
The complexity of the quantum algorithm, s	4 sec	18 sec	84 sec

Also quite interesting is the quantum Grover search algorithm, which allows you to speed up algorithms for solving some problems of the NP class - those problems for which a better algorithm than direct search is unknown. For example, to speed up the search for a key to cryptosystems such as the well-known DES algorithm. Also interesting is the quantum Fourier transform, which allows you to solve the problems of calculating the discrete logarithm and factorization and "hack" with the help of a quantum computer many cryptosystems, for example, RSA.

According to the reports of the American National Standards Institute NIST, of the crypto algorithms used in the USA and NATO countries, AES, SHA-2, SHA-3, RSA, ECDSA, ECDH, and DSA are susceptible to the quantum threat. It is noted that quantum computers allow computing at completely different speeds than modern 5th generation Supercomputers, which makes the problem of decrypting ciphertext a real threat.

Table 5

Basic quantum algorithms for solving cryptanalysis problems

Full brute-force search of encryption algorithms	Grover's Algorithm
Slide attack, discrimination method for CBC-MAC, PMAC, GMAC, GCM, OCB, Feistel networks	Simon's algorithm
Determination of the key of the Evan - Mansoor scheme, FX-constructions, generalized Feistel networks	Combination of Grover's and Simon's algorithms
Matching Method, Meet-in-the-Middle Attack	Random walks, a combination of Grover's and Simon's algorithms
Factorization and discrete logarithm	Shor's algorithm, Ecker's algorithm
Search for linear and difference relations, key recovery from the difference ratio	Bernstein - Vazirani, Grover, and Simon algorithms
Special methods	Grover's Algorithm
Search for collisions, multi-collision	Random walks, Grover's algorithm, etc.
SLN solution, algebraic attack AES, Trivium, SHA-3, MRKS	Harrow, Hassidim, Lloyd

Thus, from the point of view of quantum computing, all cryptography can be conditionally divided into quantum-safe and quantum-unsafe (see Table 6). Algorithms and cryptosystems of symmetric encryption (including AES or GOST R 34.12–2015), but with a key length increased at least twice (how long will be sufficient is still unknown), can be classified as quantum-safe. Asymmetric encryption algorithms and cryptosystems based on the complexity of the factorization of integers (for example, RSA) or discrete logarithm (for example, El Gamal or elliptic curves) can be classified as quantum insecure.

Table 6

Estimates of crypto-resistance of the most common cryptographic algorithms in the United States and NATO countries

Cryptoscheme	Key size, bits	Effective resistance, bits	Required number of logical qubits	Required number of physical qubits	Time estimate
AES	128	128	2953	$4{,}61*10^6$	$2{,}61*10^{12}$ years
	192	192	4449	$1{,}68*10^7$	$1{,}97*10^{22}$ years
	256	256	6681	$3{,}36*10^7$	$2{,}29*10^{32}$ years
RSA	1024	80	2290	$2{,}56*10^6$	3,58 h
	2048	112	4338	$6{,}2*10^6$	28,63 h
	4096	128	8434	$1{,}47*10^7$	229 h
ECDLP (NIST P-256, NIST P-386, NIST P-521)	256	128	2330	$3{,}21*10^6$	10,5 h
	356	192	3484	$5{,}01*10^6$	37,67 h
	512	256	4719	$7{,}81*10^6$	35 h
SHA-256	N/A	72	2403	$2{,}23*10^6$	1,8*104 years

In addition, quantum computers pose a real threat to the security of most well-known blockchain platforms, which widely use asymmetric cryptographic algorithms to create a public-private key pair and an address, which is obtained using hash operations and a public key checksum.

As a result, in some countries, mainly in the USA and the European Union, the transition to the use of stable quantum cryptography is already planned. For example, the aforementioned NIST is in the

process of developing quantum cryptography standards, and the NSA recommends its suppliers to implement SHA-384 instead of SHA-256.

4. Security Threat Model

Considering the above, we propose the following model of information security threats to the critical information infrastructure (CII) of the Russian Federation [6, 21, 22, 34-36].

- Some foreign countries are building up the potential of quantum technologies for carrying out information and technical impacts on the CII of the Russian Federation for military-political purposes. At the same time, there is an increase in the activities of foreign technical intelligence, using the capabilities of quantum cryptanalysis of asymmetric and symmetric encryption schemes based on quantum algorithms of Shor, Grover, Simon, and others to conduct technical intelligence about Russian government agencies, scientific organizations and enterprises of the military-industrial complex.
- Application of quantum technologies for military-political purposes, including for the implementation of actions contrary to international law, aimed at undermining the sovereignty, political and social stability, territorial integrity of the Russian Federation and its allies, and posing a threat to international peace, global and regional security.
- The growth of quantum crypto attacks on CII objects, the strengthening of the intelligence activities of foreign states about the Russian Federation, as well as the growing threats of the use of quantum technologies to damage the sovereignty, territorial integrity, political and social stability of the Russian Federation.
- An increase in the number of crypto attacks on blockchain platforms of leading financial institutions and organizations of the Russian Federation, using cryptographic algorithms to create a pair of public and private keys and an address, which is obtained using hashing operations and a public key checksum. In this case, disclosing only one address is not a big risk. However, disclosing the address and the public key used in the transaction is potentially dangerous, since, if there is sufficient progress in quantum computing, it will allow the private key to be obtained.
- Insufficient level of development of competitive domestic quantum technologies and their use for the production of products and services. The high degree of dependence of the domestic industry on foreign information technologies in terms of the electronic component base, software, computers, and communications, which determines the dependence of the socio-economic development of the Russian Federation on the geopolitical interests of foreign countries [21, 23, 24, 28].
- Insufficient efficiency of scientific research in the field of quantum technologies aimed at creating promising quantum computers, low level of implementation of domestic developments, and insufficient staffing in the field of information security, as well as low awareness of citizens in matters of personal information security. Measures to ensure the security of information infrastructure, including its integrity, availability, and sustainable operation, using domestic information technologies and domestic products often do not have an integrated framework.
- The desire of individual states to use technological superiority in quantum technologies to dominate the information space.

For the timely prevention of the listed security threats, in 2019 Russia adopted a "Roadmap for the development of quantum technologies" (hereinafter referred to as the Roadmap) [20]. Its main goal is to achieve, in the medium and long term, practically significant scientific, technical and practical results of the world level in some areas.

- Quantum computers and computing. Quantum computers and simulators are computing systems that use quantum phenomena to solve problems. Devices created based on quantum computing can many times exceed the capabilities of classical computers in solving problems of cryptanalysis, modeling complex systems, as well as machine learning and artificial intelligence. With the development of existing quantum computers, the emergence of the first applied results can be expected in the direction of accelerating machine learning problems and modeling new promising materials. The most promising platforms in the world are the following: superconducting chains, neutral atoms, and ions in traps. According to the QTRL classification, the development of

companies in the world at the moment corresponds to QTRL levels 4-5. That is, the problem of implementing quantum error correction codes has not yet been solved in the computational data systems of companies and practically significant algorithms cannot be fully implemented on them (including Shor's algorithm). To date, prototypes of quantum computers with 2 qubits (according to the roadmap for the development of quantum information processing technologies of the Advanced Research Foundation, 2–10 qubits) and quantum simulators with 10–20 qubits have been implemented in the Russian Federation. This corresponds to a QTRL level 3-4.

- Quantum communications. Technologies aimed at eliminating threats to information security, including from quantum computers, include using the properties of quantum systems to transfer keys. The main technology here is quantum key distribution (QKD). The main advantage of the QKD is the security of information guaranteed by the laws of physics. The global availability level is TRL 924 both in point-to-point solutions and in networks with a trusted node. QKD equipment for networks with untrusted nodes is at the laboratory testing level. Today, the level of readiness of domestic point-to-point solutions can be estimated as TRL 8, while in terms of quantum networks based on trusted nodes, domestic developments of quantum networks are far behind the level of China and the EU: TRL 6 versus TRL 9.
- Quantum sensors and metrology. Quantum sensors are high-precision measuring instruments based on quantum effects. It is expected that quantum sensors will have the high spatial and temporal resolution. This will improve the measurement accuracy in comparison with existing classical sensors. And the use of the properties of superposition, entanglement, and compression of quantum states, in turn, will provide in the long term the maximum possible measurement sensitivity by overcoming the standard quantum limit. The high degree of control over the state of individual microscopic systems, provided by quantum technologies, makes it possible to create quantum sensors with high sensitivity. The development of technologies for a variety of new generation sensors can give a powerful impetus in several areas at once: defense and security, navigation (space, unmanned vehicles), construction, mining and exploration, medical diagnostics/therapy, Industry 4.0, general assessment of the level of readiness of quantum technologies. sensors in the world (TRL 3–9) and in the Russian Federation (TRL 1–5).

A prerequisite for a breakthrough in the field of quantum technologies is the support of research and the launch of infrastructure projects on a national scale. The total budget for the implementation of the Roadmap (for 2019-2024) amounted to 51.1 billion rubles, including extrabudgetary funding of 8.7 billion rubles.

The main tasks of the Roadmap are:

- comprehensive support for breakthrough scientific and technological projects aimed at the development of quantum technologies;
- consolidation of the scientific and technological community in the framework of the creation of projects of national and global scale;
- the creation of an innovation ecosystem in Russia and the creation of conditions for the transition of quantum developments from laboratories to the industrial sector, as well as the formation of an appropriate business community;
- organization of cooperation between research departments and potential consumers of quantum technologies from key industries;
- development of human resources in the field of quantum technologies by introducing new types of educational programs at all levels;
- carrying out a set of organizational measures aimed at reducing bureaucratic friction.

Note that the Roadmap is fully consistent with the "Strategy for Scientific and Technological Development of the Russian Federation (SSTD)", as well as the "Strategy for the Development of the Information Society of the Russian Federation (SDIO)".

It is significant that the support of all three major sub-technologies of quantum technologies is critical for national security and ensuring the digital sovereignty of the Russian Federation. The role of quantum computing sub-technology is especially important for state security; the effects of its use are quite large. There is also a risk of restricting access to products from foreign manufacturers in this area.

And from the point of view of technological maturity, the closest to entering the market is the technology of quantum communications. The Roadmap emphasizes that in this area of Russia it is required to have its technical solutions with the maximum degree of localization of production (both end devices and components) to eliminate the risk of introducing destructive hardware and software (undeclared capabilities, NDV) into hardware and software, and, as a consequence, access to protected information.

5. Conclusion

Some Western states, primarily the United States and its NATO allies, seek to use technological superiority in the field of artificial intelligence (AI), quantum technologies (Q), collection and processing of big data (Big Data + ETL), high and ultra-high performance to dominate the information space. At the same time, the growing concern is caused by the desire of these states to use information technologies for military-political purposes, including for the implementation of actions aimed at undermining the sovereignty, political and social stability, and the territorial integrity of the Russian Federation.

The US National Quantum Initiative (2018) aims to maintain technological leadership in the field of quantum technologies in the medium and long term. For this, starting in 2019, a series of (more than 80) dual-use R&D projects have been launched under the control of the NSA, IERPA, DARPA, NFS, the US Department of Energy, etc.

The US Department of Defense approved and is implementing the Plan for Advanced Research and Development on Quantum Technologies for the period 2019-2024 in some areas, including the development of promising models and methods for collecting and processing big data based on quantum technologies, artificial intelligence methods, and machine learning, quantum algorithms for solving military-technical problems of analysis and synthesis (including cryptanalysis problems), creating trusted quantum communication systems, models and methods of quantum cryptography. The total US budget for the development of quantum technologies in 2021 exceeded $ 2.5 billion.

To prevent possible security threats, in 2019 Russia adopted a Roadmap for the development of quantum technologies. The total budget for its implementation (for 2019-2024) amounted to 51.1 billion rubles. ($ 691 million). The main goal of the Roadmap is to achieve, in the medium and long term, practically significant scientific, technical and practical world-class results in the following areas: quantum computers and computing, quantum communications, quantum sensors, and metrology, quantum and post-quantum cryptography. At the same time, in quantum cryptography, a special place is given to the effective solution of quantum cryptanalysis problems based on the promising quantum algorithms of Shor, Grover, Simon, etc. Thus, Shor's algorithm provides an exponential acceleration of the solution of factorization problems, discrete logarithm (DLP), and discrete logarithm with an elliptic curve (ECDLP). The mentioned tasks are widely used in cryptographic applications TLS, SSH or IPSec of Internet / Intranet and IIoT / IoT networks, communication protocols based on Diffie-Hellman key agreements (depending on DLP or ECDLP strength), in digital signature algorithms (DSA, ECDSA, RSA-PSS), public key encryption algorithms (El Gamal, RSA-OAEP), etc. In other words, Shor's quantum algorithm is capable of breaking the listed algorithms, and with them all public-key cryptography mechanisms deployed in cyberspace.

6. Acknowledgments

The article was prepared based on the results of research carried out with the support of the RFBR grant (No. 20-04-60080).

7. References

[1] D. V. Denisenko, G. B. Marshalko, M. V. Nikitenkova, V. I. Rudskoj, V. A. Shishkin, Ocenka slozhnosti realizacii algoritma Grovera dlya perebora klyuchej algoritmov blochnogo shifrovaniya GOST R 34.12-2015 [Estimation of the complexity of the Grover algorithm implementation for

enumerating keys of block cipher algorithms GOST R 34.12-2015], Zhurnal e`ksperimental`noj i teoreticheskoj Fiziki [Journal of Experimental and Theoretical Physics], Kapitza Institute for Physical Problems, RAS, Moscow, 2019, volume 155, 4, pp. 645–653. doi: 10.1134/S0044451019040072.

[2] A.V. Korol`kov, O nekotory`x prikladny`x aspektax kvantovoj kriptografii v kontekste razvitiya kvantovy`x vy`chislenij i poyavleniya kvantovy`x komp`yuterov [A.V. Korolkov On some applied aspects of quantum cryptography in the context of the development of quantum computing and the emergence of quantum computers], Voprosy` kiberbezopasnosti [Issues of Cybersecurity], Moscow, 2015, 1(9), pp. 6 - 13. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_09_02.pdf.

[3] P. G. Klyucharev, Algoritmicheskoe i programmnoe obespechenie dlya modelirovaniya kvantovogo komp`yutera [Algorithmic and software for modeling a quantum computer], Avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata texnicheskix nauk [Abstract of dissertation for the degree of candidate of technical sciences], Bauman Moscow State Technical University, Moscow, 2009, 18 pages.

[4] E. A. Matveev, Primenenie kvantovomexanicheskix e`ffektov v sistemax zashhity` informacii [Application of quantum-mechanical effects in information security systems], Dissertaciya na soiskanie kandidata fiziko-matematicheskix nauk [Dissertation for a candidate of physical and mathematical sciences], Scientific and technical enterprise "Cryptosoft", Penza, 2019, 157 pages.

[5] A. A. Moldovyan, N. A. Moldovyan, Novy`e formy` zadaniya skry`toj zadachi diskretnogo logarifmirovaniya [New forms of specifying the hidden discrete logarithm problem], Trudy` SPIIRAN [Proceedings of SPIIRAS], St. Petersburg, 2019, 18(2), pp. 504-529. doi:10.15622/sp.18.2.504-529.

[6] A. S. Petrenko, A. M. Romanchenko, Perspektivny`j metod kriptoanaliza na osnove algoritma Shora [A promising method of cryptanalysis based on the shore algorithm], Zashhita informacii. Inside, Izdatel`stvo Afina [Information security. Inside, Athena Publishing House], St. Petersburg, 2020, 2, pp. 17-23.

[7] P. A. Pravil`shhikov, Kvantovy`j parallelizm i reshenie uravnenij v zadachax upravleniya na baze novoj modeli vy`chislenij [Quantum Parallelism and Solution of Equations in Control Problems Based on a New Computation Model], Institut problem upravleniya im. V.A. Trapeznikova RAN [V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences], Moscow, 2014, pp. 7335-7351. URL: https://www.elibrary.ru/item.asp?id=22231427.

[8] A. S. Xolevo, Matematicheskie osnovy` kvantovoj informatiki [Mathematical Foundations of Quantum Informatics], Lekcionny`e kursy` Nauchno-obrazovatel`nogo centra, Matematicheskij institut im. V.A. Steklova Rossijskoj akademii nauk [Lecture Courses of the Scientific and Educational Center, Steklov Mathematical Institute of Russian Academy of Sciences], Moscow, 2018, 30, pp. 3-117. URL: https://doi.org/10.4213/lkn30.

[9] A. V. Cheremushkin, Kriptograficheskie protokoly`: osnovny`e svojstva i uyazvimosti [Cryptographic Protocols: Basic Properties and Vulnerabilities], Prikladnaya diskretnaya matematika, Institut kriptografii, svyazi i informatiki [Applied Discrete Mathematics, Institute of Cryptography, Communications and Informatics], Moscow, 2009, appendix to No. 2, pp. 115–150. URL: http://mi.mathnet.ru/pdm141.

[10] Klod E`. Shennon, Raboty` po teorii informacii i kibernetike, Perevod s angl., S predisloviem A. N. Kolmogorova; Pod redakciej R. L. Dobrushina i O. B. Lupanova [Claude E. Shannon, Works on Information Theory and Cybernetics, Translated from English, with a foreword by A. N. Kolmogorov; Edited by R. L. Dobrushin and O. B. Lupanov], Izdatel`stvo inostrannoj literatury` [Foreign Literature Publishing House], Moscow, 1963, 829 pages.

[11] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Foundations of Computer Science, 1994, 10, 134 pages.

[12] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society A, 1985, 400 (1818), pp. 97-117.

[13] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London A, 1992, 439 (1907), pp. 553-558.

[14] D. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 1976, volume 22, issue 6.

[15] R. Feynman, Simulating physics with computers, Internat. J. Theoret. Phys., 1982, 21, pp. 467 - 488.
[16] L. K. Grover, A fast quantum mechanical algorithm for database search, In Proceedings of the twenty-eighth, annual ACM symposium on Theory of computing, ACM, 1996, pp. 212 – 219.
[17] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing, 1997, 26, pp. 1484 – 1509.
[18] D. R. Simon, On the power of quantum computation, SFCS '94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994, 116 – 123.
[19] S. P. Jordan, Y. Liu, Quantum Cryptanalysis: Shor, Grover, and Beyond, IEEE Security & Privacy, 2018, volume 16, 5, pp. 14-21. doi: 10.1109/MSP.2018.3761719.
[20] Dorozhnaya karta razvitiya «skvoznoj» cifrovoj texnologii «Kvantovy`e texnologii» [Roadmap for the development of "end-to-end" digital technology "Quantum technologies"], Ministerstvo cifrovogo razvitiya, svyazi i massovy`x kommunikacij Rossijskoj Federacii [Ministry of Digital Development, Communications and Mass Media of the Russian Federation], Moscow, 2019, 26 pages. URL: https://digital.gov.ru/ru/documents/6650.
[21] A. A. Petrenko, S. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, Methodological recommendations for the cyber risks management, CEUR Workshop Proceedings, volume 2914, (2021), pp. 234-247. URL: http://ceur-ws.org/Vol-2914/paper20.pdf.
[22] A. S. Petrenko, S. A. Petrenko, K. A. Makoveichuk, P. V. Chetyrbok, Protection model of PCS of subway from attacks type «wanna cry», «petya» and «bad rabbit» IoT, Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018, 2018-January, pp. 945-949. doi: 10.1109/EIConRus.2018.8317245.
[23] A. V. Barabanov, A. S. Markov, V. L. Tsirlov, Methodological framework for analysis and synthesis of a set of secure software development controls, Journal of Theoretical and Applied Information Technology, volume 88(1) (2016), pp. 77-88. URL: http://www.jatit.org/volumes/Vol88No1/9Vol88No1.pdf.
[24] A. V. Barabanov, A. S. Markov, V. L. Tsirlov, Statistics of software vulnerability detection in certification testing, Journal of Physics: Conference Series, volume 1015(4) (2018) 042033. doi: 10.1088/1742-6596/1015/4/042033.
[25] C. Wang, H.-N. Yao, B.-N. Wang, F. Hu, X.-M. Ji, H.-G. Zhang, Progress in Quantum Computing Cryptography Attacks, Jisuanji Xuebao, 2020, volume 43, 9, pp. 1691 - 1707. doi: 10.11897/SP.J.1016.2020.01691.
[26] D. Denisenko, Quantum Differential Cryptanalysis. Journal of Computer Virology and Hacking Techniques, 2021. doi: 10.1007/s11416-021-00395-x
[27] G. Khalimov, S. Khalimova, Y. Kotukh, Encryption Scheme Based on the Automorphism Group of the Ree Function Field, 7th International Conference on Internet of Things: Systems, Management, and Security, 2020, volume 7. doi: 10.1109/IOTSMS52051.2020.9340192
[28] H. Krachunov, T. G. Sheremet, Parameters for estimate the digital national economy in the EAEU Member Countries. CEUR Workshop Proceedings, volume 2834 (2021), pp. 219-230. URL: http://ceur-ws.org/Vol-2834/Paper19.pdf.
[29] I. Gorbenko, V. Ponomar, Examining a Possibility to Use and the Benefits of Post-Quantum Algorithms Dependent on the Conditions of Their Application, Eastern-European Journal of Enterprise Technologies, 2017, volume 2, 9(86), pp. 21 - 32. doi: 10.15587/1729-4061.2017.96321.
[30] J. Bobrysheva, S. Zapechnikov, Post-Quantum Security of Messaging Protocols: Analysis of Double Ratcheting Algorithm, Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, 2020, pp. 2041-2044. doi: 10.1109/EIConRus49466.2020.9039075.
[31] M. Lutsenko, A. Kuznetsov, A. Kiian, T. Kuznetsova, O. Smirnov, Biometric Cryptosystems: Overview, State-Of-The-Art and Perspective Directions, Lecture Notes in Networks and Systems, 2021, volume 152, pp. 66-84. doi: 10.1007/978-3-030-58359-0_5.
[32] N. Abdinurova, B. Kynabay, Revealing Encryption Algorithm for Integrating with Quantum Technologies by Using Cryptanalysis, 14th International Conference on Electronics Computer and Computation, 2019, volume 14. doi: 10.1109/ICECCO.2018.8634689.

[33] Ovcharova, S., Krachunov, H. Innovation activities in entrepreneurial firms: The case of Bulgaria. Entrepreneurship in the Balkans: Diversity, Support and Prospects, 2013, pp. 37-55. DOI: 10.1007/978-3-642-36577-5_3.
[34] S. A. Petrenko, A. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, Development of a Cyber-Resistant Platform for the Internet of Things Based on Dynamic Control Technology. In: Singh P.K., Veselov G., Vyatkin V., Pljonkin A., Dodero J.M., Kumar Y. (eds) Futuristic Trends in Network and Communication Technologies. FTNCT 2020. Communications in Computer and Information Science, volume 1395 (2021), pp. 144-154. Springer, Singapore. URL: https://doi.org/10.1007/978-981-16-1480-4_13.
[35] S. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, Concept of cyber immunity of industry 4.0, CEUR Workshop Proceedings, volume 2603, (2019), pp. 93-99. URL: http://ceur-ws.org/Vol-2603/paper20.pdf.
[36] S. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, New Methods of the Cybersecurity Knowledge Management Analytics. In: Sukhomlin V., Zubareva E. (eds) Convergent Cognitive Information Technologies. Convergent 2018. Communications in Computer and Information Science, volume 1140 (2020), pp. 296-310. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-37436-5_27.