Computing, Telecommunication and Control, 2024, Vol. 17, No. 4, Pp. 16–34.
Информатика, телекоммуникации и управление. 2024. Том 17, № 4. С. 16–34.

Review article
DOI: https://doi.org/10.18721/JCSTCS.17402
UDC 004.03

NEW TYPES OF THREATS AND ASSESSMENT OF QUANTUM STABILITY OF INFORMATION SYSTEMS IN THE FIELD OF FOREIGN TRADE ACTIVITY

V.Yu. Skiba[1,2] ✉ , *S.A. Petrenko*[1], *A.A. Murzina*[1], *K.R. Popova*[1]

[1] Sirius University of Science and Technology, Sirius Federal Territory, Krasnodar region, Russian Federation;

[2] Bauman Moscow State Technical University, Moscow, Russian Federation

✉ vskiba69@mail.ru

Abstract. The introduction of technologies for performing customs operations through information systems without the direct participation of customs officials, as well as the evolving political situation and the adoption of sanctions against the Russian Federation by the United Stated and its allied states, significantly increase the importance of ensuring information security of customs authorities. The results obtained in the field of quantum informatics clearly demonstrate the high technological potential of quantum technologies. A cryptanalytically relevant or significant quantum computer can threaten civil and military communication systems, including information systems of customs authorities and individual participants in foreign trade activity. In this situation, there is a growing need to prepare in advance for possible collisions and take all necessary measures to protect against the mentioned quantum threat, including developing a plan for relevant priority measures.

Keywords: foreign trade activity, information security, quantum security threat, quantum stability, critical information infrastructure

Acknowledgements: The project “Technologies for countering previously unknown quantum cyber threats” was selected for support within the framework of event 2.3 of the state program of the federal territory Sirius “Scientific and technological development of the federal territory Sirius” (application registration No. FCS-2024-2.3-VY-1160-5744, leading scientist – Petrenko S.A., PhD).

Citation: Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R. New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity. Computing, Telecommunications and Control, 2024, Vol. 17, No. 4, Pp. 16–34. DOI: 10.18721/JCSTCS.17402

Обзорная статья
DOI: https://doi.org/10.18721/JCSTCS.17402
УДК 004.03

НОВЫЕ ВИДЫ УГРОЗ И ОЦЕНКА КВАНТОВОЙ УСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В СФЕРЕ ВНЕШНЕЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

В.Ю. Скиба[1,2] ✉ , *С.А. Петренко*[1], *А.А. Мурзина*[1], *К.Р. Попова*[1]

[1] Научно-технологический университет «Сириус», федеральная территория «Сириус», Краснодарский край, Российская Федерация;

[2] Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва, Российская Федерация

✉ vskiba69@mail.ru

Аннотация. Внедрение технологий совершения таможенных операций посредством информационной системы без непосредственного участия должностных лиц таможенных органов, а также складывающаяся геополитическая обстановка и принятие США и примкнувшими к ним государствами санкций в отношении Российской Федерации существенным образом повышают значимость обеспечения информационной безопасности таможенных органов. Полученные результаты в области квантовой информатики наглядно показывают высокий технологический потенциал квантовых технологий. Криптоаналитически релевантный или значимый квантовый компьютер может поставить под угрозу системы гражданской и военной связи, в том числе информационных систем таможенных органов и отдельных участников внешнеэкономической деятельности. В этой ситуации назревает необходимость заранее готовиться к возможным коллизиям и выполнять все необходимые мероприятия по защите от упомянутой квантовой угрозы, в том числе разработать план соответствующих первоочередных мероприятий.

Ключевые слова: внешнеэкономическая деятельность, информационная безопасность, квантовая угроза безопасности, квантовая устойчивость, критическая информационная инфраструктура

Финансирование: Проект «Технологии противодействия ранее неизвестным квантовым киберугрозам» был отобран для поддержки в рамках мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории “Сириус”» (регистрационный номер заявки ФТС-2024-2.3-VY-1160-5744, ведущий ученый – д.т.н. Петренко С.А.).

Для цитирования: Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R. New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity // Computing, Telecommunications and Control. 2024. Т. 17, № 4. С. 16–34. DOI: 10.18721/JCSTCS.17402

Introduction

One of the key goals of the creation of the Eurasian Economic Union (EAEU) is “comprehensive modernisation and improving competitiveness of national economies within the framework of the global economy”[1]. The creation of competitive conditions directly depends on the reduction of time costs on the route of goods from the manufacturer to the end consumer [1].

The rate of technological change is constantly increasing, which leads to the need to master new skills and knowledge that allow taking into account such factors as instability, uncertainty, complexity

[1] Treaty on the Eurasian Economic Union, Available: https://docs.eaeunion.org/ru-ru/Pages/DisplayDocument.aspx?s=bef9c798-3978-42f3-9ef2-d0fb3d53b75f&w=632c7868-4ee2-4b21-bc64-1995328e6ef3&l=540294ae-c3c9-4511-9bf8-aaf5d6e0d169&EntityID=3610 (Accessed: 28.01.2025)

and ambiguity in the economic models used. The concept of economic development in the context of VUCA (volatility, uncertainty, complexity and ambiguity) conditions is becoming increasingly popular [2], which has a direct impact on the processes of foreign trade activities (FTA) management.

In these conditions, FTA acquires new specifics, which was proposed in [3] to consider from the standpoint of reducing the time costs of information and logistics operations by eliminating "false disagreements" by creating services for implementing trade operations in the format of smart contracts; for forming indicators that directly characterize the integrative aspects of trade transactions within FTA.

Information systems that directly support FTA have begun to actively develop in the direction of creating platform solutions that involve the implementation of smart contracts and blockchain technologies.

In the context of growing volumes of cross-border trade, the Federal Customs Service of Russian Federation was one of the first customs services in the world to take a course on reducing the time it takes to complete customs formalities through the digitalization of its activities and the introduction of innovative technologies for interaction with all participants involved in the process of international movement of goods [4]. In the current conditions, there was an urgent need to develop and implement fundamentally new approaches, technologies and means of performing customs operations through information systems and information and communication technologies without the participation of customs officials, i.e. in automatic mode.

At the same time, the global information space (GIS) and its main component – the Internet – is used and will be used in the foreseeable future in the interests of the functioning of critical infrastructure facilities of customs authorities and individual participants in FTA, expanding citizens' access to information. On the other hand, it is already being used by criminal structures, international terrorist organizations and unfriendly states to disrupt the functioning of these facilities and create centers of social tension [5].

The results obtained in the field of quantum information science clearly demonstrate the high technological potential of quantum technologies. At the same time, it becomes clear that a cryptanalytically relevant or significant quantum computer could threaten civil and military communications systems and undermine the combat capability of strategic control and management systems of the Russian Federation's critical information infrastructure [6], including critical information infrastructure facilities of customs authorities and individual participants in FTA.

In these conditions, the relevance of conducting research in the field of quantum technologies and information security, the creation of safe quantum-resistant ecosystems and platforms for conducting FTA is beyond doubt.

GIS and modern threats to international information security

It is necessary to conduct a permanent detailed analysis of the current situation in the GIS, primarily an analysis of the quantity and quality of threats from states, criminals and terrorists using information and communication technologies for destructive purposes. It is also necessary to constantly clarify and classify threats to international information security (IIS), make a detailed assessment of these threats, clarify plans and the format of activities to counter threats to the IIS for the future.

The main basic concepts of IIS, the classification of IIS threats, their types and mechanisms (or channels) for their implementation are defined in [6] and subsequently clarified[2,3] in a series of works devoted to modern IIS threats. It should be noted that with the adoption of sanctions against the Russian Federation by the United States and its allied states, the number of attempts to violate the information security of various critical information infrastructure facilities, including customs authorities, has increased significantly.

[2] Updated concept of the convention of the United Nations on ensuring international information security, Available: http://www.scrf.gov.ru/security/information/Inf_conc/ (Accessed: 29.01.2025)

[3] Decree of the President of the Russian Federation on approval of the Fundamentals of the state policy of the Russian Federation in the field of international information security, Available: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=602148302 (Accessed: 29.01.2025)

Over the past decades, the scale of IIS threats has increased significantly under the influence of such a complex and contradictory phenomenon as globalization. On the one hand, in the context of globalization, the interdependence of states has increased sharply and conflicts in the GIS seriously threaten global security and stability. On the other hand, by deepening the unevenness of economic development of states, globalization creates a fertile ground for the accumulation of crisis potential in many countries of the world. It is on this basis that new types of IIS threats arise and grow, various new actors of the GIS appear, who have made violence and lawlessness their weapon in it [5].

Over the past three decades, so many threats to information security have emerged that it would seem that there is no room for new ones. Examples of the ingenuity and resourcefulness of manufacturers and developers of new means of conducting cyberattacks and hostile use of content (new mechanisms of information-technical and/or information-humanitarian influence) and, accordingly, the emergence of new threats [5].

Since 2022, many Russian services have been subjected to cyberattacks: Gosuslugi – the Unified Portal of State and Municipal Services (Functions), websites of Russian banks, courts, media, federal companies, electronic document management systems, as well as Android-based equipment. Over the past two years, there have been large-scale leaks of personal data of Russians. In the spring of 2024, on the eve of the admissions campaign, university websites were attacked, as well as TV channels, where the broadcast of the Victory Parade was interrupted.

It is now clear that cyber operations against transport infrastructure, power grids, dams, chemical plants, nuclear power plants, customs authorities, and other critical infrastructures are technically possible. Such operations can have far-reaching consequences, causing significant damage and large numbers of civilian casualties [5].

In accordance with the passport of the national program "Digital Economy of the Russian Federation"[4], ensuring the integral, sustainable and secure functioning of critical information infrastructure and services for the transmission, processing and storage of large volumes of data in the context of the growth of both classical and previously unknown (and, accordingly, poorly studied) security threats is one of the key goals of the "Information Security" project.

In the current geopolitical situation and in accordance with the Concept of ensuring information security of customs authorities, the priority areas for ensuring information security and technical protection of information of customs authorities are:

- ensuring resistance to deliberate destructive impacts on the information and telecommunications infrastructure of customs authorities;
- ensuring trust in the processes implemented (including without human participation) by automated information systems of customs authorities and the generated electronic documents;
- unconditional compliance with the requirements for ensuring information security at all stages of the creation, development, operation, use and decommissioning of components of the information and telecommunications infrastructure of customs authorities.

At the same time, the destructive impact is exerted not only on the information systems of customs authorities, but also on the information systems of participants in FTA [7] and other interested parties, information interaction with whom is ensured in accordance with the legislation of the EAEU and the Russian Federation.

There are a number of IIS threats arising within the framework of the activities of international (regional) economic organizations. Thus, in the scheme of exchanging electronic documents during cross-border interaction of government bodies of the EAEU member states with each other and with the Eurasian Economic Commission with the participation of a trusted third party, collisions arise. They are associated with the emergence of a situation in which the subject of interaction (legal entity or

[4] Passport of the national program "Digital Economy of the Russian Federation", Available: https://digital.gov.ru/uploaded/files/tsifrovaya-ekonomika-rossijskoj-federatsii.pdf (Accessed: 29.01.2025)

individual) can potentially submit to the government body an electronic document that it received from another subject located in a jurisdiction different from the government body of submission. In this case, the government body will not be able to correctly verify such an electronic document.

Another type of threat in case of violation of the cross-border transfer of electronic documents is associated with an electronic document with uncertain legal force that has already entered the recipient's jurisdiction, but its legal force has not yet been confirmed using receipts from a trusted third party. For example, it is possible that an electronic document was signed with an electronic signature and sent to the recipient, but before the recipient initiated the procedure for generating receipts, the public key certificate for verifying the signature was compromised. Obviously, such an electronic document will have no legal force in the recipient's jurisdiction. At the same time, at the time of the electronic document's formation and during its transfer from the sender to the recipient, the document had all the properties that allow it to be considered legally significant [5].

The achievements of IBM, as well as a number of other high-tech manufacturers of quantum computers, convincingly demonstrate the reality of the so-called "quantum threat". For this reason, a number of technological countries in the world have already begun preparations to counter future quantum cyberattacks. For example, the administration of former US President Joe Biden has issued two new directives to prepare the state and business for future quantum cyberattacks.

Thus, it should be considered that computer attacks and impacts using specially prepared content (information-technical and information-humanitarian impacts) would constantly develop, and their number would grow. Therefore, it is necessary to systematically update the existing lists of information security threats and conduct predictive research in this area in order to counter them in the near and medium term.

Automated information systems in the customs sphere

Currently, the customs sphere not only ensures 100% electronic declaration[5] [1, 4], but also various customs technologies for carrying out customs operations through information systems without the participation of customs officials are actively used.

Thus, for the first time, self-regulating mathematical methods, algorithms and software for format-logical control, interdepartmental exchange and verification of permits, as well as decision-making by information systems without the participation of customs officials have been developed and implemented.

In this case, electronic signature mechanisms are used to ensure the legal significance of decisions made by information systems. The proposed system-technical and information-technological solutions ensured the implementation of technologies for automatic registration of customs declarations, automatic verification of the risks of violation of the customs law of the EAEU and automatic release of goods in accordance with the declared customs procedure, as well as writing off customs duties and payments from the single personal accounts of participants in FEA [1].

Information systems of the customs authorities of the Russian Federation ensure the implementation of information and communication technologies used in the performance of customs operations and customs control of goods and vehicles, the use of the risk management system, accounting and control of the completeness and timeliness of receipt of customs payments and their payment, the maintenance and analysis of customs statistics of foreign trade, currency control, the analysis and assessment of the effectiveness of the activities of customs authorities, the implementation of other functions assigned to customs authorities in the field of customs affairs in accordance with the current EAEU Customs Code.

The basis for the implementation of various customs technologies was the creation, since 1998, of information systems of customs authorities in a secure design [1], first of all, Unified automated information

[5] The first electronic declaration was submitted to customs authorities on 25.11.2002.

system of customs authorities (UAIS CA)[6]. This system is designed to ensure automation of the activities of customs authorities and the implementation of information customs technologies in accordance with the legislation of the EAEU, the legislation of the Russian Federation in the customs sphere, as well as other relevant regulatory legal and acts of the Russian Federation and international treaties. The UAIS CA is a hierarchical multi-level information system corresponding to the organizational and staff structure of the customs authorities of the Russian Federation.

The set of components (objects) of the UAIS CA is operated in the central office of the Federal Customs Service of Russian Federation, specialized and regional customs departments, customs offices, at customs posts and checkpoints on the external border of the EAEU.

Information interaction between customs authorities is carried out using the Departmental Integrated Telecommunications Network (DITN) of the Federal Customs Service of Russian Federation, which is a system of telecommunications nodes of customs authorities that are interconnected according to the hierarchical principle.

Since 2002, when the first departmental certification center of the State Customs Committee of Russian Federation was created and the first electronic declaration of goods was filed, customs authorities have consistently created, put into operation and developed a system of departmental certification centers of customs authorities and automated information system for external access of customs authorities[7].

The automated information system for external access of customs authorities ensures secure information interaction between the information and software systems of the UAIS CA and external information systems (information systems of FTA participants, federal executive authorities, customs authorities of foreign states, including members of the EAEU, international organizations, etc.).

The system of departmental certification centers of customs authorities ensures the issuance of qualified certificates of electronic signature verification keys to customs officials and server components of the UAIS CA. Qualified certificates of the electronic signature key are required to create electronic documents within the framework of the procedures for automatic registration of declarations and automatic release of goods, as well as to check the status of a document at various stages of customs clearance and customs control, including after the release of goods within five years.

Since 2002, information interaction with the information systems of FTA participants and other interested parties has developed in the direction of a complete transition to the use of legally significant electronic documents.

Since 2018, the implementation of customs technologies has begun, which provide for the adoption of legally significant decisions when carrying out customs operations through information systems without the participation of customs officials.

Since November 2021, the process of automatic processing of goods declarations has been carried out by the customs authorities' information system around the clock. If a decision on the automatic release of goods in accordance with the declared customs procedure is not made by the information system, then such a declaration is automatically sent to the customs authority (electronic declaration center), whose officials make the final decision on the submitted declaration "manually". Simultaneously with the goods declaration, the official receives the results of inspections carried out by the information system, which he uses to make decisions. In this case, the decision is made by officials during the working hours of a specific customs authority where the declaration was received (most electronic declaration centers work daily in a 12-hour mode).

Along with this, work was carried out to develop the information and software tools of the UAIS CA, implementing in automatic mode the verification of format-logical control, algorithms for automatic registration of customs declarations and algorithms for the automatic release of goods.

---

[6] Order of the Federal Customs Service of Russia dated 17.06.2010 No. 1154 "On approval of the Regulation on the Unified Automated Information System of Customs Authorities", Available: https://www.alta.ru/tamdoc/10pr1154/?ysclid=m6izdrt2k5240885086 (Accessed: 30.01.2025)

[7] In 2002, the Departmental Certification Center of the State Customs Committee of Russia began its work, on the basis of which a system of departmental certification centers of customs authorities was subsequently created, which was put into operation on 11.03.2005. On 06.04.2009, an automated information system for external access of customs authorities was created and put into operation.

The digitalization of customs authorities' activities was accompanied by changes in international and national legislation. For example, the Customs Code of the Customs Union established the priority of using paper documents, and all customs operations were provided for only by customs officials. Since 2014, the electronic form of declaration has become mandatory in the Russian Federation, with the exception of cases determined by the Government of the Russian Federation or supranational legislation. Since 01.01.2018, the Customs Code of the EAEU has already entered into force, which established the priority of the electronic form of documents and the possibility of carrying out customs operations through an information system without the direct participation of customs officials.

Thus, currently developed technologies for performing customs operations through the information systems without the participation of customs officials (in automatic mode) involve the use, together with the UAIS CA, of the System of Departmental Certification Centers of Customs Authorities and the Automated System of External Access of Customs Authorities, ensuring interaction with the information systems of FTA participants and other interested parties, as well as the System of Interdepartmental Electronic Interaction, ensuring interaction with the information systems of more than 40 other federal executive authorities).

The transition of the customs authorities of the Russian Federation to the use of digital technologies served as the basis for the use of electronic documents by other federal executive authorities whose powers include the issuance of permits necessary for the movement of goods and vehicles across the customs border of the EAEU.

The introduction of an electronic form for submitting documents, the organization of obtaining permits in electronic form directly from the agency that issued them, and a number of other measures related to the organization of electronic document flow between participants in the cross-border movement of goods, made it possible for FTA participants to submit an electronic declaration for goods from any point in the Russian Federation and, as a result, eliminate the need for the personal presence of a representative of a participant in FTA at the customs authority when declaring goods.

The development of information systems of FTA participants took place, although the development and implementation of the CUCA interaction model scheme [3], which ensures increased management efficiency based on the processing of data on goods and thereby minimizing the impact of the so-called VUCA processes, had a greater influence on the development of information systems in the sphere of FTA.

When creating a digital information and logistics platform under VUCA conditions, it becomes possible to control all routine operations: from concluding a contract to successfully closing a deal, subsequent warranty service and compliance with the rights to the intellectual property used, processing and storage in distributed ledgers in the format of smart contracts. Automatic execution of smart contracts reduces the risk of logistical errors, unifies the document flow process, visualizes in real time the processes of movement of goods and the status of customs documents [3].

This model scheme consists of coordinating operations: data transfer during the implementation of business processes, defining the goal, in terms of knowledge of laws and regulations of FTA, observability of the current state of resources and controlled distribution of decision-making powers (Fig. 1).

The CUCA model scheme allows for a radical increase in the reliability and security of the chain of foreign trade transactions, the level of automation of accounting and control systems, a reduction in the time and financial costs of exporting enterprises, and the introduction of the principle of one-time provision of data (the “single window” principle) [8, 9].

The use of CUCA significantly reduces the potential for fraud, violation of liability regulations, certification rules and the use of false information. Thanks to the peer-to-peer architecture of the CUCA database, the FTA information space is endowed with new functions, which allows the exporter and importer to directly exchange legally significant documents organized in the form of a cryptographically protected chain of blocks (blockchain). The correctness of the information update is confirmed by all nodes of the blockchain network, and specially organized chains of records (sidechain) allow customs

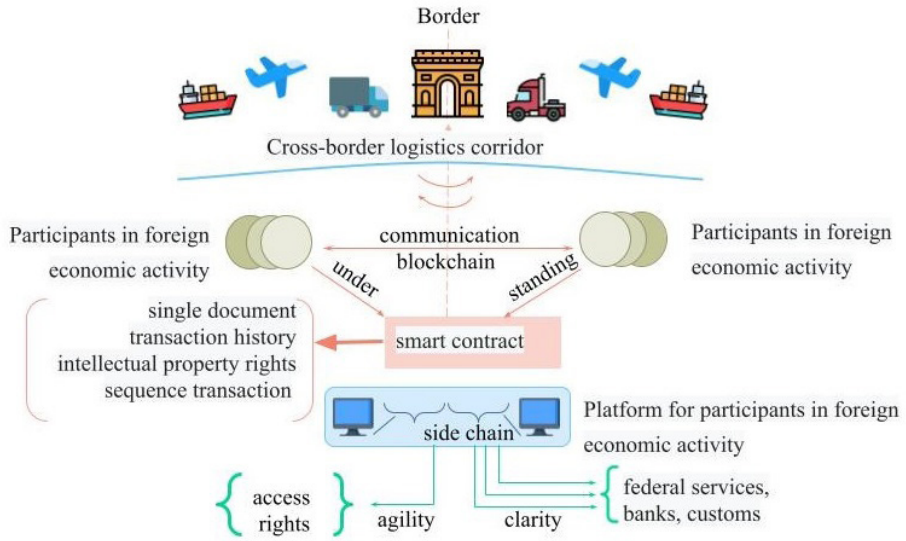

Fig. 1. CUCA model scheme

and currency control authorities to automatically receive the necessary information, which reduces administrative costs and speeds up all FTA processes.

Considering that distributed ledgers are decentralized network-centric technology for storing and processing data that includes meta-information about previous operations, a new addition operation using ledgers is executed taking into account the context of previous operations. This ensures verification of new operations in the future.

Each result of a successful operation is called "smart contract" and stored in a distributed ledger and is duplicated multiple times in the system, which ensures automated control of its correctness, radically reducing the number of violations in the preparation of documentation and customs clearance, reducing logistics costs due to:

- processing of all transactions in a common cryptographically protected information space of manufacturing enterprises, licensed exporting enterprises, customers of high-tech products, financial organizations and state customs control authorities;
- creating a distributed cross-border digital infrastructure for operational management and planning of FTA;
- integrating production and logistics capabilities for export-import operations, typical for enterprises engaged in high-tech production.

In the context under consideration, the essence of digital transformation of FTA comes down to using the capabilities of end-to-end information and computing systems and IoT networks to stimulate the activities of industrial enterprises to dramatically increase the volume of exports of high-tech products, including changes in business models of relationships with partners and competitors through the introduction of smart contracts.

An information and logistics model of FTA (using the example of transportation between Russia and China) with transaction control technology using distributed ledgers and smart contracts, is presented in Fig. 2.

All regulatory financial and logistical operations, up to the successful closing of a deal and subsequent warranty service, are proposed to be recorded and stored in distributed secure ledgers. In this case, the basis of FTA is smart contracts (application, description, letter of credit etc.), which automatically guarantee the regulatory correct settlement of requirements in accordance with the model of FTA adopted by the company and approved by the customs authorities (smart contract FTA).

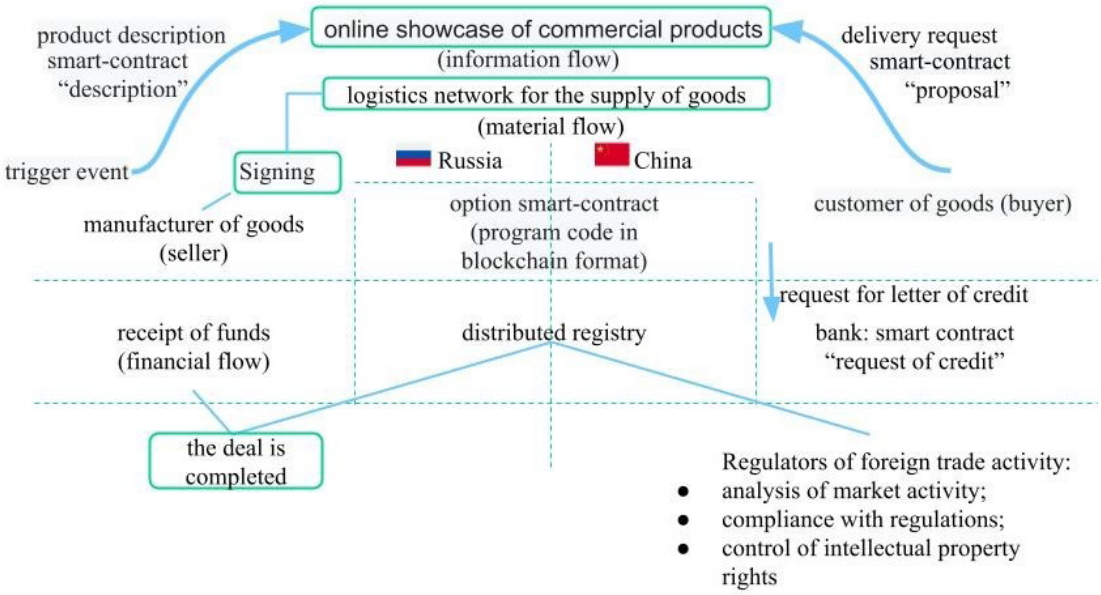

Fig. 2. Information and logistics model

It should be noted that a smart contract implements an algorithm executed in a local or cloud computing environment, which describes the sequence of fulfillment of contractual obligations agreed upon by the supplier and customer. When creating an information platform for the implementation of Russian-Chinese FTA, it must be taken into account that the processed data used, for example, to certify goods in accordance with national quality standards, are in "constant motion" [10], the trajectory of which can be clearly displayed on a multi-layer telematics map.

In modern conditions, the formation of a register of "obligations plus regulations", which characterizes the time sequence of fulfillment of contractual obligations, using traditional paper declarations significantly reduces the speed of trade transactions and at the same time increases the amount of inaccurate information associated with the influence of the "human factor". That is why the considered information and logistics model of foreign trade operations is based on digital technologies that allow the creation of a new class of network infrastructure for the implementation of FTA or the "Internet" of economically significant values. Such infrastructure can be created on the basis of an intelligent digital information and logistics platform that implements and controls material and information flows formed during the implementation of export contractual obligations and customs control regulations.

As noted above, business processes occurring during the implementation of FTA can be used to design smart contracts at the normative-algorithmic level regulating the sequence of both preparatory and customs-logistics operations [11, 12]. In this case, preparatory operations include the processes of selling and purchasing finished products or materials, drawing up relevant foreign trade contracts and carrying out banking transactions. Customs and logistics processes include the processes of obtaining permits (certificates of conformity, etc.), passing customs formalities, handling cargo along the entire route or transferring goods using information carriers through computer networks.

In the digital information and logistics platform, the distributed ledger actually functions as an information integrator, which receives information from both participants in export transactions and from equipment that forms the IoT class transport infrastructure used by the logistics operator or IaaS service provider. RFID sensors, digital video cameras, temperature and humidity sensors, GPS navigators and other telematic devices that transmit information about the current state, route, and location in the warehouse or other logistic attributes of the goods being transported can be used as sources of data processed during customs support of the smart contract.

At the same time, the technology of distributed ledgers at the algorithmic level fixes the list of requirements for the goods, their transportation and storage, which is mandatory for the supplier and the logistics operator company. Subsequently, the smart contract automatically prepares financial flows and forms a neutral account, where the recipient of the goods transfers payment for the completed goods transaction. At the same time, the funds are in this account until the goods cross the customs border and become the object of control of the smart contract.

An analysis of the structure of the digital information and logistics platform shows that the information used in it, being a carrier of events and facts, forms a distributed ledger or a set of data ordered according to certain rules, which are endowed with attributes that characterize how both rights and fact their ownership. These attributes ensure "high accuracy" of data accounting and management, which opens up fundamentally new possibilities for the use of distributed ledgers for the implementation and control of foreign trade transactions. Increasing the accuracy of data accounting reduces uncertainty in the planning process and economic risks of logistics transactions, which creates the preconditions for a radical change in business models based on the fulfillment of mutual obligations. This is especially important in the implementation of FTA, as it allows for the automation of the processes of control over the fulfillment of obligations, analyzing the ledgers of financial resources of suppliers, clients, intellectual property and applicable standards based on agreed algorithms. Considering that contract ledgers or smart contracts can be complete (take into account any possible situations) or open (can be supplemented or changed depending on the situation), the operational management of economic processes within the framework of FTA can be considered as a collective and non-authoritarian technology that allows for immediate and public confirmation of the accuracy and authenticity of the data provided.

The CUCA model scheme that forms the basis of the digital information and logistics platform allows for increasing the efficiency of operational management of logistics operations and automating the processes of FTA control by customs authorities. At the same time, enterprises exporting high-tech products have the opportunity to use new business models of FTA that increase the reliability, security and speed of trade operations.

Using similar approaches, the information system of the Russian Export Center is being developed. The digital platform "My Export" (state information system "Single Window") and the National digital transport and logistics platform (DTLP) are being created.

My Export platform was created within the framework of the national project "International cooperation and export", which is aimed at increasing the export of non-resource non-energy goods. Eleven relevant ministries, federal executive bodies and business associations worked together with the Russian Export Center to create the platform, including the Ministry of Industry and Trade of Russian Federation, the Ministry of Agriculture of Russian Federation, Rosselkhoznadzor, the Federal Customs Service of Russian Federation and the Federal Tax Service of Russian Federation. The digital platform "My Export" provides online access to government and business services that support companies' export activities. The platform's services provide solutions to key tasks at each stage of the export cycle[8].

The National DTLP is being created as a state information system that defines uniform standards of digital interaction for all participants in transport and logistics activities and government agencies. It is designed to unite digital logistics services on one platform and become a kind of a "single window" for interaction between the state and carriers. One of the goals is to implement electronic document management at all stages of cargo transportation by road, sea, river, rail and air[9].

[8] Over 115 thousand services rendered and over 23 thousand users. Digital platform "My export" is three years old. News of Russian export. Available: https://www.exportcenter.ru/press_center/svyshe-115-tysyach-okazannykh-uslug-i-bolee-23-tysyach-polzovateley-tsifrovoy-platforme-moy-eksport-/?ysclid=m6jdtzaob1137958268 (Accessed: 30.01.2025)

[9] National Digital Transport and Logistics Platform | Ministry of Transport of the Russian Federation, Available: https://mintrans.gov.ru/activities/297/367?ysclid=m6je3lweyh694738446 (Accessed: 30.01.2025)

Threats to the information infrastructure of customs authorities associated with the development of quantum computing technologies

The creation of secure quantum-resistant ecosystems and platforms for the digital economy of Russia, including the FTA sphere, is a long-term challenge due to the current lack of unified scientific, methodological and technical base for creating the aforementioned systems. In particular, there are no technologies to counter the new quantum threat to cybersecurity. This is a fundamental scientific problem, without solving which it is impossible to talk about achieving the goals of the national project "Data Economy".

According to [6], today we are in the so-called era of noisy intermediate-size quantum devices (NISQ) [13–19].

Quantum computers are capable of solving some computational problems much more efficiently than any modern classical computer (fifth-generation supercomputer) of the von Neumann architecture [20, 21].

The components of a quantum computer that can be implemented in practice are imperfect in terms of accuracy and are highly susceptible to interference and errors. However, if these components are used in combination with classical computers and fifth-generation supercomputers, it is possible to achieve significant acceleration in calculations in the field of solving a wide class of multidimensional optimization problems. It should be noted that these problems include the problems of ensuring information security for critical infrastructure and problems associated with information impact (primarily unfriendly) on this infrastructure.

Here the question of "price vs quality" arises: how much more expensive is such a quantum component of a computing system than a classical one, capable of doing the same work, but in a longer time?

The results obtained in the field of quantum information scince clearly demonstrate the high technological potential of quantum technologies. At the same time, it becomes clear that a cryptanalytically relevant or significant quantum computer can threaten civil and military communication systems and undermine the combat capability of strategic control and management systems of critical information infrastructure [6], including critical information infrastructure facilities of customs authorities and individual participants in FTA.

In this situation, there is a growing need to carry out all necessary measures to protect against the aforementioned quantum threat, including developing a plan of relevant priority measures at the state and military levels.

Touching upon the task of ensuring the security of critical information infrastructure in the context of the introduction (full-scale or limited) of quantum computing systems and quantum computing based on them, one can try to identify two main "scenarios" for the development of events [21].

The first scenario assumes the direct use of quantum technologies in computing facilities that provide control, processing of all types of information and modeling of all levels in the elements of the critical information infrastructure facility. It is obvious that quantum computing will be used in this case in parallel with calculations and control operations implemented on classical computing facilities (modern supercomputers in this approach will also be considered classical facilities).

The second scenario assumes that quantum technologies in the near future will not find wide application in critical information infrastructure due to insufficient reliability and maturity, and will most likely be used outside the real control and information processing circuits to solve individual local computationally intensive tasks. In this case, the processes of forming "hostile" information impacts can be implemented using quantum technologies outside the real control and computing circuits with subsequent "introduction" into structures related to critical information infrastructure facilities that are potential targets of impact.

It should be noted that the second scenario may become feasible in the near future, while the first one is associated with the need to master the serial production of basic elements that are (by analogy with

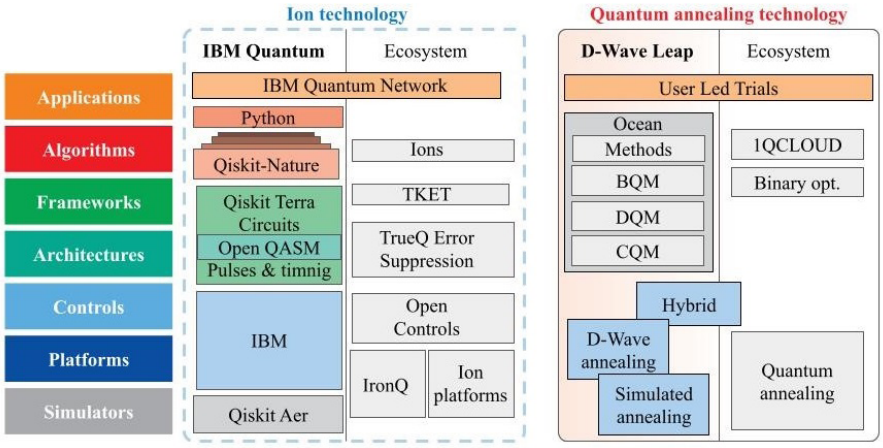

Fig. 3. The emergence of the first quantum computing technologies

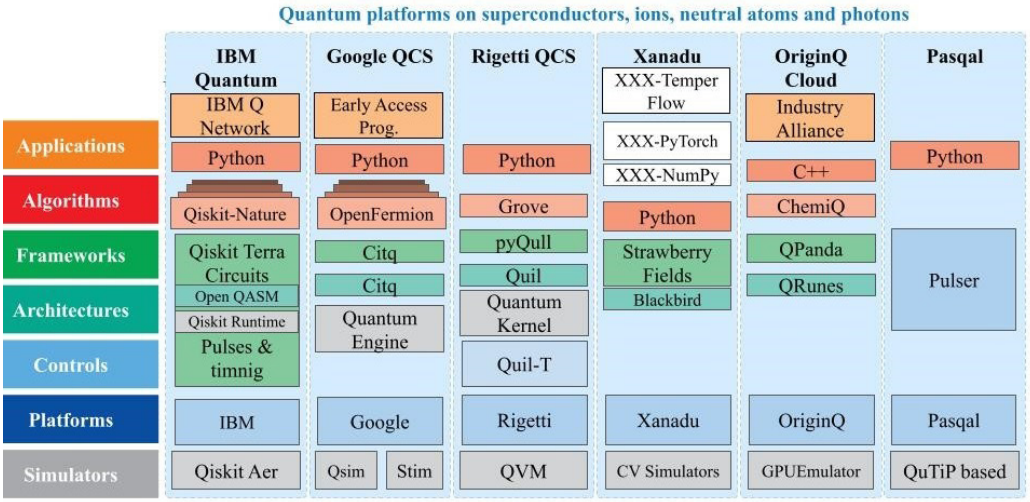

Fig. 4. The first quantum computing systems

microelectronic chips) the basis for hardware solutions for quantum computers (so-called "quantum chips"). The general situation here is that, despite active research in the field of quantum computers, there are still no technologies for the mass production of "quantum chips". Moreover, a physical platform for the creation and production (at least small-scale) of quantum computers has not been selected.

Currently, researchers around the world are working on the creation of quantum computers on four main platforms (Fig. 3 and 4): superconductors, ions, neutral atoms and photons.

The main features of these platforms are studied in [6]. The first prototypes of quantum computers do not differ fundamentally from each other in performance and are practically at the same stage of development. At the same time, if we talk about specific models of quantum computers, then at present, computing devices on superconductors have become more widespread.

The situation in the field of quantum computing is characterized by a kind of "technological race" between leading companies. Periodically, there are reports of achieving "quantum supremacy", i.e. the ability to solve problems that are impossible for classical von Neumann supercomputers.

Thus, in 2019, Google claimed to have achieved quantum supremacy on a 54-qubit array[10].

[10] **Arute F., Arya K., Babbush R. et al.** Quantum supremacy using a programmable superconducting processor. Nature, 2019, Vol. 574, 505–510. DOI: 10.1038/s41586-019-1666-5

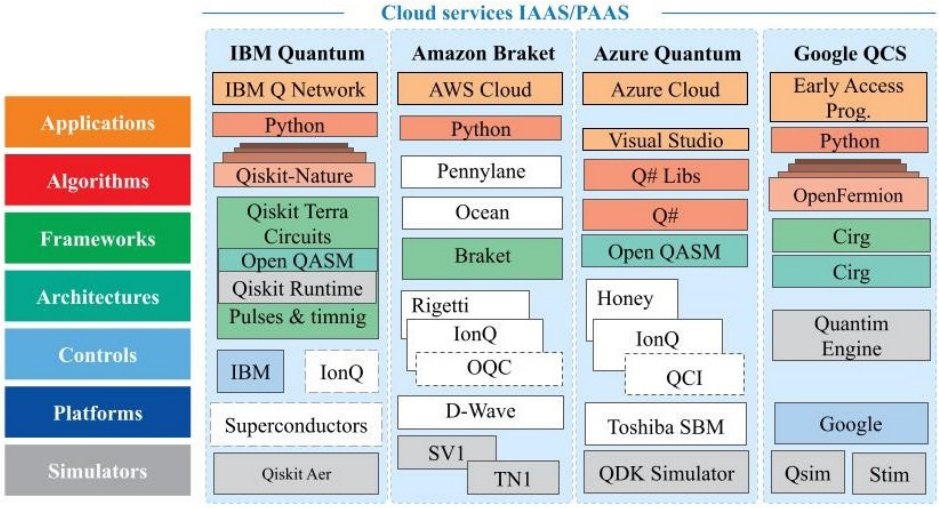

Fig. 5. First quantum computing services

In 2021, Chinese scientists reported[11] achieving quantum supremacy with the Jiuzhang 2 quantum computer on photons (the problem of sampling Gaussian bosons was solved 107 times faster than on classical supercomputers).

At the IBM Quantum Summit 2022[12], the Osprey quantum processor was presented, consisting of 433 qubits. Google, IBM, and D-Wave have provided access to their prototypes of cloud quantum computers under the Iaas and PaaS models. IBM plans to develop a quantum system with more than 4000 qubits by 2025. Google plans to introduce a cloud quantum computer with 1 million qubits by 2029. For comparison, the current leader among cloud computers is the Canadian company D-Wave with a 7000-qubit D-Wave Advantage 2 processor based on quantum annealing technology. An open cloud service Leap has been developed to work with this computer, which allows you to create and run various quantum applications (Fig. 5 and 6).

In Russian Federation, scientific research is also being conducted aimed at creating the first domestic quantum computers. For example, scientists from the Russian Quantum Center and the P.N. Lebedev Physical Institute of the Russian Academy of Sciences have developed a prototype of a quantum computer based on ytterbium ions[13].

The emergence of a relevant quantum computer capable of cracking traditional cryptographic algorithms is expected in the period 2026–2030.

In the context of the emergence of a new quantum security threat, it is necessary to set and solve the problem of ensuring the stability of customs authorities' information systems in such a way that quantum stability is ensured for technologies for performing customs operations through information systems without the participation of customs officials when making the following decisions:

- registration of goods declarations;
- release of goods and vehicles;
- registration of transit declaration;
- issue of transit declarations;
- risk level category of FTA participants;
- results of format-logical control of goods declarations;

[11] The Jiuzhang 2.0 Photonic Quantum Computer, Available: https://www.youtube.com/watch?v=R57M0SmTPHI (Accessed: 31.01.2025)
[12] The Next Wave – IBM Quantum Summit 2022 Keynote, Available: https://www.youtube.com/watch?v=8ySjHqfioJM (Accessed: 31.01.2025)
[13] **Dorohova I.** Sozdan prototip kvantovogo komp'yutera na ionah itterbiya. 2022, Available: https://strana-rosatom.ru/2022/02/25/sozdan-prototip-kvantovogo-kompjute/ (Accessed: 31.01.2025)

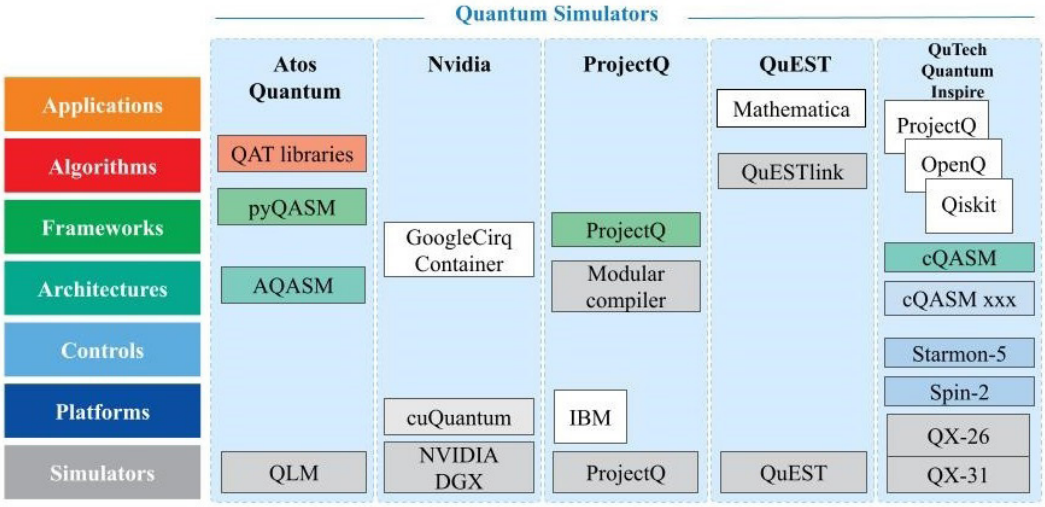

Fig. 6. First models of quantum simulators

- results of reconciliation of permits with the information declared in goods declarations;
- accrual and write-off of customs duties and fees.

At the same time, the main problematic issues of ensuring quantum stability of critical information infrastructure facilities of customs authorities include:

- insufficient level of readiness for the growth of quantum cyberattacks by intruders;
- growing complexity of the structure and behavior of critical information infrastructure facilities of customs authorities in the context of unfinished import substitution and technological security;
- difficulty of identifying quantitative patterns that allow us to study the cyber-resilience of customs authorities' critical information infrastructure facilities in the context of classical and quantum cyber-attacks by intruders.

Ignorance of the above-mentioned problematic issues leads to a decrease in the efficiency of the functioning of the critical information infrastructure facilities of customs authorities.

Moreover, this problem is significantly aggravated by the growth in the number of classical and quantum cyberattacks by intruders. Of particular concern are the so-called quantum attacks or attacks using a quantum computer. The fact is that most of the crypto primitives used in modern information systems (including hash functions, electronic signatures, asymmetric cryptographic algorithms and corresponding protocols) are no longer resistant to such attacks.

Today, effective quantum algorithms are known, in particular, Shor's algorithm for factorization and discrete logarithm, which can be successfully used to hack the listed crypto primitives [22–24].

The functioning of critical information infrastructure facilities are also strongly influenced by factors of the external and internal environment, which are either fundamentally impossible to manage, or can be controlled with an unacceptable delay. In addition, the external and internal environments have incomplete certainty of their possible states in the future.

That is, the factors influencing the behavior of critical information infrastructure facilities of the Russian Federation undergo changes over time that can radically change their functioning algorithms or make the set goals unattainable. Changes in the external and internal environment occur regularly and randomly, therefore generally they cannot be accurately predicted, resulting in uncertainty in their values. These facilities have a certain "safety margin" – features that allow achieving the set goals with certain deviations in the influencing factors of the external and internal environment.

Until recently, two main approaches were used to identify the above-mentioned patterns of functioning of critical information infrastructure facilities: experimental (for example, methods of mathematical

statistics and experimental design) and analytical (for example, analytical verification methods). Unlike experimental methods, which make it possible to study the individual behavior of a critical information infrastructure facility, analytical methods allow us to consider the most general properties of the behavior of this facility, characteristic of the class of functioning processes as a whole. These approaches have significant shortcomings.

For experimental methods, this is the impossibility of extending the results obtained during the experiment to other behavior of a critical information infrastructure facility that differs from the one studied, and for analytical verification methods, this is the difficulty of moving from a class of processes of functioning of a critical information infrastructure facility, characterized by the derivation of generally significant properties, to a single process that is additionally characterized by corresponding conditions of functioning (in particular, specific values of the behavioral parameters of this facility under conditions of classical and quantum cyberattacks by intruders).

Consequently, each of the named approaches separately is insufficient for effective research of quantum stability of customs authorities' critical information infrastructure facilities. The necessary mathematical apparatus for identifying the required quantitative patterns of behavior and ensuring quantum stability of critical information infrastructure facilities can be obtained only by using the strengths of both approaches and combining them.

Thus, the practice of operating and maintaining critical information infrastructure facilities both in customs authorities and in other areas indicates the following. The conditions of modern confrontation in cyberspace impart to the mentioned facilities features that exclude the possibility of creating quantum-resistant facilities of critical information infrastructure of customs authorities by traditional methods.

At present, three main directions can be identified for resolving the scientific problem of ensuring quantum stability of information systems.

The first direction is the justification and preparation for the transition to the emerging domestic post-quantum crypto-primitives of blockchain and electronic signature. For example, to the post-quantum electronic signature "Rosehip" (2022), the stability of which is based on the mathematical problem of decoding a random linear code, which is computationally complex, and to the protocol for generating a common key based on the apparatus of isogenies of supersingular elliptic curves "Forsythia" (2022).

The second direction is the justification of the application of the first quantum-resistant solutions of quantum cryptography on physical principles and laws of quantum mechanics with mathematically provable stability. Including data transfer protocols that cannot be intercepted and decrypted unnoticed, quantum key distribution systems, quantum generators of truly random numbers, etc.

The third direction is the creation of a fully quantum model of customs authorities' information systems. It is clear that such an approach will require the creation of a full-fledged quantum (physical) infrastructure of customs authorities, which is a distant prospect.

Note that before this, information theory and information security dealt exclusively with attacks by intruders using traditional von Neumann computers. For example, using the recommendations and corresponding Threat Models of domestic regulators[14].

In practice, a number of interesting results have already been obtained. For example, high-speed hardware symmetric key encoders and quantum key distribution devices, which provided these encoders with secret keys, were integrated into highly loaded communication channels. A dedicated fiber optic core was used to transmit single photons. Since networks are often overloaded, scientists are working to ensure that quantum and classical signals can coexist in one fiber optic at different wavelengths. Thus, a pilot project of the Rosatom state corporation connected two offices of the organization in Moscow.

[14] Methodology paper dated February 5, 2021, Available: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=m6kmwynfoo336914156 (Accessed: 31.01.2025); MITRE ATT&CK®, Available: https://attack.mitre.org (Accessed: 31.01.2025)

This project is a pilot fiber-optic communication line using quantum key distribution technology and was implemented with the support of Rostelecom PJSC on equipment from the QRate research and production company.

It is interesting that during the testing, a quantum channel rupture was simulated, during which the secret key storage buffer worked. Successful testing confirmed the required level of reliability for the implementation of the current solution in the network infrastructure. Another project is being implemented by Russian Railways, which is responsible for the implementation of the roadmap for the development of the high-tech field of Quantum Communications in the Russian Federation. The project involves the creation of an 800 km long quantum network, based on domestic solutions ViPNet Quantum Trusted System from InfoTeKS. At present, the largest backbone quantum network in Europe from Moscow to St. Petersburg has already been created.

At the same time, the following must be taken into account. Firstly:

- relative youth of the field, and therefore insufficient study and trust in post-quantum crypto primitives (performance and security issues). For example, in 2023, researchers from the Royal Institute of Technology in Sweden discovered a vulnerability in the post-quantum algorithm CRYSTALS-Kyber, one of the finalists of the well-known NIS competition;
- emergence of quantum algorithms that effectively solve "new" mathematical complex problems, i.e. "new" post-quantum crypto-primitives immediately become unstable. The sensational story of a new algorithm by Chinese scientists based on the Schnorr method, which used quantum acceleration to obtain approximate results for one of its stages – solving the problem of finding a short vector in a lattice of small dimension;
- emergence of a large number of open and commercial libraries for developers of digital platforms, SDKs implementing new cryptographic schemes, and, consequently, a high probability of the presence of so-called undeclared capabilities and software backdoors (up to 95% of the software code of open libraries contains the aforementioned backdoors);
- lower efficiency of post-quantum cryptographic schemes compared to classical ones: large sizes of keys, ciphertexts and signatures, low productivity etc.;
- practical complexity of a mass transition to post-quantum schemes and the unclear timeframe for implementing such a transition, etc.

Secondly, the creation and transition to quantum-resistant solutions and components of the RF CII facilities based on quantum cryptography with mathematically provable resistance. Including data transfer protocols that cannot be intercepted and decrypted unnoticed, quantum key distribution systems, quantum generators of truly random numbers.

Well-known Russian mathematicians have made significant contributions to this area of knowledge, for example, employees of the Steklov Mathematical Institute of the Russian Academy of Sciences:

- Volovich I.V., PhD, – head of the Department of Mathematical Physics, corresponding member of the Russian Academy of Sciences;
- Kholevo A.S., PhD, – head of the Department of Probability Theory and Mathematical Statistics, laureate of the Claude E. Shannon Prize for outstanding achievements in information theory, academician of the Russian Academy of Sciences.

Conclusion

An analysis of the information and software tools, technologies and information resources of the customs authorities of the Russian Federation has shown that they are currently the only complex in the Russian Federation that ensures the performance of legally significant actions electronically around the clock without human participation (registration of customs declarations, automatic verification of risks of violation of the customs legislation of the EAEU and automatic release of goods in accordance with the declared customs procedure).

In the future, the implementation of automatic customs operations will be transformed into a new vector – automatic business processes, for example, automatic intelligent control at checkpoints (using elements of artificial intelligence). One of the elements of such an intelligent business process is already a qualitatively new project of the Federal Customs Service – analysis of images of inspection and screening complexes using machine learning technology.

The results obtained in the field of quantum information science clearly demonstrate the high technological potential of quantum technologies. A cryptanalytically relevant or significant quantum computer can threaten civil and military communication systems and undermine the combat capability of strategic control and management systems of critical information infrastructure.

It has been shown that critical information infrastructure facilities, including those of customs authorities, do not have the required stability for their intended functioning in the face of previously unknown quantum attacks by intruders.

In this situation, there is a growing need to prepare in advance for possible collisions and carry out all necessary measures to protect against the aforementioned quantum threat, including developing a plan for relevant priority measures at the level of the Federal Customs Service of Russian Federation and, possibly, at the level of FTA participants who ensure the largest volume of customs operations or carry them out in the interests of critical information infrastructure facilities in other areas.

REFERENCES

1. **Skiba V.Yu., Pozdnyakova K.E.** Modern automated information systems for customs operations without the participation of customs officials. Vestnic of Russian Customs Academy, 2022, Vol. 59, no. 2, pp. 19–33. DOI: 10.54048/20727240_2022_02_19

2. **Giles S.** How VUCA is reshaping the business environment, and what it means for innovation. Forbes, 2018. URL: https://www.forbes.com/sites/sunniegiles/2018/05/09/how-vuca-is-reshaping-the-business-environment-and-what-it-means-for-innovation/ (Accessed: 10.12.2024)

3. **Zaborovsky V.S., Lei Dzhan, Skiba V.Yu., Strekalov S.V.** Digital information and logistic platform for operational management of foreign trade activities of high-tech products suppliers. St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control Systems, 2018, Vol. 11, no. 4, pp. 7–20. DOI: 10.18721/JCSTCS.11401

4. **Bulavin V.I., Vasil'ev D.A., Skiba V.Yu., Tereshchenko D.V. et al.** 30 let avtomatizatsii tamozhennykh organov. Ot zamysla sozdaniia avtomatizirovannykh sistem obrabotki informatsii v organakh gosudarstvennogo tamozhennogo kontrolia do Strategii razvitiia tamozhennoi sluzhby Rossiiskoi Federatsii do 2030 goda [30 years of automation of customs authorities. From the idea of creating automated information processing systems in state customs control bodies to the Strategy for the Development of the Customs Service of the Russian Federation until 2030]: monograph. Moscow: TsBT, 2021. 304 p.

5. **Kazarin O.V., Skiba V.Yu., Sharyapov R.A.** Novye raznovidnosti ugroz mezhdunarodnoi informatsionnoi bezopasnosti [New types of threats to international information security]. History and Archives, 2016, Vol. 3, no. 1, pp. 54–72.

6. **Stupin D.D., Petrenko A.S., Petrenko S.A.** Razvitie tekhnologii kvantovykh vychislenii i sviazannye s nim ugrozy dlia kriticheskoi informatsionnoi infrastruktury rossiiskoi federatsii [Development of quantum computing technologies and associated threats to the critical information infrastructure of the Russian Federation]. XVI Vserossiiskaia Mul'tikonferentsiia po Problemam Upravleniia [All-Russian Multi-Conference on Management Problems] (MKPU-2023), 2023. pp. 168–172.

7. **Skiba V.Yu.** Rol informatsionnoy bezopasnosti vo vneshneekonomicheskoy deyatelnosti [The role of information security in foreign economic activity], Mezhotraslevoy forum direktorov po informatsionnoy bezopasnosti [Abstracts of reports of the Inter-industry Forum of Directors of Information Security] (Moscow, November 17 – 182008.). Inform-media Russia, 2008.

8. Ot evraziiskoi integratsii k dal'nevostochnomu vektoru politiko-ekonomicheskikh interesov Rossii: sbornik nauchnykh trudov [From Eurasian integration to the Far Eastern vector of Russia's political and economic interests: a collection of scientific papers]. Vladivostok: Vladivostokskii filial Rossiiskoi tamozhennoi akademii, 2015. 265 p.

9. **Skiba V.Yu., Strekalov S.V.** Implementing the "Single Window" Concept in the European Union and Asian-Pacific Region: Organizational and Financial Aspects. Tamozhennaia politika Rossii na Dal'nem Vostoke [Customs policy of Russia in the Far East], 2016. Vol. 76, no. 3, pp. 32–44.

10. **Zubakov G.V., Strekalov S.V.** Current issues of information's interaction of participants in logistics chains while the cross-border air cargo carriage executing. Academic Vestnic of the Rostov Branch of the Russian Customs Academy, 2016, Vol. 24, no. 3, pp. 21–24.

11. **Motorin D.E., Popov S.G.** Algoritm mnogokriterial'nogo poiska traektorii dvizheniia robota na mnogosloinoi karte [Algorithm for multi-criteria search of robot movement trajectory on multi-layer map]. Information and Control Systems, 2018, no. 3, pp. 45–53. DOI: 10.15217/issn1684-8853.2018.3.45

12. **Motorin D.E., Popov S.G., Chuvatov M.V., Kurochkin M.A., Kurochkin L.M.** A study of the evaluation function for the cost of transport operations in distribution of purpose in a group of robots. 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), 2017, pp. 536–538. DOI: 10.1109/SCM.2017.7970642

13. **Valiev K.A.** Quantum computers and quantum computing. Physics-Uspekhi, 2005, Vol. 48, no. 1, pp. 1–36. DOI: 10.1070/pu2005v048n01abeh002024

14. **Kitaev A., Shen' A., Vialyi M.** Klassicheskie i kvantovye vychisleniia [Classical and quantum computing]. Moscow: MCNO, CheRo Publishing House, 1999. 192 p.

15. **Nielsen M.A., Chang I.L.** Quantum computing and quantum information. Cambridge: Cambridge University Press, 2011. 702 p.

16. **Petrenko A.S.** Kvantovaia ugroza bezopasnosti tekhnologii blokchein [Quantum Threat to Blockchain Security]. St. Petersburg: Athena, 2022. 105 p.

17. **Kholevo A.S.** Vvedenie v kvantovuiu teoriiu informatsii [Introduction to Quantum Information Theory]. Moscow: MTsNMO, 2002. 128 p.

18. **Kholevo A.S.** Veroiatnostnye i statisticheskie aspekty kvantovoi teorii [Probabilistic and statistical aspects of quantum theory], 2nd ed. Moscow, Izhevsk: Institut Komp'iuternykh Issledovanii, 2002. 128 p.

19. **Bennett C.H., Shor P.W.** Quantum information theory. IEEE Transactions on Information Theory, 1998, Vol. 44, no. 6, pp. 2724–2742. DOI: 10.1109/18.720553

20. **Petrenko S.A., Petrenko A.S., Kostyukov A.D.** Countermeasures technologies previously unknown quantum cyber threats. Zaŝita informacii. Inside, 2024, Vol. 118, no. 4, pp. 66–76.

21. **Petrenko A.S., Petrenko S.A.** Quantum resilience estimation method blockchain. Cybersecurity Issues, 2022, Vol. 49, no. 3, pp. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22

22. **Simon D.R.** On the power of quantum computation. Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 116–123. DOI: 10.1109/SFCS.1994.365701

23. **Shor P.W.** Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal of Computing, 1997, Vol. 26, no. 5, pp. 1484–1509. DOI: 10.1137/S0097539795293172

24. **Shor P.W.** Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700

INFORMATION ABOUT AUTHORS / СВЕДЕНИЯ ОБ АВТОРАХ

Skiba Vladimir Yu.
Скиба Владимир Юрьевич
E-mail: vskiba69@mail.ru

Petrenko Sergei A.
Петренко Сергей Анатольевич
E-mail: petrenko.sa@talantiuspeh.ru

Murzina Anastasiya A.
Мурзина Анастасия Алексеевна
E-mail: myrzina.aa@talantiuspeh.ru

Popova Kristina R.
Попова Кристина Романовна
E-mail: popova.kr@talantiuspeh.ru

Submitted: 11.11.2024; Approved: 23.12.2024; Accepted: 27.12.2024.
Поступила: 11.11.2024; Одобрена: 23.12.2024; Принята: 27.12.2024.