Monitoring of international legal regulation trends for the development of legislation in the digital economy in Russia

Data reuse in healthcare, protection of personal data in the insurance industry, taxation of multinational companies, development of the regulation of quantum technologies

Monitoring No. 1(13) (January 2025)

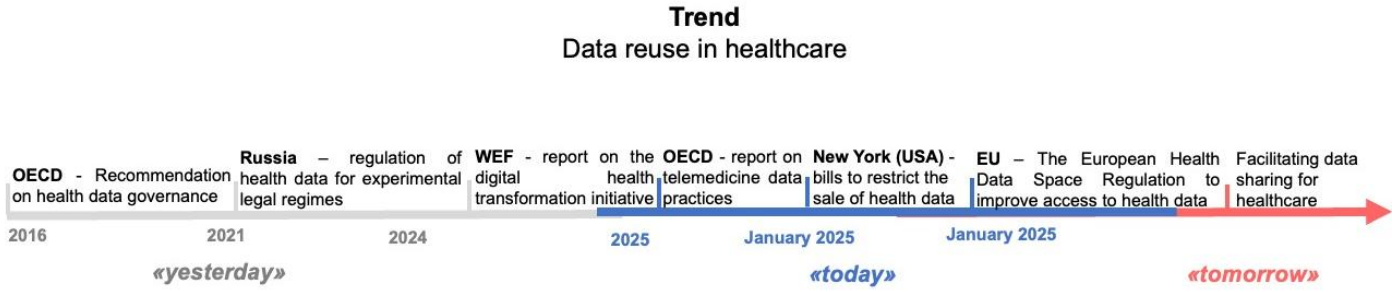
Monitoring was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Ivan Ermokhin, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Olga Magomedova, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Kirill Chernovol, Researcher, International Best Practices Analysis Department, Gaidar Institute

"This is a winter month.
First on the calendar
I shall begin to speak
When I'm fed up with the dark".
Joseph Brodsky

In August 2024, there were 4 events that define the trends in the development of digital economy regulation in the world.

Trend No. 1. Data reuse in healthcare

In January 2025, the EU adopted a Regulation governing the automatic access of healthcare providers to a patient's health data records in each member state. New York is enhancing individuals' control over their health data, for example, when using medical devices, the user must be provided with the option to delete the data. The OECD released a report on telemedicine, showing that telemedicine data collection facilitates more detailed medical research, and the World Economic Forum (WEF) report projects the development of predictive analytics in medicine due to access to such data.



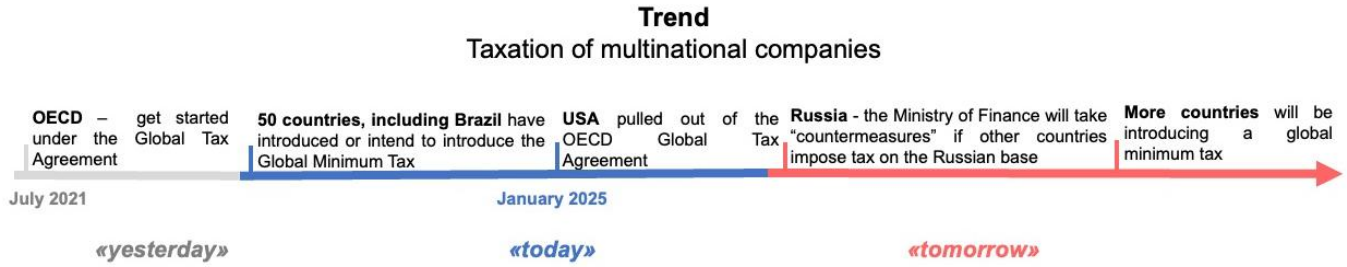
Trend No. 2. Protection of personal data in the insurance industry

In the US, there are lawsuits against insurance companies for illegally accessing data, and the state of Texas has even initiated a ban on the use of AI in the insurance industry to prevent unreasonable denials of coverage for claims.

Trend No. 3. Taxation of multinational companies

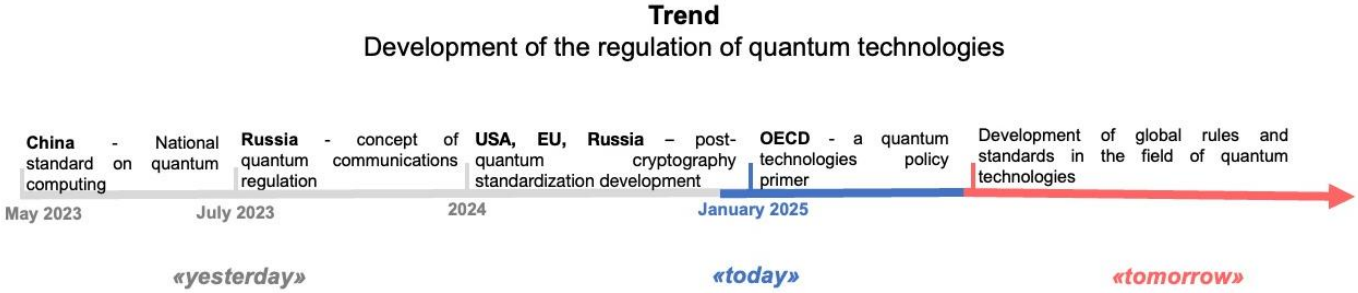
In January 2025, the U.S. announced that it would not recognize the right of other countries to collect the global minimum tax on U.S. companies under the OECD Global Tax Agreement.[1] The U.S. will impose economic measures against countries that collect such a tax, including levies on the income of residents of such countries earned in the United States. The Russian Ministry of Finance may adopt a similar approach by mid-2025. Brazil, on the contrary, has introduced a global minimum tax starting from January 2025.

[1] The Agreement is the OECD's two Pillar action plan to reform the international cross-border tax system to combat Base Erosion and Profit Shifting (BEPS).



Trend No. 4. Development of the regulation of quantum technologies

In January 2025, the OECD released a Quantum Technologies Policy Primer, highlighting the main risks of such technologies - the risks of digital security and data leakage, as a quantum computer allows to decrypt data many times faster than a classical computer and breaks the tools used to encrypt information.



January 2025 also saw a number of significant developments in Russia's regulation of the digital economy:

1. New cryptocurrency taxation regulations

From January 2025, new taxation regulations for digital currencies will come into force.[2] The following innovations in the Tax Code can be highlighted:

1. For tax purposes, cryptocurrency is recognized as property within the meaning of civil law.
2. Mining and transactions involving the sale of cryptocurrencies are not subject to VAT.
3. Establishes special rules for the taxation of cryptocurrency mining.

For i*ndividuals*, income from mining in Russia is recognized as income from sources in Russia (not abroad), is included in the personal income tax base, and is taxed at a progressive rate of 13-22%. It is possible to receive a property deduction in the amount of actually incurred and documented expenses of a miner, i.e. deduct expenses, for example, for renting mining equipment, power consumption, etc., which are deductible.

It is important to note that as a result of mining, it is not income from the sale of cryptocurrency that is taxable, but the receipt of cryptocurrency itself in kind (similar to income in the form of property rights or goods, etc.). The question arises: how to calculate the value of the received mined cryptocurrency? The value of the digital currency is determined based on its market quotation on the date of its actual receipt - crediting the cryptocurrency to the miner's account, when the miner has the right to dispose of such digital currency (for example, to sell and credit the digital currency to the account of another person).

It should also be noted that the receipt of cryptocurrency under a gift agreement from an interdependent person (for example, a family member) is not subject to personal income tax.

For *organizations*, income from mining will be taxed at a rate of 25% and will be considered non-operating income. As with personal income tax, the tax base will be the market quotation of the mined cryptocurrency on the date of its receipt, for example, at the time of crediting the cryptocurrency to the miner's account.

[2] The Federal Law No. 418-FZ dated November 29, 2024 "On Amending Parts One and Two of the Tax Code of the Russian Federation and Certain Legislative Acts of the Russian Federation". https://base.garant.ru/411020694/

To pay personal income tax and profit tax on mining, it is necessary to determine the market quotation of cryptocurrency. The market quote is the final price of the cryptocurrency at the end of each trading day. Given that the activities of crypto exchanges in Russia are not regulated, then market quotes of foreign crypto exchanges are used. Such a foreign crypto exchange must meet two conditions: (1) have a crypto trading volume of more than 100 billion rubles per day and (2) publish information on market quotes for the last 3 years on its website.

If crypto is traded on several exchanges at once, the taxpayer independently chooses the market quotation on one of the exchanges. If transactions on exchanges were carried out in foreign currency or in other cryptocurrencies (the value must be linked to the foreign currency exchange rate), the taxpayer has the right to choose the value of the cryptocurrency by recalculating the foreign currency exchange rate into rubles at the official exchange rate of the Bank of Russia.

It is also worth noting that special tax regimes such as the simplified taxation system, patent taxation system, professional income tax (for the self-employed), etc. do not apply to mining.

4. Establishes special taxation rules for the resale of cryptocurrencies.

As a result of mining, the cryptocurrency itself is subject to taxation as income in “in-kind” (described above), the value of which is calculated on the basis of market quotations on foreign crypto exchanges. At the same time, special rules apply to further resale of cryptocurrency. At resale, income will already be recognized as “material benefit”, so to calculate the tax, it will be necessary to deduct the difference in the value of the cryptocurrency at the time of its crediting to the account of the miner and at the time of its resale to third parties. Tax is levied on the capital gain that occurs from the moment the cryptocurrency is credited to the account of the miner (or buyer) until it is resold.

Where *personal income tax is applicable*, income up to 2.4 million rubles from the sale and purchase of cryptocurrency is taxable at the rate of 13%. When exceeding 2.4 million rubles, the tax will be calculated according to the formula: 312 thousand rubles + 15% of the amount of the excess. The rate for non-residents is 30%. When paying *corporate income tax*, income is determined based on the actual sale price of cryptocurrency, but not below the market quotation reduced by 20%. If a person incurred losses when selling cryptocurrency, it is possible to reduce the tax base by cryptocurrency income in the future (but not more than 50% of the amount of the loss) - the rule works for both personal income tax and corporate income tax.

It is worth noting that in respect of cryptocurrencies already held, there will be no revaluation of their value for taxation purposes.

5. Establishes the obligation of an operator of a mining infrastructure to send a report to the Federal Tax Service every quarter on the persons to whom it provides services.

2. Automated tracking of personal data circulation violations by Roskomnadzor

The Ministry for Digital Technology, Communications and Mass Media has drafted amendments to the Regulation on State Control over Compliance with the Personal Data Processing Regime.[3] If earlier violations of the law on personal data were detected by citizens' appeals to Roskomnadzor, now Roskomnadzor will monitor such violations “with the use of automated information systems”, which will make it possible to monitor, including online resources. If a violation is detected, the operator will be notified to stop illegal data processing within 10 working days. Which systems will be used by Roskomnadzor and how they will affect the integrity of data operators' information systems has not been determined.

[3] Decree of the Government of the Russian Federation of June 29, 2021, No. 1046 “On Federal State Control (Supervision) over Processing of Personal Data” (together with “Provision on Federal State Control (Supervision) over Processing of Personal Data”).

Key aspects

1. Data reuse in healthcare

The EU experience

The Regulation on the European Health Data Space (EHDS) was adopted in January 2025.[4] There are 2 categories of health data:

1. For primary use - the use of patient data by healthcare providers in the delivery of services.

2. For secondary use - use of health data by third parties for research, statistics, etc.

For each category, the Regulation defines lists of data types and rules for accessing them and provides for the establishment of two digital platforms for accessing such data: MyHealth@EU for the first category and HealthData@EU for the second one.

The regulation provides patients with additional data management tools beyond those provided for in the GDPR:[5]

1) The patient's right to refuse ~~to allow~~ healthcare institutions to continue to use health data that has already been collected. For example, a patient may request to stop storing data on his/her test results - the grounds for such a request are not limited.

2) The right to restrict access to collected data. For example, a hospital may use data only when there is an emergency - in the event of a pandemic.

3) The right to manage health data - accessing and downloading data in machine-readable format, transferring data to another healthcare provider's system, receiving notifications about access to their data, etc.

It also provides for States to establish a system of “trusted data holders” that take over the storage, processing and provision of health data upon request. For example, if a patient comes to a new health center, their health data can be requested from a trusted holder without having to re-collect data from the patient. The goal of the new institution is to eliminate duplication of data in the information systems of hospitals and other institutions by making it the responsibility of one person to store patient data for use by different institutions.

Secondary use data includes 17 categories of data, such as electronic health data, data on expenditures for medical services, etc. There is a closed list of purposes for which access to such data may be granted: statistical research, educational purposes, scientific research (medical, technological), etc.

The New York experience (USA)

Two bills have been introduced to regulate health information.

The first bill sets out the conditions for processing health-related data,[6] including any financial or geolocation information related to physical or mental health. In other words, both health data directly and information related to this area of a person's life, such as what medications they purchase, where, how often, etc., are protected.

In the US, personal data holders are assumed to be able to sell it unless the data subject expressly prohibits its sale. However, health information is recognized as the most sensitive one for patients, so the bill proposes an explicit prohibition on the sale of such data. The bill also provides patients with the right to manage certain types of data, for example, to consent to data processing not in relation to all data but only certain data, or to withdraw consent in relation to individual data operations rather than the whole data processing.

The consent form may (but does not necessarily) include the price of the company's processing of the data, that allows companies to be compensated for the costs of processing the data. In view of the prohibition on commercialization of data. It may also specify the forms of compensation that a data processor can receive for data operations.

The second bill deals with the privacy of data collected by electronic health products, services[7] and devices.[8] The bill obliges the

[4] https://digitalpolicyalert.org/event/26173-council-of-the-eu-adopts-regulation-on-european-health-data-space-ehds

[5] European Union General Data Protection Regulation (GDPR) 2016/679.

[6] https://digitalpolicyalert.org/event/25961-introduced-new-york-health-information-privacy-act-s-929-to-the-senate
https://legiscan.com/NY/text/S00929/id/3040218

[7] https://digitalpolicyalert.org/event/25962-introduced-electronic-health-products-and-services-privacy-act-a-1415-to-the-new-york-assembly
https://legiscan.com/NY/text/A01415/2025

[8] Any software or hardware and software package, including applications, websites, and other information products, designed to process personal health information for the purpose of providing that

provider of devices that collect health-related data to provide detailed information about data processing. For example, the provider must obtain permission to share the data with third parties and inform the user about to whom the data will be transferred. In this way, the draft law restricts the uncontrolled dissemination of health-related data collected from medical devices (including their commercialization).

The OECD experience

The OECD has released the Telemedicine Development Report.[9] In 2019 (before the pandemic), there was an average of 0.6 telemedicine consultations per person per year; in 2021, there were already 1.4. Analysis of healthcare data showed that online consultations do not increase the workload of first aid departments, which means that the growth of telemedicine does not overburden the healthcare system. In the aftermath of the COVID-19 pandemic, a number of countries have taken steps to develop online health services and improve health-related data management. In case of Australia the government not only collects data on health services provided through public insurance[10] but also assigns distinctive identifiers to compare data from different sources or categories of subjects. For example, data on indigenous peoples, data on residents of residential care homes for the elderly, etc., are not included in the data on health services. Such information is not included in health data, however, classification of data according to such criteria is necessary for health research.

The WEF experience

The WEF presented the Digital Health Transformation Initiative, which aims to expand health data collection and sharing practices to more than 150 organizations, in a report on data collaboration.[11] Initiative participants will share data such as medical records, health-related behavioral and social indicators, insurance claims data, health monitoring data, and more.

Sharing such data will have a positive impact on innovation and the healthcare system. For example, data sharing will increase early detection of diseases (especially in the diagnosis of diabetes and cardiovascular disease, which account for 20 million deaths annually), develop predictive analysis of pandemics or morbidity, and support the spread of preventive medicine.

Russia's experience

There is a general trend in the world to develop rules for handling health data: on the one hand, in terms of accessibility of such data for research (as in the EU), and on the other hand, in terms of protection of such data from uncoordinated circulation (as in the USA). In Russia, the agenda for the development of conditions for handling such data has not been outlined. As a consequence, the economic and innovative potential of medical data collected in Russia is not realized to full extent, for example, there are difficulties in transferring health-related data for medical research.

2. Protection of personal data in the insurance industry

In January 2025, the insurance company Allstate is sued for illegally obtaining customer data, and the state of Texas proposed to prohibit the use of AI to make health insurance decisions by insurance companies. It is worth noting that back in 2022-2023, a number of insurance companies faced major data breaches: MCNA Dental (USA) lost the data of 9 million customers, Medibank (Australia) - 9.7 million,[12] Zurich Insurance (Switzerland) - 1 million.

The US experience

In January 2025, the Texas Attorney General filed a lawsuit against insurance companies Allstate and its subsidiary, Arity, for the alleged unlawful collection, use, and sale of auto users' location data.[13,14] Allstate purchased geolocation data from Toyota, Lexus, Mazda, Chrysler, Dodge from the mobile apps

information to the user or his or her health care provider upon the user's request.

[9] https://www.oecd.org/en/publications/leading-practices-for-the-future-of-telemedicine_496a8ffe-en.html

[10] https://www.aihw.gov.au/about-our-data/our-data-collections/medicare-benefits-schedule-mbs

[11] https://www.weforum.org/publications/better-together-building-a-global-health-network-economy-through-data-collaboration/

[12] https://www.syteca.com/en/blog/data-protection-compliance-insurance-industry

[13] https://digitalpolicyalert.org/event/25955-texas-attorney-generals-issued-fine-following-investigation-into-allstate-and-arity-for-allegedly-unlawful-collection-use-and-sale-of-user-data

[14] https://www.malwarebytes.com/blog/news/2025/01/texas-scrutinizes-four-more-car-manufacturers-on-privacy-issues

GasBuddy, Fuel Rewards, Routely.[15] The collected geolocation data was used to adjust insurance premiums and claims coverage (e.g., real-time driver observation data allows for conclusions about driving patterns and detailed calculation of incident risks).[16] This unfair practice affected the rights of 45 million users and caused them to incur unnecessary insurance costs.

In January 2025, the State of Texas also considers a bill to regulate the use of AI technology in procedures for evaluating patients' use of health insurance.[17,18] Adoption of the bill could prevent insurance companies from making automated decisions to deny coverage.

Russia's experience

In Russia, insurance companies can request medical data for expert examination from territorial funds of mandatory health insurance, and in 2022 the Ministry of Health confirmed the right of insurers to receive such data directly from medical organizations.[19] However, Russian legislation does not provide for special requirements for insurers to process personal data.

3. Taxation of multinational companies

To combat tax dilution by multinational companies (hereinafter - MNCs), the OECD has formed the Global Tax Deal, which consists of two components. The first pillar (Pillar 1) stipulates that large MNCs, especially digital MNCs, must pay taxes in the countries where their customers are located, even if they do not have a physical presence in those countries. The second pillar (Pillar 2) sets the Global Minimum Tax (GMT) on corporate income at 15% for MNCs. (In Monitoring No. 10, we described how the GMT works).

More than 50 countries have already implemented or are planning to implement GMT,[20] with GMT being introduced in Brazil[21] from January 2025. However, in January 2025, the United States announced that it does not recognize GMT for MNCs with headquarters in the United States.

The US experience

In January 2025, the US Presidential Memorandum on the OECD Global Tax Deal was released. The document is directed against the levying the GMT on US companies, in particular against the levy rules on under-taxed income of multinationals.[22] This rule allows countries to levy an additional tax on multinationals (particularly US) if their tax rate in another country is below 15% (the size of the GMT). This compensates for the missing tax revenue if the country where the income is earned does not bring the tax to the 15% level proposed by the OECD.

As a follow-up to the Memorandum, a bill entitled "Protecting American Jobs and Investment Act"[23] was introduced aimed against extraterritorial taxes imposed by foreign countries on U.S. citizens and companies (including against countries that impose the GMT). The U.S. Treasury Department must regularly report on such taxes and then seek their elimination through bilateral negotiations. If a country fails to eliminate such taxes, retaliatory measures may be introduced, including higher taxes on that country's citizens and companies, as well as trade restrictions.

The experience of Brazil

From January 1, 2025, Brazil applies the OECD GMT in the form of an additional levy to the social tax on net income[24] for multinationals with revenues over €750 million. While the previous rate was 9%, foreign multinational companies will now pay an additional 6% on Brazilian income to reach the minimum GMT rate of 15%.

Russia's experience

[15] https://natlawreview.com/article/texas-ag-sues-allstate-violations-texas-privacy-law-first-enforcement-action-under

[16] https://www.theregister.com/2025/01/14/allstate_accused_of_paying_app/

[17] It should be explained that in the United States, the health insurance system provides procedures for regular review of what health services a patient receives under the insurance in order to form individual health benefit plans.

[18] https://digitalpolicyalert.org/event/26245-act-relating-to-use-of-artificial-intelligence-in-utilization-review-conducted-for-health-benefit-plans-sb-815-was-introduced-to-the-senate

[19] https://medvestnik.ru/content/news/Minzdrav-podtverdil-obyazannost-meduchrejdenii-predostavlyat-SMO-originaly-dokumentov.html

[20] https://www.pwc.com/gx/en/tax/international-tax-planning/pillar-two/pwc-pillar-two-country-tracker-summary-v2.pdf

[21] https://legislacao.presidencia.gov.br/atos?tipo=LEI&numero=15079&ano=2024&ato=452EzaE1UNZpWTa29

[22] Undertaxed Profits Rule

[23] https://gop-waysandmeans.house.gov/wp-content/uploads/2023/05/Defending-American-Jobs-and-Investment.pdf

[24] Social Contribution on Net Income, part of the corporate income tax in Brazil.

As early as December 2024, the Russian Finance Ministry released a statement that in mid-2025 a decision will be made “on the need to fine-tune national legislation” in connection with Pillar 2, and if “in 2024 a company paid tax from the Russian tax base outside of Russia”, “countermeasures” will be taken.[25] The statement suggests that the Russian Ministry of Finance may follow a similar approach to the United States when it comes to the implementation of Pillar 2: not implementing GMT and not recognizing the rights of other countries to levy it on Russian companies.

4. Development of regulation of quantum technologies

The OECD experience

In January 2025, the OECD released a Quantum Technologies Policy Primer.[26] Quantum technologies - technologies that use quantum effects (the unique behavior of very small particles at the atomic and subatomic level) to collect, process and transmit information, including quantum sensors,[27] quantum computing,[28] and quantum communication.[29]

The OECD highlights several benefits of quanta. For example, quantum sensors (such as atomic clocks) can facilitate precise time synchronization (down to microseconds) in high-frequency trading on stock exchanges, allowing to determine the optimal moment of time to buy and sell assets in trades. Quantum random number generator generates secure passwords for online transactions. Quantum communication through encryption increases the security of data storage in data centers.[30] For example, in London, BT and Toshiba in 2021 launched a data network with quantum protection for the security of financial transactions (joined by HSBC[31]). The powerful computing capabilities of quantum computers can reduce the cost of expensive training of new AI models - the cost of training the OpenAI model for the first version of ChatGPT GPT-3 was estimated at $4.6 million, and for the GPT-4 version - more than $100 million.

OECD highlights risks related to quantum development:

1. The threat to internet privacy. A quantum computer can decrypt data faster. For example, the fastest supercomputer can crack RSA-2048 (cryptographic algorithm for data protection) in 300 trillion years, while a quantum computer can do it in a few hours. For the reason that hackers could steal encrypted data now and store it until quantum computers arrive to decrypt it in the future, the UK's National Cyber Security Centre recommends companies to implement quantum-resistant solutions - special methods to protect data from quantum computers.

2. Privacy risks. For example, quantum sensors can track people (see through clothes, buildings, materials), intercept communication signals of devices located at a close distance (which allows obtaining information from bank cards and smartphones). The use of quantum sensors in medicine raises the issue of personal data protection: it is required to obtain “informed consent” from the patient for data collection and use - the patient may not understand what information is collected by highly sensitive quantum sensors.

For the development of quantum technologies, the OECD proposes to develop benchmarks (metrics, benchmarks) to evaluate and compare the capabilities of such technologies (e.g. calculated error rate, computational accuracy, code generation speed, sensitivity of sensors); to develop international standards for the development of the technology. For example, standards of the International Organization for Standardization (ISO) (ISO/IEC 4879:2024 dictionary on quantum computing), International Electrotechnical Commission (IEC), European Telecommunications Standards Institute (ETSI) standards (“Quantum Key Distribution” (QKD)), etc. have already been released.

Russia’s experience

[25] https://minfin.gov.ru/ru/press-center/?id_4=39517-aleksei_sazanov_zakonoproekt_o_prodlenii_nulevoi_stavki_nds_dlya_gostinits_budet_podgotovlen_v_pervoi_polovine_2025_goda

[26] https://www.oecd.org/en/publications/a-quantum-technologies-policy-primer_fd1153c3-en.html

[27] Measures physical quantities such as mass, time and light intensity, for example, atomic clocks, photon detectors.

[28] Designed to operate with data; their speed of solving tasks is much faster than a classical computer.

[29] Uses quantum properties of particles to encode and transmit information, for example, quantum key distribution - encrypts cryptographic keys in qubits (quantum cryptography).

[30] For example, used for secure data transmission between Siemens data centers in the Netherlands in 2010.

[31] https://www.toshiba.eu/solutions/quantum/news/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network/

In Russia in 2023, the Concept of regulation of the quantum communications industry (until 2030) was adopted, aimed at creating unified national technical requirements for quantum networks and suppliers of such equipment. Standards defining basic concepts (PNST 830-2023), standards for cryptographic protection of information (PNST 799-2022) and others have been adopted. However, Russia has not solved the problem of assessing security risks and vulnerability to quantum threats at the level of state and public information systems and communication channels (e.g., banking or using blockchain technology), etc. The problem of assessing security risks and vulnerability to quantum threats has not been solved in Russia.