Possible risks of the development of the digital economy

S.A. Livshits
Institute of Digital Technology and Economics
Kazan State Energy University
Kazan, Russian Federation
semen19772004@mail.ru

O.V. Novikova
Nuclear and Thermal Energy
Peter the Great St.Petersburg Polytechnic University
Saint-Petersburg, Russian Federation
novikova-olga1970@yandex.ru

N.A. Yudina
Institute of Digital Technology and Economics
Kazan State Energy University
Kazan, Russian Federation
yudinato@gmail.com

E.K. Nikolaeva
Institute of Digital Technology and Economics
Kazan State Energy University
Kazan, Russian Federation
queennhelenn@yandex.ru

D. B. Katz
N.I. Lobachevsky Institute of Mathematics and Mechanics
Kazan Federal University
Kazan, Russian Federation
katzdavid89@gmail.com

Abstract — **We study the problems of the main types of risks that may be faced by the Russian economy in the transition to the digital format, the likely activities that will help to smooth the negative responses of the risks of the digital economy. State was advised accurately to anticipate and react to rapidly emerging trends in socio-ethical orientation associated with the formation of national and global digital space.**

Keywords — digital economy, risk, digitization, interface, programmers, state

I. Introduction

The digital economy is understood not only as “digitizing” existing state and business processes, but also as the embodiment of something completely new and impossible in the “analog” world. A digital entity carries not only new opportunities and development prospects, but also visible risks.

Everyone has become accustomed to the elements of the digital economy. For example, a lot of interfaces with the state, banks and telecommunications companies in the present, digital, you can do without the participation of people. We use money transfers, make purchases, pay taxes and utility bills, and more. In business, there is also an active use of elements of the digital economy, for example, with the help of information systems, it is possible to attract and serve customers, conduct purchases of the necessary raw materials for production, and so on. All this is perceived as a given, which brings with it not only development, but also problems, which it is more logical to call risks. The huge role of the digital economy is assigned in the development of the banking sector. The digital economy is becoming an increasingly important engine of global economic growth and plays a significant role in accelerating economic development, increasing the productivity of existing industries, shaping new markets and industries, ensuring sustainable growth and development, especially in the Russian banking sector.

II. Materials and methods

Traditional banks define new ways in which they can effectively compete in today's market. Banks of one approach are beginning to embrace open banking, which allows them to better meet customer needs, safely share data with other applications, or use data from third-party sources, providing new innovative services. This allows banks to provide easily manageable information to their customers so that they can independently make the best choice in terms of financial planning, products and services.

III. Results

Banks that want to implement an open banking business model have the opportunity to reduce costs, develop their business and improve customer service using an ecosystem that includes technology platforms, Internet application services, analytical systems and many other applications and services. The main advantages that will be provided to banks and their customers in the transition to open banking services:

- Improving customer service: Banks need to use technologies that manage a customer-centric business model for sales, marketing and service with real-time execution capabilities. It is imperative to provide a consistent, channeloptimized model focused on customer experience that will satisfy the requirements and increase loyalty.
- Predetermine customer needs: “big data” and sophisticated intelligent analytics of structured and unstructured data provide a 360-degree overview of customers, allowing banks to respond to customer needs and offer customized products and services in real time. Paying special attention to highly personalized customer interactions will ultimately pay off, providing the convenience of choice for users.
- Reduced operating costs: increased competition leads to lower profits in the modern global economy. Banks need to implement machine learning algorithms and cloud technologies to help automate and standardize business processes in order to compete effectively. Chat bots and digital

Copyright © 2019, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

helpers can also help employees improve productivity without making large investments.

- Compliance with regulatory requirements and standards: global regulation puts significant pressure on banks. To adapt to changing standards, banks must implement an open system architecture that supports an integrated approach to risk and compliance. This will help support new business processes and future regulatory requirements to which banks may not always be ready.
- Incorporating business models on the platform: investment in open and flexible software platforms and APIs allow banks to respond to competitive challenges created by reforms such as PSD2. Banks need to work with OEMs and suppliers of financial technology to develop new business models and product innovations.

Banks that are planning to move into an open banking sector need to analyze their capabilities, having considered several key steps:

- Evaluate and integrate business processes: Banks need to review their business processes and see if they can connect channels, such as transaction banking and data analytics, in real time to work faster and more flexibly.
- Joint efforts: Banks need to evaluate their network cooperation and determine where it makes sense to joint implementation with partners to achieve growth. This is not a quick process, but it is important to start checking the parameters.
- Employee priority: one of the most important, but often overlooked factors is the priority of the workforce and ensuring that employees are engaged in the digital transformation process and report on how to use new tools.

The time spent on introducing an open banking service is worth because it offers functional advantages. This will lead to even more innovative models and ways of doing business. Let’s denote the main risks.

IV. Discussion

Basic risk is associated with a lack of personnel. It turned out to be very advantageous to go about managing digital methods in business; it became less expensive for companies to serve their customers than in offices. It turns out significant savings on rental space and maintenance of operators. But there was a problem in the staff as there are no so many competent programmers who were able to develop the necessary service system in the labor market. Our talents lure Chinese and American companies, promising them a bright future and huge salaries. On the Russian segment only "Mail.ru" and "Yandex" companies are not lagging behind in recruiting specialists [1]. Of course, there was an imbalance of supply and demand in the market. Where does the satisfaction of demand led us? It led to the training of unskilled web programmers, since it is impossible to master everything in a short time, about a month. Teams from such web developers often win in contests or tenders "who request less for a specific functionality". Such experts are inexpensive. These quick courses are not about secure design and secure architecture. What do we get at the output? Web applications are becoming more sophisticated, because the entire focus of developers is on functionality, although security remains paramount. The same can be compared with information security officers who have been instructed to set up security features, or to the engineers who set up the infrastructure for applications. The rapid growth of digital economy applications also requires the growth of testers, engineers, developers, and security developers. It will take years to train good specialists. It is necessary to make a worthy competition to the Americans and the Chinese on salary and interesting tasks. If you produce weak specialists, you can get a vulnerability and a lot of incidents.

Business does not stand still and requires constant changes, today it is implemented in applications. Accordingly, the applications must also change, be more flexible. We need to change the approach to digital business, starting with the experts and ending with each participant in the process. Some time ago, the “transition to agile” was announced, but since people find it difficult to move from old habits to new ones, there are no expected results yet. Agile is a variety of new approaches and management techniques that: focus the team on the goals and needs of clients; greatly simplify the organizational structure and processes; actively use feedback; work in short cycles; increase employee empowerment; are based on a humanistic approach; are a way of thinking and a way of life. Therefore, not having an army of competent “digitizers” in the field of business and information technology, it is not entirely clear how to “digitize” the economy [2].

The next problem of “digitizing” the economy, which is not so obvious, is the change of places of business and the business of information technology. In a traditional business, information technology is a reflection of it, say, for the purpose of analytics or accounting. First, transactions and contracts take place in the paper-and-cash world, and then all this is recorded in the information technology of the system for the purpose of further analysis and accounting. Suppose that something went wrong with the information technology of the system and the data disappeared. In this case, the business will not suffer, you just have to spend a lot of time to recover data, "recover from the primary." In the digital economy, there is no such thing as a “primary”. Information technology does not reflect the business, they themselves are it. All transactions are made in business applications and digital space. If earlier information technology failed, then payment orders were written out manually, work continued. Now, if the information technology fails, it will lead to a collapse — even analog processes will stop working, because their control is digital. Thus, information technology is the core of a business and in no way its official function. If you slow down the process of introducing such knowledge, then digitalization will not happen soon. So far, innovators and Internet giants, or banks without offices, have a good understanding of this issue [2]. Next, consider the risk of the “Internet of Things”. The Internet of Things is firmly entrenched in our daily lives. We have the ability to manage our car, home appliances, stationary mobile (drones) video surveillance and we can open the door through the use of a mobile application. Such applications bring comfort and optimize resources. For all this it is worth saying thanks to the small controller modules in our devices. Controller modules collect and process information, exchange commands with other devices and respond to commands. Most often, this function of goods is service and not the key one, and, respectively, is cheap. It follows that the manufacturer has saved on security. When the owner of the device, in its digital illiteracy, leaves passwords freely available, this is a loophole for intruders. The minimum resource of the controller modules does not allow for the insertion of "additional" safety into them, while the manufacturers have not yet done anything about the "built-in" safety. There were cases of the most powerful DDoS attacks [3], when video cameras were combined into a botnet. The interception of control and blocking systems have become more frequent lately.

No less important is the risk of artificial intelligence. In the coming years, tools based on artificial intelligence will be a hit in the field of automating recruitment, artificial intelligence technologies have considerable potential for optimizing or even fully automating many routine and volume recruiting tasks and are already showing impressive results. At the same time, they have some limitations and carry certain risks that may affect the quality of your selection, the work of the organization and candidates. The world considers machines to be impartial and fact-oriented, not personal judgments by default, and theoretically it is. The problem is that the "facts", on the basis of which they generate their decisions, are supplied to machines by people. How does this happen? An important aspect of artificial intelligence is that it is capable of learning. "Machine learning" allows you to take a set of data, for example, a number of decisions made by a person, and based on them create an algorithm for making similar decisions for future pieces of information. Here lies the main risk: if past decisions that the artificial intelligence studied contained human cognitive distortions and bias, artificial intelligence would include them in its decisions. This means that artificial intelligence is critically dependent on the information supplied to it for training, not only its volume (and for AI, large amounts of data are needed, for example, from several hundred to several thousand summaries for a particular position), but also quality, since this is directly will affect the quality of subsequent decisions. Artificial intelligence cannot replace a person uniquely. The previous problem has another important aspect. The world can teach artificial intelligence to focus on truly predictive indicators of potential, ignoring useless or false signals and factors. And in this case, artificial intelligence will act much faster and more efficiently for human recruiters. But faster or cheaper forecasting does not solve the fundamental problem when recruiting staff: the need to have reliable criteria or indicators of the success of an employee in his position or in a company. Only when you have reliable employee performance indicators can you create meaningful models to predict future performance and quantify a person's suitability for a role or job. That is, artificial intelligence does not replace, but modifies the work of recruiters; The success of using artificial intelligence algorithms in your company will primarily depend on your ability to determine the indicators that are meaningful to you and teach artificial intelligence to work according to them. This requires human abilities (besides, recruiters are still needed when it comes to building relationships, improving the employer's brand, negotiations, and all other activities where "human touch" is necessary). So, if recruiting is now based on intuitive decisions, is chaotic, depends on personal preferences, does not use confirmed criteria and indicators, then tools based on artificial intelligence will not improve it (or rather even worsen it).

Today, such technologies as voice command recognition, retinal scanning, face recognition from city and home surveillance cameras, user preferences analysis and much more are in great demand. If artificial intelligence is in the hands of an intruder, he will easily pick up a password and prove that he is not a robot. With the introduction and use of artificial intelligence in the digital economy, the ways of malicious use of its vulnerability to commit crimes increase. It is likely the confrontation of two artificial intelligences, in the civil field or the field of weapons. Some technology companies that promote their artificial intelligence tools do not even use machine learning but rely on complex decision trees to move depending on the answers and anticipate the candidate's questions. These types of technologies are not artificial intelligence. They go through the options (a large number of options), but they don't learn. They may be useful, but they are not flexible or "smart." At the moment, this is a marketing noise that can potentially distract from more important problems: the company has a lot of data with which it does not do anything, because it does not know what they can give or what to do with them. Or the company still does not even collect data about the people that it actually has. Or the company does not have a clear understanding of how to select the indicators that are really significant for hiring from the existing data. Machines will not solve these problems for us. There is a possibility of reverse development.

The risk of using the blockchain. In recent years, blockchain has gained considerable popularity both in the financial field and in business, and even in the social sphere. Technologies are used in the Internet of Things, in trade, and blockchain services are constantly being developed for healthcare institutions. The fact that the information already entered into the blocks of the chain cannot be altered or forged is one of the main values of the blockchain. Thanks to this, users can be sure that their transactions will be sent to the address, the balance on cryptowallets will remain unchanged, etc. Despite the fact that sometimes there are annoying exceptions, like attacks on DAO and Bitfinex, in general this thesis remains valid.

However, such a "monolithic" reliability has a reverse side of the coin. For example, an inexperienced user can direct a transaction to the wrong address, and the money will be transferred to a completely different person or company. In this case, EPS service support will not come to the rescue, because Bitcoin and other cryptocurrencies work on a completely different principle.

There is also a risk that the blockchain-wallet address will be entered incorrectly, and the transaction will be "frozen" (that is, the money will not reach the addressee, and it will not be possible to return them). At some point, such transactions are dealt with (for example, during a fork), but how long the process will be in a frozen state is unknown. The risk of making incorrect information in the blockchain is present not only in the financial sphere. For example, when introducing blockchain-medical cards into the health care system, the health worker may make a mistake when entering information into the database. Further, this erroneous information falls into the block, and is duplicated in all subsequent ones. In the end, this can lead to the appointment of improper treatment with serious consequences for health, and sometimes even with a risk to the patient's life. Even if an error is identified, it will be necessary to “rewind” back huge amounts of information, which would entail the risk of data loss and additional resource costs. In essence, the blockchain is a technology for storing data and information about the processing of the data itself. But, there is a difference from other systems, it has a unique principle of operation. The vocation of technology in making a revolution in the economy. If you transfer the processes on the blockchain, the benefits will be obvious, as well as threats. The blockchain platform, as fastdeveloping software, is not ideal and vulnerable, which in turn are grouped with the vulnerability in other smart contacts developed by experts on other blockchain platforms. Vulnerability in the blockchain platform can lead to branching ("forks") in the cryptocurrency ecosystem [2]. The basic principle of branching is the immutability of transactions. For example, if the transaction was confirmed, but was caused by a failure, turned out to be erroneous, incorrect, or fraudulent, it cannot be corrected in any case. From the moment Bitcoin attracted public attention, a certain category of people began to blame cryptocurrency for tokens as a means of money laundering, terrorist financing, drug trafficking, human trafficking and other types of criminal activity. But after Bitcoin appeared Monero, Dash and a number of digital coins, providing greater anonymity and confidentiality of transactions.

In addition, nothing prevents criminals and fraudsters from launching their own cryptocurrency. Already, hype projects aimed only at attracting as many investments as possible, are entering the ICO. As soon as the cash flow dries out, the company disappears with investors' money. Similar schemes were implemented before the blockchain, however, cryptography allows you to run almost a complete analogue of the issue of shares of the company. At the same time, the process is not regulated by anyone, and the company assumes almost no obligations. Although many options for using the blockchain are designed to provide people with greater freedom and, accordingly, security and protection of personal data, in certain situations cryptography can play a reverse role. In 2017, a law on the right to oblivion was passed in Europe. This law provides an opportunity for a citizen of any EU country, subject to certain conditions, to request the removal of personal data from most of the existing databases, first of all, publicly available. Thus, a person can start life "from scratch." However, if the data will be entered into the system based on the blockchain, the possibility of their deletion is questionable. Even though it is technically possible, the consequences of losing a huge amount of other data due to “rewinding” make the concept unrealizable. In addition to the objective risks and drawbacks of the blockchain, there are very controversial theories that can be considered both from a positive and from a negative point of view. For example, a number of experts believe that the blockchain, like other process automation systems, threatens the loss of jobs to millions of specialists. Despite the fact that automation is economically beneficial, from a social point of view it is a problem.

The risks that the blockchain development entails are justified many times by the benefits this technology brings to the world. However, knowledge and a sober assessment of negative factors will help avoid a number of problems that may result from the thoughtless use of the mechanism.

V. Conclusion

Digital economy is a useful goal and quite promising. Achievements in the development process will undoubtedly benefit; inefficient business processes are optimized, huge resources will be released, government management processes will be optimized, and government and business will be more manageable and transparent. The serious risks described above may overwhelm advances in the digital economy. When designing a digital system, one should think over in advance all possible risks in order to reduce their influence and slowing down the development of the digital economy. When constructing the system architecture and its design, its safety must first be taken into account. It is necessary to eradicate the principle, which is still appropriate, “here's the system that we have done, and now your job is to come up with a security.” It is necessary to create information security not with the additional systems. It is necessary to make it a built-in function for each information technology system. Only in this case is it possible to avoid risks.

References

[1] Akhromeeva T. S., Malinetsky G. G., Posashkov S. A., “ Digital reality strategies and risks,” http://sec.chgik.ru/ctrategiii-riskitsifrovoy-realnosti/

[2] Andriyashin Yu. N., “About goals, possible risks and consequences of a “digital economy”, ”http://reosh.ru/yu-n-andriyashin-o-celyaxvozmozhnyx-riskax-i-posledstviyax-cifrovoj-ekonomiki.html

[3] Rossiyskaya Gazeta RG.RU, https://rg.ru/2018/02/28/

[4] Avdeeva I.L., Golovina T.A., Parakhina L.V. “ Development of digital technologies in economics and management: Russian and foreign experience,” -2017.-11p.

[5] Order of the Government of the Russian Federation of 28.07.2017 N 1632 On approval of the program "Digital economy of the Russian Federation".

[6] «Bet Expert» https://bitexpert.io/wiki/riski-tehnologii-blokchejn/

[7] «Talent Skan» https://www.talentscan.pro/ru/blog/riski_ispolzovaniya_ii/

[8] RCFA (Russian Council on Foreign Affairs)

[9] Sibac.info https://sibac.info/studconf/science/lxi/131530 https://russiancouncil.ru/analytics-and-comments/analytics/iskusstvennyy-intellekt-blago-ili-ugroza-dlya-chelovechestva/