

Cybersecurity Measures of the Digital Payment Ecosystem

Alexander Olifirov¹, Krystina A. Makoveichuk¹, Sergei Petrenko²

¹ V.I. Vernadsky Crimean Federal University, 4, Akademika Vernadsky Avenue, Simferopol, 295007, Russia

² Saint Petersburg Electrotechnical University "LETI", 5, Professor Popov Street, St. Petersburg, 197376, Russia

Abstract

The article discusses the cybersecurity measures of digital payment ecosystems in modern conditions. It is shown that new instruments and work with digital national currencies supplement payment ecosystems. The cybersecurity of its platform and ecosystem has been identified as a major challenge in the implementation of the digital currency concept. Cybersecurity measures are classified: legal, technical, organizational, capacity-building, joint actions. The set of cybersecurity measures that need to be applied for the successful implementation of the digital ruble is highlighted: continuous monitoring and updating of the national cybersecurity strategy; creation and development of national and industry Computer Incident Response Teams; the use of a specialized software module of the Bank of Russia integrated with mobile applications of credit institutions; implementation of cryptographic protection of channels of user interaction with the infrastructure of the credit institution; generation and storage of a cryptographic key for a credit institution's client to access a digital wallet; conducting research by the central bank in the field of ensuring the offline regime in the transition to the digital ruble, providing access to the digital ruble platform based on the exchange of incident notifications, exchange of best practices, harmonization of minimum security measures within the framework of multilateral agreements on cybersecurity. It is proposed to form a budget and assess the feasibility of investments in cybersecurity, taking into account the definition of all risks, their quantitative measurement, and their prioritization.

Keywords

Digital ruble, cybersecurity measures, platform model, digital payment ecosystem

1. Introduction

Digital technologies (big data, wireless technologies, artificial intelligence, virtual and augmented reality technologies) are the basis for all levels of the digital economy, as are distributed registry systems and platform solutions. Today, platforms are becoming technological ecosystem giants, more and more the rules of the game in the economy. These ecosystem formation processes take place in electronic payment systems. The electronic payment system is a technology that is a set of methods and arrangements to provide a payment service between parties on the Internet and in other data transmission networks.

An E-payment (digital) ecosystem is a set of services, including platform solutions, of one group of companies or companies and partners, allowing users to receive a wide range of payment services within a single seamless integrated process (Fig. 1).

The ecosystem may include closed and open platforms (Table 2 and 3).

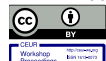
A closed platform does not publicly announce the rules by which participants are admitted to it. In the open model of the platform, competing suppliers of goods and services have access to it; their admission to the platform is based on publicly disclosed criteria.

The problems of digital payments are relevant and are addressed in many works by domestic and foreign authors [1-7].

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia

EMAIL: alex.olifirov@gmail.com (A. 1); christin2003@yandex.ru (A. 2); s.petrenko@rambler.ru (A. 3)

ORCID: 0000-0002-5288-2725 (A. 1); 0000-0003-1258-0463 (A. 2); 0000-0003-0644-1731 (A. 3)

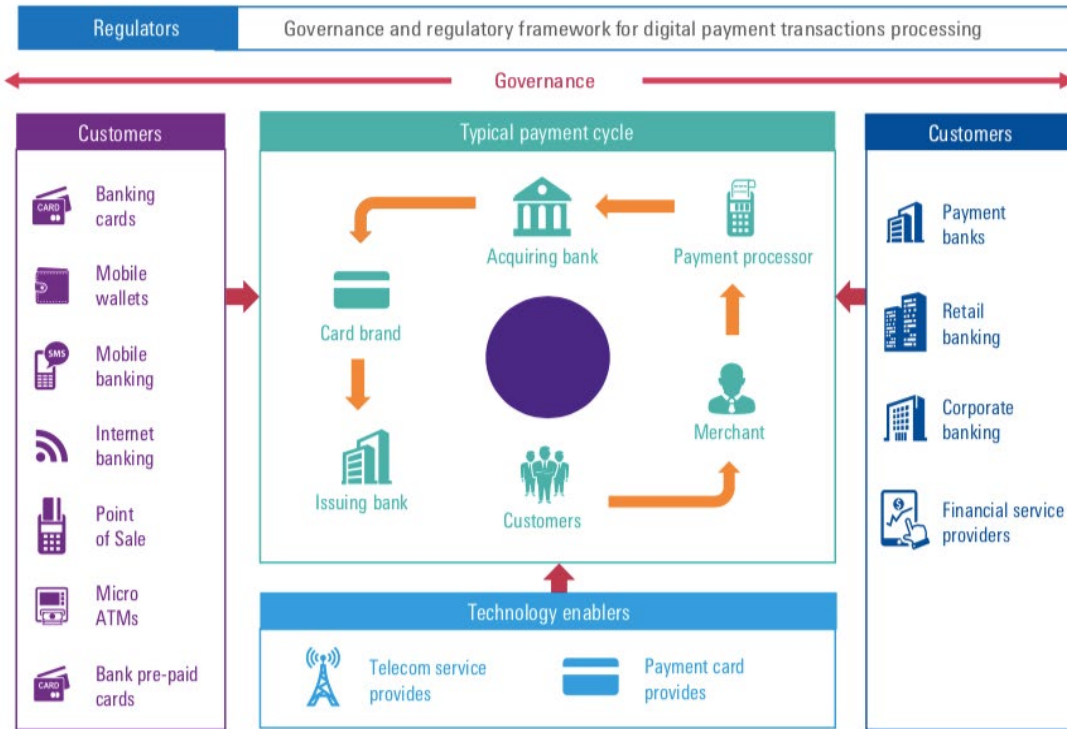


© 2021 Copyright for this paper by its authors.

Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings (CEUR-WS.org)

Digital payment - Ecosystem



Source: For illustrative purpose only, KPMG in India

Figure 1: Digital payment ecosystem scheme³

Table 1
Largest global payment ecosystems














Ecosystem platform	Finance	
	Payments	Other financial services
Google	Google Pay	
Apple	Apple Pay	Apple Card
Facebook	Friend to friend pay	
Amazon	Amazon pay	Amazon lending
Alibaba	Ant Financial	Ant Financial
Tencent	WeChat Pay	WeBank

- Closed platform model

³ https://www.cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf

 - Open platform model

Table 2
The largest Russian payment ecosystems

Ecosystem platform	Finance	
	Payments	Other financial services
SBER	SBER 	SBER 
Yandex	Yandex Pay 	Yandex.plus bill 
Tinkoff	Tinkoff 	Tinkoff 
@mail	Money.Mail.ru 	VK Pay 
VTB	VTB 	VTB  Meter square 
MTS	MTS 	MTS 

 - Closed platform model

 - Open platform model

The introduction of the Bank of Russia Digital Ruble (RBDR)⁴ is a response to the challenges of global technology companies, which, through their global presence, are uniquely positioned to offer services in the area of global cross-border transactions. Today, the new major players in the financial services market (Big Tech, also known as the Tech Giants) are the digital companies that dominate the US information technology industry, namely Amazon, Apple, Google (Alphabet), Facebook, and Microsoft.

The proliferation of digital currencies offered by foreign companies will make Russian payments dependent on technologies developed and regulated in other countries. At the same time, digital currency as a new digital asset creates a new vulnerability to cyber-attack. In this regard, Russia, like other states, in the transition to digital currency, has to do a lot of work to create the necessary technical solutions to ensure the appropriate level of cybersecurity of the corresponding system.

Therefore, it seems logical to consider what cybersecurity of a payment system can be when paying with a digital ruble, based on possible models and mechanisms for implementing a digital currency, and what cybersecurity measures can be applied.

2. Research methodology

The sphere of cybersecurity is constantly changing, as threats, vulnerabilities, risks, countermeasures in the internal and external environment are constantly changing [8, 9]. In this case, for defining cybersecurity measures, a methodology is needed that would take into account these changes and would meet the challenges of today.

The work provided a critical review of the literature on the study conducted in areas of interest and references to the Global Cybersecurity Index (GCI) and its methodology. This helped to define and apply the following guidelines in this study.

⁴ Concept of the digital ruble. Bank of Russia. URL: http://www.consultant.ru/document/cons_doc_LAW_381918

1. Cybersecurity issues are addressed through a multidisciplinary and holistic approach in line with the national concept of cybersecurity.
2. The structure of cybersecurity measures is based on five pillars: legal measures; technical measures; institutional measures; capacity-building measures; and cooperation measures.
3. The implementation of the digital currency concept is based on the development of both the national, and industry (financial and credit) Computer Emergency Response Team (CERT). The Bank of Russia Computer Emergency Response Team (FinCERT) was established in 2015 to consolidate financial and information security market participants in the fight against computer crime.

The study aims to help payments ecosystem actors identify threats and cybersecurity measures, improve overall cyber-security, harmonize practices and promote a culture of cybersecurity in the payments ecosystem, in the context of digitization.

3. The main part of the research

At the end of June 2021, the International Telecommunication Union (ITU) of the United Nations published a new edition of the Cybersecurity Ranking of Countries. Russia ranked fifth with 98.06 out of 100 possible (table 1).

Table 3
Global Cybersecurity Index of Russia

No.	Indicators	Year of publication GCI-3 2019	Year of publication GCI-4 2021
1	Ranking place	28	5
2	Countries providing focal points	155	169
3	Years of data collection	2017-2018	2020

The structure of the cybersecurity index of Russia is shown in Figure 2.

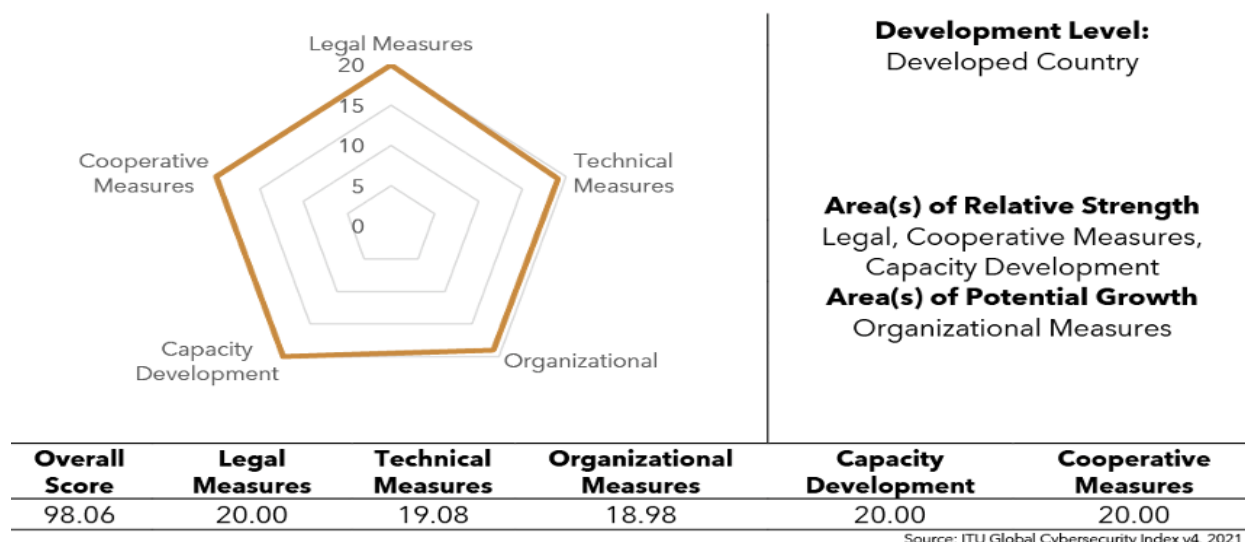


Figure 2: The structure of the cybersecurity index of Russia

The rating showed that the number of countries with cybercrime legislation had increased. The number of countries with a National Cyber Security Strategy has also increased. More than 50 percent of States reported that they had set up “Computer Emergency Response Team”. This represents an increase of 11 percent over 2018. In 2020, 64 percent of States reported that they had adopted national cybersecurity strategies (58 percent in 2018), and more than 70 percent had conducted awareness-raising campaigns (66 percent in 2018)⁵.

To implement the concept of the digital ruble, it is necessary to create a new payment infrastructure, integrated with the main one, allowing online and offline payments. Transactions with the digital ruble can be carried out through special payment applications similar to Google Pay, Apple Pay, and other similar services, or using remote banking services, mobile and online banks, using contactless payment technology.

Over the past two decades in Russia, the financial sector, as well as those companies that develop ecosystems that use payment technologies, have done a great job of introducing a culture of cashless payments. In recent years, according to literary sources, there has been an increase in the use of remote channels of access to financial services and non-cash payments by the population. According to the studied statistics, the share of non-cash payments by the population for goods and services in the total volume of retail trade, catering, and paid services to the population increased from 39% in 2016 to 70% in 2020. It is expected that the technology of using the national digital currency will be similar to the existing technologies of payments based on mobile phones, making it understandable for users.

Next, consider the conceptual two-tier retail model of the digital ruble shown in Fig. 1.

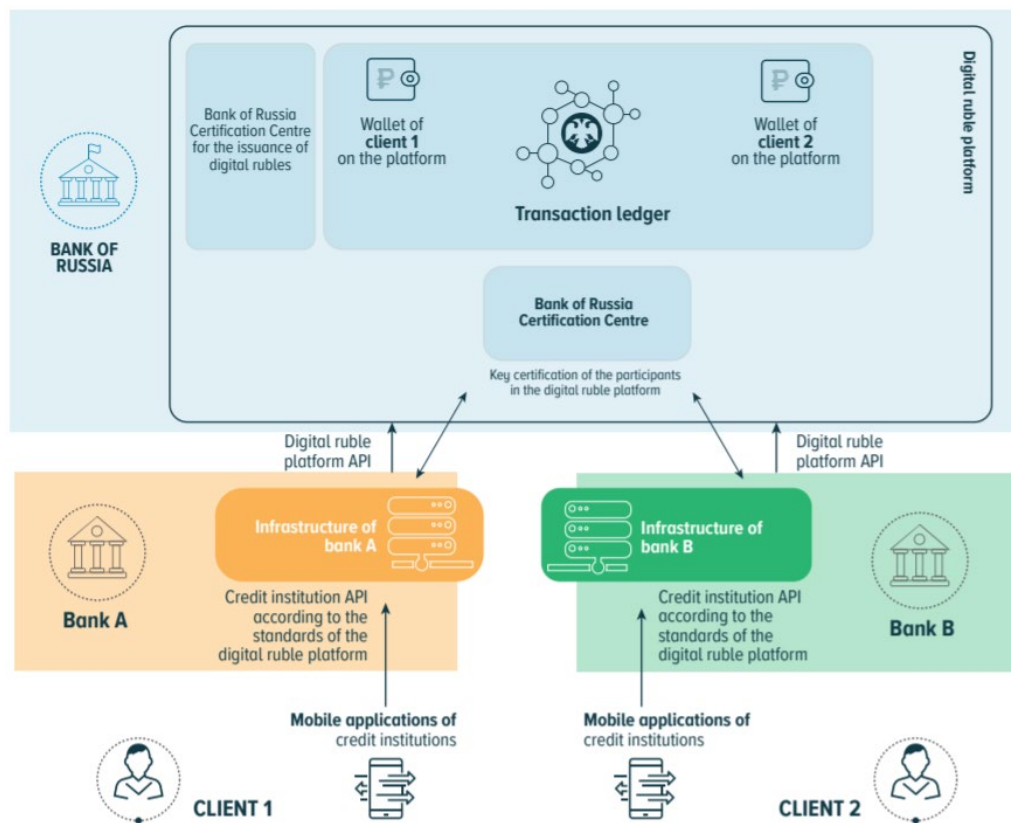


Figure 3: Two-tier retail model of the digital ruble⁵

So, at the first stage of the transition to the digital ruble, it is necessary to test the emission of the digital ruble, transfers between individuals, and the interaction of the client, the bank, and the digital ruble platform. At the second stage of the transition to digital currency, it is necessary to conduct tests on payment for goods and services, on transferring non-cash money into digital rubles, and vice versa -

⁵ https://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf

digital rubles into non-cash funds. The new functionality, which is the most complex and has not yet been fully studied in terms of implementation details, is offline calculations, that is, calculations in the absence of Internet access. If the possibility of offline settlements in digital rubles is realized (when implementing the government's plans to provide access to the Internet for every resident of the country in every locality), it is planned to provide for some measures aimed at protecting the interests of users (the possibility of restoring payments in case of loss of a device, limiting the number and total amount of transactions that can be performed during a certain period, the introduction of a limit on the amount of a single transaction).

The main types of computer attacks in the sphere of credit and finance in 2019-2020 are presented in materials prepared by the Bank of Russia Computer Emergency Response Team (FinCERT) of the Information Security Department of the Bank of Russia. The Federal Service for Technical and Export Control (FSTEC) has developed the Information Security Threat Assessment Methodology. These materials can be used to create a cybersecurity system for the transition to digital currency. As the analysis of literary sources on cyber-threats and cyberattacks, in general, has shown, the threats to the digital ruble are the same as those to the clearing of bank accounts and cards, as well as the risks inherent in the segment of cryptocurrencies [10-15]. The types of threats to cybersecurity in the digital payment system when switching to the digital ruble are presented in Table 4.

Table 4

Types of cybersecurity threats in the digital payment system during the transition to the digital ruble

Type of threat	Threat name
Breach of confidentiality	<ol style="list-style-type: none"> 1. Risk of unauthorized access to the digital ruble platform 2. Risk of Digital Ruble User Profile being stolen through personal hacking 3. Risk of unauthorized access when using a credit organization's mobile application
Breach of integrity	<ol style="list-style-type: none"> 1. Risk of integrity loss when signing transactions with the digital ruble. 2. Risk of integrity loss in the case of digital ruble emissions.
Accessibility disrupt	<ol style="list-style-type: none"> 1. The risk of underperforming distributed ledger technology 2. Risk of refusal to implement offline mode on the digital ruble platform 3. Unavailability of the infrastructure of trade and service enterprises and credit organizations, small and medium-sized enterprises

Cybersecurity is a multi-disciplinary area, involving all sectors, industries, and stakeholders, both vertically and horizontally [16-23]. The Multi-stakeholder Framework on Cybersecurity seeks to create synergies between ongoing and future initiatives and focuses on the following five pillars, which form the building blocks of a national cybersecurity culture (Table 5).

Table 5

Cybersecurity measures for digital payment systems when switching to digital ruble

Type of cybersecurity measures (pillars)	Cybersecurity measures
1. Legal measures	<ol style="list-style-type: none"> 1. Federal Law 259-FZ, dated July 31, 2020, "On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation" (last edition). 2. National standard (governmental standard) of the Russian Federation GOST R 57580.1-2017 "Security of financial (banking) operations. Protection of information of financial institutions. Basic composition of organizational and technical measures".

Type of cybersecurity measures (pillars)	Cybersecurity measures
	<p>3. Bank of Russia Standard “Ensuring information security of organizations of the banking system of the Russian Federation. Collection and analysis of technical data in response to information security incidents during money transfers” STO BR IBBS-1.3-2016.</p> <p>4. Federal Law 115-FZ, dated Aug. 07, 2001, «On Prevention of Legalization (Laundering) of Proceeds from Crime and Financing of Terrorism»).</p>
2. Technical measures	<p>1. Technical measures of cybersecurity are presented in the form of various electronic equipment and communication networks, specialized software that performs protective functions (together with other means of protecting information or independently). In addition, cybersecurity measures are represented by systems for supporting search and applied research in the field of new technologies that ensure national security.</p> <p>2. Cryptographic protection of user interaction channels with the infrastructure of a credit institution (encryption) when using a mobile application using cryptographic information protection tools, certified by the FSB of Russia.</p> <p>3. Generation and storage of a cryptographic key for a credit institution's client to access a digital wallet</p> <p>4. Creating Computer Incident Response Teams (CIRTs) or Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) allows you to respond to incidents at the national level with a centralized contact point.</p>
3. Organizational measures	<p>Organizational measures include the definition of cybersecurity goals and strategic plans, as well as the formal definition of institutional roles, responsibilities, and responsibilities to ensure their implementation. These measures are indispensable in supporting the development and implementation of effective cybersecurity policies. The Bank of Russia should establish general strategic goals and objectives, as well as a comprehensive implementation and measurement plan. National agencies should be present to implement the strategy and evaluate the results. Without a national strategy, governance model, and oversight body, efforts across sectors collide, hampering efforts to achieve effective harmonization in cybersecurity development.</p>
4. Capacity development measures	<p>Public awareness measures, certification, and accreditation of cybersecurity professionals, cybersecurity training courses, educational or academic programs, etc.). Measures to raise awareness, knowledge, and know-how in all sectors, for systematic and appropriate solutions and to promote the development of qualified professionals.</p>
5. Cooperative measures	<p>Ensuring cybersecurity on the digital ruble platform based on joint structures and networks for the exchange of information, exchange of notification of incidents, exchange of best practices within the framework of multilateral agreements on cybersecurity.</p>

Cybersecurity measures (technical, strategic planning, capacity building) are investigated in [24].

Effective mechanisms and institutional structures at the national level are needed to reliably counter cyber risks and incidents. Computer Incident Response Teams (CIRTs) or Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) enable countries to respond to incidents at the national level through a centralized point of contact and facilitate rapid and systematic action, allowing countries to learn from experience and build cyber resilience [24].

The cybersecurity costs of introducing the digital ruble will not necessarily reduce risks. Most of the funds will be spent on the introduction of new technologies that may be useless if you do not consider how the tool will be used and what threats it will be aimed at. Cybersecurity budgeting should begin with a thorough assessment of the threats, as well as the existing and potential risks associated with the digital ruble. After identifying all these risks, quantifying them, and prioritizing them, the Central Bank of the Russian Federation must determine a strategy to ensure cybersecurity. Only when all risks are taken into account in the strategy and the means of their control are determined, the Central Bank will be able to ensure proper effective and continuous management of cyber risks, and will be able to correctly form the budget in the field of cybersecurity. Assessing the feasibility of investing in cybersecurity can be performed using the guidelines presented to the US Agency for International Development in May 2020.

4. Conclusions

As a result of the research, the following main cybersecurity measures in the digital payments ecosystem during the transition to the digital ruble have been identified.

1. Continuous monitoring and updating of the national cybersecurity strategy with clear implementation plans.
2. Continuation of the creation and development of national and sectoral CIRT.
3. Application of a specialized software module of the Bank of Russia integrated with mobile applications of credit institutions.
4. Implementation of cryptographic protection of the channels of user interaction with the infrastructure of the credit institution (encryption) when using the mobile application of the credit institution with the use of cryptographic information protection tools, certified by the FSB (Federal Security Service) of Russia.
5. Generation and storage of a cryptographic key for a credit institution's client to access a digital wallet and sign orders for transactions with digital rubles.
6. Application of complex technological measures for information protection (logical control, structural control, duplication control, authorship control); organization of control over the integrity of "smart contracts".
7. Creation of digital rubles exclusively with the use of the issue key of the Bank of Russia. The Bank of Russia issue key is registered in the specially designated Certifying Center of the Bank of Russia (CC BR) for issues.
8. Conducting by the Central Bank of scientific research in the field of providing an offline regime in the transition to digital ruble.
9. The introduction of the digital ruble in stages, which will allow banks and trade and service enterprises, small and medium-sized enterprises to increase their potential and adapt their infrastructure for settlements in the digital ruble.
10. Ensuring access to the digital ruble platform and business continuity based on information exchange networks, exchange of incident notifications, exchange of best practices, harmonization of minimum security measures within the framework of multilateral agreements on cybersecurity.
11. Budgeting and assessing the feasibility of investments in cybersecurity, taking into account the identification of all risks, their quantitative measurement, and their prioritization.

5. References

- [1] Benoît Dupont. The cyber-resilience of financial institutions: significance and applicability, *Journal of Cybersecurity*, volume 5, issue 1, 2019, tyz013. DOI: 10.1093/cybsec/tyz013.
- [2] E. G. Xomenko, E`lektronny`e platzhny`e sistemy` v Rossii i v zarubezhny`x stranax [E. G. Khomenko, Electronic payment systems in Russia and in foreign countries] / Aktual`ny`e problemy` rossijskogo prava [Actual problems of Russian law], 2019. DOI: 10.17803/1994-1471.2019.105.8.159-164. (In Russ).
- [3] H. C. Yu, K. H. Hsi, P. J. Kuo, Electronic payment systems: an analysis and comparison of types, *Technology in Society*, 24(3) (2002), pp. 331-347. DOI: 10.1016/s0160- 791x(02)00012-x.
- [4] K. S. Staykova, J. Damsgaard, Adoption of mobile payment platforms: managing reach and range, *Journal of Theoretical and Applied Electronic Commerce Research*, 11(3) (2016). DOI: 10.4067/S0718- 18762016000300006.
- [5] B. Sivathanu, Adoption of digital payment systems in the era of demonetization in India, *Journal of Science and Technology Policy Management*, 10(1) (2019), pp. 143-171. DOI: 10.1108/jstpm-07-2017-0033.
- [6] S. U. J. Raharja, H. A. Muhyi, T. Herawaty, Digital payment as an enabler for business opportunities: A go-pay case study, *Review of Integrative Business and Economics Research*, 9(1) (2020), pp. 319-329. URL: http://buscompress.com/uploads/3/4/9/8/34980536/riber_9-s1_25_b19-102_319-329.pdf.
- [7] Wan Rung Lin, Chun-Yueh Lin and Yu-Heng Ding, Factors Affecting the Behavioral Intention to Adopt Mobile Payment: An Empirical Study in Taiwan, *Mathematics*, 8(10) (2020) 1851. DOI: 10.3390/math8101851.
- [8] Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of Software Vulnerability Detection in Certification Testing. *Journal of Physics: Conference Series*. 2018. V. 1015. P. 042033. DOI :10.1088/1742-6596/1015/4/042033
- [9] Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
- [10] Max Boholm, Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019), *Journal of Cybersecurity*, volume 7, issue 1, 2021, tyab016. URL: <https://doi.org/10.1093/cybsec/tyab016>.
- [11] Amir Feder, Neil Gandal, J. T. Hamrick, Tyler Moore, The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox, *Journal of Cybersecurity*, volume 3, issue 2, June 2017, pp. 137–144. DOI: 10.1093/cybsec/tyx012.
- [12] Ioannis Agraftotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, David Upton, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, *Journal of Cybersecurity*, volume 4, issue 1, 2018, tyy006. DOI: 10.1093/cybsec/tyy006.
- [13] Aaron F. Brantly, Risk and uncertainty can be analyzed in cyberspace, *Journal of Cybersecurity*, volume 7, issue 1, 2021, tyab001. DOI: 10.1093/cybsec/tyab001.
- [14] J. Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*, Cambridge: Harvard University Press, 2018.
- [15] E. Conrad, S. Misenar, J. Feldman, *CISSP Study Guide*, 3rd edition, Boston: Syngress, 2015, pages 622. doi: 10.1016/C2009-0-61065-5.
- [16] A.V. Olifirov, K.A. Makoveichuk, P.Y. Zhytnyy, T.N. Filimonenkova, S.A. Petrenko, Models of Processes for Governance of Enterprise IT and Personnel Training for Digital Economy, *Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES 2018*, 8604166, pp. 216-219. doi: 10.1109/PTES.2018.8604166.
- [17] Jonathan Z Bakdash, Steve Hutchinson, Erin G Zaroukian, Laura R Marusich, Saravanan Thirumuruganathan, Charmaine Sample, Blaine Hoffman, Gautam Das, Malware in the future? Forecasting of analyst detection of cyber events, *Journal of Cybersecurity*, volume 4, issue 1, 2018, tyy007. URL: <https://doi.org/10.1093/cybsec/tyy007>.

- [18] A. A. Petrenko, S. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, Methodological recommendations for the cyber risks management, CEUR Workshop Proceedings, volume 2914, (2021), pp. 234-247. URL: <http://ceur-ws.org/Vol-2914/paper20.pdf>.
- [19] A. S. Petrenko, S. A. Petrenko, K. A. Makoveichuk, P. V. Chetyrbok, Protection model of PCS of subway from attacks type «wanna cry», «petya» and «bad rabbit» IoT, Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2018, 2018-January, pp. 945-949. DOI: 10.1109/EIConRus.2018.8317245.
- [20] Petrenko S. Cyber resilient platform for internet of things (IIoT/IoT)ed systems: survey of architecture patterns. *Voprosy kiberbezopasnosti [Cybersecurity issues]*. 2021. N 2 (42). P. 81-91. DOI: 10.21681/2311-3456-2021-2-81-91.
- [21] S. A. Petrenko, A. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, Development of a Cyber-Resistant Platform for the Internet of Things Based on Dynamic Control Technology. In: Singh P.K., Veselov G., Vyatkin V., Pljonkin A., Doderio J.M., Kumar Y. (eds) *Futuristic Trends in Network and Communication Technologies. FTNCT 2020. Communications in Computer and Information Science*, volume 1395 (2021), pp. 144-154. Springer, Singapore. URL: DOI: 10.1007/978-981-16-1480-4_13.
- [22] S. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, Concept of cyber immunity of industry 4.0, CEUR Workshop Proceedings, volume 2603, (2019), pp. 93-99. URL: <http://ceur-ws.org/Vol-2603/paper20.pdf>.
- [23] S. A. Petrenko, K. A. Makoveichuk, A. V. Olifirov, New Methods of the Cybersecurity Knowledge Management Analytics. In: Sukhomlin V., Zubareva E. (eds) *Convergent Cognitive Information Technologies. Convergent 2018. Communications in Computer and Information Science*, volume 1140 (2020), pp. 296-310. Springer, Cham. URL: DOI: 10.1007/978-3-030-37436-5_27.
- [24] Petrenko S. *La Administración de la Ciberseguridad. Industria 4.0. Publicado según la decisión del consejo de redacción de la Universidad de Innopolis. Universidad de Oviedo, Universidad de Innopolis. Oviedo, Asturias, 2019.*