IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/38DigECO/2021/3821321/
Vol. 2021 (37), Article ID 3821321

Analyzing the Risks and Security of Electronic and Digital Money

Natalia V. GORODNOVA
Ural Federal University, Ekaterinburg, Russia, n.v.gorodnova@urfu.ru

Elena G. SHABLOVA
Ural Federal University, Ekaterinburg, Russia, e.g.shablova@urfu.ru

Dmitry L. SKIPIN
Tyumen Territorial Institute of Professional Accountants, Russia, d.l.skipin@utmn.ru

Anastasiya A. PESHKOVA
Ural State University of Economics, Ekaterinburg, Russia, np91@list.ru

Ivan S. ROZHENTSOV
Ural Federal University, Ekaterinburg, Russia, rozivan@yandex.ru

Correspondence should be addressed to: Natalia V. GORODNOVA; n.v.gorodnova@urfu.ru

* Presented at the 38th IBIMA International Conference, 23-24 November 2021, Seville, Spain

Abstract

Building a digital economy allows, on the one hand, opening up additional social and economic opportunities for society (the introduction of digital monetary systems), thus increasing the quality of life. However, on the other hand, it may generate various risks and threats to the security of electronic and digital platforms in the form of hacks and cyber-attacks. Electronic money (EM) (or electronic funds (EF)) is one of the most important elements of the current stage of economic development. The relevance of the research topic is due to the insufficient elaboration of the legislative framework for the circulation of electronic money and digital currencies, and, consequently, the possibility of the emergence of various economic and legal risks and threats that reduce the security of electronic money transfer operations.

The purpose of the research paper is to identify and assess the economic and legal risks of the EM system, as well as to develop recommendations for improving the safety of the EM application.

Based on the systematization of the EM regulation models, the authors make a conclusion regarding the need for a special regulatory and legal framework regulating the sphere of circulation of electronic and digital money in Russia. Based on the analysis of the risks and security associated with the emission of electronic and digital money, recommendations for managing these risks are developed.

Keywords: Electronic Money (EM), Digital Money, Cryptocurrencies, Transactions, Risk, Cyber-Attacks, Security.

Cite this Article as: Natalia V. GORODNOVA, Elena G. SHABLOVA, Dmitry L. SKIPIN, Anastasiya A. PESHKOVA and Ivan S. ROZHENTSOV, Vol. 2021 (37) "Analyzing the Risks and Security of Electronic and Digital Money", Communications of International Proceedings, Vol. 2021 (37), ISBN: 978-0-9998551-7-1, ISSN: 2767-9640. Article ID 3821321

Introduction

According to expert forecasts, in the next 5-10 years, humanity will enter the era of the digital economy in full. Following the digital economy, digital actions, digital products, digital money, etc. will move into the world of numbers. In this regard, the Central Bank of the Russian Federation has outlined the prospects for the introduction of the digital ruble, and China has already issued the digital yuan. Digital money and cryptocurrencies are not intended to replace existing cash and non-cash money supply, but to supplement existing tools with new opportunities. The financial regulator (Bank of Russia) indicates the prospects for the cryptoruble - the three forms of the Russian ruble will be equivalent and will have equal value, so money owners will be able to freely transform rubles from one form to another and accumulate digital money in electronic wallets created by the regulator. From a technical point of view, a digital ruble is a unique digital code recorded on a medium.

Today, the digital economy is more often identified with digital commerce over the Internet using electronic money (EM) or electronic funds (EF) (Savelyev, 2016). The digital economy is an economy based simultaneously on digital carriers (digital products, digital money, and the digital economy - this is what is associated with the digital essence of space) and material carriers (goods, transport, infrastructure, cash). A digital product should be created in the digital space based on digital methods and models, and applied there, in the digital space, by digital users. A digital image of a product or service (if it is protected against digital viruses) can exist indefinitely within a certain digital territory. Digital territories are a way of expanding real territories where the production and sale of goods and services is located via digital technologies.

Using digital technologies, we can connect to any continent and any territory and form a repository of large databases there or use this territory as a virtual volume of data storage, thus creating a new virtual reality. Conceptually, this technical solution has been found and the main vector for the development of the digital economy has been identified. The main task is to find mechanical solutions since the digital space has already been created in the form of the global network - the Internet and a huge variety of digital platforms, programs, and models. It is necessary to create hardware and methods for digitizing a person's personality for the purpose of communication between a person and the digital space. In addition, it is necessary to find mechanisms that will give to a living being (intelligence) an opportunity to penetrate the virtual digital space. All of the above is fundamentally different from the ideas that mankind now has about the digital space, using which it will have to learn how to make profit and create conditions for work.

In this regard, electronic money (EM) and digital money are some of the most important elements of the modern stage of transiting to the digital economy. The relevance of the research topic is due to the possibility of the emergence of various economic and legal risks and threats that reduce the security of electronic money transfer operations.

The main purpose of the research paper is to identify and assess the economic and legal risks of the EM system, as well as to develop recommendations for improving the safety of the EM application.

In the context of the colossal influence of the rapidly developing social networks and social digital platforms, the system of cash and non-cash funds is gradually becoming history due to obsolescence and a decrease in the comfort of use. By mid-2020, Ecuador, Uruguay and Ukraine have already completed test studies of the digital national currency, a number of countries (Canada, England, Japan, Sweden, Switzerland, China) are at the stage of implementation of pilot projects.

Methods. Models of economic and legal regulation of the electronic money system

The methodological basis of the research is the general scientific dialectical method of cognition, the system method, the method of comparative legal analysis, the formal logical method of interpreting law, as well as the normative and the formal legal methods. The empirical basis of the research is made up of materials from both published and unpublished case history.

There is a variety of expert opinions in the issue of economic and legal regulation of EM: on the one hand, EM is a right of claim, a debt document, an equivalent of money, an electronic record, an account, a program code, money, etc.; on the other hand, the existing models of regulating cash and non-cash monetary circulation do not fully ensure the adaptation of EM in the legal environment (Savelyev, 2016).

Modern scientific approaches should be focused on forming a new economic and legal concept of electronic (digital) money in order to obtain a unified regulatory and legal approach to regulating the circulation of electronic money, taking into account international practice (among other things).

The systematization of the accumulated world experience and the assessment of existing approaches make it possible to single out such trends for implementing the EM system as the European, Asian, and American. This distinction is based on the concept of legal regulation. In the European system, EM is assigned the status of a new payment instrument as a right of claim, that is, EM means money that is stored electronically, on a magnetic medium, and that is issued by the operator upon receipt of money and is accepted by legal entities and individuals that are not EM issuers. Thus, a conditional emission of funds is carried out, which is identical in its meaning to non-cash funds, where, by transferring money to an issuer (operator), a client receives the right to request that the operator carry out the necessary payment transactions.

In the Asian system, EM is recognized as a legal payment instrument, and the conventional emission of EM is performed on the basis of state financial institutions without the participation of the Central Bank [14]. This system can be called transitional, it allows the emission of EM, but there are restrictions not only in terms of the financial stability of the issuer but also in the volume of EM issuance. The American trend is based on recognizing EM as a new type of monetary services, therefore, the emphasis on using EM is shifting to the sphere of rules for the forms of payment (Bazhanov, Booth, 2016).

In Russia, one can see the process of establishing the institution of legal regulation of EM. The impetus for the development of the regulatory framework is the adoption of federal law No. 161-FZ dated 27 June 2011 “On the National Payment System”. However, the provisions of this law require revision in terms of defining the term “electronic money”, settlement mechanisms, and the structure of the system itself.

The text of the law provides a definition of “electronic money” - it is “money that is previously provided by one person to another person, taking into account information on the amount of funds provided without opening a bank account, to fulfil the monetary obligations of the person who provided the funds to third parties and in respect of which the person who provided the funds has the right to transmit orders exclusively using electronic payment instrument”.

Recognizing EM as “funds” is, undoubtedly, a revolutionary position that requires the development of a sound economic and legal concept. The simultaneous existence of two payment instruments as types of funds (cash and EM) presupposes their independent existence, excluding double counting of the money supply and distortion of data in the circulation of funds (Korostelev, 2013). It should be noted that the independent existence of funds begins upon their issuance. Recognizing EM as an independent type of funds is determined by the moment of their creation.

Russian laws provide for derivative methods of generating EM (using cash) excluding any possible methods of initial placement (emission) of EM. The fact that no emission is mentioned is supplemented by provisions that exclude the possibility of providing EM to a client as a loan or the accrual of interest in the form of EM. Thus, the lawmaking body excludes the possibility of drawing an analogy between the e-money system and a bank deposit agreement (Bazhanov, 2017).

The widespread use of EM will increase the dynamics of settlements and the volume of transactions, as well as increase the competitiveness of financial services. The concept of economic and legal regulation of the emission and circulation of EM requires a comprehensive and thorough elaboration, taking into account scientific and technological progress, economic and legal research. The most pressing issues of EM turnover regulation are applicable contractual structures, security, and universality of the payment instrument. A critical analysis of foreign laws shows that the circulation of electronic money in Russia must be regulated on the basis of specially created laws and regulations (Sitnik, 2017; Khrustaleva, 2016).

Results. Analyzing the specific features of an Electronic Funds Transfer Agreement

An Electronic Funds Transfer Agreement is an agreement, under which one party - the EF operator - upon the client’s order transmitted using an electronic payment instrument (EPI) transfers the electronic funds belonging to it to a third party (Abramova, 2018). The agreement in question is real, non-gratuitous, gratuitous, or reciprocal. In case of entering into a gratuitous agreement, the recipient of the payment pays for the electronic funds transfer and the operator will provide the service for transferring electronic funds to the client free of charge. It should be noted that, unlike the paid services agreement where the payment can be made both under an agreement between the parties and on the basis of tariffs approved by the state (since this agreement is a standard form agreement), in the electronic funds transfer agreement the payment for services is not regulated by the tariffs, since this agreement is not a standard form agreement.

Under the current laws, the identification of electronic payment instruments (EPI) is strictly required for legal entities or individual entrepreneurs; they are provided with a personalized EPI (called “corporate”) that they can use for transferring up to RUB 600,000.

Reduced limits for EF transfers cause great inconvenience for individuals as well. Taking into account the material wellbeing of Russian citizens, limiting the amount of transfers to RUB 15,000 when using non-personalized EPI seems extremely low.

The rights and obligations of the EM issuer (operator) and the client (legal entities and individuals, as well as individual entrepreneurs) are presented in Table 1.

Table 1. Rights and obligations of the participants of the electronic funds transfer system

Obligations of the EM Operator	**Rights of the EM Operator**
− to transfer funds upon client's orders in favor of recipients; − to inform a client about the execution of its orders for the electronic funds transfer; − to notify a client immediately about the refusal to transfer electronic funds and the reason thereof; − to inform a client about the completion of each transaction using electronic payment instruments (EPI); − to notify clients about the loss of an EPI and (or) about its use without the client's consent; − to suspend or terminate the use of EPI, according to the client's order; − to record notifications sent to and received from a client and to store this information for at least three years; − to provide to a client documents and information related to the client's use of its EPI; − to keep records of the information regarding the client's electronic funds balance and transfers made; − to consider the applications received from a client, to inform a client about the results of the consideration thereof; − to ensure the confidentiality of any information received from a client; − to freeze the client's funds upon receipt of official information regarding its involvement in extremist activities or terrorism; − to establish reliable methods of communication between the EM operator and a client.	− to process the client's personal data; − to refuse to transfer electronic funds if they are insufficient or if there is no complete/simplified customer identification; − to suspend or terminate the client's use of EPI in case of any violation of the order of its use; − not to execute the client's orders received by the EM operator, for which the documents that are necessary to record information in the framework of combating money laundering and terrorist financing have not been submitted; − to refuse to execute the client's order if there is a suspicion that the transaction is being carried out for the purpose of laundering proceeds from crime or financing terrorism; − to request additional information and documents from a client on transactions with funds, including those confirming the source of the origin of funds; − to update information about the client, beneficiaries, and beneficial owners at least once a year, and in case of doubts regarding the reliability and accuracy of previously received information - within seven working days following the day such doubts arise; − to enter into contracts with communication service providers to increase the electronic funds balance of a client who is a subscriber of this provider, at the expense of funds contributed to a communication service provider.
Obligations of the Client	**Rights of the Client**
− to provide the EM operator with funds for the transfer thereof as intended; − to provide reliable information for communication and sending to a client notifications about transactions using its EPI; − to provide personal data in the course of simplified or complete identification; − to promptly inform the EM operator of any change of its personal data and details of documents; − to ensure secure storage of authorization data that allow authenticating a client without third party access; − to provide information and documents confirming the source of origin of funds, as well as information of its beneficiaries, founders	− to give orders to the operator regarding the electronic funds transfer; − to receive notifications about transactions using electronic payment instruments (EPI) in the manner prescribed by the contract; − to block the EPI in case of its loss, as well as if there is suspicion of unauthorized access thereto; − to demand the return of the EM balance upon termination of the contractual relationship with the EM operator.

(members), and beneficial owners, the purpose of the transaction; − to inform the EM operator immediately of the loss of the EPI.	
Compiled by the authors based on Federal Law № 161-FZ dated 27 June 2011 “On the National Payment System”, [Online], [Retrieved February 4, 2021], http://ivo.garant.ru/#/document/12187279/paragraph/1/doclist/14142/showentries/0/highlight/О%20национальной%20платежной%20системе:1; Regulation on the Funds Transfer Rules № 383-P approved by the Bank of Russia on 19 June 2012, [Online], [Retrieved February 1, 2021], http://ivo.garant.ru/#/document/70194476/paragraph/1/doclist/14938/showentries/0/highlight/Положение%20о%20правилах%20осуществления%20перевода%20денежных%20средств%20№%2.	

It should be noted that, unlike a service agreement, where the Civil Code of the Russian Federation provides for the obligation of the personal performance thereof, in most cases, the personal performance of an Electronic Funds Transfer Agreement is impossible due to the necessity to involve other EM operators, bank payment agents, an operation center, a clearing center, settlement center, etc. Besides, there are some specific features regarding the termination of an Electronic Funds Transfer Agreement, according to which a client may terminate the agreement by sending to an EM operator a written notification thereof or by notifying the operator of closing the EPI owned by a client. In this case, a client shall dispose of the electronic funds balance. In turn, the EM operator may unilaterally refuse to perform the agreement by sending to a client a written notification thereof, should a client lose the funds that provide for the technical ability to confirm the electronic funds transfer, or fail to comply with the security requirements when using the EPI, as well as in other cases set forth by an agreement (Standard of the Bank of Russia “Ensuring the Information Security of the Russian Banking System Organizations. Methodology for Assessing the Compliance of Information Security of Russian Banking System Organizations with the Requirements of STO BR IBBS-1.0-2014 STO BR IBBS-1.2-2014” (Order of the Bank of Russia No. P-399 dd. 17 May 2014)).

In the Russian laws, the issue of choosing the criteria for distributing the risks of losses that were caused to the client in the process of electronic funds transfer with the participation of other EM operators, as well as a bank payment agent, an operation center, a payment clearing center, a settlement center, and etc that are involved in the transfer remains unaddressed still (Recommendations on organizing the management of risks arising when credit institutions carry out transactions using Internet banking systems: approved by Letter of the Central Bank of the Russian Federation No. 36-T dd. 31 March 2008). The mechanism of imposing responsibility for unauthorized electronic funds transfer with the participation of a mobile service provider under an issued duplicate of the client’s SIM card has not been worked out. Case history shows that risks may be imposed on both the operator and the client, who, in turn, file claims against the mobile service provider.

The problem of releasing an EM operator from the liability is recognized as relevant in cases where the client uses malicious software, which may entail completing a payment transaction without its consent. However, it should be noted that an EM operator must bear civil liability in cases when the web interface of the "electronic wallet" is inoperable or when there are failures in its operation (Karnushin, 2017).

The existing gaps in the legislation are counterproductive, complicate the application of regulatory requirements in everyday practice, may lead to risks occurring, and are factors of reducing the economic security of electronic payment instruments.

Discussion. Assessing Risks and Security Level of Electronic Money

The operations of the EM issuer (an operator) and EM service consumers (a client) are associated with certain risks. Some of them are of a general nature and are inherent in a wide range of economic agents’ operations; however, unique risks inherent in the EM system can be singled out. The list of EM risks is not universal, since EM systems differ significantly in functions and methods of implementation - therefore, risks that have critical consequences for some systems may be practically insignificant for others. In particular, in the publication “Risk Management for Electronic Banking and Electronic Money Activities” the Bank for International Settlements identifies the following five main risk groups for the issuer (operator) of electronic money (Vavilova, 2020):

1. Operational risk.

2. Reputational risk.

3. Legal risk.
4. Strategic risk.
5. Other risks.

Operational Risk

Operational risk is understood as the probability of direct and/or indirect losses that may be caused by internal errors of staff, technical failure, or unstable operation of the system, as well as various external circumstances (Panova, 2020).

In case of violation of the principles and algorithms of the security system at the level of the EM issuer (operator), the extent of the adverse consequences may be rather significant. For example, a system attacker may gain access to clients' "electronic wallets". At the same time, cybercriminals will have a serious problem of cashing in stolen funds due to the submission of personal data to the issuer [9]. In the event that a cybercriminal transfers stolen electronic money to their own "electronic wallet", the limit set by the operator on the amount of transactions can significantly slow down the process of the use thereof until the issuer detects a hack and blocks the wallet.

In addition, the operations of the EM issuer (operator) and user (client) may be affected by various types of fraudulent actions, which include:

- theft of personal data of the owner of the electronic wallet (client) and carrying out payment transactions on his or her behalf;
- transferring an incorrect amount when making payment transactions;
- creating a false rejection of a payment transaction (Vavilova, 2020);
- carrying out false emission of electronic money.

Theft of personal data of the wallet's owner is a danger, first of all, for electronic money systems based on such networks as Qiwi and Webmoney (Bank of Russia Statistical Bulletin № 4, 2019), since these electronic funds allow making electronic payments on the Internet without identity verification (Gavrin, 2021) . Transferring an incorrect payment amount may be caused both by a failure of the system itself, or by illegal actions of the seller. The risk of rejecting a transaction (the risk of the issuer of traditional electronic money) is inherent in a number of countries, including Russia. According to the current laws of the Russian Federation, if an EM user refuses to pay within the first day, the issuer shall return the funds. In this case, the issuer has a problem with the counterparty who received and spent the payment. The risk of false EM emission is that a cybercriminal that finds a vulnerability in the security system can independently issue unsecured EM (Ahamed, 2010). With a large amount of false emission, the issuer's ability will be compromised. It should be noted that the probability of this risk is extremely low, since issuers have the highest level of technical protection.

Other types of risk of EM issuing companies include the likelihood of changes in the terms of cooperation with the EM system developers, the risks of introducing systems with an insufficient level of quality, external risks (for example, power outages, failures of the Internet). Large banks - issuers, as a rule, independently develop special software for issuing electronic money (Gavrin, 2021).

In addition, it is necessary to take into account the risk of errors of bank personnel that may arise in the process of tracking transactions in electronic funds, as well as the risk of other kinds of errors associated with the human factor, which do not allow reducing the level of losses and minimize negative consequences.

Reputational Risk

This risk is associated with a deterioration of public opinion about the issuer's operations or the quality of the system's functioning, which may have such negative consequences as drop off of clients, outflow of funds, as well as a drop in the value of the company's shares. The specific feature of reputation risk is the possibility of its occurrence as a result of both unfair competition and the issuer's activities, including the consequences of operational risks or poor-quality marketing and information support.

Legal Risk

Legal risk includes the risk of violating the current laws, which is caused by:

- low level of elaboration of the legal and regulatory framework in this area;
- the differences in Russian and international laws;
- development and adoption of decisions in the framework of electronic payments that are difficult to classify;
- insufficient law enforcement practice.

The negative consequences of legal risks can be legal costs and various sanctions. Differences in the countries' laws entail different requirements for the issuer's operations, in particular, with respect to taxation.

One of the main sources of legal risks is money laundering and terrorism financing due to the anonymity or quasi-anonymity of most electronic payments. This risk is minimized by setting maximum wallet limits and the amount of anonymous and non-anonymous payments (Ahamed, 2010).

Legal risk may also arise when the client's personal data are leaked or a client is not informed in full of the possible use of his or her personal data.

Strategic Risk

This type of risk reflects the current and future impact on the volume of income of erroneous management decisions, ineffective implementation of decisions, or insufficient ability (flexibility) to respond to various changes and challenges. The risk depends on the compatibility of the issuer's strategic goals, business strategies developed to achieve them, allocated resources, the quality of implementing strategies in the existing economic, technological, competitive, regulatory, and other conditions (Bazhanov, 2017; Bazhanov, 2016).

Other Risks

Other risks include such types of risk as credit risk (the risk of default on obligations due to various reasons), liquidity risk (the risk of unsuccessful use of funds that secure EM, or the desire of most customers to convert EM into cash), currency risk (risk of the issuer accepting foreign currency as collateral due to changes in its rate), the risk of inflation, the risk of reducing the effectiveness of traditional methods of monetary policy, etc. The current international and Russian laws are aimed at protecting participants of the electronic money system from such risks (Bazhanov, 2016). Another type of risk is the denomination of the transaction, i.e. obtaining information of it being carried out or its participants by third parties, for example, a large company operating in the electronic commerce sector, with all the negative consequences indicated above.

Tables 2 and 3 provide an analysis of the impact of various risks on the EM market.

Table 2: Risks of companies – issuers on the EM market

Types of Risks	Probability of Occurrence	Level of Negative Implications
Operational risk	High	High
Legal risk	Medium	High
Strategic risk	Medium	Medium
Reputational risk	Medium	Medium
Other risks	Low	High

Compiled by the authors: The List of EM Operators, [Online], [Retrieved December 15, 2018], http://www.cbr.ru/psystem/oper_zip/

Table 3: Risks of consumers (clients) on the EM market

Types of Risks	Probability of Occurrence	Level of Negative Implications
Operational risk	Medium	Low
Cost exposure	Medium	Low
Risk of liquidity loss	Medium	High
Risk of data collapse	Medium	Low

Compiled by the authors: The List of EM Operators, [Online], [Retrieved December 15, 2018], http://www.cbr.ru/psystem/oper_zip/

Risk analysis shows that the most difficult type of risk from the point of view of its identification and assessment of the overall impact on the security of the EM system is the operational risk in the (often) authorized emission of electronic money - in other words, the appearance of counterfeit electronic money in the system. The negative consequences of this risk can be catastrophic for the entire system since they are directly related to the emergence of reputational, legal, and strategic risks. For EM users (clients), the most significant risk is the leakage of personal data, which can lead to hidden use of the clients' electronic wallet by cybercriminals.

EM risk management is not a separate specific area of risk management; therefore, for the risks associated with electronic money, there is no specially developed unique classification of risk management methods. The EM risk management process can also be divided into three stages: risk assessment, development of risk management measures, and further continuous risk monitoring (Trifonov, 2015). The main well-known methods of EM risk management can be risk avoidance, risk localization, risk diversification, as well as risk compensation.

In particular, the method of risk avoidance is aimed at avoiding the occurrence of risk events by excluding risky activities, from implementing high-risk projects and programs, careful selection of partners, implementing insurance programs, dismissal of incompetent employees, etc.

Within the framework of the EM, the issuing company can entrust the creation of technology to a proven and experienced developer, or use a ready-made, reliable technology that has proven itself in the market.

As a method of reducing risks in the field of electronic money, insurance does not seem to be optimal and effective, since insurance companies do not have enough data in order to accurately determine insurance rates for participants in the EM market.

The risk localization method is applicable in cases of easily identifiable risk events and the creation of a venture capital company. In addition, the issuing company may establish a risk joint venture with another company. In the EM market, this method can be used by fairly large banks operating through subsidiaries, or a number of banks can create one subsidiary - the EM issuer.

The risk diversification method allows distributing risks by diversifying activities, using a range of technologies, as well as expanding the range of services and geography of EM-related operations.

The method of risk compensation implies the formation of various mechanisms for preventing the occurrence of risk events (Pavin, 2019), which will require deep preliminary analytical work, as well as high-quality education and training of personnel. Risks are compensated by the EM issuer forming a system of reserves in the form of free funds, which implies constant social and economic and regulatory monitoring, as well as modeling and forecasting the situation taking into account the available information.

The main trends for increasing the level of security in the EM market are:

1. developing, adopting, and implementing security policies, selecting the most effective and optimal tools such as hardware and software, defining security tools (passwords, encryption protocols, the level of employee access to data, protection against malware, etc.);
2. optimizing internal communication of personnel of various links and levels of the system, continuous training of employees, improving their qualifications and the level of teamwork;
3. continuous improvement of technical and technological aspects, the use of modern software products, computing power, and tracking modern trends in the computer and digital industry;
4. using outsourcing based on a thorough analysis of the situation and thus transferring part of the risks to other market participants. The decision to outsource should not be spontaneous, but based on a thorough analysis of the situation;

5. constantly informing customers about new products, algorithms for their work, recommended security systems, as well as creating backup copies of databases in case of their loss or the appearance of force majeure

The risk of false EM emission may arise as a result of deliberate illegal actions and access to the system by dishonest employees, the vulnerability of the process of falsifying electronic money, or hacking of the EM system as a result of a cyber-attack (Au et al., 2011). The most effective direction of risk management in such cases is to increase the reliability and security of the system as a whole, improve the technical component, complicate the verification procedure, as well as the informational development of society, expanding the list of cryptographic protection methods, and using various programs that track the correctness of transactions and the integrity of the system, permanent monitoring in the form of external and internal audits.

In connection with the above, it should be noted that currently there is a breakdown of the existing economic structure. Obviously, the requirements for the security of EM increase against the background of the development of the digital economy based on social digital platforms.

Conclusions

The research systematizes and summarizes the Russian and foreign approaches to the definition of the economic and legal nature and regulation of the EM system as a mandatory right of claim that significantly differs from cash and non-cash funds. In this regard, the specific features of the EM system in the sphere of legal relations of economic turnover and the transfer of EM to third parties should be reflected in the development of special norms of domestic legal regulation. In particular, it is necessary to clearly define the responsibility of the parties for non-compliance with contractual obligations in the EM system in order to reduce the risk and threats in this area of public relations. In addition, the risks associated with issuing the EM are analyzed, and recommendations for managing these risks are proposed in order to increase the security level of the system under consideration.

Based on the above and in the opinion of the authors/ the stated main goal of the work – to identify and assess the economic and legal risks of the EM system, as well as to develop recommendations for improving the safety of the EM application – was achieved.

Acknowledgment

Our research was supported by the Ural Federal University, Ural State University of Economics and Tyumen Territorial Institute of Professional Accountants during preparation of the manuscript.

References

- Abramova, E.N. (2018) “Electronic means of payment as a complex object of civil rights”, *Banking law*, 1, 22-32.
- Bazhanov, S.V. (2017) “The state of legality in the credit and banking industry of the Russian economy”, *Russian Journal of Legal Research*, 3 (12), 224-229.
- Bazhanov, S.V., Booth, N.D. (2016) “The state of legality in the credit and financial sphere in the context of the economic crisis”, *Banking law*, 2, 23-28.
- Vavilova, E.M. (2020) “Electronic money: the problem of determining the place in the system of objects of civil rights”, Legal paradigm, 19 (2), 110-115.
- Gavrin, D.A. (2021) “Electronic money: problems of legal regulation”, *Wise lawyer*, [Online], [Retrieved March 02, 2021], https://wiselawyer.ru/poleznoe/96698-elektronnye-denezhnye-sredstva-problemy-pravovogo-regulirovaniya.
- Karnushin, V.E. (2017) “Civil-legal essence of money as objects of civil rights”, Lawyer, 3, 22-26.
- Korostelev, M.A. (2013) “Electronic money circulation: civil law issues”, Journal of Russian law, 12, 130-135.
- Pavin, A.V. (2019) “Legal regime of electronic money (electronic money) “, *Legislation*, [Online], [Retrieved December 12, 2019], http://ivo.garant.ru/#/basesearch/Legal .
- Panova, G.S. (2020) “Fund for Consolidation of the Banking Sector as a Tool to Improve Security in the Financial Services Market”, Economic Security, 3(1), 41-52.
- Savelyev, A.I. (2016) “Electronic commerce in Russia and abroad: legal regulation”, 2nd ed, Moscow, Statut,. Ch. 7.§ 3.
- Sitnik, A.A. (2017) “Regulation of money circulation in Great Britain”, *Lex russica*, 2, 166-183.
- Trifonov, A. (2015) “Electronic money risk management”, *Insurance law*, 1(60), 57.
- Khrustaleva, A.V. (2016) “Electronic money in the Russian Federation and the European Union”, *Banking law*, 3, 55-62.

- Ahamed, S.S.R. (2010) “A novel view on electronic cash and electronic payment schemes: a comprehensive study”, Computer Sciences and Telecommunications, 3(26), 180-197.
- Au, M.H., Susilo, W., Mu, Y. (2011) “Electric cash with anonymous user suspension”, *Lecture Notes in Computer Science*, 6812, LNCS, 172-188.