УДК 336.7
https://doi.org/10.32342/3041-2137-2026-2-65-8

R. G. Snishchenko,
Doctor Sciences (Economics), Professor, Head of the Department of Management and Information Technologies of the Communal Institution of Higher Education «Kremenchuk Humanitarian and Technological Academy» of the Poltava Regional Council, Kremenchuk, (Ukraine)
https://orcid.org/0000-0003-2857-0980

FINANCIAL RISK MANAGEMENT OF ELECTRONIC MONEY

The purpose of the article is to identify and study the main types of financial risks of electronic money in modern conditions of digitalization of the economy.

When preparing the scientific publication, general scientific and special research methods were used: the method of critical analysis, scientific abstraction, and generalization of scientific experience of modern theoretical research, as well as a systemic and comprehensive approach.

The study results are as follows: the areas of use of electronic money were clarified; the main types of financial risks of electronic money were defined and analyzed; the structure was investigated, and a classification of financial risks of electronic money was provided; specific risks of electronic money caused by the war between Russia and Ukraine were identified. Based on the research, a list was provided, and the content of the main measures to ensure the security of transactions with electronic money was disclosed.

The scientific novelty of the results of the study is as follows. The types of financial risks of electronic money identified in the article allow us to adjust the tasks aimed at increasing the level of their security. The proposed main measures to achieve the security of transactions with electronic money contribute to the formation of a strategy for maximum security of the activities of business structures in modern conditions of digitalization of the economy. The methodological approach to the selection of organizational measures for the safe issuance, use, and storage of electronic money and to determining their reliability has received further development. This will allow for the optimal use of the financial resources of business entities while maintaining an acceptable level of their economic security.

The practical significance lies in the fact that the theoretical provisions of the study regarding financial risks and the content of the main measures to achieve the security of electronic money transactions can be used in the strategic and tactical planning of the economic activities of financial market participants.

Keywords: electronic money, risk, management, payment instruments, payment systems, electronic wallets, cryptocurrency, hacker attacks, cybersecurity, fraud

JEL classification: ***D81, D83, D84, E52, E66, O23***

Метою статті є виявлення і дослідження основних видів фінансових ризиків електронних грошей у сучасних умовах діджиталізації економіки.

При підготовці наукової публікації було використано загальнонаукові і спеціальні методи дослідження: метод критичного аналізу, наукової абстракції та узагальнення наукового досвіду сучасних теоретичних досліджень, системно-комплексний підхід.

Підсумком дослідження є наступні отримані результати: уточнені сфери використання електронних грошей, визначено основні види фінансового ризику електронних грошей, проведено їх аналіз; досліджено структуру та надана класифікація фінансових ризиків електронних грошей; визначено специфічні ризики електронних грошей, зумовлені війною між

росією та Україною. На підставі досліджень надано перелік та розкрито зміст основних заходів із забезпечення безпеки операцій з електронними грошима.

Наукова новизна результатів дослідження полягає в наступному. Визначені у статті види фінансових ризиків електронних грошей дозволяють скоригувати завдання по підвищенню рівня їх захищеності. Запропоновані основні заходи з досягнення безпеки операцій з електронними грошима сприяють формуванню стратегії максимальної безпеки діяльності бізнес-структур в сучасних умовах діджиталізації економіки. Дістав подальшого розвитку методичний підхід до вибору організаційних заходів щодо безпечного емітування, використання, та збереження електронних грошей та визначення їх надійності. Це дозволить оптимально використовувати фінансові ресурси суб'єктів господарювання із дотриманням допустимого рівня їх економічної безпеки.

Практична значущість полягає в тому, що теоретичні положення дослідження щодо фінансових ризиків та змісту основних заходів із досягнення безпеки операцій з електронними грошима можуть використовуватися при стратегічному і тактичному плануванні господарської діяльності учасників фінансового ринку.

Ключові слова: електронні гроші, ризик, господарювання, платіжні інструменти, платіжні системи, електронні гаманці, криптовалюта, хакерські атаки, кібербезпека, шахрайство

JEL classification: ***D81, D83, D84, E52, E66, O23***

Statement of the problem. Money as a payment instrument plays a key role in the development of the economy and modern society. It provides a universal exchange between owners of millions of goods and services, and also supports the functioning of credit systems and public finances. Electronic payment instruments, such as card payments and electronic transfers, are gradually replacing cash and paper checks, especially in the field of retail payments. However, paper money is still widely used, remaining a convenient means for small payments and for servicing the informal sector of the economy. Electronic money as a payment instrument, based on modern innovative solutions, provides economic agents with a new way to make payments, and also represents a new payment technology that allows the storage of assets in electronic form. The importance of electronic money for the economy is clearly confirmed by the fact that, despite the continuation of a full-scale war, the majority of settlement operations in Ukraine are carried out in a non-cash form. Like every innovative technology, electronic money has its weaknesses. One of the main ones is the presence of financial risks when storing and using it. Despite the progress of electronic money protection technologies, the methods of criminal attacks on them are also constantly improving. Therefore, the need for constant monitoring and identification of risks and threats that arise during the digitalization of economic processes is always relevant.

Analysis of recent research and publications. Electronic money in the modern digitalized world is becoming more and more widespread and is gradually absorbing all types of payments. The availability and convenience of electronic money make it vulnerable and attractive for criminal attacks. The issues of creation, use and protection of electronic money due to its relevance and significance are studied by both scientists and financial market specialists. Research is conducted in all areas of use. In particular, Tarasenko I. in [1] investigates the main aspects of ensuring financial stability in the digital age, European approaches and features of their implementation in Ukraine, Burakovsky I., Kravchuk V., Naumenko D., and Glybovets A. in [2] assess the volume of the electronic money market, its main players, and determine the geographical and institutional aspects of development. Korolenko O., Ryabykina N. and Ryabykina K. in [3] conduct research on the investment attractiveness and opportunities of Ukrainian business in the context of global risks. O. Dovgan, L. Lytvynova, and S. Dear in [4] highlight cybersecurity issues that are becoming particularly relevant in the context of the development of the information

society and the creation of an effective cybersecurity system in Ukraine. Pavlyuk Ya. in [5] considers the future of digital money in Ukraine, while Schmidt D. in [6] analyzes the possibilities of educating a cybersecurity culture in society. The pool of experts [7] and members of the NBU financial club [8] conduct constant monitoring of the Ukrainian e-commerce market, while Google employees study the general factors of the Internet's impact on the Ukrainian economy [9], and specialists from professional and public organizations study ways and methods of protecting the property interests of consumers of digital products. In particular, EMA specialists in [10] conduct an analysis of fraudulent and phishing sites and provide professional security recommendations to clients, Chainalysis analysts [11] expose criminal money laundering schemes using cryptocurrencies, Climate & Tech [12] analyze the use of electronic money in illegal gambling, News Track Live specialists [13] deal with the problems of protecting entrepreneurship in the digital environment, and SonicWall [14] conducts an annual in-depth analysis of cyber risks, etc.

Highlighting previously unresolved parts of the overall problem. It can be stated that the problems of detecting, identifying and protecting the property rights of owners at all stages of the use of electronic money are extremely important, relevant and, unfortunately, have not yet been sufficiently researched. In particular, this concerns the detection, classification and study of significant financial risks associated with electronic money in modern conditions.

Formulation of the article's goals (task statement). The purpose of the article is to identify and study the main types of financial risks of electronic money in modern conditions of digitalization of the economy.

The object of the research is the processes of digitalization of finance in the rapidly changing conditions of the modern economy.

The subject of the study is the theoretical and practical aspects of managing the financial risks of electronic money.

Description of the research methodology. The study used general scientific and special research methods: methods of critical analysis, scientific abstraction, and generalization of scientific experience from modern theoretical research, and a systemic and comprehensive approach.

Presentation of the main research material with a full justification of the scientific results obtained. With the spread of Internet technologies and the development of e-commerce, electronic money is becoming an important tool in the modern economy, and an alternative to traditional instruments of cash and non-cash circulation (Fig. 1).

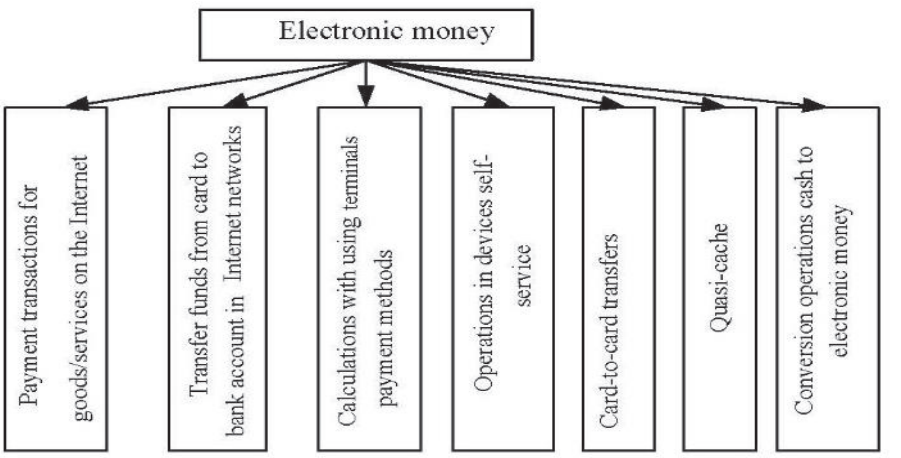

Fig. 1. Areas of the use of electronic money
Source:based on [2]

The degree of use of electronic money by the population of a country depends on the standard of living of its citizens as well as on the pace of implementation and use of modern technologies. According to expert assessments by NBU employees [7], Ukraine ranks seventh among European countries in the number of non-cash transactions using payment cards per person (Table 1).

According to the National Bank of Ukraine [8], the number of electronic money transactions in Ukraine is almost three times greater than the number of cash transactions.

Electronic money guarantees the speed and convenience of transactions, but at the same time it carries significant financial risks. These risks require detailed analysis to ensure the safe use of electronic money for both businesses and consumers.

Based on the analysis of scientific sources, the following main types of financial risks of electronic money can be distinguished (Fig. 2).

1. Military risks:

– economic recession – caused by the need to change the location of enterprises, logistics, and the militarization of the economy. The main indicators are increased inflation, an increased discount rate, a decline in production (Fig. 3), and devaluation of the national currency (Fig. 4), which reduces the efficiency of capitalizing electronic money;

– attacks on critical infrastructure – constant outages negatively affect the processes of electronic document management and cryptocurrency mining. According to [16, 20], from September 28, 2022, to September 1, 2024, almost 11.5 thousand launches of cruise missiles, ballistic missiles, anti-aircraft missiles of the S-300 complex used for strikes on ground targets, and kamikaze UAVs of the Shahed-131/136 type were registered.

An analysis by Forescout Research/ Vedere Labs [21] showed that in 2023 the number of cyberattacks on global critical infrastructure increased by 30% compared to 2022. In particular, 420 million attacks were recorded for the period from January to December 2023 (an average of 13 attacks every second). Constant pressure is felt by communications systems, healthcare facilities, energy, waste processing, manufacturing, and logistics enterprises, etc.;

– skills or labor shortage – a negative impact on the creation, conversion, and circulation of electronic money due to migration processes associated with the armed invasion.

According to data published by the Office of the United Nations High Commissioner for Refugees [6], approximately 6.29 million people left Ukraine at the beginning of the war and have not returned. Since

Table 1

Number of non-cash transactions using payment cards per person per year*

	Country	Number of transactions per person, pcs.
1.	Estonia	235.0
2.	Latvia	140.0
3.	Poland	100.0
4.	Lithuania	97.5
5.	Slovenia	90.0
6.	Czech Republic	86.5
7.	Ukraine	**72.9**
8.	Croatia	70.0
9.	Hungary	66.5
10.	Slovakia	65.5
11.	Romania	25.2
12.	Bulgaria	18.5

*Source: [7]

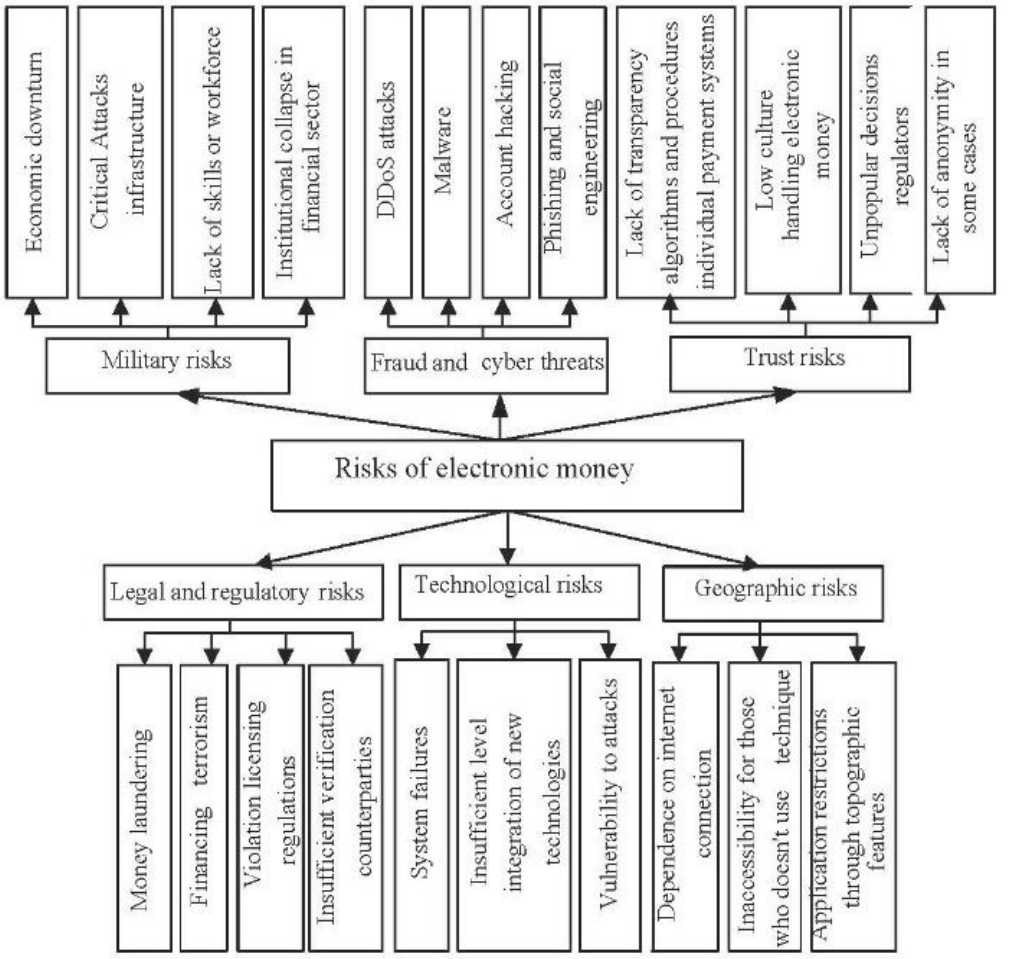

Fig. 2. Main types of financial risks of electronic money
Source: classified by the author

mid-October 2022, this number has been increasing annually. From February 24, 2022, to June 26, 2023, alone, excluding data from Russia and Belarus, 20.64 million departures and 14.34 million entries were recorded in Ukraine.

– institutional collapse in the financial sector – the destabilizing impact of the war on the functioning of financial institutions and erroneous management decisions in the areas of financial monitoring, currency supervision, and the implementation of sanctions policies can lead to significant losses for the economy and pose a real threat to national security. Distrust in state institutions and political decisions creates an atmosphere of uncertainty that deters foreign investors.

The structure of the most significant financial risks of electronic money caused by the war is presented in Fig. 3.

2. Fraud and cyber threats:

– phishing (phishing sites, vishing, smishing, deepfake phishing) – the use by attackers of psychological methods to influence the owners of electronic resources and to seize their confidential data.

Phishing remains the main threat to Ukrainian Internet users, and its scale is constantly growing. The structure of online fraud is presented in Fig. 4.

EMA specialists in [7] found that phishing sites account for 88% of all blocked cybercrime resources. The remaining 12% are fraudulent online stores, fake earning schemes, scams with "investments," or

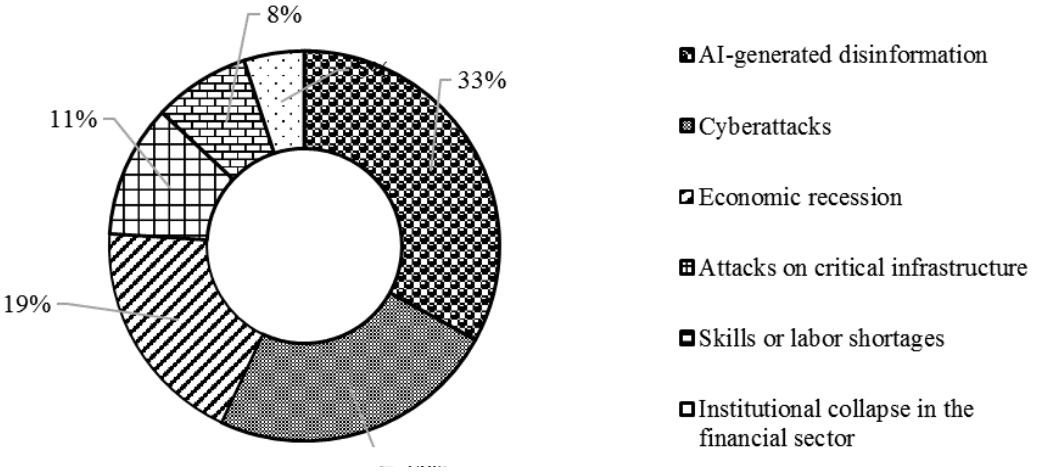

Fig. 3. Structure of financial risks of electronic money caused by war
Source: based on [19, 23]

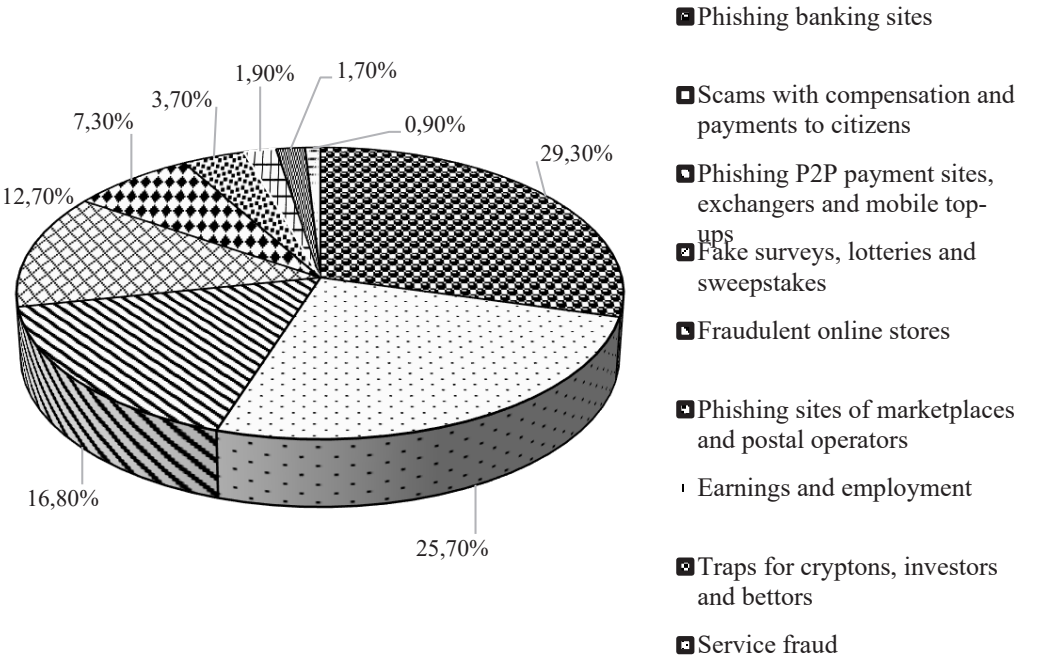

Fig. 4. Phishing structure (most common methods)
Source: based on [19, 23]

services aimed at defrauding citizens of money, as well as sites distributing malicious software;

– account hacking – the use of shortcomings in personal data protection and vulnerabilities in security systems to gain access to an electronic wallet and transfer money without the knowledge of its owner. In 2023, the number of attacks using cryptojacking increased by 43%, and the spread of Internet of Things (IoT) malware increased by 87% [8].

– malware – the installation of special programs on a user's device without their knowledge to track transactions, steal passwords, and make unauthorized payments. According to SonicWall [14], 493.3 million ransomware attacks were recorded in 2023, which is 21% less than the previous year. For comparison, in 2022 this figure increased by 62%, and in 2021 – by another 105%;

– DDoS attacks – the conduct of large-scale attacks on payment system servers with the aim of stopping transactions, blocking transactions, or creating a critical situation with subsequent data loss. The number of DDoS attacks in the world is growing every year. The surge in such cyber threats was especially noticeable in 2022, when Russia launched a full-scale war against Ukraine, using the cyber front as one of its components. Russian special services and hacker groups affiliated with them seek to paralyze the activities of state institutions, critical infrastructure, banks, and businesses both in Ukraine and abroad. In response to these challenges, the Government Computer Emergency Response Team of Ukraine (CERT-UA) reported that in 2022 the number of registered cyberattacks in Ukraine increased almost threefold compared to 2021 [9]. In addition, in March–April 2023, experts [9] recorded an almost twofold increase in attacks on commercial organizations compared to the period January-February 2023.

3. Legal and regulatory risks:

– the use of electronic money has significantly facilitated money laundering and the concealment of illicit income sources, thereby complicating regulatory oversight and traceability. As illustrated in Figure 5, since 2019, illegal cryptocurrency wallets have transferred nearly $100 billion to conversion services.

The peak volume of such transactions was recorded in 2022, reaching approximately $30 billion. This surge is largely attributable to activity involving sanctioned platforms, particularly the Russian cryptocurrency exchange Garantex;

– the use of electronic money, due to its anonymity, to finance terrorist groups or pay for criminal activities. According to the NBU [7, 8], in the first half of 2024, banks blocked the activities of 80 thousand "droppers" (money mules) who provided their accounts for the transfer of illegal funds to third parties.

This scheme supports the shadow economy and causes billions in losses to the state. Drops are actively used in various industries, in particular: for operations in online casinos, in the trade of cigarettes, drugs, and weapons (via the darknet), and for the implementation of fraudulent schemes (Fig. 6).

Most cybercriminals aim to quickly cash in their ill-gotten funds. Over 50% of such funds end up on centralized exchanges, either directly or through intermediaries,

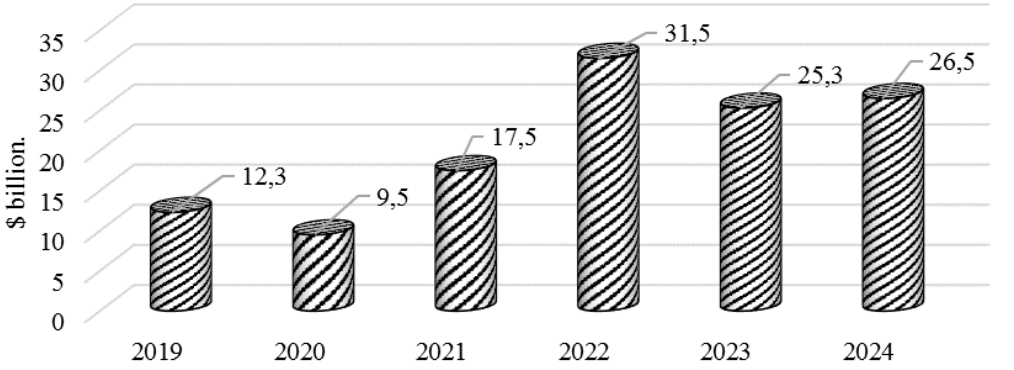

Fig. 5. Total amount of funds converted from illegal wallets
Source: based on [15, 23]

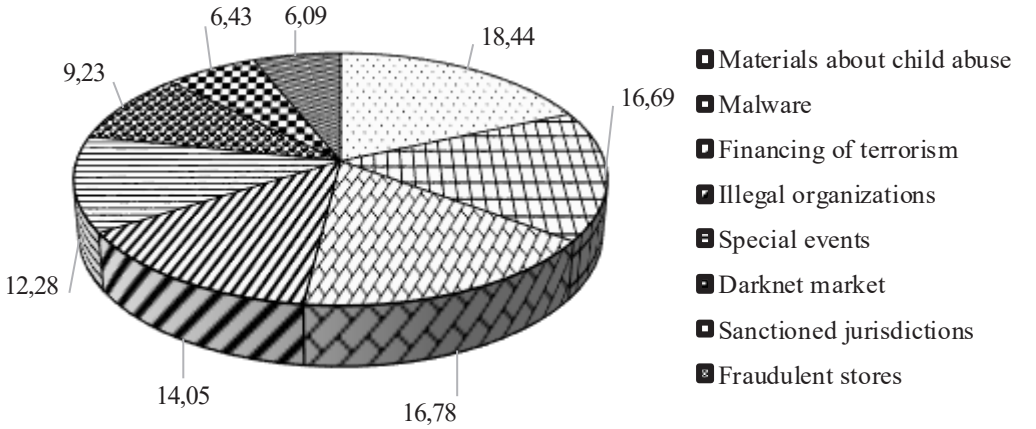

Fig. 6. Share of illegal funds entering the wallets of TOP-100 intermediaries by type of crime
Source: based on [10, 19]

after using obfuscation techniques, which are designed to complicate or completely hide the traces of cryptocurrency transactions.

– Violation of licensing regulations: Often the activities of online casinos or exchangers are carried out without appropriate licenses, which contributes to the evasion of taxes and other financial obligations. A Sky News investigation [12] into Roblox alone identified the three largest illegal casinos – BloxFlip, Bloxmoon, and RBLXWild. Between April and October 2024, bets worth $22.3 million were placed on them. The casinos paid out $20.1 million in winnings and kept $2.2 million as revenue. On average, a Roblox casino earns approximately $10,000 per day.

– verification complications with counterparties: some banks or financial institutions do not exercise proper control over the activities of partners, which creates risks of cooperation with illegal organizations [19]. According to [12], as of July 1, 2024, there are approximately 68 million bank customers and 116 million payment cards in Ukraine. Of these, 51 million are active, which means they have at least one spending transaction per month. There is also a significant number of inactive accounts and cards in the system that can be involved in the drop scheme at any time.

4. Geographic risks:

– dependence on the quality of the Internet connection: Authentication procedures when using electronic money impose higher requirements on the availability and stability of communication between counterparties and servers (Fig. 7);

– inaccessibility of electronic money for persons who do not use the appropriate technical support or do not have it available. The study [9] showed that in Ukraine, a developed infrastructure for business access to the Internet has been created, and companies have sufficient technical resources to use it. In particular, 76% of enterprises provide Internet access for all their computers, and 79% use a broadband wired connection. However, the ways of using the Internet by Ukrainian companies remain limited to a few popular areas.

Most often, enterprises use the Internet to advertise themselves and inform others about their activities: 62% of respondents have their own website. About 34% of companies place online advertising, and 25% of them have only one-time experience (less than once per year). Additionally, 22% of enterprises are engaged in promotion through social networks. A third of companies purchase products for their own needs through online stores, but only 12% of enterprises sell their goods online [9].

– limited use of electronic money for business transactions due to the topographical features of the area. According to a study by the Bank for International Settlements

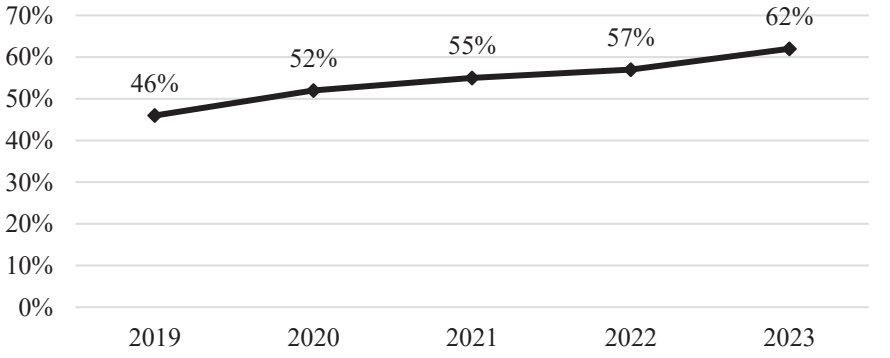

Fig. 7 Level of coverage of the population of Ukraine with Internet services
Source: [9]

[23], the development of electronic money in the world has clear geographical features, which is due, first of all, to different levels of development of information technologies and the corresponding infrastructure, electronic commerce, and different approaches to regulation. This creates specific requirements for the activities of companies engaged in the issuance and maintenance of electronic money, as well as for the payment infrastructure that has been formed historically.

5. Technological risks. According to research results [14, 19], the following risks specific to the cybersecurity problem area can be distinguished:

– delays in transactions, loss of funds, or unavailability of the service due to server or payment system software failure;

– vulnerability to hacker attacks due to outdated infrastructure or insufficient layering of protection in payment systems;

– reduction in the competitiveness of payment systems and increased vulnerability to modern cyber threats due to an insufficient level of integration of new technologies.

6. Trust risks:

– lack of anonymity due to the illegal sale of confidential data of online shoppers and website users. According to Verizon's 2023 Data Breach Investigations Report [15], 74% of all cyber threats are human-related. This is down from 82% in 2022, but this decline is likely a coincidence rather than the result of effective management;

– a large number of fraud cases, long payment delays, and a low probability of compensation for losses in the event of fraudulent transactions or user errors in transferring funds. According to the NBU, the total losses of payment service providers, merchants, and customers from illegal transactions with payment cards in 2023 amounted to almost 833 million hryvnias. According to Statista, in 2022 the volume of such transactions increased by 3.4%, reaching $33.45 billion. In 2023, the amount of card fraud increased to $36 billion (excluding the US market);

– low transparency of algorithms and procedures, insufficient information provided to users about their transactions, and unpopular decisions of the National Bank of Ukraine due to the imperfection of methods and techniques for regulating non-cash transactions.

The above indicates that electronic money, as an innovative high-tech product, requires constant and reliable protection. This protection should cover the stages of issuing electronic money and performing payment transactions with it, including the opening and maintenance of electronic wallets.

The security of electronic money transactions can be achieved through [15, 17]:

– mandatory verification and identification of electronic money users;

– setting limits for electronic money transactions;

– strengthening requirements for banks issuing electronic money regarding control over the activities of commercial agents;

– increasing the level of protection for the rights of electronic money users;

– encryption of payment system pages with reliable algorithms;

– making payments and transfers only through certified payment systems. The Payment Industry Security Standards Council (PCI SSC) was founded on September 7, 2006, by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. Its main goal is to regulate and develop security standards in the payment card industry [17, 18]. The Payment Industry Data Security Standard (PCI DSS) contains twelve core requirements and numerous sub-requirements that help companies evaluate their policies, procedures, and security measures related to payment card processing. To counter the growing cyber threats in the payment industry, the PCI SSC currently manages 15 security standards that cover various aspects of the activities of card issuers, merchants, service providers, solutions, acquirers, and processors. PCI DSS certification requirements apply to: banks (in Ukraine, compliance with the standard is mandatory for all banks); trading enterprises; retail stores; call centers; payment gateways; and other organizations involved in the processing, transmission, and storage of payment cardholder data.

– cooperation with cybersecurity authorities at all levels (international, national, electronic money issuer, etc.), and conducting a mandatory cybersecurity audit. The audit should cover: the physical level (protection of physical equipment); the virtual level (protection of virtual infrastructure); and the software level (protection of the payment application);

– confidentiality, non-disclosure of trade secrets, and protection of intellectual property rights for electronic money issuance technologies and the execution of payment transactions with them;

– protection against criminal attacks and monitoring of operations in real time;

– taking preventive measures to prevent the circulation of electronic money issued by aggressor countries and the use of their payment systems. Thus, in 2016, the NBU banned the use of electronic money related to Russian payment systems [15]: WebMoney, Yandex Money, QIWI Wallet, Wallet One ("Single Wallet"). In Ukraine, the use of electronic wallets [16] is allowed: Paysera, Payoneer, Payeer, Global24, PayPal, AdvCash, Perfect Money, SettlePay Wallet. On April 1, 2023, Law No. 2654-IX "On Amendments to the Tax Code of Ukraine and Certain Other Laws of Ukraine Regarding the Features of Taxation of Entrepreneurial Activities of Electronic Residents" [25] came into force.

– promoting the issuance of national electronic money and increasing the effectiveness of monetary policy;

– promoting the development of national payment systems and the evolution of Ukraine's payment infrastructure in accordance with global trends in the strategy of digitalization of the country's economy as a whole. The most developed payment systems in Ukraine are listed in Table 2.

As part of its oversight function, the National Bank, based on the results of monitoring its activities in 2023, identified a

Table 2

The most developed payment systems in Ukraine*

No.	Name	Accessibility	Transfer speed	Commission within Ukraine
1.	SPACE	no mobile app	Instantly	0.3%
2.	NovaPay	100%	Instantly	1.5%
3.	EasyPay	100%	Instantly	0.5% – 1%
4.	Wallet	100%	Instantly	1%
5.	Sense (Alfa-Bank)	100%	Instantly	3%
6.	City24	100%	Instantly	2%
7.	4bill	no mobile app, and several useful features are still in the demo version	Instantly	1.25%
8.	Postal order	100%	from 15 minutes	0.3% – 2.5%
9.	Western Union	100%	15 – 30 minutes	1 – 2%

*Source: [16]

list of key payment infrastructure facilities in Ukraine. As in previous years, the Electronic Payment System (EPS) of the National Bank of Ukraine was recognized as the only systemically important payment system. In 2024, approximately 483 million payments were made through the EPS for a total amount of almost UAH 241 trillion, of which 19 million payments for a total amount of UAH 56.5 billion were made within the framework of state programs. Compared to 2023, when 423 million payments for over UAH 210 trillion were made, the volume of transactions increased by 14% both in number and in amount [8]. Six systems were included in the category of important payment systems, namely: MasterCard, MasterCard International Incorporated, USA; Visa, Visa International Service Association, USA; NovaPay, LLC NovaPay, Ukraine; "PrivatMoney", JSC CB "PrivatBank", Ukraine; "MONEYCOM", LLC "SWIFT GARANT", Ukraine; "Financial World", LLC "Ukrainian Payment System", Ukraine.

Analysis of scientific publications indicates that most scientists classify electronic money by their areas of application or origin and distinguish the following main types: electronic wallets of banks, mobile payment applications, electronic wallets and payment systems, electronic payment cards, and cryptocurrency. Each type has both general and specific financial risks inherent only to it. In our opinion, the reliability of each type of electronic money is characterized by an integral risk indicator, which can be represented in the form of a multiple regression equation:

$$I_{em} = \sum_{i=1}^{n} a_i x_i$$

where I_{em} is the dependent variable; a_i is the coefficient of the regression model; xi are the model factors, i= 1, … n.

The weighting coefficients of significant financial risks for each type of electronic money are selected as coefficients of the regression model, and the statistical data on financial losses during their implementation are selected as factors. Thus, the task of assessing the financial risk of using a given type of electronic money is reduced to conducting a multifactor correlation-regression analysis.

Conclusions and suggestions. Summarizing the above, it can be argued that electronic money plays an important role in the modern economy, acting as an alternative to traditional instruments of circulation, storage, and accumulation of financial resources. Performing the established functions of money, their digitized analogues open up broad prospects for the manifestation of their unique qualities, which will provide new business opportunities and become an impetus for the development of civilized economic relations worldwide. Like every revolutionary technology, electronic money is far from ideal; its development and implementation are only at the initial stage, marked by constant improvement and the emergence of new types and forms. These processes are accompanied by significant financial risks and threats. The development of digital financial technologies is carried out in both positive and negative directions: along with the improvement of means and methods of management, methods and means of criminal encroachments are also being improved. Economic instability, political, and military upheavals only increase external and internal threats to the use of electronic money. Today, in Ukraine, a significant share of the financial risks of electronic money is due to the implementation of threats caused by the Russian military invasion. The main threats are: economic recession, attacks on critical infrastructure, lack of skills or labor, and institutional collapse in the financial sector. Significant financial risks include those that are part of the groups of technological, geographical, legal, and regulatory risks. The low level of digital literacy of the population and business increases cybersecurity risks, creates a crisis of confidence, and fosters fertile conditions for fraud. Electronic money is characterized by diversity; its types can be determined by areas of application or origin. It is proposed to use an integral risk

indicator when determining the reliability of each type of electronic money. Thus, the task of assessing the financial risk of using a type of electronic money is reduced to conducting a multifactor correlation-regression analysis.

The financial risks of electronic money are a serious problem for today's digital economy. Their effective management requires a joint effort of technology companies, financial institutions, governments, and users themselves. Despite the risks, electronic money is likely to continue developing if security and transparency become a priority for all market participants.

Bibliography

1. Тарасенко І. О. Фінансова стабільність в цифрову епоху: європейські підходи та особливості їх імплементації в Україні. *Зб. наук. праць V Міжнародної науково-практичної інтернет-конференції «Імперативи економічного зростання в контексті реалізації глобальних цілей сталого розвитку»* КНУТД, 23.04.2024 р. С. 395–399. URL: https://surl.li/mldqde

2. Віталій Кравчук, Дмитро Науменко, Андрій Глибовець. Електронні гроші в Україні. *Аналітичний звіт.* К.: Альфа-ПІК, 2012. 64с. ISBN: 978-966-1670-10-4.

3. Короленко О. Б., Рябикіна Н. І., Рябикіна К. Г. Інвестиційний клімат України в умовах глобальних ризиків: виклики та можливості для бізнесу. *Актуальні питання у сучасній науці.* № 11(29) 2024. С.159–172. https://doi.org/10.52058/2786-6300-2024-11(29)-159-172

4. Кібербезпека в інформаційному суспільстві: *Інформаційно-аналітичний дайджест* / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України». К., 2024. №6 (червень). 364 с. URL: https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi

5. Павлюк Я. Майбутнє цифрових грошей в Україні. *Українська правда*. URL: https://epravda.com.ua/columns/2023/04/12/699012/

6. David Schmidtchen. From awareness to behaviour change: The micro-foundations of cybersecurity culture // Private Media Pty Ltd. URL: http://surl.li/lsmgsj

7. Українці активно починають використовувати платіжні картки для безготівкових розрахунків *Сайт експертних оцінок співробітників Національного банку України* URL: https://surl.li/owmtzv

8. Офіційний сайт НБУ. URL: https://bank.gov.ua

9. Вплив Інтернету на економіку України. *Офіційний Блог Google Україна.* URL: https://ukraine.googleblog.com

10. Шахрайські та фішингові сайти. Аналіз, тренди та рекомендації для клієнтів. *ЄМА: Дайджест платіжного шахрайства*. Лютий 2023. URL: https://www.ema.com.ua/news/

11. Деркач М. Як криптовалюти використовуються для відмивання коштів. Звіт Chainalysis. *Vagazine PaySpase.* URL: http://surl.li/awrqnr

12. Illegal casinos are using Roblox to draw children into online gambling. *Sky News.* Science, Climate & Tech. URL: http://surl.li/vcavld

13. Industry-Specific Cybersecurity Concerns: Safeguarding Your Business in the Digital Age. *News Track Live*. URL: http://surl.li/vemhjs

14. 2024 SonicWall Mid-Year Cyber Threat Report. *SonicWall* URL: http://surl.li/yzdopc

15. Чепурко Г. Електронні гроші: особливості електронного гаманця в Україні. *MCtoday 2022*. URL: http://surl.li/qgdwbr

16. Цимбалюк І. Електронні гроші: види цифрових грошей, переваги та недоліки інтернет-грошей. *Rates.fm 2024*. URL: http://surl.li/maggit

17. Official PCI Security Standards Council Site. URL: https://surl.li/uhzgab

18. Fruhlinger, Josh (17 July 2020). «PCI DSS explained: Requirements, fines, and steps to compliance». CSO Online. URL: http://surl.li/saucmv

19. Cyber digest. *Огляд подій в сфері кібербезпеки, липень 2024.* URL: https://ufss.com.ua/wp-content/uploads/2024/08/Cyber-digest_Jul_2024_UA.pdf

20. Benjamin Jensen, Yasir Atalan (2024). Assessing Russian Firepower Strikes in Ukraine. *CSIS*. URL: https://surl.li/stjxoy

21. World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023. *Forescout Research/Vedere Labs* URL: http://surl.li/qnhgjm

22. Через повномасштабне вторгнення Росії за кордоном перебуває близько 20% українців. *Дослідження ОПОРИ* URL: http://surl.li/bwunri

23. Tap, click and pay: how digital payments seize the day. Bank for International Settlements 2024. URL: https://www.bis.org/statistics/payment_stats/commentary2402.pdf

24. Постанова Правління Національного банку України від 29 вересня 2022 року № 210 «Про затвердження Положення про випуск електронних грошей та здійснення платіжних операцій з ними». URL: http://surl.li/mecpsi

25. Закон України № 2654-IX «Про внесення змін до Податкового кодексу України та деяких інших законів України щодо особливостей оподаткування підприємницької діяльності електронних резидентів». URL: https://surl.li/srcjha

References

1. 2024 SonicWall Mid-Year Cyber Threat Report. *SonicWall* Available at: http://surl.li/yzdopc (Accessed 25 January 2025)

2. Bank for International Settlements (2024). Tap, click and pay: how digital payments seize the day. Available at: https://www.bis.org/statistics/payment_stats/commentary2402.pdf (Accessed 25 January 2025)

3. Benjamin Jensen, Yasir Atalan (2024). Assessing Russian Firepower Strikes in Ukraine. *CSIS*. Available at: https://surl.li/stjxoy (Accessed 25 January 2025)

4. Chepurko, G. (2022) *Elektronni hroshi: osoblyvosti elektronnoho hamantsya v Ukrayini* [Electronic money: features of an electronic wallet in Ukraine]. *MCtoday.* Available at: http://surl.li/qgdwbr (Accessed 25 January 2025) (in Ukrainian) (in Ukrainian)

5. Cyberdigest (2024) Overview of events in the field of cybersecurity, Available at: https://ufss.com.ua/wp-content/uploads/2024/08/Cyber-digest_Jul_2024_UA.pdf (Accessed 25 January 2025)

6. Derkach, M. (2024). Yak kryptovalyuty vykorystovuyut′sya dlya vidmyvannya koshtiv. Zvit Chainalysis [How cryptocurrencies are used for money laundering. Chainalysis report]. *Vagazine PaySpase*. Available at: http://surl.li/awrqnr. (in Ukrainian).

7. Dovgan, O., Lytvynova, L., Dorogykh, S. (2024) *Kiberbezpeka v informatsiynomu suspil'stvi: Informatsiyno-analitychnyy daydzhest* [Cybersecurity in the information society: Information and analytical digest] *State Scientific Institution "Institute of Information, Security and Law of the National Academy of Sciences of Ukraine"*. No. 6 (June). 364 p. Available at: https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi (Accessed 25 January 2025) (in Ukrainian)

8. EMA (2023). *Shakhrays'ki ta fishynhovi veb-sayty. Analityka, tendentsiyi ta rekomendatsiyi kliyentam* [Fraudulent and phishing websites. Analysis, trends and recommendations for customers]. EMA: Payment Fraud Digest. Available at: https://www.ema.com.ua/news/ (Accessed 25 January 2025) (in Ukrainian)

9. Fruhlinger, Josh (2020). «PCI DSS explained: Requirements, fines, and steps to compliance». CSO Online. Available at: http://surl.li/saucmv (Accessed 25 January 2025)

10. Korolenko, O.B., Ryabykina, N.I., Ryabykina, K.G. (2024). *Investytsiynyy klimat Ukrayiny v umovakh hlobal'nykh ryzykiv: vyklyky ta mozhlyvosti dlya biznesu* [Investment climate of Ukraine in conditions of global risks: challenges and opportunities for business]. Current issues in modern science. No. 11(29). P.159–172. http://doi.org/10.52058/2786-6300-2024-11(29)-159-172 (in Ukrainian)

11. Kravchuk, V., Naumenko, D., Hlybovets, A. (2012) *Elektronni hroshi v Ukrayini. Analitychnyy zvit* [Electronic money in Ukraine. Analytical report]. Kyiv: Alfa-PIK, 2012. 64p. ISBN: 978-966-1670-10-4. (in Ukrainian)

12. News Track Live (2024). Industry-Specific Cybersecurity Concerns: Safeguarding Your Business in the Digital Age. Available at: http://surl.li/vemhjs (Accessed 25 January 2025

13. Official Google Ukraine Blog (2024). The impact of the Internet on the economy of Ukraine. Available at: https://ukraine.googleblog.com (Accessed 25 January 2025)

14. Official PCI Security Standards Council Site. Available at: https://surl.li/uhzgab (Accessed 25 January 2025)

15. Official website of the National Bank of Ukraine. Available at: https://bank.gov.ua (Accessed 25 January 2025) (in Ukrainian)

16. OPORA (2023). Due to the full-scale Russian invasion, about 20% of Ukrainians are abroad. *OPORA research.* Available at: http://surl.li/bwunri (Accessed 25 January 2025) (in Ukrainian)

17. Pavlyuk, Ya. (2023). *Maybutnye tsyfrovykh hroshey v Ukrayini* [The Future of Digital Money in Ukraine]. Ukrainska Pravda. Available at: https://epravda.com.ua/columns/2023/04/12/699012/ (Accessed 25 January 2025) (in Ukrainian)

18. Schmidtchen, David (2023) From awareness to behavior change: The micro-foundations of cybersecurity culture, Private Media Pty Ltd. Available at: http://surl.li/lsmgsj (Accessed 25 January 2025)

19. Site of expert assessments of employees of the National Bank of Ukraine (2024). *Ukrayintsi aktyvno pochynayut' vykorystovuvaty platizhni kartky dlya bez·hotivkovykh rozrakhunkiv* [Ukrainians are actively starting to use payment cards for cashless payments] Available at: https://surl.li/owmtzv (Accessed 25 January 2025) (in Ukrainian)

20. Sky News. Science (2024). Illegal casinos are using Roblox to draw children into online gambling. Climate & Tech. Available at: http://surl.li/vcavld (Accessed 25 January 2025)

21. Tarasenko, I. O. (2024). *Finansova stabil'nist' v tsyfrovu epokhu: yevropeys'ki pidkhody ta osoblyvosti yikh implementatsiyi v Ukrayini* [Financial stability in the digital age: European approaches and features of their implementation in Ukraine]. Imperatyvy ekonomichnoho zrostannya v konteksti realizatsiyi hlobal′nykh tsiley staloho rozvytku [Imperatives of economic growth in the context of implementing global sustainable development goals] Coll. 5th Int. sc. Prac. Internet conf. Kyiv, pp. 395–399. Available at: https://surl.li/mldqde (in Ukrainian)

22. The Board of the National Bank of Ukraine Resolution No. 210 (2022) "On Approval of the Regulations on the Issuance of Electronic Money and the Implementation of Payment Transactions with Them". Available at: http://surl.li/mecpsi (Accessed 25 January 2025) (in Ukrainian)

23. The Verkhovna Rada of Ukraine (2012). Law of Ukraine No. 2654-IX "On Amendments to the Tax Code of Ukraine and Certain Other Laws of Ukraine Regarding the Peculiarities of Taxation of Business Activities of Electronic Residents". Available at: https://surl.li/srcjha (Accessed 25 January 2025)

24. Tsymbalyuk I. *Elektronni hroshi: vydy tsyfrovykh hroshey, perevahy ta nedoliky internet-hroshey* [Electronic money: types of digital money, advantages and disadvantages of Internet money] Rates.fm 2024. Available at: http://surl.li/maggit (Accessed 25 January 2025) (in Ukrainian)

25. Vedere Labs (2024). World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023. Forescout Research. Available at: http://surl.li/qnhgjm (Accessed 25 January 2025)

FINANCIAL RISK MANAGEMENT OF ELECTRONIC MONEY

Roman G. Snishchenko, Communal Institution of Higher Education «Kremenchuk Humanitarian and Technological Academy» of the Poltava Regional Council, Kremenchuk, (Ukraine).
E-mail: Rosnishchenco@gmail.com

https://doi.org/10.32342/3041-2137-2026-2-65-8

Keywords: electronic money, risk, management, payment instruments, payment systems, electronic wallets, cryptocurrency, hacker attacks, cybersecurity, fraud
JEL classification: ***D81, D83, D84, E52, E66, O23***

The purpose of the article is to identify and study the main types of financial risks of electronic money in modern conditions of digitalization of the economy.

When preparing the scientific publication, general scientific and special research methods were used: the method of critical analysis, scientific abstraction, and generalization of scientific experience of modern theoretical research, as well as a systemic and comprehensive approach.

The study results are as follows: the areas of use of electronic money were clarified; the main types of financial risks of electronic money were defined and analyzed; the structure was investigated, and a classification of financial risks of electronic money was provided; specific risks of electronic money caused by the war between Russia and Ukraine were identified. Based on the research, a list was provided, and the content of the main measures to ensure the security of transactions with electronic money was disclosed.

The scientific novelty of the results of the study is as follows. The types of financial risks of electronic money identified in the article allow us to adjust the tasks aimed at increasing the level of their security. The proposed main measures to achieve the security of transactions with electronic money contribute to the formation of a strategy for maximum security of the activities of business structures in modern conditions of digitalization of the economy. The methodological approach to the selection of organizational measures for the safe issuance, use, and storage of electronic money and to determining their reliability has received further development. This will allow for the optimal use of the financial resources of business entities while maintaining an acceptable level of their economic security.

The practical significance lies in the fact that the theoretical provisions of the study regarding financial risks and the content of the main measures to achieve the security of electronic money transactions can be used in the strategic and tactical planning of the economic activities of financial market participants.

Дата надходження до редакції / Submitted: 08.04.25
Дата прийняття до публікації / Accepted: 29.01.26
Дата публікації / Published: 02.07.2026