

## THE ROLE PLAYED BY THE DIGITAL TRANSFORMATION OF UKRAINE'S FINANCIAL SECTOR IN THE CONTEXT OF POST-WAR RECONSTRUCTION: OPPORTUNITIES AND RISKS

©2022 KORNIVSKA V. O.

UDC 330.34:336.717  
JEL: G21; G29; O16; O31

### Kornivska V. O. The Role Played by the Digital Transformation of Ukraine's Financial Sector in the Context of Post-War Reconstruction: Opportunities and Risks

*The purpose of the article is to systematize the main directions of digital transformation of the financial sector of Ukraine, to characterize their impact on the post-war recovery of the Ukrainian economy and to analyze the risks of forming an information-digital society in connection with the active implementation of a digital strategy. As a result of the study, it is proved that special conditions that are established at present in Ukraine make inevitable the digital development strategy to ensure economic activity under martial law and post-war recovery. The publication systematizes the main mechanisms for ensuring financial access under conditions of martial law. The advantages of the actively implemented conception of open banking for investment processes and post-war reconstruction are demonstrated, while the risks of information availability related to open banking are shown. The role of neobanks in the context of post-war recovery is characterized. Given that the development of digital financial services will be associated with the further introduction of service personalization technologies, it is concluded that this will lead to the growth of financial inclusion and the deep integration of digital financial institutions into the economic and social existence of financial services consumers. The risks of these processes are identified, in particular the risks of cybersecurity and the growth of information asymmetry.*

**Keywords:** digital technologies, financial sector, martial law, post-war recovery, risks of digitalization.

**Bibl.:** 37.

**Kornivska Valeriia O.** – D. Sc (Economics), Senior Research Fellow of the Department of Economic Theory, Institute for Economics and Forecasting of NAS of Ukraine (26 Panasa Myrnoho Str., Kyiv, 01011, Ukraine)

**E-mail:** [vkornivska@ukr.net](mailto:vkornivska@ukr.net)

**ORCID:** <https://orcid.org/0000-0002-0348-0404>

УДК 330.34:336.717  
JEL: G21; G29; O16; O31

**Корнівська В. О. Роль цифрової трансформації фінансового сектора України в контексті повоєнного відновлення: можливості та ризики**  
*Метою статті є систематизація основних напрямків цифрової трансформації фінансового сектора України, характеристика їх впливу на повоєнне відновлення української економіки та аналіз ризиків формування інформаційно-цифрового суспільства у зв'язку із активною реалізацією цифрової стратегії. У результаті проведеного дослідження доведено, що в Україні сьогодні склалися особливі умови, що роблять невідворотною цифрову стратегію розвитку для забезпечення економічної діяльності в умовах воєнного стану та повоєнного відновлення. У роботі систематизовано основні механізми забезпечення фінансового доступу в умовах воєнного стану. Показано переваги активно впроваджуваної сьогодні концепції відкритого банкінгу для забезпечення інвестиційних процесів і повоєнної реконструкції, водночас показані ризики доступності інформації, що виникають у зв'язку із open banking. Охарактеризовано роль необанків у контексті повоєнного відновлення. Зважаючи на те, що розвиток цифрових фінансових послуг буде пов'язаний із подальшим впровадженням технологій персоналізації обслуговування, зроблено висновок, що це зумовить зростання фінансової інклюзії та глибоку інтеграцію цифрових фінансових установ у економічне та соціальне буття споживачів фінансових послуг. Визначено ризики цих процесів, зокрема ризики кібербезпеки та зростання інформаційної асиметрії.*

**Ключові слова:** цифрові технології, фінансовий сектор, воєнний стан, повоєнне відновлення, ризики цифровізації.

**Бібл.:** 37.

**Корнівська Валерія Олегівна** – доктор економічних наук, старший науковий співробітник відділу економічної теорії, Інститут економіки та прогнозування НАН України (вул. Панаса Мирного, 26, Київ, 01011, Україна)

**E-mail:** [vkornivska@ukr.net](mailto:vkornivska@ukr.net)

**ORCID:** <https://orcid.org/0000-0002-0348-0404>

One of the basic characteristics of digital economy is its inclusiveness. Digital economy is an economy whose development creates opportunities to fully involve actors in social and economic communication. Paul Mason in his famous work *Postcapitalism: A Guide to Our Future*, defining the advantages of modern society, proves that the main thing is connections, communication in space and time, mobile access to information, services, and financial resources [1].

Digitization of financial services develops in order to ensure that financial resources be delivered to the end user in the most efficient and convenient way. Due to the

use of remote identification systems, a client is no longer required to be physically present in a financial institution to obtain a financial service. Online digital technologies provide access to financial resources and meet the growing financial needs of market actors by overcoming the spatial and temporal limitations of economic activity.

Intensification in using digital technologies, increase in the number of startups in the financial sector, significant amounts of bank investments in digital regulatory solutions, and expanding the range of digital financial services provided together indicate an increase in the digital capabilities of Ukrainian financial intermediaries

against the background of the growing global consumer demand for digital financial services. In 2026, more than half of the world's population (53%) will receive access to digital banking services; the number of digital banking users will grow from 2.5 billion people in 2021 to more than 4.2 billion people in 2026 [2].

Before the COVID-19 pandemic, digital financial services were positioned as just another possible way to obtain financial access, but during the crisis it became obvious that under the circumstances of global destabilization, digital channels become a cornerstone mechanism to ensure that market entities continue their operational activity. Digital technologies help to do the following: 1) meet consumers' needs; 2) sell a company's products; 3) provide the population with social assistance; 4) implement state programs to support small and medium-sized businesses.

The impact of the digital finance development on various spheres of economic and social genesis is considered in a significant number of modern scientific studies. Most of the authors point out that digital transformation in the financial services industry helps companies and individuals improve and expand their access to finance. Such articles analyze the way how digital technologies developing in the financial sector can contribute to the growth of employment and wages; demonstrate market advantages, in particular, the way how the intensification of electronic commerce can cause decrease in product prices and increase in turnover [3]. The positive impact of financial services digitization on increasing "green credits" and reducing carbon emissions is characterized [4]. The potential of digital finance in the context of enhancing business is determined [5] and its development in African countries is substantiated.

At the same time, as some previous works predicted [6], digital banking also brings significant risks to the stability of household finances, as it leads to increase in household debt, which fact is highlighted, in particular, by research on digital financial inclusion and household debt in China [7]. There are widely presented developments proving that digital finance has a greater beneficial effect on the consumption of households with fewer assets, lower incomes, smaller financial literacy [8], thus supporting the argument for digital financial inclusion as a way of financial activity typical for low-income households [9]. Financial stability risks are more often becoming the subject of research due to the digital finance development [10; 11]. The issues of their influence on allocating household income are being discussed, as well [12].

It is obvious that the mechanisms, rates and results of introducing digital technologies in the financial sphere depend on the conditions that initially created a motivational basis for digital transformation. No less significant is the influence of socio-institutional and economic factors, the previous experience of the financial development in a country, geopolitical factors, and the activity of state bodies in implementing a digital strategy.

In developing countries, digital banking is becoming an important mechanism for ensuring economic activity, while advanced countries with effective financial intermediation experience the benefits of digital finance to a lesser extent. At the same time, the COVID-19 pandemic has shown that during crisis even advanced countries faced forced suspension of economic activity, and thus not only the economic activity of market actors, but also their everyday existence and survival depended on the degree of their financial inclusion and the breadth of implementing digital technologies in the financial sector.

The Russian aggression against Ukraine created specific conditions under which a digital development strategy becomes vital and inevitable for ensuring economic activity under martial law and during post-war recovery. During the first months of the Russian-Ukrainian war, the Ministry of Digital Transformation of Ukraine implemented important initiatives to support business on the Diya portal, which simplified the procedures for opening, transferring to a safer place and resuming the work of Ukrainian enterprises as much as possible; made it accessible and less bureaucratic to receive grant and credit funds to conducting economic activity in times of war; and created a single register of exporting enterprises so that foreign importers could use it to find partners in Ukraine [13].

Digital financial products have proved to be of decisive importance in a country at war. At the same time, it should be realized that intensifying the implementation of the digital strategy, one can face growing risks both of the technological and institutional nature. It should also be taken into account that, expanding the scope of use of digital financial services, we are increasingly connecting the criteria of convenience and mobility with the issues of economic activity and social life. Thus, significant risks appear of rooting illiberal approaches in the country's economy.

The article *aims* at showing the role which can be played by the digital transformation of Ukraine's financial sector in the post-war recovery of its economy, and at characterizing the risks awaiting us on the way of forming an information and digital society through actively implementing a digital strategy.

The development of digital technologies in the financial sector leads to the formation of a fundamentally new approach to building the interaction between a financial institution and consumers of financial services through creating ecosystems in which a financial institution is effectively integrated into the economic activity and everyday life of consumers. Banking services are becoming more convenient and customer-oriented thanks to remote identification technologies, artificial intelligence, personal finance management software, Internet of Things, voice banking, digital service delivery platforms, and chatbots. Digital channels allow users to receive most financial services remotely.

The benefits of remote service have been fully demonstrated during both the COVID-19 pandemic and the current crisis. The use of digital channels made it possible to make retail non-cash payments (P2P, P2B, B2B), targeted social payments (G2P), corporate payments of legal entities (B2B), and cross-border payments (B2B, P2P, P2B), allowing the financial market to work stably and perform its functions.

**M**artial law conditions further exacerbated the problem of financial access; its effective solution directly affected the continuity of liquidity flow and maintenance of economic ties. Considering the fact that digital transformations in the financial sphere are most actively developing in order to meet the clients' payment needs, since the start of war in Ukraine, transaction services have been provided as quickly as possible, and the amounts of non-cash transactions have grown despite the war. According to the National Bank of Ukraine, 'in May 2022, the number of transactions (non-cash and cash receipts) using payment cards issued by Ukrainian banks in Ukraine and abroad reached 637 million transactions, amounting to UAH 573.7 billion. If compared with pre-war January 2022, the number of transactions decreased insignificantly (by 3.4%), while their amount increased by almost a third (by 31.5%). In particular, in May 2022 more than 582 million transactions worth about UAH 502.4 billion were carried out in Ukraine using payment cards. This is 7.5% less in terms of quantity and 20.4% more in terms of amount compared to January 2022. Beyond Ukraine, the amount of paying for goods at payment terminals placed in retail network and receiving cash at ATMs using payment cards amounted to UAH 57.5 billion in May this year (in January it made up about UAH 7 billion). As for non-cash transactions with payment cards made in May this year, as compared to January, their number decreased by only 2.3% to 588 million, and the amount increased by 43.0% to UAH 395.0 billion' [14].

International online payments are of particular importance for maintaining the economic activity and livelihood of many millions of refugees and war-torn Ukrainian families. This segment of payment operations is developing rather rapidly against the background of more often usage of global trading platforms. In twelve years, the global volume of international payments has increased tenfold, from \$15 trillion in 2010 to \$156 trillion in 2022 [15]. The international money transfer system of the neobank Revolut, the Polish fast international money transfer system Perekaz24, the instant transfer platform Fin.do, TransferGo, the Paysera payment service, two card payment systems (Diners Club International (USA) and JCB Payment System (Japan)), and some other operators are present in the Ukrainian market.

Taking into account the peculiar character of the future post-war reconstruction of Ukraine which is to involve financial resources from world donors, further

technological harmonization of the Ukrainian and European financial markets is as up-to-date as never before. The National Bank of Ukraine is working on implementing instant payments, the advantages of which are risk minimization, protection, lower tariffs for users, convenience and transparency of transfers [16]. The advantages of instant payments will help increase customer engagement in the system of digital financial transactions and affect overall financial inclusion.

The introduction of remote customer identification was another step towards greater financial inclusion of the population in Ukraine and greater access of the general public to financial services. Today, 70% of the monthly deposit portfolio of a Ukrainian bank is attracted through remote channels, and about 80% of deposits are processed online [17]. Further implementation of digital financial services will lead to an increase in the current level of financial inclusion from the existing 72% [18] to 85–90%.

**G**iven the sufficient level of financial inclusion in Ukraine and the active development of digitalization in the post-war recovery period, the digital financial sector can become a center to form ecosystems encompassing the reconstruction process. In the world of digital finance, digital investment platforms have been developing for more than a year, representing a digital solution that combines automated functions of financial management used for savings, and investments in shares and investment funds. Digital investment platforms reduce the cost of providing financial services through automation, artificial intelligence, and machine learning technologies, thus replacing human decision-making with algorithm-based decision-making.

The implementation of digital technologies in the investment process will be facilitated by the concept of open banking implemented today, which will develop on the basis of the Law of Ukraine "On Payment Services". This law adapts Ukrainian legislation to the EU legal field and in the future will make it possible to integrate Ukraine's payment system with that of the EU. The norms of the new law establish the transition of the Ukrainian payment infrastructure to the ISO20022 international standard which serves as the basis for the functioning of European payment systems, and lay the foundation for Ukraine's accession to the Single Euro Payments Area (SEPA) [19].

Open banking enables clients to manage their financial information and provide accredited companies with access to it [20]. As a result of implementing open banking, new Fintech (i.e. new products and services for customers) will be created by using open API technology, thus enabling Fintech companies to cooperate with banks in various directions. Open banking will promote price and non-price competition in the market due to an increase in the presence of new service providers in the banking market, thus leading to even more targeted use

of client-oriented approaches in service, and tighter financial involvement. The formation of a single financial services ecosystem in the national financial space and joining it to supranational platforms is seen as the final result of open banking implementation.

High levels of digitization in the Ukrainian financial and institutional environment have created conditions for digital financial institutions to achieve a sufficient level of subjectivity. Today, Ukrainian banks are participating the global trend and digitizing the main components of their activities: they are using digital platforms to provide services in the most effective way, developing chatbots, and actively implementing technologies aimed at individualizing the processes of meeting the needs of the population and small and medium-sized businesses. The neobanks segment is actively developing, providing services based on the license of traditional founding banks without creating a physical office or a branch.

**T**he neobanks segment of Ukrainian economy began to form in 2017, and now Ukrainian market has 8 such neobanks, the most active of which are monobank, Vlasny Rakhunok, sportbank, izibank, and Sense SuperApp. The market leader monobank provides such services as: card products, loans, payments, crowdfunding operations, operations with military bonds. Starting with December 2021, operations with shares of foreign companies are carried out using the mono invest application. Today, there are 6.1 million monobank customers who, as of July 2022, have made purchases worth UAH 3.3 billion, and 476 million incoming and 549 million outgoing payments between cards [21].

The world practice of neobanks development shows that in order to take the proper place among the providers of digital financial services in the Fintech industry, it is necessary to use innovative approaches both in technology and in achieving the the social effect of attracting new customers. Therefore, growing activity in the field of socially significant projects is typical for neobanks. This is proven, in particular, by their work in the field of green banking and in servicing markets that used to be “non-bank”. Such institutions, while offering classic digital financial services to their clients, at the same time tend to fund environmental projects, and provide Fintech-lending to the population with a low level of financial access. The social point of Ukrainian banks manifested after martial law was implemented, when non-banks took an active part in crowdfunding activities.

Taking into account global experience in implementing socially significant investment projects in neobanks, the growing consumer trust in the Ukrainian segment of neo-banking, and its significant client base, digital banks can become a source of investment for post-war recovery.

The fact that Ukraine’s financial sector is on the way to entering the global consumer and financial space can be proven by its compliance with the global trends of

digital development, the obvious stability of the payment services, and its faster movement towards open banking. Further development of digital financial products will be connected with the introduction of technologies helping to personalize services using artificial intelligence, development of voice and biometric services, personalization of credit products, replacement of traditional banking products with context-relevant ones, and platformization of services. These marketing activities will further contribute to the growth of financial inclusion and integration of digital financial institutions into the economic and social lives of consumers of financial services.

At the same time, it should be taken into account that the growing financial inclusion of market actors is associated with growing risks of digital development, and cyber security risks, in particular.

**A**ccording to the Trend Micro report, the number of ransomware attacks in the banking industry increased by 1,318% in 2021. Financial companies experience cyberattacks 300 times more often than other industries do [22]. In January and February 2022, Ukraine faced the most significant hacker attacks on the websites of banks and state institutions. Due to a powerful DDoS attack, the PrivatBank and Oschadbank applications failed; in addition, monobank, Alfa-Bank, the Diya portal, the websites of the Ministry of Defense and the Armed Forces [23] were attacked, too. The common target of cybercriminals is data. In 2018, due to data leakage that occurred at a major passenger airline, hackers obtained confidential details of more than 244,000 credit cards. Damages amounted to about \$12.2 million [24]. The precedent with Banco de Chile, a Chilean bank (May 24, 2018) showed that a large-scale system failure taking place as a result of a cyber attack may not be the final goal of the attack, but a curtain for withdrawing a significant amount of money from the bank (in the Banco de Chile case, it was \$11 million) [25]. The hacking of the systems of the American bank Capital One in 2019 remains the most high-profile case, as a result of which the hacker gained access to the data of 100 million customers and 80 thousand bank accounts. Losses caused by this data leak were estimated at up to \$150 million [26].

Global trends in organizing fight against cyber-crime demonstrate general strengthening of the responsibility born by financial institutions and centralizing control over cyber security. In the USA, UK, and EU, banking institutions are responsible for being informed as for the trends in cyber security; they must maintain contact with regulators and report hacking attacks that may affect their capability to provide services; they are obliged to inform the corresponding authorities about all the incidents that make up a potential threat to the institution and everything that can affect the stability of the country’s financial sector. The aggravation of the situation around Ukraine in early February 2022 (just before Russia’s invasion) led to a special attention of global fi-

financial regulators to cyber security. The ECB required banks to thoroughly prepare for cyberattacks; banks conducted cybergames to test their ability to withstand hackers' actions; New York's Department of Financial Services issued a warning to financial institutions, noting the increasing likelihood of cyberattacks; finally, the British National Cyber Security Center urged large companies to increase their attention to this area [27].

Ukrainian cyber security norms in the financial and institutional space are in the global trend. Thus, Regulation No. 178 of the Board of the National Bank of Ukraine dated August 12, 2022 "On the approval of the Regulation on organizing cyber defense in the banking system of Ukraine and amendments to the Regulation on identifying critical infrastructure objects in the banking system of Ukraine" [28] defines the following: the basic principles on which cyber defense systems function; principles of providing information exchange between the Cyber Defense Center of the National Bank and other banks in Ukraine; requirements for measures to ensure cyber defense of critical information infrastructure objects; requirements for conducting an independent audit of information security of banks. Regulation No. 4 of the NBU Board dated January 16, 2021 "On the approval of the Regulation on monitoring banks' compliance with the requirements of legislation on information security, cyber defense and electronic trust services" [29] introduced a new type of control over banks in the form of on-site inspections and on-site supervision, which will be carried out by specialists of the National Bank in the field of cyber defense and information security.

The problem of illegal acquisition of data by using social engineering technologies requires special attention amid growing digitization. According to the 2019 survey conducted by Zogby Analytics for the US National Cyber Security Alliance, nearly half (44%) of companies with 251–500 employees said they had experienced data losses in the past 12 months. The FBI Internet Fraud Center estimates that in 2018 alone, cyberattacks cost US companies more than \$2.7 billion, \$1.2 billion of which was lost in business email compromise attacks [30]. In the financial space, fraudulent data acquisition techniques are targeted both at financial institutions and straight at bank cardholders. It is not uncommon when artificial intelligence is used in phishing attacks. Fraudulent activities include stealing personal data and taking control of victims' accounts, cyberattacks, cardless transaction fraud, and fraudulent schemes with push payment authorization. The sums of losses caused by criminal fraudulent groups in Ukraine amount to millions of hryvnias and are constantly growing. In August 2022, employees of the Cyber Police Department, with the assistance of PrivatBank security service, exposed a fraud scheme, using which attackers stole UAH 36 million from citizens' bank cards [31].

With the increasing pace of digitalization, the problem is going to become more acute, and the only way to

solve it is to bring the pace of digitalization in line with the population's digital literacy while strengthening the cyber defense systems of institutions. More than half of respondents to the Global Banking Fraud Survey (2019) reported that the share of fraud losses reimbursed was less than 25% of the amount of losses incurred. This low rate demonstrates the importance of fraud prediction and prevention. That is why banks invest in new fraud prevention technologies, namely, machine learning, real-time fraud reporting, voice, face and fingerprint recognition (biometrics) and profiling of customers' interactions with their devices and online banking (behavioral biometrics) [32].

It should be taken into account that in parallel with the intensification of the fight against cybercrime led by banks, institutional levelling is taking place, creating objective conditions for fraud to increase in the financial markets. Thus, the concept of open banking, which is being actively implemented today, along with its obvious advantages of developing the national financial market and integrating it into the global financial space, at the same time creates implicit threats to data accessibility.

The ambivalence of open banking lies in the fact that, on the one hand, it will provide an additional opportunity to obtain more data about the customer, which can be used to prevent and detect fraud and compensate for losses caused by fraudulent attacks. On the other hand, open banking can make the data of financial services consumers accessible to many interested parties (not only the providers of these services) and thus increase the problem of fraud in the market. The feigned convenience of creating a single information base for the ecosystem of meeting consumer and financial needs actually causes a closed information platform to appear, where subject information emitted once can be used by many participants without its owner's consent for the benefit of interested parties, and not obligatory within the legal field. In financial markets, opportunism in using information can never be ruled out.

Historically, the controversial implementation of open banking is strongly related to another initial and deep problem of unwanted collection, systematization and analysis of information about the consumer and financial behavior of market actors in the situation when client-oriented business approach and direct marketing prevail. The problem of protecting financial services consumers in Ukraine from unwanted marketing collection and use of information about them has remained unresolved for many years. In the EU, repeated attempts to solve this problem by consensus resulted in the development of the EU Regulation on Privacy and Electronic Communications, or ePrivacy Regulation (now it is at the stage of adoption) [33]. This document:

- ✦ clearly defines the legal principles and adequate limits of carrying out any marketing campaigns;

- ✦ establishes the requirement to obtain the users' prior consent to receive commercial electronic messages and collect information about them;
- ✦ introduces the principle of openness of information about advertisers (it prohibits masking the identity and using false identifications, false return addresses or numbers when sending unwanted commercial messages for direct marketing purposes).

This document while regulating the space of information about financial services consumers in terms of its formation and responsible use, still does not solve a very important and up-to-date problem typical for digital transition, namely, misinformation.

The *Information and Analytical Digest* issued by the State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine" states the following: "From politics to medicine and cyber security, digital innovations have created a favorable environment for spreading disinformation. AI programming systems can now create false information and present it as fact – and even fool cybersecurity experts into thinking the information is true. The spread of misinformation is a problem that originates in human consciousness and is concretized with the help of big data, social networks and mass media. When misinformation is presented effectively, it is almost impossible to separate fact from fiction. And available data volume allows machine learning algorithms and artificial intelligence to constantly learn and adapt their results, which makes it even more difficult to detect the difference" [34].

**H**ow does this problem play out in the field of digital finance? It is directly related to the regulation of financial markets, which is increasingly tending towards automation. RegTech technologies are becoming widespread in the world, in general, and in Ukraine, in particular, thus providing opportunities to implement regulatory processes in the financial industry through digital solutions, e. g. BigData. RegTech solutions are implemented for a wide range of regulatory areas, namely regulatory changes tracking, fraud detection, know-your-customer (KYC), countering the financing of terrorism (CFT), risk management, systematic regulatory reporting and auditable accounting. They are among the goals of the National Bank as defined by the Financial Sector Development Strategy till 2025, the Fintech Development Strategy in Ukraine till 2025, and the Strategy of the National Bank of Ukraine till 2025.

RegTech tools allow banks to achieve better results in risk management and in the field of compliance, reduce costs through automation and release of back office workers, adapt to changes in regulation. RegTech is also designed to monitor transactions to detect violations in the field of digital payments. RegTech services are provided by some platforms.

For example, the Trulioo platform offers data verification, business verification and data sharing. The solution can identify 4 billion customers in more than 40 countries, thus making the platform most attractive in the competitive RegTech environment. The Hexanika platform is used to monitor and audit transactions in real time using distributed ledger technology [35].

The positive point of using these technologies is that institutions detecting potential threats at an early stage can minimize risks and costs. But this is just the surface of economic reality.

**D**ue to the significant risks of disinformation, an unobvious side effect of using RegTech technologies is the fact that it creates a negative reputation of the analyzed business partners by recognizing their operations and activities as being conducted outside the legal field, while no one can rule out deliberate misinformation or a simple mistake [36]. Such information, once erroneously created, leads to the emergence of long-term reputational risks, distorts the information field and forms additional information asymmetry.

In this context, the question arises, whether errors can occur in the field of digital information. Recent events regarding the provision of state financial assistance have shown that such mistakes are quite possible. Thus, within the framework of the eSupport program, at the beginning of the full-scale invasion of the Russian Federation into Ukraine, more than 25 thousand Ukrainians received the payment of UAH 6.500 by mistake. Here we mean employees of budget institutions who were not entitled to such assistance from the state. The amount of erroneous assistance amounted to UAH 166 million. As of early August, only UAH 12 million out of this amount was returned to the budget [37].

## CONCLUSIONS

The natural actualization of digital financial services under martial law will further accelerate during the post-war recovery to stimulate economic activity and investment process. This path will significantly simplify the further integration of a digital financial institution into the economic and everyday life of financial services consumers, making them part of the global consumer-financial space based on the open banking concept implemented today, opening up the space for their economic, social, and cultural activity, so that financial services providers could implement their strategies of in-depth financial involvement. Still, as a result, cyber security risks and information asymmetry will increase due to the acute problem of disinformation and the fact that marketing collection and use of information about financial services consumers lacks regulation. Nowadays, when we have no alternatives to the digital path, these problems become an integral part of economic activity. ■

## BIBLIOGRAPHY

1. Мейсон П. Посткапитализм: путеводитель по нашему будущему. / пер. с англ. М., 2016. 416 с.
2. Juniper-Research: Over Half of Global Population to Use Digital Banking in 2026; Driven by Banking Digital Transformation. URL: <https://www.businesswire.com/news/home/20210718005001/en/Juniper-Research-Over-Half-of-Global-Population-to-Use-Digital-Banking-in-2026-Driven-by-Banking-Digital-Transformation>
3. Liu N., Gu X., Lei Ch. K. The equilibrium effects of digital technology on banking, production, and employment. *Finance Research Letters*. 2022. Vol. 49. Art. 103196. DOI: <https://doi.org/10.1016/j.frl.2022.103196>
4. Lee Ch.-Ch., Wang F. How does digital inclusive finance affect carbon intensity? *Economic Analysis and Policy*. 2022. Vol. 75. P. 174–190. DOI: <https://doi.org/10.1016/j.eap.2022.05.010>
5. Koomson I., Martey E., Etwire P. M. Mobile money and entrepreneurship in East Africa: the mediating roles of digital savings and access to digital credit. *Information Technology & People*. 2022. DOI: <https://doi.org/10.1016/j.eap.2022.05.010>
6. Корнівська В. О. Цифровий банкінг: ризики фінансової дигіталізації. *Проблеми економіки*. 2017. № 3. С. 254–261. URL: [https://www.problecon.com/export\\_pdf/problems-of-economy-2017-3\\_0-pages-254\\_261.pdf](https://www.problecon.com/export_pdf/problems-of-economy-2017-3_0-pages-254_261.pdf)
7. Li G., Lv X., Han X. Digital financial inclusion and household debt in China. *Applied Economics Letters*. 2022. DOI: <https://doi.org/10.1080/13504851.2022.2110560>
8. Li J., Wu Y., Xiao J. J. The impact of digital finance on household consumption: Evidence from China. *Economic Modelling*. 2020. Vol. 86. P. 317–326. DOI: <https://doi.org/10.1016/j.econmod.2019.09.027>
9. Корнівська В. Інституційні ризики фінансової інклюзії. *Економічна теорія*. 2020. № 4. С. 45–64. DOI: <https://doi.org/10.15407/etet2020.04.045>
10. Ozili P. K. Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*. 2018. Vol. 18. Iss. 4. P. 329–340. DOI: <https://doi.org/10.1016/j.bir.2017.12.003>
11. Risman A., Mulyana B., Silvatika B., Sulaeman A. The effect of digital finance on financial stability. *Management Science Letters*. 2021. Vol. 11. Iss. 7. P. 1979–1984. DOI: <https://doi.org/10.5267/j.msl.2021.3.012>
12. Yao L., Ma X. Has digital finance widened the income gap? *PLoS ONE*. 2022. Vol. 17. Iss. 2. Art. e0263915. DOI: <https://doi.org/10.1371/journal.pone.0263915>
13. ТОП-5 сервісів для бізнесу, які з'явилися в умовах війни. URL: <https://landlord.ua/news/top-5-servisiv-dlia-biznesu-iaki-z-iyavylis-v-umovakh-viiny/>
14. Обсяги безготівкових розрахунків в Україні зростають попри війну / Національний банк України. 29.07.2022 URL: <https://bank.gov.ua/ua/news/all/obsyagi-bezgotivkovih-rozrahunkiv-v-ukrayini-zrostayut-popri-viynu>
15. Цифрова трансформація: як онлайн-транзакції глобалізують український бізнес / Forbes. 14.12.2021 URL: <https://forbes.ua/money/tsifrova-transformatsiya-yak-onlayn-tranzaktsii-globalizuyut-ukrainskiy-biznes-14122021-2910>
16. Система миттєвих платежів / Національний банк України. URL: <https://bank.gov.ua/ua/payments/ips>
17. Слесарук С. Банківська цифровізація / Financial Club. 02.06.2021. URL: <https://banksrating.com.ua/analytics/bankivska-tsifrovizatsiya/>
18. Фінансова грамотність, фінансова інклюзія та фінансовий добробут в Україні у 2021. Звіт за результатами дослідження. Вересень 2021 р. Київ, 2021. 83 с. URL: [https://bank.gov.ua/admin\\_uploads/article/Research\\_Financial\\_Literacy\\_Inclusion\\_Welfare\\_2021.pdf?v=4](https://bank.gov.ua/admin_uploads/article/Research_Financial_Literacy_Inclusion_Welfare_2021.pdf?v=4)
19. Запроцював Закон України «Про платіжні послуги» / Національний банк України. URL: <https://www.facebook.com/photo/?fbid=423289216508397&set=a.289108383259815>
20. Тигипко А. Open banking – что это и кто выиграет от его введения в Украине / НВ. Бизнес. 22.02.2021. URL: <https://biz.nv.ua/experts/open-banking-cto-eto-kogda-poyavitsya-v-ukraine-i-kto-vyigraet-novosti-ukrainy-50143253.html>
21. Офіційний сайт monobank. URL: <https://www.monobank.ua/>
22. Количество атак с использованием вымогателей увеличилось на 1318% в 2021 году. URL: <https://www.securitylab.ru/news/524479.php>
23. Тарасовский Ю., Шевчук С. ПриватБанк, Ощадбанк, monobank, Альфа-Банк, правительственные сайты и портал «Дія» подверглись кибератаке / Forbes. 15.02.2022. URL: <https://forbes.ua/ru/news/dzherelav-nbu-privatbank-ta-oshchadbank-zaznali-kiberataki-servisi-vzhe-vidnovlyuyut-robotu-15022022-3691>
24. Кібератаки та крадіжка даних клієнтів: чим ризикують банки через шахраїв / Financial Club. 29.01.2020. URL: <https://finclub.net/ua/priama-mova/kiberatayta-kradizhka-danykh-kliientiv-chym-ryzykuiut-bankycherez-shakhraiv.html>
25. Хакеры «положили» ИТ-системы огромного банка, маскируя взлом SWIFT. URL: <https://internetua.com/haker-polojili-it-sistem-ogromnogo-bankamaskiruya-vzlom-swift>
26. Як банкам встояти у випадку кібератаки / Financial Club. 25.10.2019. URL: <https://finclub.net/ua/priama-mova/yak-bankam-vstoiaty-u-vypadku-kiberatay.html>
27. Банки ЄС та США попередили про загрозу кібератак з боку РФ / Financial Club. 09.02.2022. URL: <https://finclub.net/ua/news/banky-yes-ta-ssha-poperedylypro-zahrozu-kiberatak-z-boku-rf.html>
28. Постанова Правління Національного банку України від 12.08.2022 р. № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України». URL: <https://zakon.rada.gov.ua/laws/show/v0178500-22#Text>
29. Постанова Правління Національного банку України від 16.01.2021 р. № 4 «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг». URL: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>

30. Соціальна інженерія. Низка нетехнічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/>
31. Шахраї вкрали 36 млн грн з карток ПриватБанку / Financial Club. 23.08.22. URL: <https://finclub.net/ua/news/shakhrai-vkraly-36-mln-hrn-z-kartok-pryvat-banku.html>
32. Глобальне дослідження з питань шахрайства у банківській сфері / KPMG. 2019. URL: <https://assets.kpmg/content/dam/kpmg/ua/pdf/2020/01/Global-Banking-Fraud-Survey.pdf>
33. Регламент про конфіденційність та електронні комунікації – ePrivacy Regulation / Eur-Lex. COM/2017/010 final – 2017/03 (COD) URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>
34. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань. Київ, 2021. № 9. 267 с. URL: <http://ippi.org.ua/sites/default/files/2021-9.pdf>
35. RegTech и Big Data – будущее банков и регуляторов / Financial Club. 10.11.2021. URL: <https://finclub.net/views/regtech-i-big-data-budushchee-bankov-i-regulyatorov.html>
36. Корнівська В. О. Наднаціональне регулювання фінансового ринку: суперечності інституціоналізації. *Економічна теорія*. 2022. № 1. С. 71–98. DOI: <https://doi.org/10.15407/etet2022.01.071>
37. Капустинська К. Тисячі українців отримали допомогу в 6500 грн помилково: гроші повертають до бюджету / Obozrevatel. 03.08.2022. URL: <https://news.obozrevatel.com/ukr/economics/analytics-and-forecasts/tisyachi-ukrainsiv-otrimali-dopomogu-v-6500-grn-pomilkovo-groshi-povertayut-do-byudzhetu.htm>

## REFERENCES

- “Banky YeS ta SSHa poperedyly pro zahrozu kiberatak z boku RF” [EU and US Banks Have Warned about the Threat of Cyberattacks from the Russian Federation]. *Financial Club*. February 09, 2022. <https://finclub.net/ua/news/banky-yes-ta-ssha-poperedyly-pro-zahrozu-kiberatak-z-boku-rf.html>
- “Finansova hramotnist, finansova inkluziia ta finansovyi dobrobut v Ukraini u 2021. Zvit za rezultatamy doslidzhennia. Veresen 2021 r.” [Financial Literacy, Financial Inclusion and Financial Well-being in Ukraine in 2021. Research Report. September 2021]. Kyiv, 2021. [https://bank.gov.ua/admin\\_uploads/article/Research\\_Financial\\_Literacy\\_Inclusion\\_Welfare\\_2021.pdf?v=4](https://bank.gov.ua/admin_uploads/article/Research_Financial_Literacy_Inclusion_Welfare_2021.pdf?v=4)
- “Hlobalne doslidzhennia z pytan shakhraistva u bankivskii sferi” [Global Banking Fraud Survey]. *KPMG*. 2019. <https://assets.kpmg/content/dam/kpmg/ua/pdf/2020/01/Global-Banking-Fraud-Survey.pdf>
- “Juniper-Research: Over Half of Global Population to Use Digital Banking in 2026; Driven by Banking Digital Transformation”. <https://www.businesswire.com/news/home/20210718005001/en/Juniper-Research-Over-Half-of-Global-Population-to-Use-Digital-Banking-in-2026-Driven-by-Banking-Digital-Transformation>

- “Khakery «polozhili» IT-sistemy ogromnogo banka, maskiruya vzlom SWIFT” [Hackers “Destroyed” the IT Systems of a Huge Bank, Masking the SWIFT Hack]. <https://internetua.com/haker-polozhili-it-sistem-ogromnogo-banka-maskiruya-vzлом-swift>
- “Kiberatomy ta kradizhka danykh kliientiv: chym ryzykuiut banky cherez shakhraiv” [Cyberattacks and Theft of Customer Data: What Banks Risk Due to Fraudsters]. *Financial Club*. January 29, 2020. <https://finclub.net/ua/priama-mova/kiberatomy-ta-kradizhka-danykh-kliientiv-chym-ryzykuiut-banky-cherez-shakhraiv.html>
- “Kiberbezpeka v informatsiinomomu suspilstvi : Informat-siino-analitychnyi daidzhest” [Cybersecurity in the Information Society: Informational and Analytical Digest]. Kyiv, 2021. <http://ippi.org.ua/sites/default/files/2021-9.pdf>
- “Kolichestvo atak s ispolzovaniem vymogateley uvelichilos na 1318% v 2021 godu” [Ransomware Attacks Increased by 1318% in 2021]. <https://www.securitylab.ru/news/524479.php>
- Kapustynska, K. “Tysiachi ukrainsiv otrymaly dopomogu v 6500 hrn pomylkovo: hroshi povertaiut do biudzhetu” [Thousands of Ukrainians Received Assistance in the Amount of UAH 6,500 by Mistake: The Money is Returned to the Budget]. *Obozrevatel*. August 03, 2022. <https://news.obozrevatel.com/ukr/economics/analytics-and-forecasts/tisyachi-ukrainsiv-otrimali-dopomogu-v-6500-grn-pomilkovo-groshi-povertayut-do-byudzhetu.htm>
- Koomson, I., Martey, E., and Etwire, P. M. “Mobile money and entrepreneurship in East Africa: the mediating roles of digital savings and access to digital credit”. *Information Technology & People* (2022). DOI: <https://doi.org/10.1016/j.eap.2022.05.010>
- Kornivska, V. “Instytutsiini ryzyky finansovoi inkluziui” [Institutional Risks of Financial Inclusion]. *Ekonomichna teoriia*, no. 4 (2020): 45–64. DOI: <https://doi.org/10.15407/etet2020.04.045>
- Kornivska, V. O. “Nadnatsionalne rehuliuвання finansovoho rynku: superechnosti instytutsionalizatsii” [Supernational Financial Market Regulation: Contradictions of Institutionalization]. *Ekonomichna teoriia*, no. 1 (2022): 71–98. DOI: <https://doi.org/10.15407/etet2022.01.071>
- Kornivska, V. O. “Tsyfrovyyi bankinh: ryzyky finansovoi dyhitalizatsii” [Digital Banking: Risks of Financial Digitalization]. *Problemy ekonomiky*, no. 3 (2017): 254–261. [https://www.problecon.com/export\\_pdf/problems-of-economy-2017-3\\_0-pages-254\\_261.pdf](https://www.problecon.com/export_pdf/problems-of-economy-2017-3_0-pages-254_261.pdf)
- [Legal Act of Ukraine] (2021). <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>
- [Legal Act of Ukraine] (2022). <https://zakon.rada.gov.ua/laws/show/v0178500-22#Text>
- Lee, Ch.-Ch., and Wang, F. “How does digital inclusive finance affect carbon intensity?” *Economic Analysis and Policy*, vol. 75 (2022): 174–190. DOI: <https://doi.org/10.1016/j.eap.2022.05.010>
- Li, G. et al. “Digital financial inclusion and household debt in China”. *Applied Economics Letters* (2022). DOI: <https://doi.org/10.1080/13504851.2022.2110560>
- Li, J., Wu, Y., and Xiao, J. J. “The impact of digital finance on household consumption: Evidence from China”. *Economic Modelling*, vol. 86 (2020): 317–326. DOI: <https://doi.org/10.1016/j.econmod.2019.09.027>

- Liu, N., Gu, X., and Lei, Ch. K. "The equilibrium effects of digital technology on banking, production, and employment". *Finance Research Letters*, art. 103196, vol. 49 (2022).  
DOI: <https://doi.org/10.1016/j.frl.2022.103196>
- Meyson, P. *Postkapitalizm: putevoditel po nashemu budushchemu* [PostCapitalism: A Guide to Our Future]. Moscow, 2016.
- "Obsiah bezhotivkovykh rozrakhunkiv v Ukraini zrostaiut popry viinu" [The Volume of Non-cash Payments in Ukraine Is Growing Despite the War]. *Natsionalnyi bank Ukrainy*. July 29, 2022. <https://bank.gov.ua/ua/news/all/obsyagi-bezgotivkovykh-rozrahunkiv-v-ukrayini-zrostayut-popri-viynu>
- Oftsiniyi sait monobank. <https://www.monobank.ua/>
- Ozili, P. K. "Impact of digital finance on financial inclusion and stability". *Borsa Istanbul Review*, vol. 18, no. 4 (2018): 329-340.  
DOI: <https://doi.org/10.1016/j.bir.2017.12.003>
- "RegTech i Big Data - budushcheye bankov i regulatorov" [RegTech and Big Data – the Future of Banks and Regulators]. *Financial Club*. November 10, 2021. <https://finclub.net/views/regtech-i-big-data-budushchee-bankov-i-regulatorov.html>
- "Rehlament pro konfidentsiinst ta elektronni komunikatsii – ePrivacy Regulation" [Regulation on Confidentiality and Electronic Communications – ePrivacy Regulation]. *Eur-Lex*. COM/2017/010 final – 2017/03 (COD). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>
- Risman, A. et al. "The effect of digital finance on financial stability". *Management Science Letters*, vol. 11, no. 7 (2021): 1979-1984.  
DOI: [10.5267/j.msl.2021.3.012](https://doi.org/10.5267/j.msl.2021.3.012)
- "Shakhray vkraly 36 mln hrn z kartok PryvatBanku" [Fraudsters Stole UAH 36 Million from PrivatBank Cards]. *Financial Club*. 23.08.22. <https://finclub.net/ua/news/shakhray-vkraly-36-mln-hrn-z-kartok-pryvatbanku.html>
- "Sotsialna inzheneriia. Nyzka ne tekhnichnykh pryimov manipuliuvannia korystuvachamy, yaki vykorystovuiutsia kiberzlochynsiamy pid chas atak" [Social Engineering. A Number of Non-technical User Manipulation Techniques Used by Cybercriminals during Attacks]. <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/>
- "Systema myttievkykh platezhiv" [System of Instant Payments]. *Natsionalnyi bank Ukrainy*. <https://bank.gov.ua/ua/payments/ips>
- Slesaruk, S. "Bankivska tsyfrovizatsiia" [Banking Digitalization]. *Financial Club*. June 02, 2021. <https://banksrating.com.ua/analytics/bankivska-tsifrovizatsiya/>
- "TOP-5 servisiv dlia biznesu, yaki z'явились в умовках війни" [TOP-5 Services for Business That Appeared during the War]. <https://landlord.ua/news/top-5-servisiv-dlia-biznesu-iaki-z-iavylis-v-umovakh-viiny/>
- "Tsyfrova transformatsiia: yak onlain-tranzaktsii hlobalizuiut ukraïnskyi biznes" [Digital Transformation: How Online Transactions are Globalizing Ukrainian Business]. *Forbes*. December 14, 2021. <https://forbes.ua/money/tsifrova-transformatsiya-yak-onlayn-tranzaktsii-globalizuyut-ukraïnskyi-biznes-14122021-2910>
- Tarasovskiy, Yu., and Shevchuk, S. "PrivatBank, Oshchadbank, monobank, Alfa-Bank, pravitelstvennyye sayty i portal «Diya» podverglis kiberatake" [PrivatBank, Oshchadbank, Monobank, Alfa-Bank, Government Websites and the Diya Portal Were Subjected to a Cyberattack]. *Forbes*. February 15, 2022. <https://forbes.ua/ru/news/dzherela-v-nbu-privatbank-ta-oshchadbank-zaznali-kiberataki-servisi-vzhe-vidnovlyuyut-robotu-15022022-3691>
- Tigipko, A. "Open banking - chto eto i kto vyigraet ot yego vvedeniya v Ukrainu" [Open Banking – What Is It and Who Will Benefit from Its Introduction in Ukraine]. *NV. Biznes*. February 22, 2021. <https://biz.nv.ua/experts/open-banking-chto-eto-kogda-poyavitsya-v-ukraine-i-kto-vyigraet-novosti-ukrainy-50143253.html>
- "Yak bankam vstoiaty u vypadku kiberataky" [How Banks Can Withstand a Cyber Attack]. *Financial Club*. October 25, 2019. <https://finclub.net/ua/priama-mova/yak-bankam-vstoiaty-u-vypadku-kiberataky.html>
- Yao, L., and Ma, X. "Has digital finance widened the income gap?" *PLoS ONE*, art. e0263915, vol. 17, no. 2 (2022).  
DOI: <https://doi.org/10.1371/journal.pone.0263915>
- "Zapratsiuvav Zakon Ukrainy «Pro platizhni posluhy»" [The Law of Ukraine "On Payment Services" Came into Force]. *Natsionalnyi bank Ukrainy*. <https://www.facebook.com/photo/?fbid=423289216508397&set=a.289108383259815>