

Viktoriia Kostiuk, Olha Faichuk, Oleksii Muravskiyi

MECHANISM FOR THE IMPLEMENTATION
OF REMOTE BANKING SERVICES
IN THE CONTEXT OF MODERN
CHALLENGES AND THREATS

Viktoriia Kostiuk, Olha Faichuk, Oleksii Muravskiy

**MECHANISM FOR THE IMPLEMENTATION OF REMOTE
BANKING SERVICES IN THE CONTEXT OF MODERN
CHALLENGES AND THREATS**

Monograph

**Tallinn
Teadmus
2024**

UDC 336.717-024.87

Reviewers:

- Zakharchuk O.V.* - Doctor of Economics, Professor, Head of the department of investments and material and technical support (Institute of Agrarian Economics of the National Academy of Agrarian Sciences of Ukraine)
- Shvets N.R.* - Doctor of economics, Professor, Acting Head of the Department of Finance (National University of Life and Environmental Sciences of Ukraine)
- Klymenko L.V.* - Head of the Department of English Philology (National University of Life and Environmental Sciences of Ukraine)

Kostiuk Viktoriia, Faichuk Olha, Muravskiy Oleksii. Mechanism for the Implementation of Remote Banking Services in the Context of Modern Challenges and Threats: monograph. Tallinn: Teadmus OÜ, 2024, 168 p.

ISBN 978-9916-752-10-4

The monograph emphasizes the importance of digital advancement in the banking sector, focusing on the digitalization of remote banking services. It analyzes the effects of remote banking on banks' positions, economic support, and its main operational aspects in Ukraine. Key cybersecurity issues are addressed, such as workforce shortages, employee awareness gaps, budget constraints, account vulnerabilities, and deficiencies in mobile applications. Challenges faced by Ukrainian banks and specific transformations in remote banking mechanisms are discussed. The study highlights the need for practical training, case studies, and cyberattack simulations for staff and clients, along with the application of AI and machine learning in predictive modeling, unstructured data processing, fraud detection, and customer behavior analysis. Proposals for enhancing the digital environment through cyber insurance and a bank-as-agent insurance model are also presented.

For scientists, teachers, doctoral and post-graduate students, students of higher education institutions, specialists and civil servants who work in the field of formation and implementation of the policy of providing the population with high-quality and safe food products.

ISBN 978-9916-752-10-4 © Kostiuk V., Faichuk O., Muravskiy O. 2024



CONTENT

<i>Introduction</i>	5
<i>Chapter I.</i> THEORETICAL FOUNDATIONS OF ORGANIZING REMOTE BANKING SERVICES IN THE CONTEXT OF MODERN CHALLENGES AND THREATS.....	9
1.1. 1.1. The Essence and Types of Remote Banking Services.....	9
1.2. 1.2. Features of Remote Banking Services under Martial Law.....	22
1.3. 1.3. The Mechanism of Providing Remote Banking Services in the Context of Current Challenges and Threats.....	33
<i>Chapter II.</i> FEATURES OF THE REMOTE BANKING SERVICE MECHANISM IN JSC "OTP BANK".....	47
2.1. Modern Trends in Remote Banking Services under Martial Law	47
2.2. Characteristics of Services Within the Framework of Remote Banking Services for Clients at JSC "OTP Bank" and the OTP Bank System.....	60

2.3. The Mechanism of Remote Client Services at JSC "OTP Bank" and Its Effectiveness.....	71
Chapter III. MAIN DIRECTIONS FOR IMPROVING THE MECHANISM OF REMOTE BANKING SERVICES FOR CLIENTS OF UKRAINE IN JSC "OTP BANK" IN THE CONTEXT OF MODERN CHALLENGES AND THREATS.....	88
3.1. Directions for Countering Modern Threats in Remote Banking Service Systems	88
3.2. Prospects for the Development of Digital Banking as a Stage in the Development of the Bank's Remote Service Mechanism in the Context of Current Challenges.....	94
3.3. Improving the Mechanism of Remote Banking Services in JSC "OTP Bank"	104
<i>Conclusions and recommendations</i>	113
<i>References</i>	118
<i>Appendices</i>	128



INTRODUCTION

Modern intensive macroeconomic changes in the global economy have significantly impacted the world banking system. The active digitization of the economy amid challenges and threats has transformed the banking system, advancing the mechanisms of remote banking services. The development of the remote banking service sector is driven by several factors.

Firstly, providing such services allows the creation of an entirely new level of service for bank clients. Secondly, high-quality remote services are increasingly seen as a competitive advantage for banks. Thirdly, the rapid growth of the banking sector requires the establishment of accessible and effective mechanisms for banks to interact with their clients.

For clients, this approach means maximum convenience in service and a reduction in time and financial costs at all stages of interaction with the bank, from obtaining information about services and banking products to filling out forms. For banks, the use of remote services enhances operational efficiency, creates a

quality banking product, reduces costs, and increases the client base without compromising the quality of customer service.

Remote banking services, also known as online or digital banking, are becoming increasingly important due to the rapid development of technologies and changing consumer preferences. In the face of modern challenges and threats, the shift to remote banking has created opportunities (convenience, accessibility, cost-effectiveness, and enhanced security measures), positively affecting the retention and economic development of not only the banking sector but also the economy as a whole.

However, it is important to recognize that war conditions and new threats can pose challenges to remote banking systems. During conflicts or heightened security risks, financial institutions must ensure the resilience and continuity of their digital infrastructure. This involves implementing robust cybersecurity measures to protect against potential attacks, fraud, and unauthorized access to confidential financial data. Moreover, geopolitical tensions and conflicts can disrupt international financial networks and cross-border transactions, potentially affecting the seamless operation of remote banking services. Banks must closely monitor geopolitical developments, prepare contingency scenarios, and collaborate with regulatory authorities to ensure uninterrupted service delivery even in adverse conditions. Despite improved access, convenience, and

economic efficiency, banks must remain vigilant to risks associated with war, new threats, and potential disruptions to ensure the integrity and security of remote banking service mechanisms.

The monograph defines the essence and types of remote banking services. It summarizes the features of remote banking in wartime conditions and highlights the mechanisms for providing such services amid current challenges and threats. It explores modern trends in remote banking under martial law, diagnoses services within the framework of remote client services at JSC "OTP Bank" and the OTP Bank system, and analyzes the mechanism of remote client service and its effectiveness. The study outlines countermeasures against modern threats to remote banking systems, identifies the prospects for the development of digital banking as a stage in the evolution of the bank's remote service mechanism amid current challenges, and proposes ways to improve the mechanism of remote banking services at JSC "OTP Bank."

The monograph explores the organization and improvement of remote banking services, particularly in the context of modern challenges and threats, with a focus on JSC "OTP Bank" in Ukraine. The introduction lays the groundwork for understanding the theoretical aspects of remote banking. Chapter 1 examines the essence and types of remote services, emphasizing the unique conditions and challenges under martial

law. It also details the mechanisms banks use to deliver these services securely and efficiently. Chapter 2 presents a case study of JSC "OTP Bank," discussing current trends in remote banking under martial law, the specifics of services offered, and an evaluation of the effectiveness of their service mechanisms. The final chapter identifies key areas for enhancing the bank's remote service mechanisms to address current threats. It also highlights the role of digital banking as an essential development stage for remote services in challenging environments. The monograph concludes by offering recommendations for strengthening remote service mechanisms to ensure continuity and resilience in Ukraine's banking sector.

The object of the research is the process of remote client service at JSC "OTP Bank." The subject of the research is the theoretical and practical aspects of the remote banking service mechanism.

This scientific work offers an innovative approach to customer service quality, data security improvement under martial law, strategy development for protection against financial threats to the bank, and adaptation to modern technological trends to ensure competitiveness in the digital sphere.

CHAPTER I

THEORETICAL FOUNDATIONS OF ORGANIZING REMOTE BANKING SERVICES IN THE CONTEXT OF MODERN CHALLENGES AND THREATS

1.1. The Essence and Types of Remote Banking Services

Remote banking services are one of the key directions in the development of both global and national banking systems. This trend is driven by the high demand for fast and flexible financial operations among bank service users. The Internet is gradually becoming a universal, accessible, and convenient means of communication, enabling a wide range of tasks across various fields. Through remote services based on internet banking, banks are able to attract additional funds and deliver wholesale and retail services to clients efficiently.

The strategic goal of remote services via internet banking is to provide individuals and legal entities the right and opportunity to access financial services from their place of residence or professional activity. This form of service is

progressive for all societal categories and specialists from various fields who may not have the ability to use bank services within a personal sales system.

Commercial banks are actively studying the latest developments in the field of remote services, adopting the best ideas and refining them. As a result, clients are provided with services distinguished by their speed of execution and high-quality functionality. Banks offer their clients a wide range of electronic services, utilizing modern automated systems, information technologies, telecommunications, and more. The Remote Banking System (abbreviated as RBS) is widely used by most commercial banks globally and is essential in the highly competitive market for banking services. Essentially, RBS is a set of services provided to clients not in the bank branch through direct contact with a bank specialist, but via remote access.

The term "remote banking services" (RBS) is legally defined through the concept of a "remote payment operation" in Article 1 of the Law of Ukraine "On Payment Services," which is described as a payment operation using remote communication means [2]. An analysis of various scientific sources shows that scholars and researchers interpret the concept of RBS in a largely similar way. Let us consider these interpretations in more detail.

The authors of the textbook "Information Systems and Technologies in Banks" define RBS as a technology through which banking operations are carried out without visiting a

banking institution. Everything that does not require a direct visit to the bank is performed remotely [25, p. 27]. According to researchers O. Dzyubliuk and L. Pryidun, the definition of RBS is a general term that outlines the technology of providing banking services based on instructions or orders that clients send remotely (i.e., without visiting a banking institution), necessarily using computer technologies and telephony [13, p. 164].

O. Kuchasny and V. Mazurak note that RBS is an interconnected set of information and internet technologies used to provide banking services to clients without their personal visit to bank branches, based on a self-service mechanism [23, p. 116]. O.V. Dzyubliuk states that RBS is a complex of informational services related to customer accounts and certain types of operations based on remote client orders [13].

O.A. Kyrychenko and V.I. Mishchenko describe RBS as a technology for performing operations on a client's bank accounts based on their remote orders, where the remote order is a request for the bank to carry out the corresponding operation as instructed by the client, using agreed access channels and a specific transmission mechanism for the orders [12, p. 747].

At the same time, researchers highlight the unique feature of RBS as a multifunctional package of hardware and software that allows clients to perform remote banking operations (such as managing accounts online, conducting settlement and payment operations, and accessing necessary financial information

without visiting banking institutions) [31]. N. Radionova equates the concept of RBS with "home banking" and "remote banking," noting that these terms refer to the provision of banking services that enable clients to access necessary services without visiting a bank office [35].

The most used basic definition of remote banking is the provision of opportunities for bank clients to gain remote access to their accounts through information systems, meaning that remote banking service rightly refers to the provision of banking services at the client's request without direct interaction with bank employees [35, p. 207].

Thus, all the definitions of remote banking services (RBS) mentioned above converge on one key point: banks provide remote or distance-based customer service, which is enabled through information and telecommunication technologies. In other words, remote banking services are a type of banking service offered by financial institutions in a remote format, or they represent the processes through which a bank creates its product and subsequently delivers it to the customer via remote access. In the RBS process, the client may interact with a bank employee, but such interaction does not occur through direct (physical) contact. Instead, it is facilitated through information technologies and telecommunications.

Therefore, the primary characteristic that distinguishes remote banking services from other commercial banking services

is that operations are conducted remotely, without the need for physical presence.

The core principle of remote banking services (RBS) is the exchange of various types of information between the client and the bank over a distance. In this process, the bank ensures a proper level of security and confidentiality for such interactions, as clients can now not only receive information about their accounts but also manage them and perform various transactions remotely. Clients have access to a wide range of capabilities, such as remote account access, payments and transfers, opening deposits, and a wealth of informational resources (exchange rates, locations of nearby ATMs, a list of branch offices, etc.).

To access RBS, the client only needs a communication channel (telephone or Internet), a technical device (computer, smartphone, tablet, etc.), and specialized software provided by the bank. Due to this, RBS is sometimes referred to as electronic or internet banking.

Trends in the development of the banking business indicate that for commercial banks and the banking system, the decisive factor is the active transition to remote banking services (RBS) as the primary form of client service. Today, the modernization of banking services primarily involves the active implementation and development of RBS, along with corresponding offerings of products and services, forms, and methods of service. This

approach allows banks to attract new clients, expand their capabilities, and strengthen their competitive positions in the market.

At the same time, innovations positively impact the bank's image, leading to an improvement in the quality of its client base. However, the cost of servicing a client in the bank is significantly higher compared to remote servicing, with some analysts estimating the ratio as 1:100. Remote banking services (RBS) provide clients with maximum convenience in using banking services, while for the bank, they ensure minimal time and financial costs at all stages of client interaction. Appendix A presents a list of advantages and disadvantages (risks) of using RBS for banks and their clients.

The analysis of literary sources showed that in practice, several main classification features are commonly used to categorize RBS: by service subjects, by system operation principles, and by the type of information systems and technologies used.

From the perspective of the service subject, RBS can be classified as electronic banking for corporate clients and electronic banking for individuals . Depending on the system operation principle, RBS can be divided into online systems (operating in real-time) and offline systems (where there is a time gap between receiving a client's request and its execution) . The most widespread approach classifies RBS technologies based on

the types of IS (software and hardware) used for banking operations (channels of access to banking services): PC banking, internet banking, mobile banking, SMS banking, video banking, telephone banking, ATMs, and online service platforms (Appendix B). Services provided to clients within RBS are typically divided into three groups (Appendix B, Table B.1): informational, operational, and auxiliary. Modern forms of RBS include CRM, payment cards, internet banking, electronic digital signatures, and personal client service managers, among others.

A strong trend toward shifting most banking processes to remote service is evident in developed countries, and the quality and practicality of RBS in Ukraine far exceed those abroad. Currently, most commercial banks, including state-owned banks like Oschadbank, PrivatBank, OTP Bank, Ukrsibbank, and others, offer RBS to their clients. The quantity and quality of these services vary from bank to bank, but they have significantly improved, helping the banking sector navigate through critical economic phases during the pandemic, the post-pandemic recession, and the full-scale military invasion and martial law. It is also important to mention the rise of online banks, which have no physical branches and operate exclusively online, providing only RBS. Examples include Monobank, Vlasny Rakhunok Bank, Izibank, Neobank, O.Bank, and others.

Thus, remote banking services systems represent a major area of banks' work with clients, allowing them to use banking

services remotely without visiting a bank branch. This method of service delivery enables banks to save resources, while clients save time and effort, receiving banking services in any convenient location. Among the many available methods of conducting banking operations, clients usually opt for traditional banking, online banking, ATM banking, and mobile banking. Each of these existing methods has its advantages and limitations, affecting clients' experience, trust, satisfaction, and willingness to continue using such services.

The economic essence of remote banking services (RBS) lies in their capacity to streamline financial operations, reduce overhead costs, and enhance access to banking services, ultimately driving significant transformations in the banking industry. These services have redefined traditional banking by enabling transactions and other financial activities to be conducted through digital platforms, thereby reducing the dependency on physical bank branches and associated expenses. RBS offers financial institutions the opportunity to operate with leaner structures, making them more cost-effective and competitive.

1. Cost Efficiency and Operational Effectiveness. The adoption of RBS has substantially reduced the cost of service provision for banks. Traditional banking services are often labor-intensive and require significant expenditure on physical infrastructure, including branch maintenance, staffing, utilities,

and security. By shifting to remote services, banks can lower these expenses by operating with fewer branches and streamlined processes. For clients, RBS allows for seamless access to services without incurring travel costs, thus saving time and effort. Economists view these savings as a considerable economic advantage for banks and clients alike, which can also translate into lower fees for banking services.

Furthermore, RBS offers scalability; it allows banks to manage a larger customer base without proportionate increases in operating costs. This capability is particularly beneficial for banks seeking to expand into rural or underserved areas where establishing branches may not be economically feasible. Through RBS, banks can serve clients in geographically dispersed areas, promoting greater financial inclusion and fostering economic growth by providing essential financial services to previously underserved populations.

2. Technological Innovation and Competitive Advantage. Remote banking relies heavily on advanced technological frameworks, including internet banking, mobile banking, and automated systems. These technologies enhance customer experiences by providing easy, around-the-clock access to banking services and reduce waiting times associated with in-person visits. The efficient processing of transactions and data-driven insights enabled by RBS provides banks with a competitive edge in a highly saturated market.

The competitive advantage gained through RBS is closely linked to the innovative use of technology. Artificial intelligence (AI) and machine learning, for instance, have become integral in RBS applications, allowing banks to develop predictive models, analyze customer behavior, and detect fraud. Additionally, digital wallets and contactless payments are part of RBS systems that have transformed payment practices globally. By providing customers with innovative solutions, banks not only enhance satisfaction and loyalty but also increase the adoption of digital services, which contributes to the overall profitability and competitive positioning of banks in the financial industry.

3. Risk Management and Security Investments. Remote banking services, while advantageous, also present unique risks, particularly in terms of cybersecurity. Protecting sensitive customer information and ensuring secure transactions are essential components of RBS. As a result, banks have increased investments in cybersecurity technologies and infrastructure to manage these risks effectively. For instance, multi-factor authentication, biometric verification, and data encryption are commonly used in RBS to ensure secure access and transaction processing.

The economic significance of these security investments cannot be overlooked. Banks that prioritize cybersecurity in their RBS platforms not only protect their clients but also build trust and credibility, which are essential in retaining a loyal customer

base. Additionally, regulatory compliance costs associated with data protection and privacy laws (such as GDPR) are factored into RBS operations. Banks that efficiently balance these security investments with operational costs can improve overall cost-effectiveness, contributing to both economic stability and long-term growth.

4. Economic Impact on Customer Accessibility and Financial Inclusion. RBS has also contributed significantly to the democratization of financial services. Remote access enables customers from all backgrounds and locations, including rural and underbanked regions, to engage in banking activities that would otherwise be inaccessible. By providing services such as mobile banking and online transactions, banks help bridge the financial inclusion gap, empowering more individuals to participate in the formal economy. Access to financial services promotes savings, enables credit access, and supports investment in local businesses, which, in turn, fosters economic development.

Moreover, RBS enhances accessibility by simplifying processes. Customers can complete essential banking tasks, such as transferring funds or checking balances, through digital platforms without needing to visit a bank branch. This convenience is crucial in today's fast-paced world, where consumers prioritize speed and accessibility. In economic terms, improved accessibility translates into increased transaction

volume and customer engagement, both of which drive revenue growth for banks.

5. Remote Banking as an Economic Growth Catalyst. The economic essence of RBS also includes its role in fostering broader economic growth. Remote banking services facilitate cashless transactions, which support the digital economy by increasing transaction efficiency and reducing dependency on cash. This shift is particularly advantageous in economies where cash remains dominant, as digital transactions promote greater transparency and reduce risks associated with cash handling.

In addition, the adoption of Remote Banking Services has spurred innovation and competition among financial institutions, encouraging them to develop more efficient and customer-centric solutions. As banks adopt advanced Remote Banking Services technologies, they contribute to the overall digital infrastructure of the economy. This interconnectedness accelerates the adoption of digital financial systems and supports the growth of fintech sectors, which are essential components of modern economies.

6. Remote Banking as a Key Response to Economic Shocks (RBS) has proven to be resilient during economic crises, including the COVID-19 pandemic and periods of political instability, such as martial law.

During such times, Remote Banking Services has enabled banks to maintain operations and serve clients despite limited

physical branch access. This adaptability demonstrates the economic resilience that RBS offers, as clients can continue to access essential financial services regardless of external disruptions.

Additionally, RBS allows banks to operate with agility, adapting to shifting economic conditions more efficiently than traditional banking models. As seen during economic shocks, RBS platforms have enabled banks to meet client demands for contactless and online services, supporting customer trust and continuity in the banking relationship.

The economic essence of remote banking services is multifaceted, encompassing cost savings, operational efficiency, technological innovation, enhanced financial inclusion, and economic resilience.

Remote Banking Services not only drives down costs for banks but also enhances customer convenience and accessibility, supporting the democratization of financial services and contributing to the growth of the digital economy. Its role in managing security and operational risks further reinforces its value to the banking industry.

As Remote Banking Services continues to evolve, it is likely to remain a crucial component of modern banking, offering economic benefits that extend beyond individual banks to the broader economy.

1.2. Features of Remote Banking Services under Martial Law

Martial law conditions significantly affect the country's economy and financial system. The need to ensure the normal functioning of financial services, particularly banking, under war conditions becomes extremely important. One of the key tools for ensuring the stability of the financial sector during military conflicts is the introduction and development of remote banking services.

To date, the war in Ukraine has led to the destruction of almost every industry in the country's economy and changed the existing ways of doing business for enterprises. The banking industry is no exception to this change. Banks are transforming digitally, moving to new business models and implementing fully digital banking services to keep up with digital banking trends. Thus, the full-scale aggression of the Russian Federation, a terrorist country, against the people of Ukraine on February 24, 2022, created a significant negative impact, primarily on the expectations of economic agents, and in general on the effectiveness of the functioning mechanism of the national economy, which undoubtedly negatively affected the Ukrainian banking system, the country's economy, and financial flows (narrowing of markets, suspension of some types of activities, unprofitability of enterprises, withdrawal of foreign investors

from the markets and growth of risks related to financial uncertainty, etc.). Taking into account the peculiarities of the functioning of the economy in the conditions of martial law and the threat of war, RBS became important and contributed to the maintenance of the country's economy at a functional level.

A significant feature of Remote Banking Services in the conditions of martial law was the formation of a significant amount of advantages, such as accessibility (accessibility at any time, from any place), convenience (27/7), promptness (immediateness of operations), multifunctionality (from review, control to the transfer/receipt of funds), cost-effectiveness (low cost compared to traditional service), fast recoverability and cyber protection (Fig. 1.1).

The rapid adaptation of banking institutions to new challenges and threats of the state of war was ensured precisely by the individual outline of the first-day reaction to the initial stage of military operations, which further determined their adaptation strategies of pre-war realities. Here, it became important to reassess strategies for the development of banking services, cyber protection, speed, expediency and flexibility in decision-making.

Guarantees of the continuity of business processes, which are associated with the satisfaction of customer needs and the effectiveness of managerial cooperation with the personnel potential of banks, have become important.

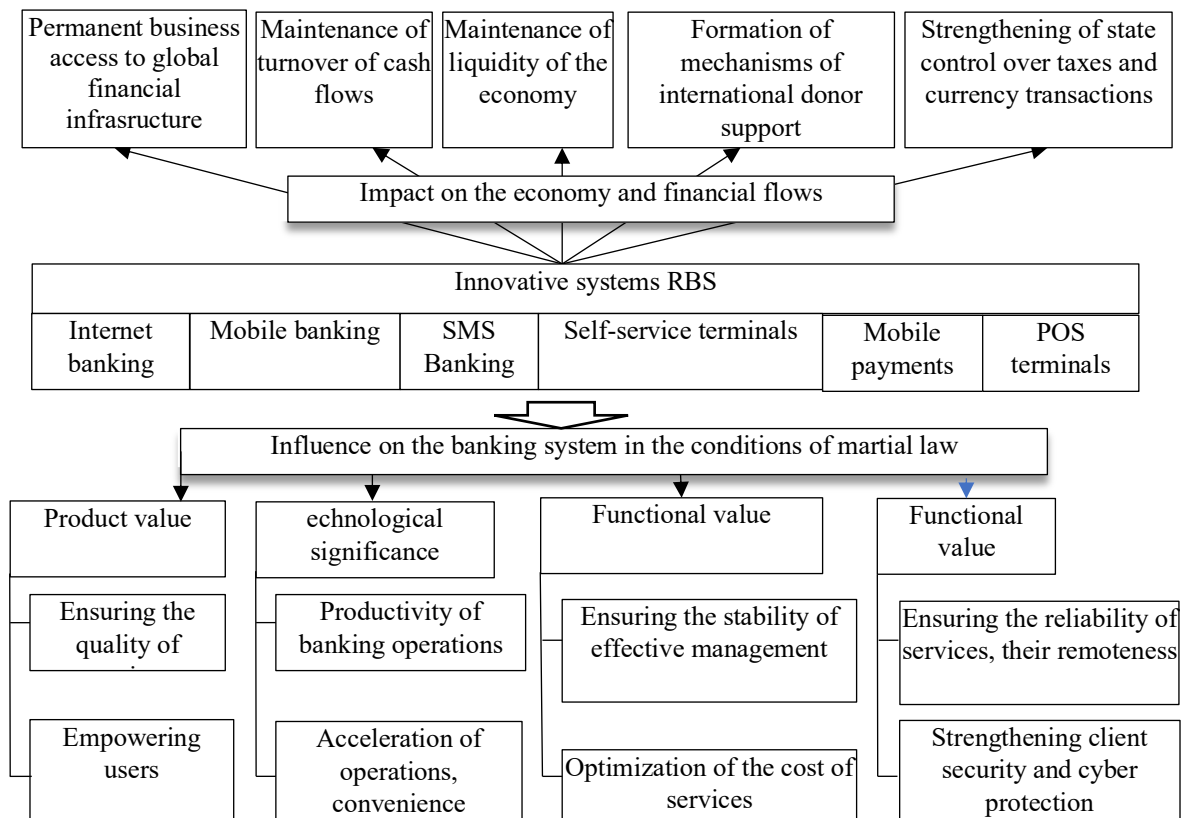


Fig. 1.1. The influence of RBS in the conditions of martial law on the banking system and economy of Ukraine

Source: built by the author based on [30; 35]

Discovering and improving innovative banking systems such as mobile apps, online banking, electronic payment systems and cryptocurrencies can help ensure uninterrupted access to financial services even under martial law restrictions.

The directions of influence of RBS on the efficiency of banks and the banking system in the conditions of the military situation in the country are:

- Product value: Remote banking allows customers to conduct financial transactions in real time, which is an important advantage in the context of military conflicts, when physical

access to banks can be limited, while the quality of service is not lost.

- Technological significance: The introduction of innovative technologies allows banks to adapt to changing conditions faster and more efficiently, ensuring reliable operation and protection of client information, increasing bank productivity and improving the quality of receiving services [38, p. 73].

- Functional significance: mechanisms for constant access to banking services are being established, their cost is being optimized (reduction of stationary employees and better service from staff who remotely provide support for services, involvement of robots in the system (chat-bot – providing answers to clients based on text messages with using artificial intelligence (AI) or programmed robot logic (BOT) to understand customer messages).

- Social importance: Online services allow banks to provide customers with the necessary financial services without the need to physically visit bank branches. Remote banking helps ensure the safety and health of citizens, allowing to avoid population clashes during military operations [37].

The expansion of the RBS functionality during the war made it possible to stabilize not only the functionality of the service for large businesses, but also for medium and small businesses and for the population. Many researchers of the banking sector in the

conditions of the war discovered certain features of the formation of remote banking services. Thus, O.E. Tkachenko draws attention to strengthening the role of RBS in digitalization of business processes and effective implementation of the latest technologies in the service system. Comprehensive adaptation of the banking system and support of the regulator bank were activated by the RBS in the field of lending both by banks and based on state programs [24, c. 77].

During the war, stabilization procedures, the almost complete absence of restrictions on non-cash services (except currency transactions), support of banking institutions, and applicable short-term methods of stabilizing the situation were the key decisions of the NBU's financial management (Fig. 1.2). Focusing on customer needs based on reducing operating time became important in the conditions of martial law [29, p. 1172].

The means of RBS have created the immediacy of performing such operations as making monthly payments on credit debt, paying for goods, money transfers, paying utilities, making deposits, etc. Effective implementation of electronic documents, electronic signatures, permission to transfer server infrastructure to external jurisdictions (into cloud storage) created opportunities for quick and efficient access of clients to almost any type of banking service.

The conditions of martial law determined the accentuation of attention on preventing panic and considering the needs and

requests of clients based on the RBS mechanism. As a result, decisions were made regarding the interests of the bank's clients, their protection, and the leveling of the bank's risks [46, p. 197]. Conditions have been created for the functioning of neobanks and non-traditional competitors.

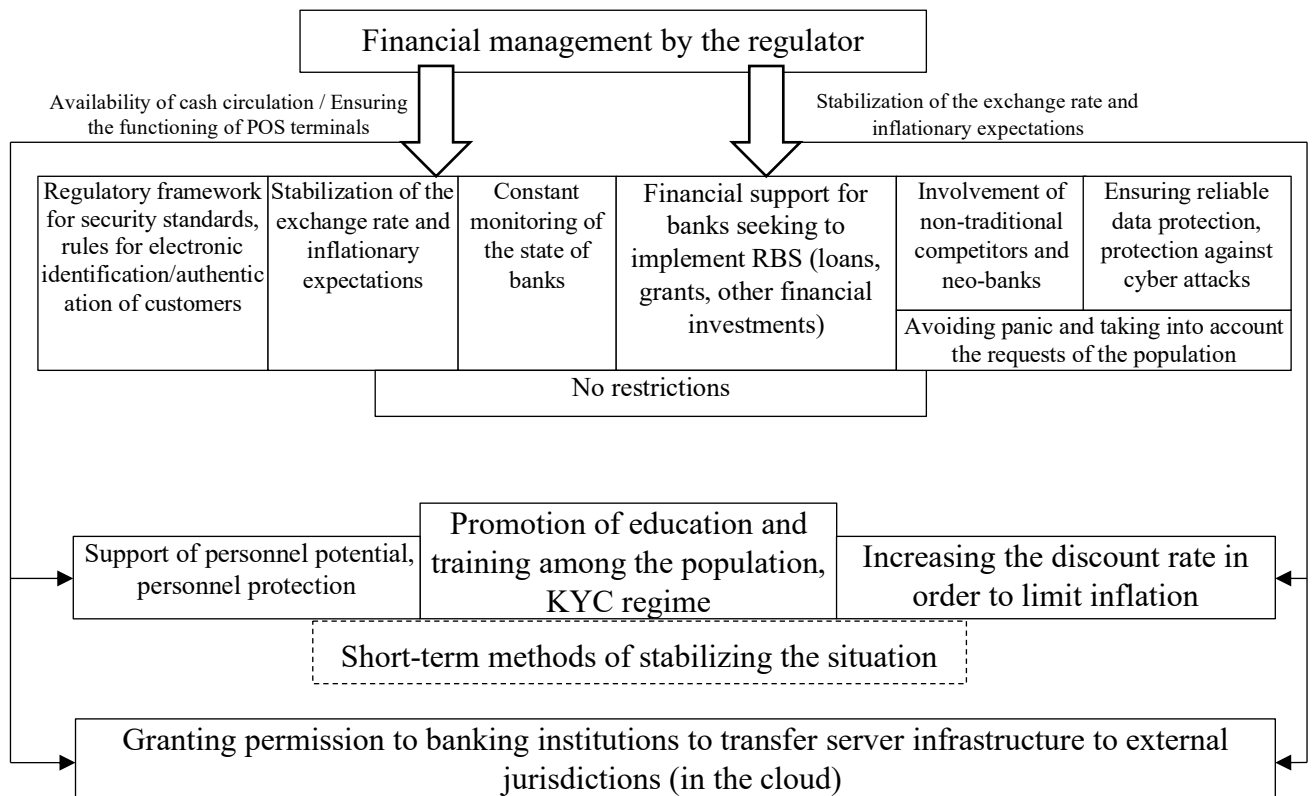


Fig. 1.2. Key decisions regarding the financial management of RBS by the NBU under martial law

Source: built by the author based on [29; 38]

We note that the modern features of the RBS are innovative, are becoming widespread, have acquired practical significance and are an important element of maintaining the country's economy at the appropriate level. At the same time, we observe a good level of regulatory and legal regulation of this area.

Currently, the main legislative acts are: Laws of Ukraine "On payment services" (taking into account the concept of "open banking" [2]), "On electronic trust services", "On electronic commerce", "On cloud services", the concept of "Development concept" was developed digital economy and society for 2018-2020", "Strategies for the development of the financial sector of Ukraine until 2025", "Strategies for the development of fintech of Ukraine until 2025", etc. The clarity of the limits of the use of RBS, the features of cyber protection and the delineation of the relevant banking services are not legally defined [25, p. 33].

The development of technologies played a significant role in promoting the development of RBS even under martial law, and here it is worth mentioning not only the digitalization of the banking system, but also the mobilization of the population by means of smartphones. Agreeing with the research of I.O. Artemiev, S.S. Zalyubovska, the expansion of the range of banking services motivated by customers has created opportunities for cashless circulation for the population using a smartphone or other NFC device with which to pay for transport services (for example, by scanning a QR code), paying for goods/services on the Internet, the possibility of withdrawing cash without a card at ATMs of the corresponding bank, making deposits or credit applications, setting limits on the funds used, etc. with 24-hour access with the support of a hotline, chatbot via the Internet -banking, without visiting the bank [11, p. 96].

Full implementation of the remote form of service in the banking system has both advantages and disadvantages. Using the Remote Banking Services system speeds up and simplifies many banking operations for both the bank and users; acceleration of data exchange, obtaining new channels of customer attraction; the demand for financial services increases, unique services are created.

From a financial point of view, RBS is also profitable: the bank reduces office maintenance costs, and the client is offered cheaper tariffs. Obtaining additional information for a client in the KYC (“know your client”) mode is simplified. But, on the other hand, despite numerous security measures, there are significant risks in the RBS management system: technical failures of the system, cyber-attacks, leakage of personal data of clients, phishing attacks (theft of funds by extracting information about the bank client's account); Pharming attack (creating a fake website to mislead the user); malware attack; other cyber-attacks (viruses, virus programs) [44]. Accordingly, protecting customers from cyber-attacks is an important task of the bank during Remote Banking Services.

Now, the country remains a problem of introducing innovative forms of remote service using remote technologies among legal entities, as larger initial investments and costs for providing new software and equipment are required. Although at the same time, additional protection systems for RBS client’s

function (additional physical keys - tokens, additional verification, protection and blocking of accounts in case of non-standard operations, inclusion of additional checks/reconciliation of documents).

Thus, we have made significant adjustments to the banking system in wartime, which thereby developed Remote Banking Services, starting from active non-standard actions on the part of the banking system regulator, ending with the convenience and security of the client, the elimination of his panic [29, p.1173].

The peculiarities of the formation of the Remote Banking Services in the conditions of martial law were granting permits for the transfer of server infrastructure to foreign jurisdictions, setting up protective mechanisms for remote access; continuity of the customer service process, cost minimization, reassessment of the state of the credit portfolio and clarification of its level of deterioration, striving to eliminate the duplication of personnel functions [47].

In general, the features of the operation of Remote Banking Services in Ukraine under martial law may include the following: popularity of use, increased security, mobile access, continuity of work, cyber-attacks, communication support, etc. (Table 1.1).

Table 1.1

Peculiarities of the operation of remote banking services in Ukraine under martial law

Feature	Characteristic
High popularity and use	The country at the beginning of the full-scale invasion had a high level of Internet adaptability and widespread use of RBS among its citizens. This ensured wide access to banking services, even in the case of martial law
Increased security	In connection with the growing threats of cyber security in the conditions of military conflicts, banks paid special attention to the security of their Internet banking systems. They use modern encryption technologies and have a high level of protection against cyber-attacks.
Mobile access	High penetration of smartphones and wide access to fast Internet. This allows customers to conveniently use mobile applications to access their bank accounts and carry out financial transactions, even in the event of military events. In the conditions of martial law, great attention is paid to the personal safety of employees, customers, support of mobilized workers and the army of Ukraine
Ensuring continuity of work	Banks have developed and adapted strategies and business continuity plans to ensure the operation of RBS even in the event of military threats or crisis situations. This may include data backup, server duplication, and systems outage prevention.
Risk of cyber-attacks	Martial law has increased the risk of cyberattacks by hostile actors of the terrorist state. Currently, banks are particularly attentive and take measures to prevent cyberattacks, including monitoring threats, developing immunity to known threats, training staff to monitor potential threats, and teaching security rules for clients' RBS.
Ensuring communication	During martial law, there may be limited access to normal means of communication, such as the Internet or mobile communications. Banks are developing alternative channels of communication with customers that can use radio, satellite connections or other technologies to ensure communication and control of quality RBS.

Source: summarized by the author

Martial law from 2022 and post-pandemic trends have increased security requirements and ensuring rapid system recovery (during alarms, blackouts): RPA (or robotics) - 24/7 customer consultation, transaction confirmation, error reporting; introduced chatbots; added OCR (or optical recognition) - the ability to convert non-copied documents into edited ones, which are often used in the bank when working with client documents; biometric identification - technology using a person's physiological and biological characteristics for the purpose of establishing identity, to facilitate work in ATMs without bank cards and smartphones (fingerprints, voice identification, face, etc.), involves the use of artificial intelligence.

And if the role of the pandemic in the formation of remote banking became a forced factor based on technological changes and mental habits of the population, then the subsequent military situation in Ukraine forced to strengthen the use of Remote Banking Services based on the influence of the factors of forced displacement of the population, departure abroad (financial support of those who remained), the outflow of personnel and the closing of branches (security in wartime, optimization of bank costs), maintenance of the economy (payments on the Internet, state programs to support the population, the importance of business maintenance, development of blockchain technologies).

Summing up, the features of RBS in the country under

martial law conditions, currently they include a high level of security, mobile access, business continuity, the risk of cyber-attacks, communication and crisis management strategies.

Banks in Ukraine are actively working on the development and implementation of measures to ensure the safety and availability of banking services even in the event of military events and threats.

1.3. The Mechanism of Providing Remote Banking Services in the Context of Current Challenges and Threats

Currently, the largest banks have already implemented a remote format in their operations. The importance of utilizing remote channels was particularly evident during the pandemic, in the post-pandemic recession, and continues to support the country's economy during the period of martial law. Remote banking services have enabled users to conduct transactions from any device connected to the global Internet network, whether from an office, apartment, on the road, or while on a business trip. Customers can make payments for goods, works, and services, create receipts, generate bank statements for a card or account for the past few days, a calendar month, or any arbitrary period, open deposits, pay off loans, transfer funds

between their accounts, perform other credit card operations, monitor exchange rates, follow bank news, and place orders for currency purchase/sale/conversion, among other functions. The operation of the remote banking services (RBS) system is based on new technologies, Web 3.0 platforms, enhanced virtual interaction, blockchain, and the implementation of artificial intelligence (AI) systems [33, p. 36].

At the same time, the remote banking services (RBS) mechanism allows banks to significantly accelerate and simplify document workflow, reduce the cost of banking operations, optimize staff numbers (by eliminating routine tasks), and decrease the volume of paperwork. Such services currently help reduce bank expenses, enhance customer convenience, and enable banks to earn additional commission income. As a result, to attract and retain customers, banks often offer more favorable terms to clients who enter into agreements via RBS, such as higher interest rates on deposits and the option for early closure, as well as introducing small fixed transaction fees and a single fee for any number of payment orders. This enables customers to choose a bank not based on geographical location but on the quality of service and the established tariffs of a particular bank [26, p. 81].

The main principles of the remote banking services (RBS) mechanism during martial law include transparency, variability (a variety of approaches to problem-solving), reflexivity

(justified impact on changes), informativeness, hierarchy (orderliness of relations), adaptability (speed and flexibility according to realities), and corporatism (systematic updating of existing values), among others [38, p. 73]. At the same time, during martial law in Ukraine, the RBS mechanism has been able to evolve based on high-quality regulatory and legal frameworks and the introduction of appropriate management methods (remote management, outsourcing (hedging), risk management, crisis management, etc.).

The key parameters ensuring proper RBS include organizing remote access (smartphones, POS terminals, the "client-bank" system), resuming work with clients, ensuring an uninterrupted service process (including during blackouts), working on cost minimization, reassessing the state of the loan portfolio and determining the degree of its deterioration, and duplicating personnel functions from in-branch services to remote services. The development of mobile banking and the shift of the population to modern smartphones with NFC functionality has enabled a transition in the RBS mechanism from direct interaction with bank employees (operators) – which is still used – to specialized automated systems (ACD and IVR, automated voice response systems) for customer interaction.

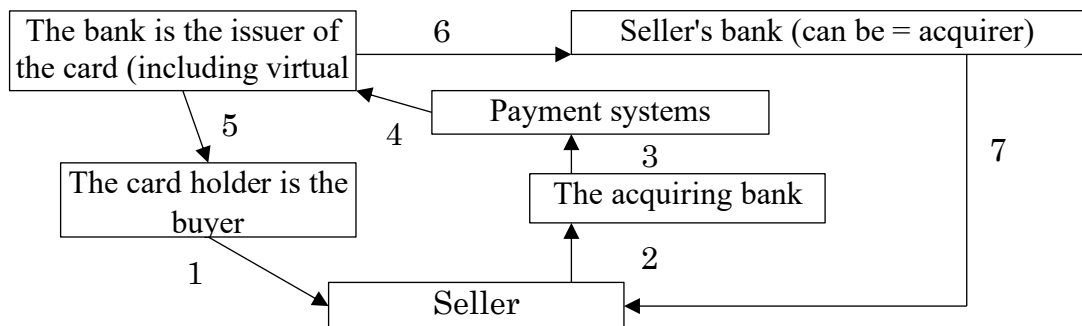
There has also been progress in the development of ATMs, with a shift from separate cash-out and cash-in ATMs to universal ATMs that allow for both withdrawal and deposit

operations, fully activating the card or reading it via chip (by tapping the card to the reader). It should be noted that during the martial law period, there has been a reduction in the number of ATMs and terminals, while the POS-terminal network (Point Of Sale) has expanded. The activation of acquiring services for small and medium-sized businesses in the RBS system became possible through POS terminals.

Acquiring is a remote banking service where, through POS terminals, payments are accepted via payment cards (read from a magnetic stripe or chip) from national or international payment systems for products, goods, and services (often with an App "Terminal", QR codes, NFC tags, Apple Pay, Google Pay, functioning within the LiqPay payment system). Acquirers are payment service providers who offer merchants access to card networks; an acquirer is a credit organization, bank, or non-bank financial institution that works with payment systems [38, p. 73]. As a result, the acquiring system is four-party, where the acquirer provides the following services: registers merchants in card networks, supplying them with the necessary equipment and/or software to accept payments or enabling the use of smartphones with NFC functionality; authorizes, processes, and settles card payments; resolves payment disputes; provides merchants with regular reports on payments received, withheld commissions, and advises merchants on integrating payment acceptance systems with accounting systems; generates receipts

and, when printing is not possible, issues them online via QR code.

Types of POS terminals today are divided into several categories: standard (issued by the bank as stationary or mobile/portable), miniPOS terminals (accepting payments with any cards), Android POS terminals, and validators for connection to vending machines (accepting payments via payment cards, smartphones with NFC, watches, or other NFC-enabled devices). Additionally, there is a mobile app for smartphones with NFC called "Terminal" (no subscription fee, receipt fiscalization is done via email, QR code, or messenger).



1 - the buyer pays the seller with a card through the POS terminal; 2 - the payment is processed by the acquirer and sent to the payment system; 3 - the payment system processes the payment, informs the card-issuing bank about the debit (when the payment goes through, the acquirer and the seller receive a message about a successful payment); 5 - the cardholder receives the debit data, the money is debited from his account by the issuer; 6 - the card issuer transfers money to the seller's or acquirer's bank, which then transfers it to the seller's bank; 7 - the seller's bank informs the seller of the actual receipt of money in this regard.

Fig. 1.3. The mechanism of action of RBS of commercial acquiring

Source: built by the author based on [21; 22]

At the current stage of business development, the "client-bank" system is also in operation, implementing modern methods and tools of information technology based on databases

and telecommunications, with a number of technological features for the automated processing of electronic documents. This system has allowed businesses to maintain the operation of legal entities at a functional level during martial law, military actions, and business relocations. Payments in the "client-bank" system occur based on the client's actions (creating a payment instruction, signing it with an electronic signature, sending it to the bank), and the bank's acceptance/rejection of e-payment documents, followed by the withdrawal/deposit of funds and the bank's notification to the client regarding the acceptance of the payment document.

To support clients' accounting needs, the system generates paper copies of electronic documents, such as bank statements and payment instructions, which serve as formal records for transactions. Additionally, clients have access to secondary electronic documents that support a range of banking activities, including detailed account statements, payment confirmations, payroll management, and more. The appendix lists the key advantages and limitations of the "client-bank" system, assessing its impact on both commercial banks and their clientele.

In breaking down the RBS mechanism element by element, we observe a functional structure of interactions (as illustrated in Figure 1.4).

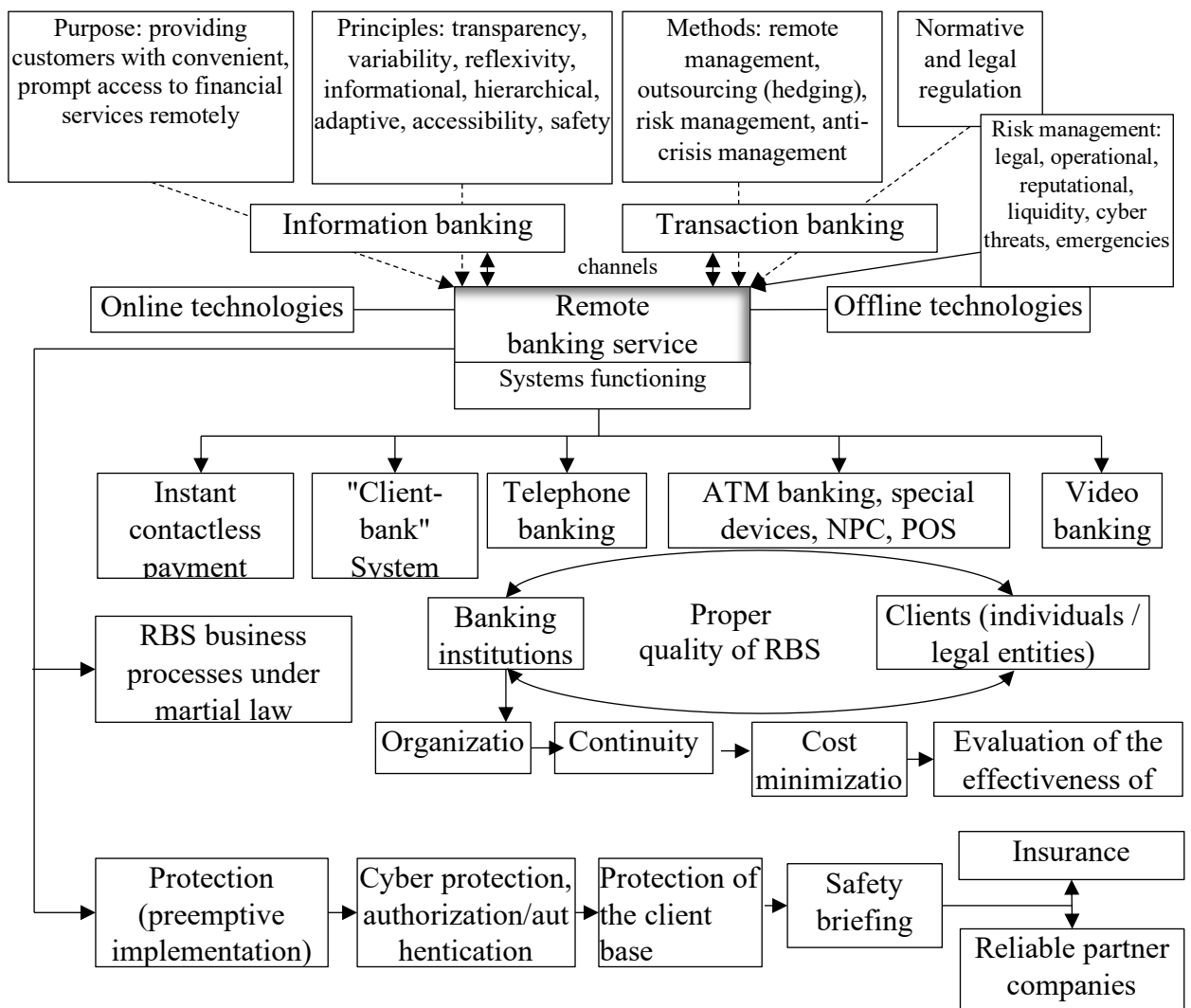


Fig. 1.4. Mechanism of operation of RBS in conditions of martial law

Source: built by the author based on [31; 35]

This structure includes essential operational components tailored for managing diverse client needs, all while maintaining a high level of security. The security aspect is vital, as it safeguards the remote handling of sensitive data and financial transactions within a secure digital framework.

Under martial law, banks face heightened risks, making it essential to adopt an adaptive approach to threat management and operational continuity. They must be vigilant and ready to respond rapidly to evolving threats and changes in operational

conditions, ensuring the resilience of remote services and maintaining client trust during times of instability. The emphasis on secure, flexible remote banking systems becomes even more pronounced, as these systems play a critical role in sustaining financial services and supporting economic stability in challenging circumstances.

Banks are thus compelled to invest heavily in cybersecurity and continually update their remote banking systems to counter potential vulnerabilities. This involves integrating advanced technologies, such as artificial intelligence and machine learning, to monitor, detect, and respond to suspicious activities in real time.

Such innovations not only enhance security but also improve service efficiency, enabling clients to perform financial transactions seamlessly and confidently from anywhere. In the long term, these robust, secure, and adaptable RBS infrastructures strengthen the overall resilience of the banking sector and support its capacity to navigate both ordinary and extraordinary operational challenges.

The implementation of appropriate cybersecurity measures, internal controls, and emergency planning is crucial to ensuring the stability and security of banking activities under such conditions. Importantly, artificial intelligence (AI) technologies are emerging as key components of cybersecurity in the future. Using predictive analytics, AI can forecast security

vulnerabilities, identify online threats, and adjust security settings in real time. Blockchain technology, which operates on the basis of distributed data storage, offers a promising solution to the issue of client confidentiality during martial law.

Thus, after examining the concept of remote banking services as defined by various authors, we can conclude that remote banking services are a technology for providing bank clients with services through the use of remote channels for information exchange (via mobile phones, smartphones, personal computers in online or offline modes). The process of technological modernization has accelerated, particularly due to the onset of martial law in February 2022 following the attack by the terrorist state of Russia, which necessitated rapid adaptation to new functionalities in order to continue operations while limiting human contact and ensuring protection. Banks were tasked with maintaining the volume of transactions and service levels despite the inability to physically visit branches.

Experience from the pandemic allowed banks to quickly adapt to the martial law conditions, thanks to their advanced digital infrastructure and remote work capabilities. All information regarding the current status of accounts, obligations, and deadlines is communicated to clients remotely or through mobile banking, which helps banks retain clients and prevent mass attrition. The swift restart of the energy system and additional support measures enabled the remote banking system

to continue functioning even during blackouts. However, the development of additional cloud infrastructure and protection against cyberattacks proved to be insufficient.

In conclusion, the evolution of remote banking services (RBS) has been critical in adapting to the challenges posed by both the pandemic and the ongoing martial law in Ukraine. Remote banking services are defined as a set of technologies that enable banks to deliver services to clients through various remote channels such as mobile phones, smartphones, personal computers, and other online and offline means. These services offer a flexible, efficient, and secure way for clients to perform financial transactions without the need for physical branch visits.

One of the most significant developments in RBS is the extensive adoption of mobile and web-based technologies by banks. The pandemic was a crucial period that accelerated the digital transformation of the banking sector, with a shift to remote channels that has only intensified with the onset of martial law.

During this time, remote banking systems have played an essential role in maintaining the functioning of legal entities and businesses, even in the most adverse conditions. Businesses that were forced to relocate or restructure due to military actions have been able to continue operating at a high level, thanks to the "client-bank" system and other automated processes.

The "client-bank" system exemplifies the integration of

modern information technologies, including databases, telecommunications, and automated electronic document processing. This system allows clients to create and send payment instructions, sign them with an electronic signature, and receive confirmation or rejection of transactions from the bank. Through this system, businesses and individuals can conduct transactions securely and efficiently.

Additionally, banks offer various secondary electronic documents, such as account statements, payment notifications, and payroll management, which further streamline banking operations for clients.

One of the key benefits of RBS is the ability to reduce operational costs for banks. Automated processes, such as electronic document management and payment processing, lower the need for manual operations, minimize paper use, and reduce the number of in-branch staff required to handle routine tasks. This efficiency translates into cost savings for banks, which can then offer more competitive terms to clients who use remote services, such as higher interest rates on deposits or reduced transaction fees. By optimizing internal processes, banks can focus more on customer service and innovation while maintaining profitability.

Security is a critical aspect of the RBS mechanism, particularly in times of crisis, such as the ongoing martial law in Ukraine. The rise of cyber threats requires banks to remain

vigilant and proactive in their approach to safeguarding client data and ensuring secure transactions. The implementation of cybersecurity measures, internal controls, and emergency preparedness plans is essential to maintaining trust and stability in the banking sector. Artificial intelligence (AI) technologies are becoming a crucial tool in this regard, as AI can analyze vast amounts of data, predict vulnerabilities, detect real-time threats, and adjust security protocols automatically. AI's role in enhancing cybersecurity will likely expand in the coming years, offering new levels of protection for both banks and their clients.

Blockchain technology also holds promise as a solution for ensuring client confidentiality, especially in the context of martial law. Blockchain operates on a decentralized model of data storage, reducing the risks associated with centralized databases and providing a higher level of data security. By adopting blockchain, banks can protect sensitive information more effectively, ensuring that client data remains confidential even in times of heightened risk.

Another key aspect of RBS is the wide range of POS terminal options available today, which are integral to facilitating remote payments. These terminals include standard stationary and mobile devices, miniPOS terminals, Android-based POS terminals, and validators connected to vending machines. Additionally, mobile apps for smartphones equipped with NFC technology allow for secure, contactless payments without the

need for physical terminals. These advancements have greatly expanded the options for businesses and individuals to process payments remotely and efficiently. The rapid development of digital infrastructure, such as mobile banking and NFC-enabled devices, has enabled banks to reduce their reliance on physical branches and ATMs, even as the number of ATMs and terminals has decreased. Instead, the expansion of POS terminals has enabled small and medium-sized businesses to continue operations, with services such as acquiring becoming more widely available. Acquiring services allow businesses to accept card payments securely and efficiently, using advanced technologies like QR codes, NFC tags, and mobile apps integrated with national and international payment systems. These services ensure that businesses can operate smoothly, even in the face of operational challenges brought on by the war. Despite these advances, there are still areas that require further development. For example, the infrastructure for cloud technologies and the security measures to protect against cyberattacks need to be strengthened. The growth of cloud technology could enhance the resilience of remote banking services, enabling banks to store and process data more efficiently and securely, while also providing greater flexibility in how services are delivered.

In conclusion, the rapid adoption of remote banking services has proven to be a lifeline for the Ukrainian banking sector

during the difficult times of the pandemic and martial law. The digital transformation has enabled banks to maintain operations, support businesses, and provide clients with convenient and secure ways to manage their finances. The integration of AI, blockchain, and advanced POS technologies will continue to play a significant role in the future development of remote banking.

However, the ongoing challenges of cybersecurity, infrastructure development, and adapting to the ever-changing conditions of military conflict will require banks to remain flexible and forward-thinking in their approach to innovation and service delivery.



CHAPTER II

FEATURES OF THE REMOTE BANKING SERVICE MECHANISM IN JSC "OTP BANK"

2.1. Modern Trends in Remote Banking Services under Martial Law

A notable feature of the current state of the banking system of Ukraine during 2022-2023 under martial law has been its maintenance at a pre-war level, stabilization, and consideration of existing blackout threats despite attacks by the Russia Federation identified as a terrorist state on Ukraine's energy infrastructure. The enhancement of the overall banking system's functionality is based on expanding the capabilities of remote banking services and adapting operational processes. The necessity of developing remote banking services (RBS) in Ukraine during martial law is critically important for several reasons: primarily, it ensures security and convenience, as well as reliability in crisis situations. This also allows for remote financial management, increasing the speed and convenience of

such operations. Monitoring and control are ensured, and protection against excessive demand for physical bank branches is activated.

At the same time, the current quality level of RBS functionality in the banking sector, established during the pandemic period, has contributed to strengthening the positions of banks and supporting and stabilizing the Ukrainian economy. In 2023, the number of active banks decreased by 9.2% during the war, amounting to 65 banks, of which only 51 provide remote banking services (78.5%). Among the leaders in remote banking are Alpha Bank, PrivatBank, Monobank, A-Bank, OTP Bank, PUMB, Oschadbank, and others. Accordingly, these banks exhibit the highest indicators in terms of RBS functionality: quality authorization and authentication services, account and statement generation, ease of payment initiation and processing, card services, online credit/deposit systems, currency operation capabilities, quality support, communication channels, and security levels.

The main elements of RBS functionality in Ukraine during martial law include:

- A 20% reduction in the territorial network of banks (or 1,349 fewer branches during the period of martial law and as a result of the occupation of southeastern territories of the country) and a parallel restoration of bank networks through remote access.

- Development of technological solutions and services (launching mobile applications in various banks – before the war, there were 38 mobile applications across 71 operating banks, and as of September 1, 2023, there are 42 mobile applications in 65 active banks, with rebranding of banking applications (Alpha Bank Ukraine, Credit Agricole, OTP Bank, Kredobank, Southern Bank, Pravex Bank, Ukrgasbank, etc.), operation of internet acquiring, transition to cloud services, and backup technological platforms). Since the onset of the full-scale invasion until August 2023, mobile banking traffic increased by 85%, and new digital registrations surged by 200%. Among Ukrainian remote banking services are Privat24, Mono, Sense, A-Bank, PUMB (via Diia), Ukrgasbank, OTP Smart, Oschad 24/7, etc. Leaders by user numbers include Privat24 (+11%), Oschad24/7 (+3.5%), and Monobank (+5%).
- Maintenance of operational stability under significant pressure on card business (transactions involving card accounts) considering regulatory requirements.
- Retention and preservation of depositor trust, inflow of funds into current accounts, growth of term deposits, and increase in bank's net asset volumes. However, demand for loans remains low, with an increase in the

share of non-performing loans.

- Ensuring uninterrupted operation of bank branches, ATMs, POS terminals, and data centers during blackouts (more than 30% of bank branches are equipped with generators, providing autonomous power supply for up to 3 days).
- Investment in the continuity of IT systems and cybersecurity of banking operations (the rise in cyberattacks has increased by 3.5 times, reaching up to 10 attacks daily).
- Staff have become the main driver of the resilience of the country's banking system (ensuring employee safety, remote working conditions, and support for the Armed Forces of Ukraine and mobilized bank employees).

Since the beginning of the military invasion of Ukraine, there has been an active transition of the population to online services. Due to the inability to visit branches, there was a sharp decline in demand for financial services from banks, with a significant portion closing during military events for safety reasons. Most clients had to interact with their servicing bank remotely using internet and mobile applications or messenger chatbots. It is worth noting that the level of digitalization of banking services in Ukraine has significantly increased since the start of the military invasion. A survey conducted by Mastercard indicates a

significant interest among Ukrainians in digital technologies: 51% of respondents expressed a positive response to using only digital banking, demonstrating a desire for remote banking services.

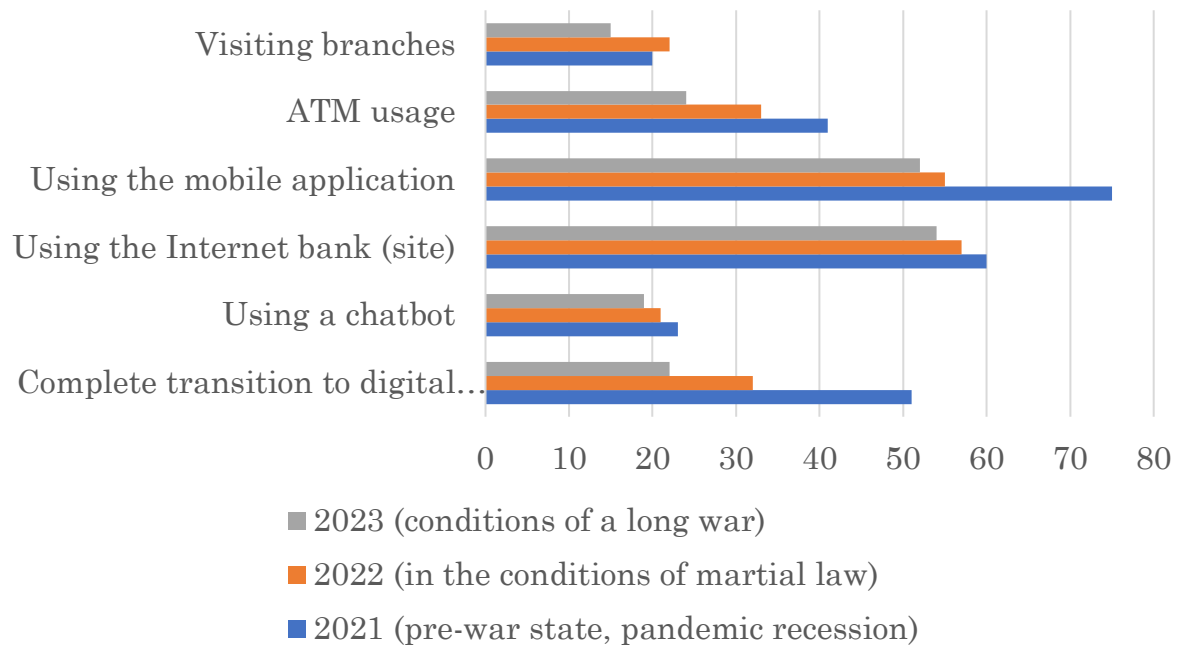


Fig. 2.1. Share of clients using various banking service channels during martial law in Ukraine (2022-2023), %

Source: summarized by the author based on data [52]

Concerned about the consequences of this period, customers most often chose to use smartphones and web browsers for banking transactions. This change in approach was prompted by the need to comply with social distancing rules because of the recessionary impact of the pandemic, and subsequently to avoid providing protection during massive attacks by the Russian aggressor. Accordingly, we have an increase in the number of RBS clients in the country (51.7 million clients of individuals and 2.4 million clients of business entities (Annex D).

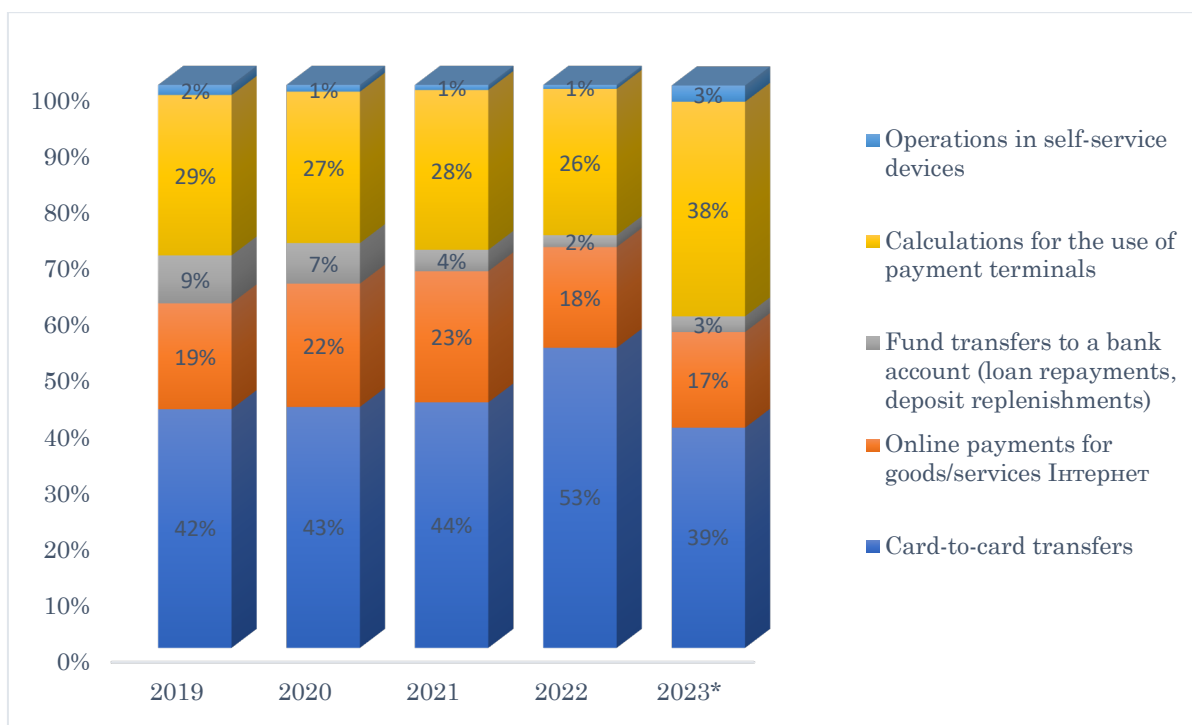


Fig. 2.2. Structure of cashless transactions by volume using payment cards in Ukraine for the 2019-2023 period, %*

the data are indicated for the period of 8 months of 2023 (the submission of statistical reporting on transactions with payment cards is incomplete).

Source: construction by the author based on data [56]

In terms of remote banking service (RBS) operations, both the monetary value (a growth of 63.4%) and the number of transactions consistently increased during the 2019-2022 period (see Appendix D). The volume of RBS operations during the first 8 months of 2023 amounted to UAH 2,939.3 billion, representing a 14.7% decrease compared to the 2022 level. However, given the incomplete reporting period, a 25% growth in operations is projected by the end of 2023. Within the structure of transaction volumes, the largest share of RBS operations was observed in card-to-card transfers (UAH 1,148.5 billion or 39.1%) and payments using payment terminals (UAH 1,121.3 billion or

38.1%) (see Figures 2.1 and 2.2). During the period of martial law, the structure showed a sharp decline in card-to-card transfer operations (by 14.2 percentage points), a reduction in online payments for goods and services (by 0.8 p.p.), and an increase in transactions via payment terminals (by 12.1 p.p.).

In line with the number of RBS transactions, similar trends are observed. The largest share of 64.8% was formed by payments using payment terminals, which increased by 12.2 percentage points, while card-to-card transfers accounted for 10.7% and decreased by 3.7 percentage points. At the same time, the share of online payments for goods dropped to 19.4%, showing a reduction of 8.5 percentage points. Overall, this situation resulted from limited access to financial resources, power outages, restricted access to online resources, and a preference for payment terminals, which were more accessible and reliable. During blackouts, banks equipped their branches, including payment terminals, with autonomous power sources, and in the absence of electricity, cash transactions were used. Nevertheless, considering that 2023 is the second year of the war, Ukrainians continue to prefer payment cards and cashless transactions (on average, 9 out of 10 transactions are cashless).

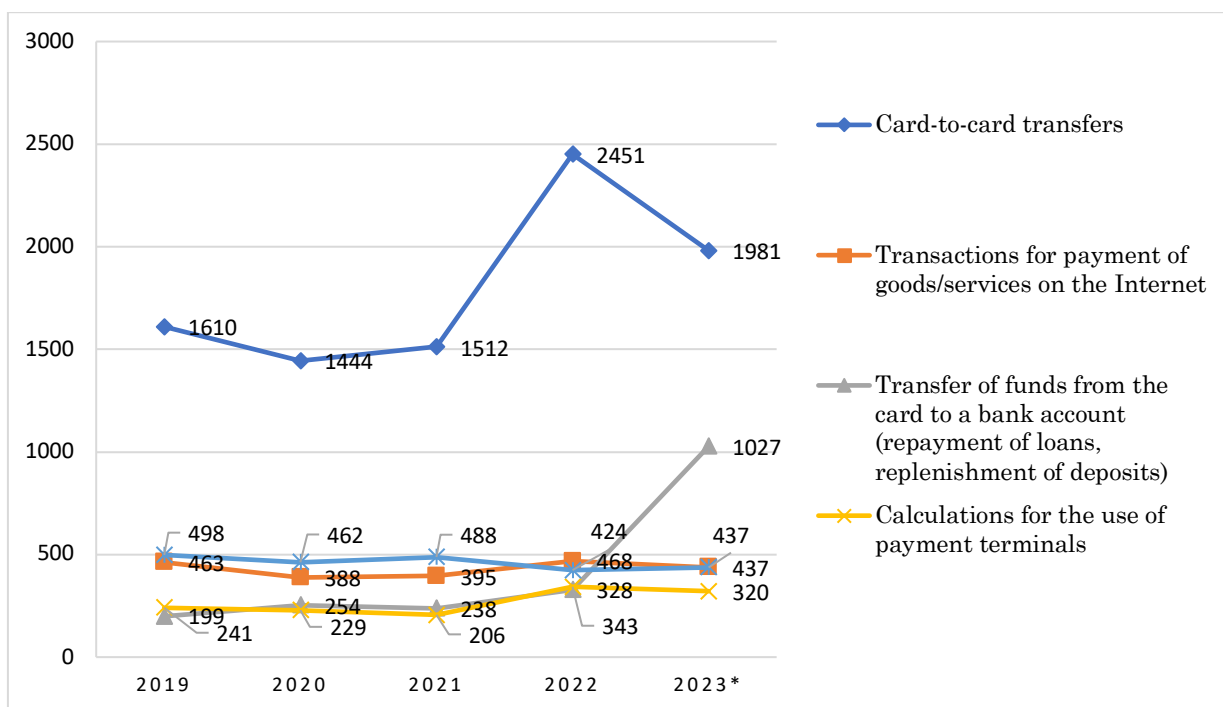


Fig. 2.3. Average value of cashless transactions using payment cards in Ukraine for the 2019–2023 period, UAH

Source: compiled by the author based on data from [56]

In 2023, the average transaction amount for RBS card-to-card transfers was UAH 1,981, significantly lower than in 2022, with a 20% decrease. For transfers from a card to a bank account, the average amount reached UAH 1,027, showing a threefold increase. In terms of online purchases, payments via payment terminals, and self-service devices, the average transaction value remained almost unchanged (up to UAH 500). This trend is largely attributed to a reduction in household income, a decrease in foreign aid, the introduction of specific conditions for small business development, and the cancellation of tax incentive periods, among other factors.

A positive aspect of RBS development has been the mass

digitization of the population, with mobile phones, both with and without NFC functionality, becoming more widely accessible. Banks' active efforts to ensure the high-quality functioning of mobile applications have enabled efficient RBS services for the public, allowing clients to perform financial transactions, check balances, pay bills, and obtain loans from their phones at any time. Moreover, the use of biometric data (fingerprints, facial recognition) on smartphones ensures a high level of financial security.

Regarding the use of mobile applications in RBS during martial law, we observe the following data (see Appendix F): 75% of Ukrainians prefer using mobile apps, while only a small fraction rely solely on online banking (11%). Among the most popular transactions are mobile top-ups, card-to-card transfers, and utility bill payments. The most widespread transaction during martial law has been donations to the Ukrainian army, accounting for 30% of all transfers. Looking ahead, Ukrainians are interested in accessing the following RBS features via mobile apps: card issuance (61%), management of multiple accounts in a single app (52%), purchasing transportation tickets (27%), cryptocurrency acquisition (27%), financial consulting for asset management (22%), and buying securities and stocks (21%), among others.

Thus, during 2022-2023, under martial law, despite active military actions, missile attacks, and blackouts, Ukrainians

continued to clearly perceive remote banking services primarily as a convenient tool for cashless transactions. As a result, the current conditions indicate the continued development of Ukraine's payment infrastructure based on remote banking services under martial law, demonstrating a high level of public trust and resilience.

The Ukrainian banking system has demonstrated remarkable resilience during 2022–2023 despite the challenges posed by the ongoing military conflict and martial law. One of the key features of this period is the banking sector's ability to maintain its functionality at pre-war levels, stabilizing and adapting to threats such as blackouts caused by Russian attacks on Ukraine's energy infrastructure. Central to this resilience is the expansion of remote banking services (RBS) and the adjustment of operational processes to meet the needs of businesses and individuals during these challenging times.

The development of RBS in Ukraine under martial law has become not just a necessity but a critical component of banking operations. Remote banking offers security, convenience, and reliability, especially in crisis situations, as clients can manage their finances remotely and perform transactions quickly and easily.

This ensures continuity in monitoring and controlling finances while reducing the strain on physical bank branches. In particular, the RBS infrastructure that was developed during the

pandemic has strengthened the banking sector's position, helping to stabilize Ukraine's economy amid the crisis.

By 2023, the number of operating banks in Ukraine had decreased by 9.2%, leaving 65 banks, of which 51 offer remote banking services (78.5%). Leading banks in the RBS sector include Alfa Bank, PrivatBank, Monobank, Universal Bank, A-Bank, OTP Bank, PUMB, and Oschadbank. These institutions stand out for their high levels of functionality, offering services such as seamless account management, efficient payment processing, online lending and deposit services, foreign currency transactions, robust customer support, and secure communication channels. The functionality of these banks' RBS platforms has been crucial to their continued operation during martial law, allowing them to serve customers efficiently, even under severe conditions.

Key elements that have supported the Ukrainian banking sector during martial law include:

- Reduction in the Territorial Network of Banks. The number of bank branches decreased by 20% (or 1,349 fewer branches) due to the occupation of southeastern Ukraine and the need to streamline operations. However, banks were able to restore service levels through remote access, ensuring continuity in providing financial services.
- Technological Advancements. Significant technological

developments were implemented, including the launch of mobile banking apps, the rebranding of existing apps, and the adoption of cloud-based services and reserve technology centers. Since the onset of the full-scale invasion, mobile banking traffic has increased by 85%, and new digital registrations have grown by 200%. Key players in the Ukrainian mobile banking market include Privat24, Mono, Sense, A-Bank, PUMB, and others, with leaders like Privat24, Oschad24/7, and Monobank seeing significant growth in user numbers.

- Operational Stability. Despite the significant load on card-based transactions, banks have maintained operational stability by complying with regulatory requirements and managing the demand for services such as account withdrawals, deposits, and credit facilities.
- Trust and Customer Retention. Banks have been able to retain depositors' trust, resulting in an influx of funds into current accounts, an increase in term deposits, and growth in net assets. However, there has been a slight increase in non-performing loans, and demand for new credit remains low.
- Uninterrupted Branch Operations. Banks have invested heavily in ensuring the uninterrupted operation of branches, ATMs, POS terminals, and data centers, even

during blackouts. More than 30% of bank branches are equipped with generators, allowing them to operate autonomously for up to three days.

- Investment in Cybersecurity. Banks have significantly increased their investments in cybersecurity measures to protect their operations from a growing number of cyberattacks, which have tripled, with up to 10 attacks occurring daily. Ensuring IT system stability and protecting against cyber threats have become critical priorities during martial law.
- Personnel as a Key Driver of Stability. Bank employees have played a vital role in maintaining the resilience of the Ukrainian banking system. Measures have been put in place to ensure the safety of employees, support remote work, and assist the armed forces and mobilized staff.

As a result of the full-scale invasion, the population's shift toward online banking has accelerated. In the absence of physical access to branches, demand for in-person banking services sharply declined, and many branches were closed to ensure security.

The majority of customers have been forced to interact with their banks remotely via internet and mobile applications, chatbots, and messaging services. The level of digitalization of banking services in Ukraine has increased significantly since the

start of the war. A Mastercard survey indicates that 51% of Ukrainians now use digital banking exclusively, highlighting a growing demand for robust RBS platforms.

In conclusion, the current state of the Ukrainian banking sector is defined by its adaptability and resilience, driven by technological advancements in remote banking services. The sector has successfully navigated the challenges of martial law by reducing its physical presence, enhancing digital infrastructure, and maintaining customer trust. However, ongoing investment in cybersecurity and IT system resilience will be essential as banks continue to face growing threats and operate under difficult conditions. The pandemic experience has prepared Ukrainian banks to adapt quickly, enabling them to maintain critical operations during the war and supporting the country's economy in the process.

2.2. Characteristics of Services Within the Framework of Remote Banking Services for Clients at JSC "OTP Bank" and the OTP Bank System

JSC "OTP Bank" has been successfully developing its online services for several years, consistently securing top positions in internet banking efficiency rankings. Currently, OTP Bank's remote banking services rank in the top three best internet

banking services in Ukraine and the top six in Central and Eastern Europe, the Caucasus, and Central Asia. Within the online service structure, key operations include OTP Bank UA internet banking, "OTP Smart" internet banking, online loan repayment, and online insurance. The entire remote banking system provides a free financial management tool for clients, with 24/7 access, free transfers, and additional deposit bonuses, among other features. OTP Bank offers clients a wide range of services and banking products, some of which are provided as part of its remote banking services (RBS). These include phone banking, internet banking, SMS banking, mobile banking, and online services, covering credit and deposit transactions.

Remote banking services account for 85% of OTP Bank's offerings. Amid the current martial law, the bank continues to support the economy through lending, services for corporate and retail segments, and significant investments in client service digitalization and IT development.

The foundation for OTP Bank's remote banking services is supported by software (the web portal www.otpbank.com.ua, OTP Smart and OTP Bank UA mobile applications), a robust authentication system, fraud prevention cybersecurity, and clear service agreements. For private clients, OTP Bank provides the following remote service channels:

– Remote service channels:

1. Internet Banking System: OTP Bank UA for

individuals, Click OTPay for corporate clients, and OTP Smart internet banking.

2. Mobile Banking System: Mobile applications including OTP Bank UA, OTP Smart, OTP Bank HU, OTP m-Bank, and Click OTPay.

3. LiqPay System: Payment via card, token-based payment, two-stage payment, subscriptions, and P2P debit.

4. Internet Acquiring Service.

5. Contact Center and 24/7 Support: Assistance via messenger services such as Facebook, Telegram, and Viber.

– Self-service devices:

6. Bank and partner ATMs (Atmosphere network).

7. Information-payment terminals (POS terminals), terminals from partner banks, and terminals within the City24 national system.

The profitability of the bank's main remote banking operations is presented in Table 2.1.

To date, the profitability of Remote banking services operations amounted to 7.7 billion hryvnias. In terms of dynamics, we observe an increase in profitability by 16.2% compared to the pre-war indicator of 2021.

Even at the beginning of the war, JSC "OTP Bank" drew attention to the need to increase the level of protection of Internet banking, therefore, the OTP Bank UA mobile application was created, and today the procedures are being carried out gradual

transfer of clients to the new system. "OTP Bank" JSC plays an important role in the RBS of ensuring payments and transfers (Table 2.2).

Table 2.1

Profitability of online RBS operations in JSC "OTP Bank" for
2021-2023, million hryvnias

Indicators	2021	2022	2023*	Deviation 2023 to 2021	
				+/-	%
Internet banking OTP Bank UA	0,0	0,0	3126,2	3126,2	-
Internet banking OTP Smart	5650,7	7901,1	3512,0	- 2138,7	62,2
Premium Banking	12,4	18,6	22,4	10,0	180,6
Repayment of a consumer loan online	845,1	1024,4	951,0	105,9	112,5
Online insurance	87,0	43,0	52,0	-35,0	59,8
In total	6595,2	8987,1	7663,6	1068,5	116,2

*here and in the future, the data is displayed for the 8th month of 2023, according to the financial statements of JSC "OTP Bank"

Source: calculated by the author based on the financial statements of JSC "OTP Bank"

According to the obtained data, the profitability of payments and transfers in 2023 has not yet reached the pre-war level of 2021, but they occupy a significant volume in the bank's revenue operations (convenience of paying for utilities, mobile communications, the Internet, education, transport, and even taxes).

Thus, the profitability of payment for services in 2023 amounted to 451 million hryvnias, the dynamics of this indicator decreased by 13.3%. Transfers from card to card in these operations occupy 32%, but the dynamics are reduced by 41.3%,

which is largely due to the unfinished period of 2023 and the weakness of the country's economy in general during the martial law.

Table 2.2

Payments and transfers at RBS in JSC "OTP Bank" for 2021-2023, million hryvnias

Indicators	2021	2022	2023*	Deviation 2023 to 2021	
				+/-	%
Payment of services	520,3	432,5	451,0	-69,3	86,7
Transfer from card to card	639,7	524,3	375,3	-264,4	58,7
Payment by card according to details	240,6	240,4	216,1	-24,6	89,8
Transfer from the MasterCard card of the European Bank	159,6	182,6	130,4	-29,2	81,7
In total	1560,2	1379,9	1172,7	-387,5	75,2

Source: calculated by the author based on the financial statements of JSC "OTP Bank"

Card payment by details is gaining popularity every year and has a steady growth trend in 2021-2022, the same trend should be maintained at the end of 2023, which is related to the requirements of the law and the increase in the number of small and medium-sized businesses that work online. Also, because of the forced migration of the population abroad, the transfer of funds to a European bank became an important service. In 2023, we have an 18.3% drop in the profitability of this type of operations compared to the pre-war level of 2021, which is due to both the depletion of the economy and the reduction in the incomes of Ukrainians during the war.

Regarding the services of the RBS, currency conversion operations prevail, which is especially relevant during martial law – forced migration of the population abroad, support of relatives, assistance from abroad (Table 2.3). As a result of the development of new remote financing programs, OTP Bank created Megawatt - a service for buying gas to the home, which is a quite popular service and brings revenue at the level of 16.3 million hryvnias in 2023. An actual service was checking the information security of workplaces where a remote access banking system is installed.

Table 2.3

RBS services at OTP Bank for 2021-2023, million hryvnias

Indicators	2021	2022	2023*	Deviation 2023 to 2021	
				+/-	%
Cash order	2,4	3,3	2,8	0,4	116,7
Currency conversion on card accounts	171,9	151,2	96,3	-75,6	56,0
Debt status under the credit agreement	1,1	0,8	1,3	0,2	118,2
Megawatt is a home gas purchase service	15,6	17,2	16,3	0,7	104,5
Checking the information security of workplaces	12,9	26,0	41,9	29,0	324,8
Registration of companies online	1,9	2,7	3,2	1,3	168,4
In total	205,8	201,2	161,8	-44,0	78,6

Source: calculated by the author based on the financial statements of JSC "OTP Bank"

The general state of services within the framework of remote banking services for clients at JSC "OTP Bank" under martial law conditions is presented in the table. 2.4.

Table 2.4

Elemental composition of RBS in Ukraine in JSC "OTP
Bank" (2022-2023)

No	Indicator	February- December 2022	January - September 2023	January- December 2023 (forecast)
1.	Share of non-cash payments by payment cards	83% (an increase of 6.5% compared to the previous year)	85% (a decrease of 16.5% compared to the previous period)	85% (an increase of 33.4% compared to the previous period)
2.	Number of new payment cards	872.1 thousand pcs. (increase in the volume of issuance by 5.9%)	963.2 thousand pcs. (increase in the volume of issuance by 10.4%)	1021.5 thousand pcs. (a 17.1% increase in the volume of issuance)
3.	Non-cash transactions using payment cards	UAH 319.7 billion (6.5% more than in previous years)	UAH 270.3 billion (16.4% less than in previous years)	UAH 426.6 billion (33.4% more than in previous years)
4.	Contactless payments	2.4 million pcs. (every fifth payment card is contactless)	3.3 million pcs. (every third card is contactless)	4.3 million pcs. (every second card is contactless)
5.	Distribution of non-cash transactions, %:			
6.	for payments in the traditional network	42,3	35,8	46.8
7.	for transfers from card to card	38,7	43,4	32.1
8.	transfer of funds from the card to a bank account	2,1	2,8	2.9
9.	to pay for goods and services on the Internet	16,9	18,0	18.2
10.	The average amount of one transaction in the retail network, hryvnias	428	534	654

Source: calculated by the author based on the data of JSC "OTP Bank"

The analysis of the distribution of non-cash transactions when paying with payment cards at the beginning of hostilities was at the level of 83%, this situation was entirely related to last year's pandemic upheavals, which already prepared the economy for the creation of a high-quality field of remote services. As of the current state of 2023, we have an increase in the share of such calculations by 2%, while the volume of transactions has so far been reduced by 16.5% compared to the pre-war level, but the year is not over, so in the forecast, the end of 2023 will show an increase of 33.4%. OTP Bank actively carries out operations for issuing and servicing payment cards: pension, credit, salary, debit, etc.

The average amount of one transaction of OTP Bank customers in the trading network in 2023 amounted to UAH 534 (at the beginning of the war - UAH 428), in the future, the average check at the end of 2023 will be UAH 654, which determines the important role of online payments under martial law.

According to the summarized data, in JSC "OTP Bank" the volume of transactions using payment cards in 2023 is 270.3 billion hryvnias, which is 8.15 less than the pre-war level, but in the future, by the end of this year, the volume should increase by 44, 9%, which is due to growing consumer demand by the end of the year, the introduction of new remote banking services, and the growing popularity of the bank. The volume of operations

carried out through ATMs is quite low (12 times smaller), since it is online and mobile banking that allows customers to obtain a high level of functionality and security in martial law conditions.

Table 2.5

Features of operations (general circulation of funds) using bank cards of JSC "OTP Bank" under martial law conditions for 2021-2023.

Indicators	2021	2022	2023*	31.12. 2023 (прогноз)	Deviation, %	
					2023*/ 2021	2023 /2021
The volume of transactions carried out using payment cards, billion hryvnias	294,3	319,7	270,3	426,6	91,9	144,9
The volume of operations carried out through ATMs, billion hryvnias	33,6	29,4	21,4	31,6	63,7	94,2
including by national currency	281,3	284,2	248,2	391,8	88,2	139,3
in foreign currency	13,0	35,5	22,1	34,8	170,0	267,4
The number of issued cards, thousand pcs	823,4	872,1	963,2	1021,5	117,0	124,1

Source: calculated by the author based on the data of JSC "OTP Bank"

The high level of issued payment cards from 2021-2023 is primarily related to the state programs of public support "eSupport" (єПідтримка). The transition to new technologies and ease of use made it possible to increase the number of contactless payment cards by 1.5 times, while every fifth active card is tokenized. In 2023, almost all transactions in the retail network are performed with a contactless card or with the help of mobile gadgets (88.9%).

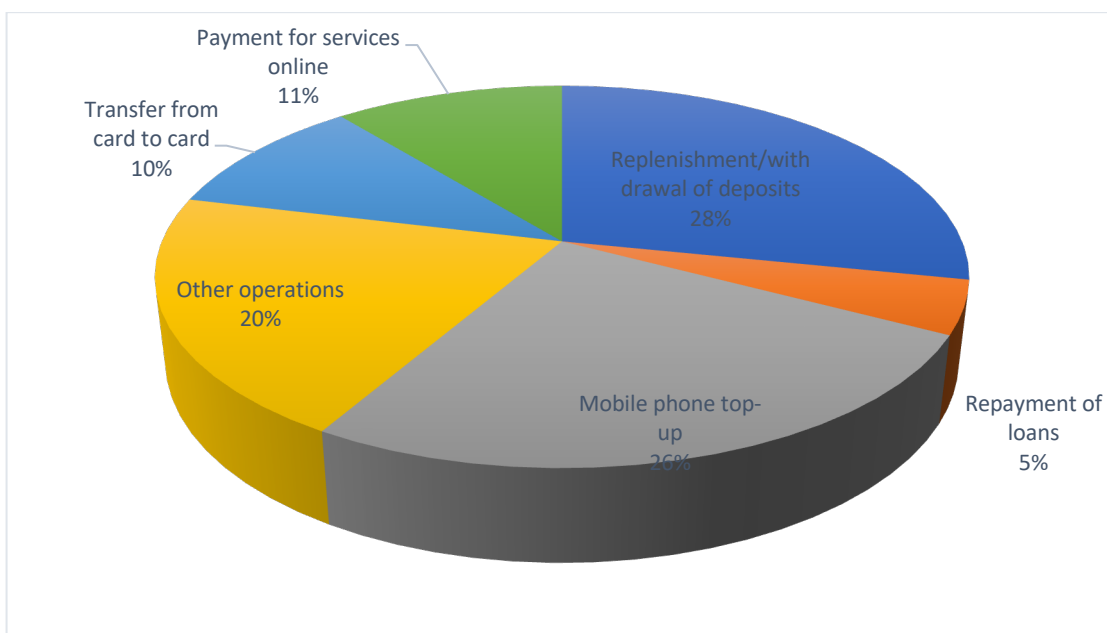


Fig. 2.4. Predominant transactions from the mobile application of active users of OTP Bank UA in 2023, %

Source: according to JSC "OTP Bank"

According to the bank's statistical data, the OTP Bank UA application is predominantly used for mobile phone top-up transactions (25.7%) and online payment services (10.9%), debit cards are characterized by top-up/withdrawal (28.2% of transactions).

Safe transfer of funds from card to card became important during the war, accounting for 10.3% of transactions from mobile applications and credit payments (4.5% of transactions).

Advantages of the OTP Bank UA mobile application (Appendix K): good functionality of the application based on issuing loans, online deposits, buying bonds, disabling double conversion. In terms of security, it competes with mono and privat24 applications - it gives the opportunity to quickly change

the code word, financial number, issues a card with delivery to the client. Among the advanced services of the mobile application is the ability to carry out transactions with securities and purchase bonds. At the level of security functionality, 3D secure has become important: at the customer's request, triple authentication based on push notifications, a one-time password and a token can be turned on/off, which reduces payment card fraud. When automating various functional capabilities, the bank paid considerable attention to the free-of-charge of most services, including security and some service operations (for example, opening accounts, topping up a mobile phone, etc.), and maintaining a competitive tariff policy.

Thus, the RBS of clients of JSC "OTP Bank" is performed at the proper level, the quality of services has positive trends towards improvement and expansion. The bank has achieved significant potential based on online banking and the mobile banking system. Even during the period of martial law, RBS are growing in terms of revenue and volume, and in the future, such types of services as payment for services, card-to-card transfer, payment by details, settlements with foreign banks, remote processing and online settlement of consumer bills are gaining popularity among customers. loans, etc. The advantages of mobile banking today are: the ability to carry out transactions with securities and purchase bonds, reasonable tariff packages, a high level of security, customer support.

2.3. The Mechanism of Remote Client Services at JSC "OTP Bank" and Its Effectiveness

The remote banking mechanism for JSC OTP Bank's clients is regulated in accordance with Ukrainian legislation, including the following laws: "On Banks and Banking Activity," "On Financial Services and State Regulation of Financial Services Markets," "On Payment Services," "On Consumer Lending," "On Personal Data Protection," "On Electronic Trust Services," "On Electronic Documents and Electronic Document Management," as well as regulations and directives from the National Bank of Ukraine (NBU), service agreements, the bank's internal policies, and security standards such as the Payment Card Industry Data Security Standard (PCI DSS).

The remote banking mechanism for bank clients begins with client registration and is primarily determined by the client type - individual or legal entity. For registration, differences in the RBS mechanism arise in the submission of documents, access rights formation, specifics of tax information, and electronic signatures (Table 2.6). In the RBS service structure, legal entities have broader functionality, including expanded payment options (more payment types and transfers to external accounts), report generation (account turnover, payroll for employees), and business services (expanded lending services, settlement, and cash services).

Table 2.6

Features of the RBS mechanism at the stage of registration
in JSC "OTP Bank"

Procedures and requirements	Private person	Juridical person
Submission of documents	Usually, a personal document and other personal data are required (passport, identification code or ID card. Identity verification takes place online.	Legal entities must provide documents confirming their legal status, such as a charter, an extract from the Unified State Register of Legal Entities, documents on the appointment of a manager, etc. Completion of registration requires a manager's visit to the bank branch.
Access rights	Have limited access rights and functionality focused on personal financial transactions.	Have more functionality, such as employee payroll operations, higher volume operations, and other business services.
Tax information	Are not involved in tax accounting in the bank.	Additional tax services and accounting are possible.
Management and representation	A natural person has a personal representative.	A legal entity can have many representatives and different levels of management.
Electronic signature	Usually uses personal logins, passwords, personal electronic signature for authorization.	Can have a qualified electronic signature for representation and signing documents on behalf of the company. Ability to restrict access to confidential information

Source: according to JSC "OTP Bank"

In general, Private persons and juridical person use similar services in online banking, but the functionality and options for legal entities may be more extensive and complex to meet their specific needs. The general mechanism of RBS specifically for JSC "OTP Bank" is shown in the diagram (Fig. 2.5): conclusion of a RBS contract, registration in the client-bank system (which differs for individuals, legal entities (including individual entrepreneur (ФОП)), passing the authentication procedure and

obtaining access to banking services (according to banking tariff packages).

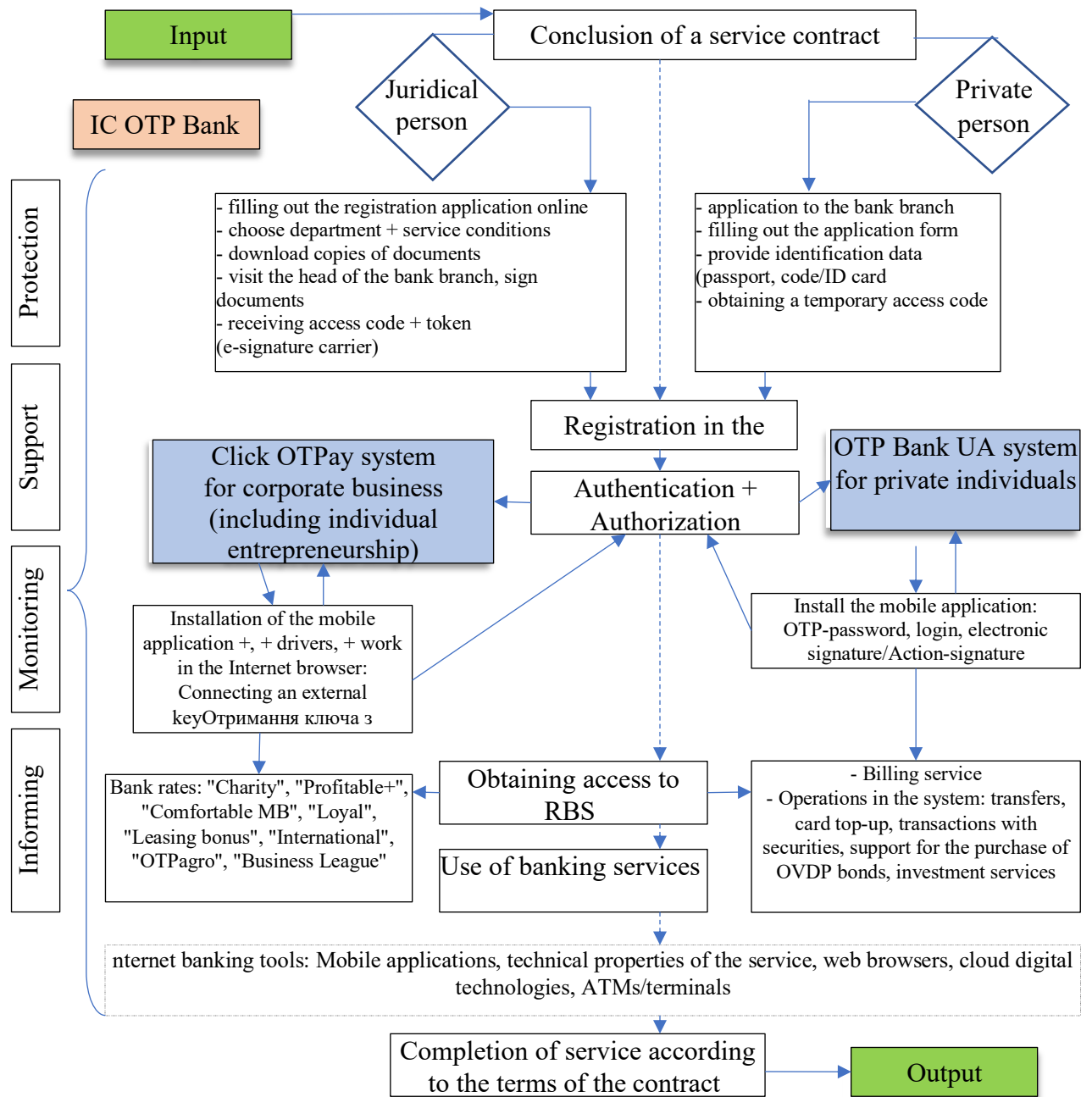


Fig. 2.5. Scheme of the mechanism of operation of the RBS of JSC "OTP Bank"

Source: Summarized by the author based on the data of JSC "OTP Bank"

System support is provided within the internet banking system, which includes a web browser, service technical features,

cloud and digital technologies, and mobile applications. Essential components of this mechanism are security (ensuring safety and confidentiality), monitoring, information dissemination, support, and additional remote service channels (ATMs, terminals, a help center, etc.). When clients register in remote access systems, download, and install mobile applications, they agree to the Terms and Conditions for Banking Services of JSC "OTP Bank," and are subject to the bank's remote banking service (RBS) policies. According to bank policies, a client's actions in registering within a remote access system or mobile application serve as acceptance of the Terms and Conditions for Banking Services, details of which are available on the bank's website. These Terms and Conditions, together with the Tariffs, constitute the remote service agreement with the client.

During martial law, problematic areas include the mandatory requirement to visit a bank branch to become a client, as online registration is currently unavailable. The OTP Internet Banking System serves as a remote banking system (RBS) for clients and acts as an official channel of communication (information exchange) between the bank and the client.

Access to the system can be achieved via a computer or through devices on iOS or Android platforms. The applications process 12 transactions per second, and over one million various banking operations are conducted daily by users of the online

and mobile versions.

To log in to the system online, users must navigate to <https://otpay.com.ua/ifobsClientSMB/ConnectingNewKey.action> (for legal entities) or <https://app.otpbank.com.ua/> (for individuals).

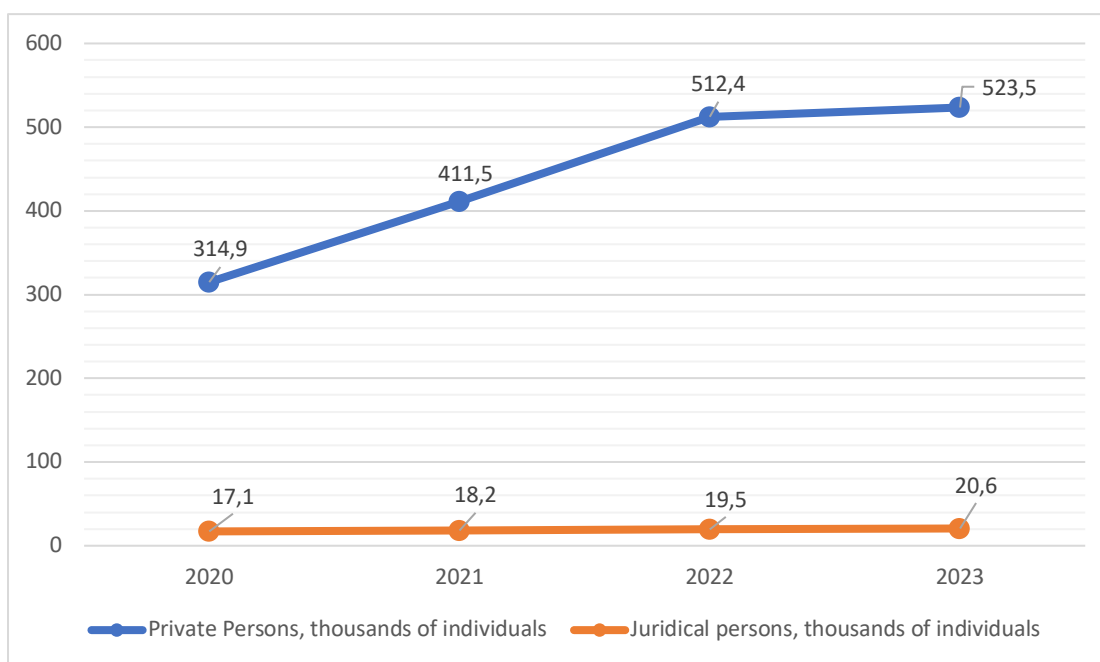


Fig. 2.6. The number of active users of the Internet Banking OTP system

Source: built by the author based on bank data [27]

For mobile access, users should download the app from Google Play or the App Store. The new OTP Bank UA app for individuals allows for service payments with cards from any bank worldwide, without needing an OTP Bank account. Available functions include viewing the loan repayment schedule and loan details, performing debt repayment transactions, checking card details, transaction history, card-to-

card transfers, mobile phone top-ups, utility payments, card activation/blocking, changing daily limits, viewing closed loans, and changing the static password for access to the OTP Bank UA system. There are no charges for individuals connecting to or using the account management tools within OTP Bank UA. The service rates for individuals are presented in Table K.1 of Appendix K.

Specific card rates and terms are provided in Appendix L, and rates for legal entities are determined by the bank's nine service categories: "Charity," "Profitable+," "Comfortable SMB," "Loyal," "Leasing Bonus," "International," "OTP Agro," "Business League." The OTP Bank UA mobile app allows users to turn their smartphones or tablets into universal payment devices. For contactless payments or ATM cash withdrawals, simply scan a QR code with the camera or hold the smartphone up to the terminal (for NFC-enabled smartphones).

To facilitate two-way communication between the bank and clients, OTP Bank JSC uses the following communication channels: SMS notifications, app notifications, postal letters, email messages, notifications at ATMs and self-service terminals, printed information on POS receipts, IVR calls, chatbot in the app (including chats with a personal manager through "Chat Sender"), and other mobile apps and communication tools.

Additionally, to reduce transaction processing time and costs for remote operations, the bank has established a

processing center equipped with modern server and technological equipment, encryption systems, and access control. Furthermore, premium clients holding co-branded cards like the OTP Tickets Travel Card, MasterCard Platinum, and others are offered 24/7 Private Banking services, along with personal manager assistance, personalized investment programs, and Mastercard airport services.

One of the primary methods is data encryption, typically involving SSL/TLS protocols, which secure data transfers and protect sensitive information from unauthorized access. Additionally, a rapid cloud migration of IT processes was executed within 45 days at the onset of the war, a remarkable achievement considering that, under normal circumstances, such a migration could take up to 1.5 years. This swift transition allowed for more resilient and secure management of critical banking data.

Beyond encryption and cloud solutions, the RBS mechanism incorporates multi-factor authentication (MFA), which adds an extra layer of verification to user identities, ensuring that access is granted only to authorized personnel. Regular security audits are also conducted to evaluate and strengthen system defenses. Moreover, mandatory training and upskilling programs for staff are implemented, emphasizing the importance of data protection and equipping employees with the latest cybersecurity practices. Detailed analysis of access rights and access logs is routinely

carried out, ensuring that permissions are appropriate and that any unauthorized access attempts are flagged. Finally, monitoring systems are in place to detect suspicious activities, providing real-time alerts to preempt potential security breaches and maintain a high level of vigilance within the RBS framework.

A significant factor is client protection, achieved through SMS alerts, transaction and limit management, and more (Figure 2.7).

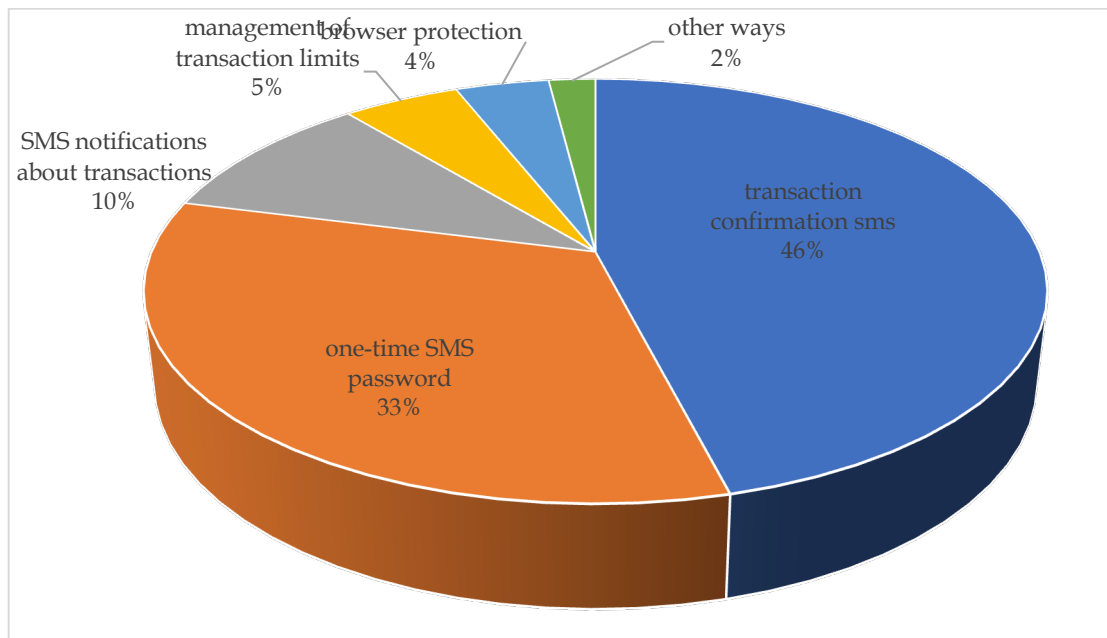


Fig. 2.7. The structure of the use of customer data protection methods in RBS, %

Source: summarized by the author based on the data of JSC "OTP Bank"

Evaluation of authentication procedures is important for ensuring the security of banking systems (Table 2.7).

The level of incomplete authentication procedures in the bank at the current stage – specifically, biometric authentication (85%) and monitoring of suspicious activities (95%) – is mainly

linked to heightened cybersecurity threats due to martial law, limited access to high-quality mobile devices among clients, and a satisfactory level of security systems that require further design and funding.

Table 2.7

Sample evaluation of authentication procedures of JSC
"OTP Bank"

No	Procedure	Description of the procedure	Rating	Performance level, %
1	Two-factor authentication (2FA):	The bank requires customers to enter not only a password, but also a one-time code that is sent to their mobile phones	Two-factor authentication is an effective method of protection because it requires two independent factors for access.	100%
2	Biometric authentication	The bank uses biometric data, such as a fingerprint or facial recognition, to verify the customer's identity	Biometric authentication can be very secure because it is difficult to forge biometric data. However, it is important to ensure that this data is protected from leakage.	85%
3	One-time passwords	Customers receive one-time passwords via SMS or special applications for each login to the system	This protection can be quite secure, but it is important that the passwords themselves and the process of their delivery are protected from attacks	100%
4	Monitoring of suspicious activities	The bank monitors customer activity and detects unusual actions, such as unsuccessful login attempts or account changes	Monitoring of suspicious activities allows timely identification of potential threats and response to them	95%

Source: summarized by the author based on the data of JSC "OTP Bank"

The implementation of quality remote banking services (RBS) at JSC "OTP Bank" was achieved through migrating operations to a cloud environment, allowing the bank to quickly adapt to ongoing uncertainty and ensure the sustainability of its investments through systems and solutions that offer flexibility, fast deployment, and functionality to meet regulatory deadlines.

Significant outcomes also included reduced costs, expanded operations, improved RBS functionality with faster updates, and enhanced services, ensuring profitable activity (Table 2.8).

Table 2.8

Direct indicators of the results of the operation of the RBS
of JSC OTP Bank, million hryvnias

№	Indicator	2021	2022	2023	Deviation 2023 to 2021		forecast 31.12. 2023
					+/-	%	
1.	Net interest income	4641	6807	6462	1821	139,2	8617
2.	interest income	5770	8788	9016	3246	156,3	12064
3.	interest expenses	1129	1981	2554	1425	226,2	3447
4.	Commission income	1990	1785	1404	-586	70,6	1863
5.	Commission costs	701	664	502	-199	71,6	671
6.	The result of foreign currency trading	99	784	465	366	469,7	601
7.	Other operating income	103	129	40	-63	38,8	50
8.	Administrative and other operating expenses	2781	8115	2675	-106	96,2	2675
9.	Net profit (loss) before taxation	3351	726	5194	1843	155,0	7785
10.	Net profit (loss)	2745	597	4249	1504	154,8	6384

Source: grouped by the author according to the financial statements of JSC "OTP Bank"

Significant achievements under wartime conditions have been made by the bank in stabilizing and increasing assets to UAH 93 billion, as indicated by the rising ROA rate of 4.62% in 2023. This success was largely driven by the implementation of innovative technologies based on the principles of maximum accessibility and user convenience of banking services.

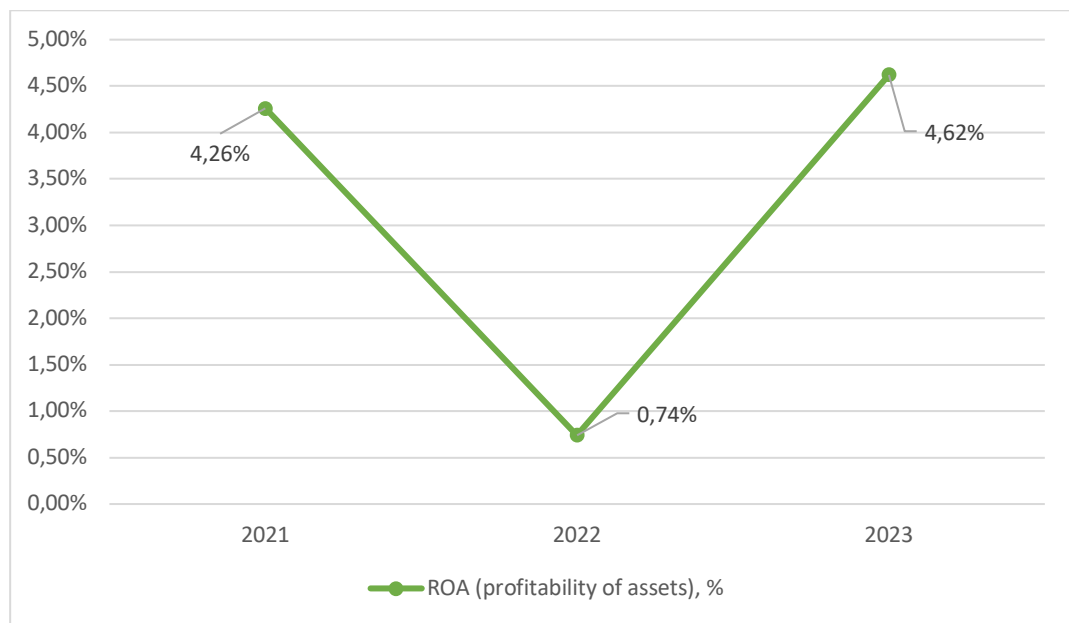


Fig. 2.8. Dynamics of indicators of profitability of assets of JSC "OTP Bank"

Source: grouped by the author according to the financial statements of JSC "OTP Bank"

According to Table 2.9, financial performance in 2023 significantly improved compared to 2021–2022. Interest income increased by 56.3%, while interest expenses grew by 2.3 times relative to 2021, resulting in a decrease in the profitability of these operations due to a faster increase in expenses over income. Commission income considerably exceeded expenses, enabling

a positive financial outcome due to high-quality remote services. The bank's profit for the first 8 months of 2023 reached UAH 4,249 million, an increase of 54.8% over the pre-war level.

The overall profitability level, reflecting the amount of profit per UAH of income (reaching UAH 5.72 profit in 2023 compared to UAH 0.88 at the start of the war in 2022), also demonstrates that the established income structure supports a trend of profit growth and reflects the effectiveness of provided remote services.

Observing other performance indicators of JSC "OTP Bank," we see positive growth trends (Table 2.9).

The net interest margin, which reached 7.03% in 2023, reveals not only the return on assets from the interest rate spread but also characterizes JSC "OTP Bank's" effectiveness in managing income-generating assets and low-cost resources. This spread is the primary source of revenue for maintaining liquidity and compensating for risks in credit, investment, and leasing operations. A reduction in the interest margin level increases the risk of banking operations and reduces the efficiency of managing interest-bearing transactions. Return on equity (ROE) reflects the bank's operational performance by assessing asset allocation efficiency, i.e., the assets' capacity to generate income. Data in Table 2.9 indicate that ROE grew by 5.45% between 2021 and 2023.

Table 2.9

Analysis of the profitability of JSC “OTP Bank”
for 2021-2023.

№	Indicator	2021	2022	2023	Відхилення 2023 до 2021, +/-
1.	General level of profitability	5,31	0,92	5,72	0,41
2.	Cost-to-income ratio	1,57	0,88	1,50	-0,06
3.	Net interest margin (return on assets)	7,21	8,47	7,03	-0,18
4.	Net spread (yield level of interest transactions)	9,66	14,48	16,94	7,29
5.	Other operating income (on average annual assets)	0,16	0,16	0,04	-0,12
6.	Return on assets, %	4,26	0,74	4,62	0,36
7.	Return on capital, %	26,61	5,26	32,06	5,45
8.	Cost effectiveness, %	59,53	5,55	74,14	14,61
9.	The ratio between commission income and commission expenses, units.	2,84	2,69	2,80	-0,04
10.	The ratio between total revenues and administrative expenses, unit	2,20	1,09	2,94	0,74

Source: grouped by the author according to the financial statements of JSC “OTP Bank”

The ratio of commission income to commission expenses shows a slight decrease of 0.04 units, indicating slightly higher commission expenses compared to the pre-war level. The ratio between total income and administrative expenses reflects a threefold coverage of administrative costs by total income, which we believe is substantially justified by the bank’s innovation

focus on technical support for financial service sales processes. This correlation suggests a relationship between OTP Bank's operational efficiency and its level of innovation implementation. To establish the links impacting the efficiency of OTP Bank's remote services under martial law conditions, a SWOT matrix has been prepared (Appendix M).

Thus, the bank's primary mission has become the creation and maintenance of a high-quality and advanced virtual banking environment that meets the needs and expectations of the modern customer, especially under current challenges and threats. The bank's remote servicing mechanism is currently quite effective, overcoming the challenges posed by the onset of the war in 2022. Problematic areas of the bank's remote services under martial law include cybersecurity (the increasing threat of cyberattacks and unauthorized access attempts, which risk clients' personal data and financial transactions), limited internet and mobile connectivity, service disruptions, and evolving customer needs.

Based on the analysis of JSC "OTP Bank" under wartime conditions, the following conclusions can be drawn.

Effective Asset Management. Through innovations and the transition of operations to a cloud environment, the bank has achieved stable asset growth and increased return on assets (ROA) to 4.62% in 2023. This indicates a balanced policy in managing income-generating assets, aligned with current

market needs.

Improvement of Financial Indicators. Despite rising costs and wartime challenges, the bank achieved significant profitability growth, evidenced by an increase in return on income to 5.72 UAH per 1 UAH of revenue in 2023. Commission income became a substantial source of financial support, covering most administrative expenses and strengthening financial stability.

Innovative Strategy. With the implementation of modern technologies, including mobile applications and remote services, the bank has significantly enhanced the functionality of its services. This also positively impacted the expansion of its client base, providing quick access to banking services even under wartime restrictions.

Cybersecurity Challenges and Infrastructure Issues. One of the most pressing concerns for the bank is the constant threat of cyber-attacks, which target sensitive data, disrupt operations, and threaten financial stability. This ongoing risk necessitates continuous updates and improvements in security systems to address emerging vulnerabilities. Enhanced monitoring systems are essential for promptly identifying and mitigating threats, as is strengthening access control to limit unauthorized access. To better protect clients' data, the bank invests in the development and refinement of sophisticated data protection protocols, staying up-to-date with the latest cybersecurity advancements.

Additionally, the war has introduced unique challenges, notably impacting the reliability of stable internet and mobile communications, which are crucial for daily operations and customer interactions. Consequently, the bank has prioritized the establishment and strengthening of alternative communication channels to ensure uninterrupted service and maintain connectivity with both internal staff and customers.

Strengthening Financial Resilience. In response to these unprecedented challenges, the bank has demonstrated remarkable financial resilience through adaptive measures and innovative approaches.

By optimizing operational processes and adjusting to the changing economic landscape, the bank has achieved substantial growth in both profit and capital profitability. This success highlights the effectiveness of the strategic decisions taken and underscores the importance of innovation in navigating and overcoming wartime obstacles.

The bank's positive financial performance serves as a testament to its robust risk management practices, commitment to stability, and dedication to upholding customer trust even in challenging circumstances.

Looking forward, JSC "OTP Bank" is actively investing in future-ready solutions to further enhance its operational resilience and client services. This includes expanding digital banking capabilities, increasing automation in key processes,

and exploring advanced technologies such as artificial intelligence for predictive analytics and risk assessment. These initiatives are not only aimed at streamlining operations and reducing response times but also at improving customer experience through personalized, efficient services. By focusing on long-term innovation and adaptability, the bank positions itself as a leader prepared to navigate and thrive amid future uncertainties, ensuring its ability to protect client interests and drive sustainable growth in any economic environment.

In conclusion, JSC “OTP Bank” exemplifies a high degree of adaptability and resilience in the face of wartime adversity. Through diligent efforts in cybersecurity, infrastructure improvements, and innovative financial strategies, the bank not only ensures its financial stability but also maintains operational efficiency and the quality of its customer service. This level of adaptability showcases the bank’s commitment to serving its clients reliably, underscoring its strong position within the financial sector despite the challenging environment.



CHAPTER III

MAIN DIRECTIONS FOR IMPROVING THE MECHANISM OF REMOTE BANKING SERVICES FOR CLIENTS OF UKRAINE IN JSC "OTP BANK" IN THE CONTEXT OF MODERN CHALLENGES AND THREATS

3.1. Directions for Countering Modern Threats in Remote Banking Service Systems

The operation of the remote banking service (RBS) system is associated with a number of issues, particularly security risks. The enhancement of banking services has led to client accounts and transactions becoming a prime target for cybercriminals, and the current RBS situation during martial law further complicates matters. This relates to the security of systems and transactions,

including data confidentiality, disclosure and modification of information, authentication, unlawful use, service refusal, and unavailability, resulting in significant threats like hacking attacks [33].

Typical examples of hacking attacks include viruses (spread via email or downloading infected files, potentially altering data on the user's computer and spying on confidential data), phishing (electronic fraud aimed at extracting user's confidential data through social engineering), and pharming (a sophisticated phishing attack redirecting users to fake banking websites by modifying DNS records), among others (Appendix).

The main reasons to stay vigilant regarding cybersecurity trends include: the rise in cashless transactions, which means more financial transactions than ever are digital; weak cybersecurity in the banking sector could jeopardize clients; the cost of recovery after a breach can be substantial and time-consuming. Awareness of cybersecurity risks has become an essential regulatory requirement for financial institutions in Ukraine (NBU Resolution No. 178 dated 12.08.2022 [7]). Today, banks are legally required to inform the NBU about any incidents that may impact the viability of their operations or their ability to provide services and products. They are also required to report any potential risks that may impact the stability of Ukraine's financial sector. These events include banking cybersecurity risks such as hacking, ransomware, and

distributed denial-of-service (DDoS) attacks. Similar regulations have also been implemented in the USA, UK, Europe, and Australia.

Some of the main cybersecurity challenges banks must overcome include: staff shortages, uninformed employees, insufficient budget allocation, credential-related vulnerabilities, and gaps in mobile banking apps, among others. For OTP Bank JSC, addressing these issues will be crucial in the future (Table 3.1).

Given the threat of cyberattacks on banking institutions, it is essential to train staff on the appropriate actions to take in such situations. Practical training should include simulations of cyberattacks, threat recognition, and situational case studies.

During the training, employees learn to avoid phishing, classify data, create complex passwords, ensure physical security, and understand cryptography, among other topics. Employee training provides dual benefits: they not only avoid risky behaviors but also become capable of identifying and reporting security issues before they escalate into full-blown breaches. Moreover, there is no room for dangerous practices regarding customer financial data.

User awareness training is a critical asset in the cybersecurity mechanism of online banking, depending on users' habits and behaviors. It is advisable to conduct training in the form of webinars or interactive seminars for greater effectiveness and the

opportunity to address participants' questions. Participants should include all consumers from various age groups, and training sessions for students and school pupils can be a good practice.

Table 3.1

Directions for solving the emerging cyber security problems of JSC "OTP Bank" for 2024, million hryvnias

No	Directions for solving cyber security problems	2023	2024	Effectiveness of influence, %
1	Overcoming the shortage of personnel (recruitment of qualified personnel, activation of outsourcing of managed security services)	40,8	154,9	10%
2	Acquire detection and response tools to help you be proactive and prevent attacks.	13,4	85,6	12%
3	Activation of quality consumer awareness programs so that customers do not disclose confidential information to cybercriminals. Use of social advertising.	10,2	35,7	15%
4	Conducting trainings for users of different age categories. Development and implementation of the "Financial Literacy and Cyber Protection" training for pupils and students, etc.	0	10,4	15%
5.	Use of corporate banners and screensavers to remind employees and service users about security issues, tips for best cyber security practices, examples of behavior	12,1	50,5	4%
6.	Training employees in the field of cyber security	50,6	96,5	11%
7.	Development of powerful mobile security systems	50,3	100,1	10%
8.	Bank account insurance service against cyber attacks	0	56,7	8%
9.	Implementation of a quality system of strict access control to confidential information. Functioning of the cyber protection control service.	12,4	44,7	15%
	In total	189,8	635,1	100%

Source: summarized by the author

Therefore, the main directions for ensuring the security and accessibility of online banking services during martial law

include implementing stringent security measures, enhancing staff training levels, introducing effective practical training for staff and clients on cybersecurity in online banking systems, activating backup systems, improving communication with clients and gathering feedback, supporting physical security through technical means, enhancing the internal cyber defense control department, and developing practical emergency response plans. Banks should devise contingency plans to address potential service disruptions in internet banking. This will help minimize financial instability risks for clients and ensure they have access to the financial services necessary for managing their finances during times of martial law or armed conflict.

The operation of the online banking system is fraught with various challenges, particularly concerning security risks. The enhancement of banking services has made customer accounts and transactions prime targets for cybercriminals, and the current conditions of martial law have exacerbated these vulnerabilities. Issues such as system and transaction security, data confidentiality, unauthorized access, and service disruptions pose significant dangers, including hacking attacks, which are prevalent in today's digital landscape.

Notably, the increasing prevalence of cashless transactions means that more financial operations are conducted digitally than ever before, highlighting the importance of robust

cybersecurity measures. Weak cybersecurity within the banking sector can jeopardize client safety, while the cost of recovering from breaches can be both substantial and time-consuming. As mandated by regulatory requirements in Ukraine, banks must inform the National Bank of Ukraine about any incidents that may impact their operational viability and the stability of the financial sector.

To mitigate these risks, banks must address key cybersecurity issues, including workforce shortages, employee ignorance regarding cyber threats, inadequate budgets for security measures, and vulnerabilities in mobile banking applications. For OTR Bank, tackling these challenges is critical to maintaining secure and reliable banking services.

Training staff in appropriate responses to cyber threats is paramount. Practical training should incorporate simulations of cyberattacks, threat recognition, and case studies to build resilience among employees. Such training not only helps avoid risky behavior but also equips staff to identify and report potential security issues before they escalate into breaches. Moreover, raising awareness among end-users is essential, as their habits and behaviors significantly impact cybersecurity. Interactive webinars and training sessions for consumers of all ages can enhance effectiveness and engagement.

In conclusion, the primary focus for ensuring the security and accessibility of online banking services amid martial law

includes implementing stringent security measures, enhancing employee training, and developing comprehensive emergency response plans. Banks should proactively address potential service disruptions, ensuring clients retain access to necessary financial services for managing their finances during periods of conflict. By prioritizing cybersecurity, financial institutions can protect their clients and maintain operational integrity in challenging times.

3.2. Prospects for the Development of Digital Banking as a Stage in the Development of the Bank's Remote Service Mechanism in the Context of Current Challenges

One of the main challenges of digital banking in a state of war is the security of customer data. Cyberattacks and data breaches can lead to significant financial losses and damage to the bank's reputation. To overcome this challenge, banks must invest in reliable security measures, such as end-to-end encryption, multi-factor authentication, and regular updates of security systems. Another challenge is the accessibility of digital banking services during wartime. In such circumstances, power outages or network disruptions may affect the availability of digital banking services. Banks must have backup plans and

alternative channels to ensure that customers can access their banking services even during such disruptions.

However, digital banking also opens up opportunities during wartime. As many people cannot leave their homes due to conflict, digital banking offers a convenient way for customers to manage their finances remotely. Banks can also use digital channels to communicate with customers, providing regular updates on their account status and the availability of banking services.

Furthermore, digital banking can help support financial inclusion in the economy during wartime. Many individuals may not have access to traditional banking services due to security risks or physical barriers. Digital banking enables these underserved populations to access essential financial services.

OTP Bank can also benefit from promoting a culture of innovation and entrepreneurship, which could foster the development of fintech startups and digital banking solutions. This would enhance competition in the banking sector, leading to improved service quality and lower costs for customers.

Comparing the foreign experience of digital banking system development with the domestic one, we can identify directions that will contribute to improving the organization of remote banking services for clients in Ukraine:

- Increasing customer awareness of new remote banking technologies and services;

- Developing online interaction channels;
- Implementing user-friendly interfaces in remote banking technologies;
- Building trust among individual customers in remote banking technologies.

For example, the decisive functions of online interaction channels include targeted interaction and quality service for customers; activating a cohesive digital platform for the bank; informing about news, promotions, and technologies; incorporating lead generation to attract new customers; and using social networks to perform HR functions and advertise banking products. It is also advisable for OTP Bank to develop its own direction for uniting people based on a social network or a bank forum focused on "People who know how to manage finances properly and protect their funds." Participation in and organization of various events and conferences for the business sector would also be beneficial.

As we can see, the development of electronic services and digital banking systems aims to eliminate the shortage of banking services, simplify access to financial services, and provide more convenient mechanisms for obtaining them, ultimately ensuring their availability to a larger number of clients. Thus, considering the rapid development of modern technologies, the widespread use of the Internet and mobile communications, as well as the increasing demand for digital

banking services, it can be confidently stated that remote banking services in Ukraine have very attractive and promising prospects.

The main prospects for the development of digital banking will be artificial intelligence (AI) and machine learning (ML). As cybercrime continues to become more sophisticated, banks are already implementing technologies that can keep pace with threats. AI and ML are among the technologies playing a crucial role in helping banks protect their systems and data from malicious attacks. One of the main ways AI and ML are currently used in banking cybersecurity is in threat detection and workforce enhancement (user behavior analytics (UBA), behavioral patterns, social engineering features, etc.). Thus, when scanning for potential patterns indicative of cybercrime, a wide range of red flags should be monitored. "Are people doing things outside their normal work? Is someone accessing files and folders they typically do not have access to? Are they searching for documents containing confidential information more frequently than usual?" Establishing baseline patterns in standard activity and identifying such deviations can be significant in preventing cybercrime. AI and ML can be critically important for detecting patterns that can then be utilized. They help conduct analyses more quickly and subsequently identify potential security incidents that need investigation more rapidly. However, this raises ethical questions. Issues may arise

regarding the automation of processes and replacing humans with robots, the absence of accountability for actions and decisions related to cybersecurity, including such an important principle as accountability (responsibility for cybersecurity measures, conducting cybersecurity audits, educating staff about their responsibilities regarding their own actions in the field of cybersecurity). The gradual development of AI and ML will allow OTP Bank in 2024-2025 to:

- Create predictive models to detect fraud and phishing schemes before they can cause harm;
- Perform natural language processing (NLP) to analyze large volumes of unstructured data;
- Develop AI-based systems to free up resources and fully automate routine security tasks, such as patch management and vulnerability scanning; detect money laundering to help banks meet regulatory requirements;
- Provide reinforcement learning, generative models, and other advanced methods used in areas such as fraud detection, anti-money laundering (AML), and customer behavior analysis.

It is worth mentioning a step towards enhancing the quality of the bank's digital environment, such as risk and loss coverage security, especially in a state of war in the country. Cyber insurance can serve as a protective measure for the clients of OTP Bank. Therefore, we believe that insurance against cyber threats

in remote banking services should ensure the improvement of the digital banking mechanism itself.

Cyber insurance is a specific insurance product that helps protect business owners from the consequences of cyberattacks and hacker threats. Cyber insurance is also known as insurance against cyber risks, data breach insurance, and cybersecurity insurance. The transfer of such risk is performed to the insurance company to assist individuals and legal entities (bank clients) in optimizing the impact of risk and compensating for losses.

Looking to the future, JSC “OTP Bank” is strategically investing in advanced, future-ready solutions designed to strengthen its operational resilience and enhance client services. One core area of focus is the expansion of digital banking capabilities, allowing customers to access a broader range of financial services from the convenience of their devices. By enhancing mobile banking platforms, the bank seeks to offer a seamless and user-friendly experience that enables clients to manage their finances, make transactions, and access support without needing to visit physical branches.

In addition to digital expansion, the bank is implementing increased automation across key processes, which not only improves efficiency but also reduces the potential for human error. Automation streamlines internal operations, accelerates response times, and allows employees to focus on more strategic and value-driven tasks, ultimately enhancing customer service.

Moreover, the bank is actively exploring the integration of artificial intelligence (AI) technologies for predictive analytics and risk assessment. By leveraging AI, the bank can gain deeper insights into market trends, customer behavior, and potential risks, enabling proactive decision-making and more accurate financial forecasting.

These initiatives reflect the bank's commitment to staying at the forefront of industry innovations. They are not only aimed at optimizing operations but also at creating a more personalized and efficient customer experience. Through digital transformation and cutting-edge technology, JSC "OTP Bank" is preparing itself to meet the evolving needs of its clients while maintaining a high standard of security and reliability. By embracing long-term innovation and a forward-thinking approach, the bank positions itself as a resilient leader equipped to navigate and succeed in an ever-changing economic environment. This commitment ensures the bank's capability to protect client interests, adapt to future challenges, and drive sustainable growth regardless of external uncertainties.

In summary, JSC "OTP Bank" exemplifies a forward-thinking approach and resilient adaptability, positioning itself as a robust player in the financial sector amidst ongoing challenges. Through significant investments in cybersecurity, innovative digital solutions, and employee development, the bank ensures a secure, efficient, and client-centered service model. Its strategic

focus on operational resilience and technological advancement not only fortifies its financial stability but also strengthens customer trust and satisfaction. By continuously adapting to the demands of an unpredictable environment, JSC "OTP Bank" reaffirms its commitment to sustainable growth, maintaining a high level of service quality and reliability that clients can depend on now and in the future.

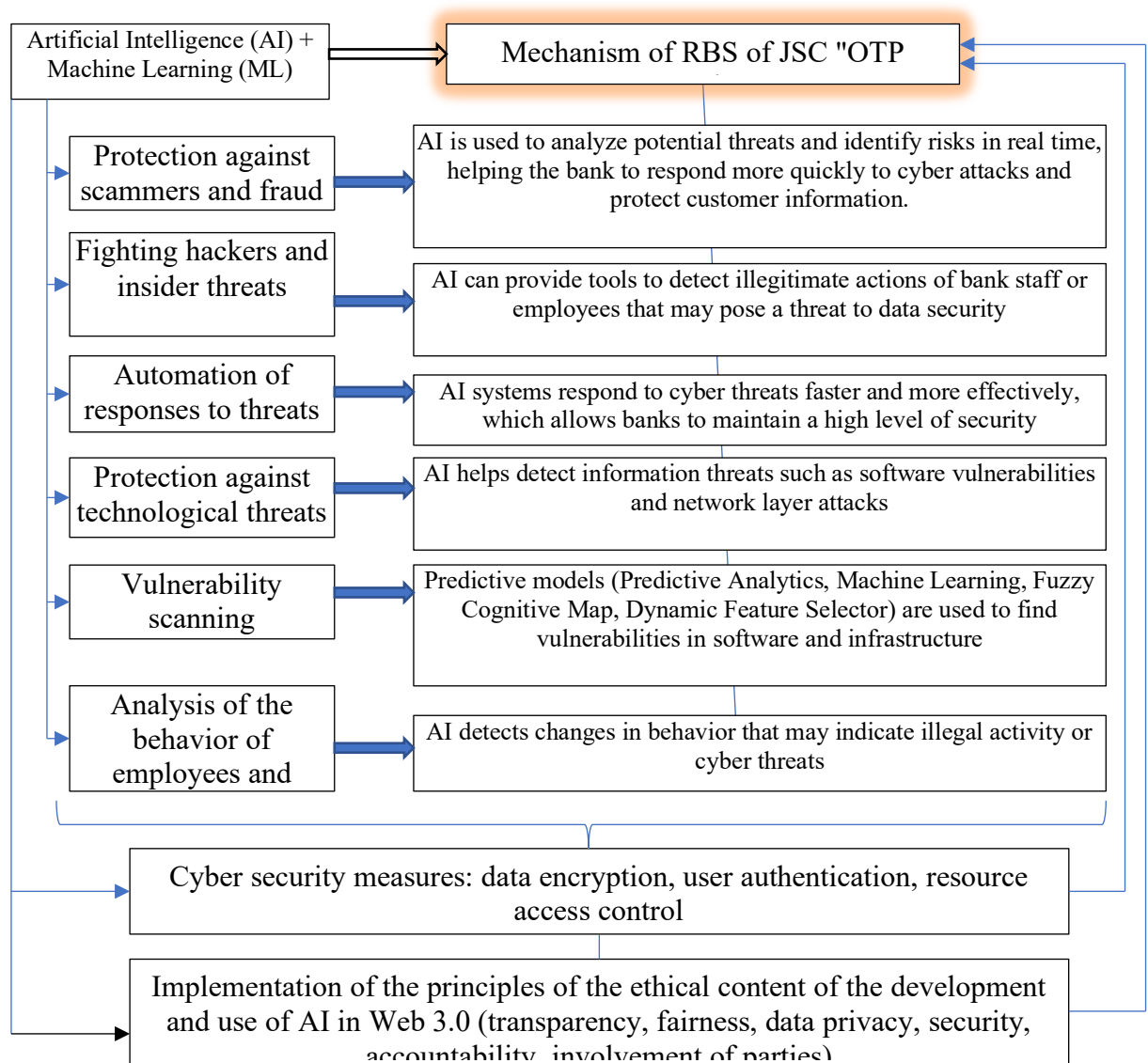


Fig.3.1. Areas of implementation of AI and ML in the RBS structure of JSC "OTP Bank"

Source: author's development

To enhance the effectiveness of this type of insurance, it is essential to focus on the risk of extortion for clients, particularly phishing (transferring funds to fraudsters' accounts under pressure, internet extortion, payment site spoofing), telephone fraud (vishing), and withdrawal of funds from lost/stolen cards, among others. We propose a possible scheme for the bank client's cyber insurance as follows (see Fig. 3.2). The cyber insurance policy is formed electronically online.

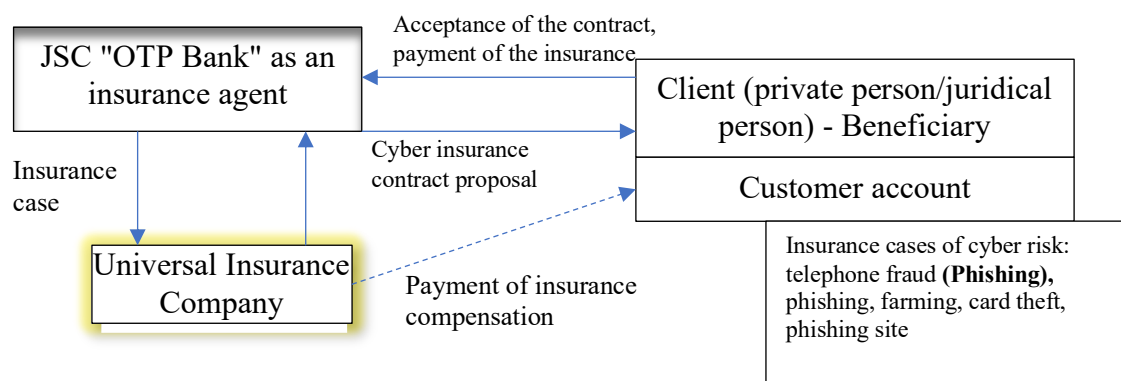


Fig. 3.2. Cyber Insurance Scheme for Client Account Protection Against Phishing

Source: Author's Development

To support clients, an effective solution would be to activate a chatbot in Telegram or the OTPBank.UA mobile app based on AI, with its primary task being to guide clients and act in emergency situations. This AI-driven chatbot could answer frequently asked questions, assist in routine transactions, and provide immediate support around the clock. In critical situations, such as temporary service disruptions or security concerns, the chatbot could offer real-time alerts and instructions

to help clients navigate challenges seamlessly. Such a solution would not only enhance customer convenience but also strengthen the bank's responsiveness and reliability in supporting clients whenever they need assistance.

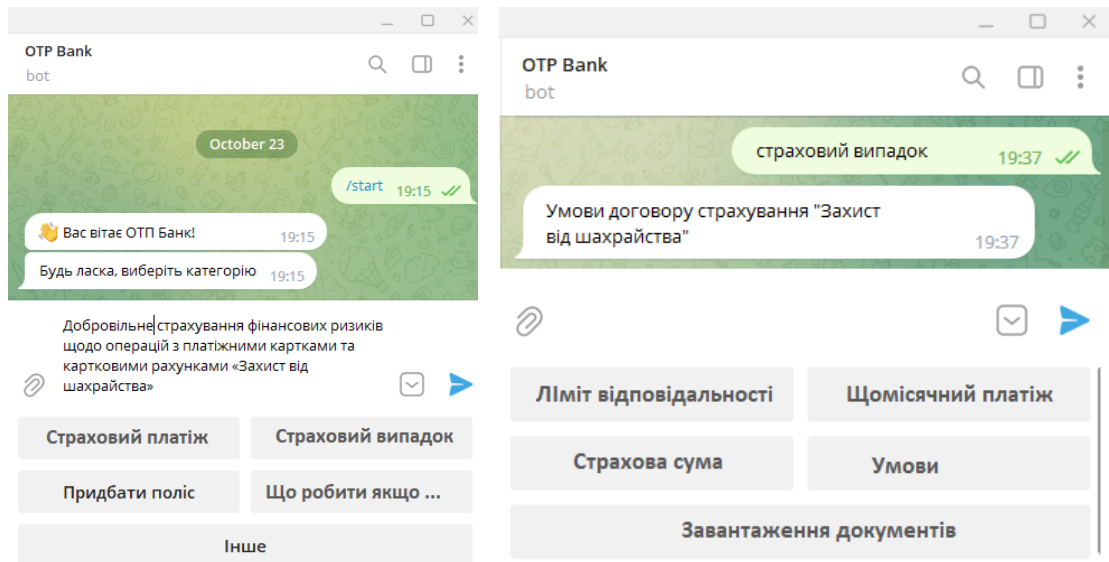


Fig. 3.3. Chatbot Interface for Client Services in Cyber Insurance

Source: Author's Development

Thus, OTP Bank should flexibly adjust its policies based on emerging opportunities, emphasizing its strengths. Through innovative technologies, OTP Bank creates new products and enhances its services. User demands are increasing, and technologies are advancing. Ideas and solutions that were optional additions to the core program just a few years ago have now become an integral part of the bank's standard operations in the digital environment.

3.3. Improving the Mechanism of Remote Banking Services in JSC "OTP Bank"

The following strategy could enhance the mechanism of remote banking services at OTP Bank:

1. Transitioning Most Remote Services to the Mobile Application.
2. Registering New Users Without Physically Visiting the Bank Branch (based on digital signatures and electronic identification through the "Diia" system).
3. Customer-Centric Orientation (educating and acquiring practical skills for managing the mobile application, creating cyber protection insurance programs, expanding the range of services, such as creating youth cards Unik-OTP for children aged 6 to 17).
4. Effective Advertising Campaign for the Innovative Brand and Updated Service (promotion, lead generation, targeted advertising on social media, developing a quality chatbot based on AI and ML, release, reinforcement – focusing on payment card services, financial planning and management, investment business services, and account insurance against cyber threats). Regarding the specifics of providing insurance against cyberattacks, we propose the following stages for insuring consumer bank accounts.

Table 3.2

Stages of cyber insurance for clients at JSC "OTP Bank"

Stage	The name of the stage	Description
1	Definition of coverage	the amount that the client wishes to insure is determined. This could be the total balance in his bank account or the specific amount he wishes to insure
2	Choice of Insurer	to choose an insurance company that offers bank account insurance services, it is also worth considering the experience and reputation of the insurance company in the specified field
3	Conclusion of the Agreement	signing a tripartite cyber insurance agreement (OTP Bank JSC - Insurance agent, SC - Insurer, natural/legal entity, beneficiary - Insured), with defined conditions, premiums and coverage volumes
3.1	Regular Awards	determination of regular premiums that the client must pay for insurance. This amount can be monthly or yearly
3.2	Terms of Payments	determining the conditions under which the insurance company will pay compensation. For example, in case of unauthorized access or fraudulent activity on the account
4	Regular risk assessment	regularly assess risks and update insurance conditions, if necessary (updated annually).
4.1	Continuous training of clients	the client's completion of the "Prevention and Counteraction of Cyber Threats from Fraudsters" training, passing the test (based on the results of the test, a risk factor can be formed to form the amount of insurance payments).
4.2	Customer support	providing affordable and high-quality customer support for solving insurance issues. Reminders of current threats, examples of phishing attacks (video message to the client based on the Telegram channel) and talking about the content of the client's behavior in case of a phishing threat.
4.3	Informing the Client	explaining to the client all the details and conditions of cyber insurance, including how he can submit a claim for payment, about the time frame in which the client must apply for an insured event (within 24 hours from the moment of detection of illegal transactions).

Source: developed by the author

This scheme helps consumers protect their bank accounts from risks and unforeseen financial losses, while providing the

bank with quality services for its clients. The options for the cyber insurance program are presented in Table 3.3.

Table 3.3

Options for Cyber Insurance Programs Against
"Phishing" Risk

Insurance conditions	Program 1	Program 2	Program 3
Sum insured, hryvnias	50,000	100,000	200,000
Insurance tariff (annual), %	0.83%	0.83%	0.83%
Annual insurance payment, UAH	415 hryvnias	UAH 830	1660 hryvnias
Monthly insurance payment (1/12 of the annual insurance payment), UAH	UAH 35	UAH 69	138 hryvnias
The amount of the Insurer's liability for one insured event from the risk of "Phishing"	UAH 35,000	UAH 70,000	140,000 UAH
The amount of the Insurer's liability for one insured event from a risk other than "Phishing"	10,000 UAH	UAH 20,000	UAH 40,000
Insurer's limit for the maximum number of insurance cases of "Phishing" risk	1 insurance case	1 insurance event	1 insurance case
Insurer's limit for the maximum number of insured events for a risk other than "Phishing"	there is no limit	there is no limit	there is no limit
Mandatory completion of the client's annual training "Prevention and Counteraction of Cyber Threats by Fraudsters"	free	free	free
Client testing, setting the insurance payment adjustment factor, %	0.85-2.0	0.80-2.3	0.80-2.5
Correction of the monthly insurance payment (1/12 of the annual insurance payment), UAH	UAH 29 - UAH 70	UAH 55 - UAH 159	110 UAH - 3818 UAH

Source: developed by the author

We believe that the motivational component in forming the monthly insurance amount (through a test) will help reduce the risk of an insurance incident and allow the client to become more aware of potential threats. The main tools for the advertising campaign should include campaigns in the Google Display Network (GDN), video campaigns in AdWords, Instagram, and Facebook; media campaigns in Instagram and Facebook; optimization of relationships in the App Store and Google Play; remarketing campaigns; and promotion in social networks. The stages and duration of advertising activities for the forecast period can be established as follows (see Figure 3.4).

Such directions for improving the activities of remote banking services require appropriate investment decisions, which should be grouped as follows (see Appendix R).

The conditions of war can significantly affect the determination of the discount rate for investment projects. The discount rate is determined based on risks and expected returns, and in wartime, these risks can be significantly higher. Therefore, we will set the discount rate at 35% (the minimum profit norm). This elevated rate reflects the heightened uncertainty and additional risk factors that investors face in such volatile conditions. Setting a higher discount rate helps ensure that projects are only pursued if they offer returns sufficient to compensate for these increased risks, thereby protecting the bank's financial stability.

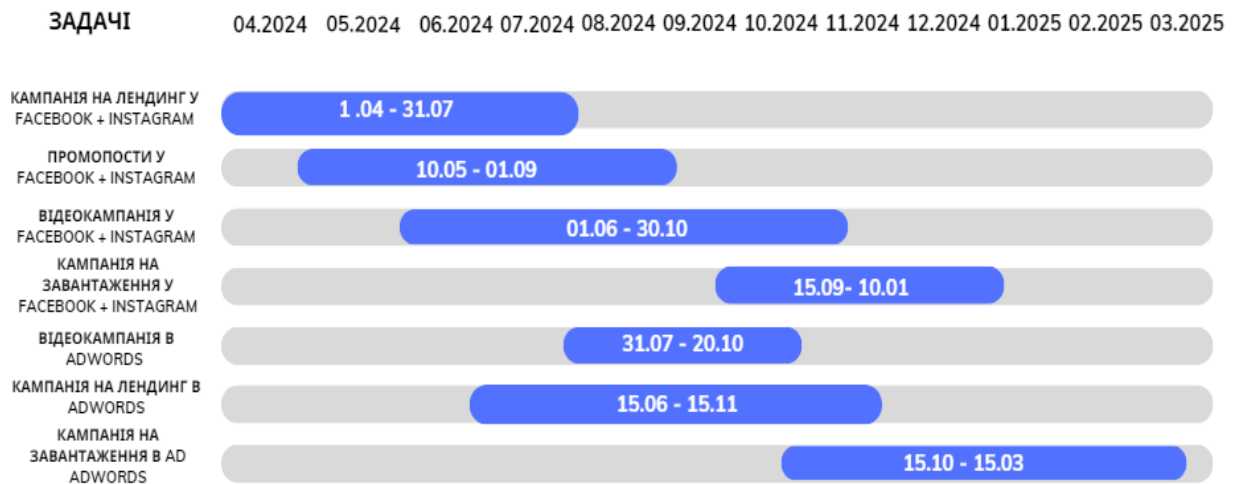


Fig. 3.4. Stages and duration of advertising activity of JSC "OTP Bank"

Source: generated by the author

The total amount of discounted cash flow from improving the remote banking services mechanism at OTP Bank for the years 2024-2027 is projected to be 1,853 million UAH. The effectiveness of the project will be assessed based on discounting indicators considering the forecast of revenues and expenses

The total amount of discounted cash flow from improving the remote banking services mechanism at OTP Bank for the years 2024-2027 is projected to be 1,853 million UAH. This calculation reflects expected cash inflows generated by enhancing remote services, such as increased client engagement, transaction volumes, and reduced operational costs associated with traditional banking. The effectiveness of the project will be assessed using key discounting indicators, which take into account projected revenue streams and anticipated expenses

over the investment period (see Table 3.4). By evaluating metrics like Net Present Value (NPV) and Internal Rate of Return (IRR), the bank can determine if the projected returns exceed the cost of capital and meet financial targets. Additionally, this assessment allows OTP Bank to measure the strategic impact of digital service improvements, ensuring that the investment aligns with long-term growth objectives and enhances customer satisfaction in an increasingly digital banking environment.

Table 3.4

Forecast of income and expenses based on the improvement of the RBS mechanism of JSC "OTP Bank"

Indicators	2023	2024	2025	2026	2027	Deviation 2024 to 2023, %
Net interest income	8617	9953	11440	12776	14030	115,5
interest income	12064	14296	16869	19399	22309	118,5
interest expenses	3447	4343	5429	6623	8279	126,0
Commission income	1863	2262	2804	3393	4004	121,4
Commission costs	671	832	998	1238	1535	124,0
The result of foreign currency trading	601	709	816	979	1174	118,0
Other operating income	50	55	69	86	107	110,0
Administrative and other operating expenses	2675	4083	3874	4726	5766	152,6
Net profit (loss) before taxation	7785	8064	10257	11270	12015	103,6
Net profit (loss)	6384	6612	8410	9241	9852	103,6

Source: grouped by the author according to the financial statements of JSC "OTP Bank"

The net present value (NPV) will be:

$$NPV = \sum_{i=1}^n \frac{CF_i}{(1+d)^i} - \sum_{i=1}^n I_i \quad (3.1)$$

where CF_i - net cash flows in the i -th year, I_i - investment

costs, d – discount, i – settlement period, n – number of years.

$$\text{Profitability index (PI): } PI = \frac{\sum_{i=1}^n \frac{CF_i}{(1+d)^i}}{I_i} \quad (3.2)$$

If the available profitability of the project is 1.17 is greater than one, the reduced revenues are equal to the reduced costs, which determines the effectiveness of the project and can be accepted as profitable. As a result, the internal rate of return (IRR) will be set at the level of 244.8%.

$$IRR = d_1 + NPV_1 \frac{d_2 - d_1}{NPV_1 - NPV_2} \quad (3.3)$$

where, NPV_1 and NPV_2 – it is the net present income from different discount rates

$$\text{(under conditions } NPV_1 > NPV_2) \quad (3.4);$$

d_1 and d_2 – discount rates (under conditions $d_1 < d_2$).

$NPV_1 =$ UAH 908 million, with $d_1 = 35\%$; $NPV_2 = -21.9$ million hryvnias, with $d_2 = 250\%$.

(%)

The calculated rate of return exceeds the discount rate (35%) and the bank loan rate (36.9%), which indicates that the investment project is profitable. And the difference of $244.8\% - 35\% = 209.8\%$ shows the strength of this investment project.

The payback period (DPP) of the proposed project will be set at

$$DPP = j + \frac{\sum_{i=1}^n I_i - C_j}{CF_{j+1}/(1+d)^{j+1}} = \quad (3.5)$$

$$DPP=2+(1358,5 - 1262,9) / 1189,3 =2,1 \text{ years (or 2 years)}$$

After completing the financial analysis, the project's net reduced cost has been determined to be uah 908 million, indicating a positive net present value (npv) and highlighting the project's effectiveness and value generation potential. An NPV greater than zero is a fundamental measure of investment attractiveness, signifying that the project is expected to yield returns beyond the initial outlay and generate value for the stakeholders. This outcome is particularly favorable, as it reflects the project's ability to exceed the discount rate and deliver net benefits over time.

The project's profitability index has been calculated at 1.17, indicating that for every hryvnia invested, there is a return of 1.17 uah. This ratio of 1.17 signifies a 17% gain on each unit invested, demonstrating a solid annual profit margin. Such a return rate is attractive, as it confirms the project's capacity to produce consistent income relative to the investment, thereby bolstering the case for its implementation. This profitability index not only meets but also exceeds common financial thresholds, reinforcing confidence in the project's financial viability.

Another key aspect of the project's feasibility is its payback period, which has been calculated at two years. This payback period represents the time needed for the project to recoup the

initial investment, and in this case, it aligns with the bank's requirements for timely capital recovery. A two-year payback period is generally deemed efficient for projects within the banking sector, as it minimizes financial exposure and ensures that the invested capital can be redirected relatively quickly if needed. The short payback period not only reduces risk but also enhances the liquidity profile of the bank by allowing faster reinvestment of returns into other potentially profitable ventures.

In sum, the project demonstrates a strong financial position characterized by a high npv, a favorable profitability index, and a rapid payback period. Together, these indicators suggest that the project will contribute positively to the bank's profitability and align with strategic investment goals. Given the calculated returns and acceptable recovery period, the project is well-positioned to proceed, and its implementation would likely yield sustainable and significant value for the bank.



CONCLUSIONS

Based on the research on the topic: "The Mechanism of Remote Banking Services in the Context of Modern Challenges and Threats," we have formulated the following conclusions and outlined possible recommendations.

Remote Banking Services (RBS) are a type of banking services provided by financial institutions remotely, or the processes through which a bank creates its product and offers it to clients via remote access. RBS classification should be conducted based on: (a) the type of service subjects (for corporate and individual clients); (b) the system's operation principle (online and offline systems); and (c) the type of information systems and technologies used (e.g., POS banking, Internet banking, mobile banking, SMS banking, video banking, telephone banking, ATMs, online services).

1. In the face of economic threats and warfare, remote banking services play a crucial role in supporting financial system stability and providing individuals and entities access to and control over their financial assets. By offering a secure and

reliable method for conducting financial transactions, online banking can mitigate the adverse economic effects of conflicts and instability, ensuring essential financial services remain accessible. However, during wartime, RBS encounters a range of challenges, including security issues, limited access, and operational difficulties.

2. Remote Banking Services represent a vital mechanism that enables financial transactions amid economic threats and military conflicts. The purpose of this mechanism is to provide individuals and entities with secure and reliable access to their financial assets, even when physical access to bank branches may be limited or impossible. The tasks of RBS include facilitating electronic transactions such as money transfers, bill payments, and online shopping, as well as providing account management tools such as balance inquiries, transaction history, and investment tracking. Online banking platforms also typically offer security features, such as multi-factor authentication, encryption, and fraud detection, to protect against cyber threats and unauthorized access. The acceleration of RBS development in Ukraine during wartime was influenced by factors such as forced population displacement, international travel (supporting those remaining in the country), workforce reduction, branch closures (safety and cost optimization), and economic resilience through online transactions, government support programs, and blockchain technology advancements.

3. In 2023, the number of operating banks during wartime decreased by 9.2%, reaching 65 banks, of which only 51 provide remote banking services (78.5%). Leading RBS providers include Alfa Bank, PrivatBank, Monobank | Universal Bank, A-Bank, OTP Bank, PUMB, and Oschadbank. Key components of RBS in Ukraine during wartime included a 20% reduction in the bank branch network and parallel recovery efforts via remote access; technological solution development; operational stability maintenance under high transaction volumes, especially in card-based transactions, as required by regulatory bodies; retention of depositor trust; and ensuring uninterrupted operation of branches, ATMs, POS terminals, and data centers during blackouts.

4. At OTP Bank, RBS accounts for 85% of its services. Despite wartime conditions, the bank continues to lend to the economy, serves both corporate and retail segments, and invests actively in digital client services and IT. The foundation for OTP Bank's RBS includes software solutions (web portal www.otpbank.com.ua, mobile apps OTP Smart and OTP Bank UA), a robust authentication system, fraud prevention cybersecurity, and clear service rules and agreements. In 2023, the volume of payment card operations at OTP Bank reached UAH 270.3 billion, which is 8.15% lower than pre-war levels; however, this volume is projected to grow by 44.9% by the year's end due to increasing consumer demand, new remote banking

services, and the growing popularity of the bank.

5. The RBS mechanism for bank clients starts with client registration, determined primarily by whether the client is an individual or a legal entity: signing an RBS agreement, registering in the client-bank system (with differences for individuals and legal entities, including sole proprietorships), passing the authentication procedure, and obtaining access to banking services (based on bank tariff packages). Security in the RBS mechanism is ensured through data encryption protocols (such as SSL/TLS), cloud-based IT process management, multi-factor authentication, security audits, mandatory employee training on data protection, access rights analysis, monitoring for suspicious or unauthorized actions, etc.

6. Key directions for ensuring the security and accessibility of RBS under wartime conditions include: strict security measures, enhanced staff training, effective practical training for staff and clients on cyber protection in online banking, the activation of backup and redundancy systems, improved client communication, feedback generation, physical security support via technical means, internal cyber protection control unit enhancement, and the development of practical emergency response plans.

7. The main prospects for digital banking development include Artificial Intelligence (AI) and Machine Learning (ML). As cybercrime becomes more sophisticated, banks are

implementing technologies that can keep pace with emerging threats. AI and ML are crucial in helping banks safeguard their systems and data from malicious attacks. Among the primary applications of AI and ML in banking cybersecurity are threat detection and staff empowerment (e.g., user behavior analytics (UBA), behavioral models, social engineering recognition, etc.).

8. Key ways to improve OTP Bank's RBS mechanism include: transferring most remote services to the mobile app; new user registration without visiting a physical branch (using digital signatures and electronic identification through the "Diia" system); customer-centric service orientation (education and practical training on mobile application management, cyber insurance programs, expanded service offerings); and effective marketing campaigns (promotion, lead generation, targeted social media advertising, developing a quality AI- and ML-based chatbot). The project assessment is effective and feasible for consideration and implementation.



REFERENCES

1. Law of Ukraine on Banks and Banking Activities (2000). Law of Ukraine No. 2121-III of December 7, 2000 (as amended on July 29, 2023). URL:

<https://zakon.rada.gov.ua/laws/show/2121-14#Text>

2. Law of Ukraine on Payment Services (2021). Law of Ukraine No. 1591-IX of June 30, 2021 (as amended on April 1, 2023). URL:

<https://zakon.rada.gov.ua/laws/show/1591-20#Text>

3. Law of Ukraine on Financial Services and State Regulation of Financial Services Markets (2001). Law of Ukraine No. 2664-III of July 12, 2001. URL:

<http://zakon1.rada.gov.ua/laws/show/2664-14>

4. Law of Ukraine on Consumer Lending (2016). Law of Ukraine No. 1734-19 of November 15, 2016 (as amended on July 2, 2023). URL:

<https://zakon.rada.gov.ua/laws/show/1734-19#Text>

5. Law of Ukraine on Personal Data Protection (2010). Law of Ukraine No. 2297-VI of June 1, 2010 (as amended on October 27, 2022). URL:

<https://zakon.rada.gov.ua/laws/show/2297-17#Text>

6. Law of Ukraine on Electronic Documents and Electronic Document Flow (2003). Law of Ukraine No. 851-IV of May 22, 2003 (as amended on August 1, 2022). URL:

<https://zakon.rada.gov.ua/laws/show/851-15#Text>

7. Resolution of the NBU on Approving the Regulation on the Organization of Cybersecurity in the Banking System of Ukraine (2022). NBU Resolution No. 178 of August 19, 2022. URL:https://bank.gov.ua/admin_uploads/law/12082022_178.docx?v=4

8. Instruction on Cashless Payments in National Currency for Payment Service Users (2022). NBU Instruction No. 163 of July 29, 2022. URL:

<https://zakon.rada.gov.ua/laws/show/v0163500-22#Text>

9. Abramova, A.S. (2021). Remote Service for Legal Entities by Commercial Banks in Ukraine. Problems of Modern Transformations. Series: Economics and Management, 2, 53-61.

10. Aleksandrova, M.M., & Maslova, S.O. (2015). Money. Finance. Credit: Educational Manual (2nd ed.). Kyiv: TsUL, 110-136.

11. Artemieva, I.O., & Zalyubovska, S.S. (2023). Digital Transformations in the Banking Sector. Scientific Herald of the

National Academy of Statistics, Accounting and Audit, 1-2, 96–103.

12. Bank Management: Textbook (2015). Edited by O.A. Kyrychenko, V.I. Mishchenko. Kyiv: Znannia, 831 p.

13. Banking Operations: Textbook (2019). Edited by Doctor of Economics, Prof. O.V. Dziublyuka. Ternopil: TNEU Publishing House "Economic Thought," 696 p.

14. Baryshevska, I.V., & Syzyonenko, Y.S. (2021). Artificial Intelligence in the Banking Sector under Globalization. Accounting and Analytical Support for Business Entities: National, Global, Eurointegration Aspects: Proceedings of the VI International Scientific and Practical Conference, Mykolaiv, 87–91.

15. Zveryakov, M.I., & Masliy, V.V. (2023). Internet Banking in EU Countries: Trends and Perspectives. Imperatives of Economic Growth in the Context of Global Sustainable Development Goals: Proceedings of the International Scientific and Practical Conference. Kyiv: KNUTD, 165-168.

16. Zaslavska, O.I. (2020). Virtual Banking: Challenges and Prospects. Business Inform, 4, 350-356.

17. Zvaryakov, M.I. (2019). Managing Financial Stability of Banks: Textbook. Kyiv: TsUL, 520 p.

18. Zayachkivska, O.V. (2023). Financial Security of the Banking Sector of Ukraine. Bulletin of the National University of

Water Management and Nature Management. Economic Sciences, 1, 33-41.

19.Ivashchuk, O. (2021). Innovations in Internet Banking of Ukrainian Commercial Banks during the Covid-19 Pandemic. Socio-Economic Problems and State, 2, 575-585.

20.Karcheva, H.T. (2020). Effectiveness and Competitiveness of the Banking System of Ukraine: Monograph by Doctor of Economic Sciences; edited by Doctor of Economic Sciences H.T. Karcheva. Kyiv: DSVNZ "University of Banking," 279 p.

21.Kovalchuk, K.F. (2022). Banking Operations: Educational Manual. Kyiv: TsUL, 162 p.

22.Kopylyuk, O.I. (2020). Banking Operations: Educational Manual. Kyiv: TsUL, 536 p.

23.Kuchanskyi, O.Yu. (2019). Prospects for the Development of Remote Banking Service Systems in Ukraine. Management of the Development of Complex Systems, 23(1), 115-119.

24.Laryonova, K.L. (2021). Remote Banking Services: Essence and Current Implementation State in the Banking Market of Ukraine. Bulletin of Khmelnytsky National University. Economic Sciences, 6(1), 280-287.

25.Ladkovska, T. (2021). Legal and Theoretical Problems of Defining Internet Banking in Ukraine. Financial and Credit Activity: Problems of Theory and Practice, 1, 27-34.

26.Lysyak, O.M., & Sahaidak, O.M. (2021). Reality and Prospects of Internet Banking as a Direction of Digitalization in

Ukraine. Scientific Notes of the National University "Ostroh Academy". Series: Economics, 21, 76-81.

27. Minyaylo, O.I., & Pokanevich, V.Yu. (2023). Competitive Policy in the Retail Banking Services Market. Investments: Practice and Experience, 4, 79-83.

28. Mishchenko, V.I., & Naumenko, S.V. (2019). Features of Banking Marketing Innovations under Uncertainty and Information Asymmetry. Black Sea Economic Studies, 46-2, 83-89.

29. Moskalyov, A.A. (2018). Internet Banking as a Development Direction for Banking Services. Young Scientist, 11(2), 1172-1175.

30. Nakonechna, A.V. (2023). Control of Bank Activity Stability during Hostilities in Ukraine. Scientific Herald of Uzhhorod National University. Series: Law, 78(2), 83-89.

31. Prasolova, S.P. (2022). Banking Operations: Educational Manual. Kyiv: TsUL, 568 p.

32. Prystiuk, L.A. (2017). Banking Management: Innovative Concepts and Models: Monograph. State Higher Educational Institution "Kyiv National Economic University named after Vadym Hetman." Kyiv: KNEU, 380 p.

33. Prystiuk, L.A. (2023). Artificial Intelligence Technologies in Banks: Prospects and Cautions. International Scientific Journal "Internauka." Series: Economic Sciences, 4(2), 36-39.

34. Prokofieva, O.V. (2023). Development of the Banking Sector of Ukraine under Martial Law. *Investments: Practice and Experience*, 8, 108-112.

35. Radionova, N.Y. (2018). Payment Operations using Remote Banking Services: Advantages and Disadvantages. *Effective Economy*, 2, 20-24.

36. Ruda, O.L. (2020). Remote Service in the Banking System. *Market Infrastructure*, 39, 353-358.

37. Tishchenko, O.I. (2021). Overview of Current Trends in the Online Banking Market in Ukraine. *Economy and Society*, 13, 1237-1243.

38. Tkachenko, O.Ye. (2022). Transformation of Financial Management in the Banking Sector of Ukraine during the War. *Scientific Notes of the National University "Ostroh Academy."* Series: Economics, 27, 73-80.

39. Tomarovych, T. V. Risk-oriented approach to managing financial flows of banks: global practice and the experience of Ukraine. *Business Inform*, 2023, No. 6, pp. 171-178.

40. Sapon, R. V., & Shamov, S. O. Improving client identification technologies during remote banking services. *Financial and Credit Activity: Problems of Theory and Practice*, 2021, Iss. 2, pp. 142-151.

41. Snishtenko, R. H. Directions for implementing banking innovations. *Transformational Economy*, 2023, No. 2, pp. 53-56.

42. Kostiuk, V. A., Stepanenko, Ya. O., & Faichuk, O. V. (2023). Development of digital banking in the structure of the remote service mechanism of banks under martial law conditions. *Economics and Business Management*, 14(4), 54-68. URL:

<http://journals.nubip.edu.ua/index.php/bioeconomy/article/view/48648>

43. Yashchuk, O., Hevko, I., Savchyn, T., & Hiltai, L. Cybersecurity in a decentralized internet ecosystem web 3.0. *Scientific Notes of the Ternopil National Pedagogical University named after Volodymyr Hnatyuk. Series: Pedagogy, Ternopil: Ternopil National Pedagogical University named after V. Hnatyuk*, 2023, No. 1, pp. 61-68.

44. Anjali, K. Digitalization in Banking: Convenience versus Security Threat. *Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019.* URL: <https://ssrn.com/abstract=3358058>

45. Chaimaa, B., Najib, E., & Rachid, H. E-banking Overview: Concepts, Challenges and Solutions. *Wireless Personal Communications*, 2021, 117(2), 1059-1078. URL: <https://doi.org/10.1007/S11277-020-07911-0>

46. Furton, G., & Martin, A. Beyond market failure and government failure. *Public Choice*, Springer New York LLC, 2019, Vol. 178, No. 1-2, pp. 197-216.

47. Westerman, G., Soule, D. L., & Eswaran, A. Building Digital-Ready Culture in Traditional Organizations. *Summer 2019 Issue Research Feature*, 2019, May. URL: <https://sloanreview.mit.edu/article/building-digitalready-culture-in-traditional-organizations>.

48. Banking-as-a-Service Market Size, Share & Trends Analysis Report by Product Type (API-, Cloud-based BaaS), by Component (Platform, Services), by Enterprise Size (Large, SME), by End-use (Banks, NBFC), and Segment Forecasts, 2022 – 2030.

49. Kumari, A., & Devi, N. C. The Impact of FinTech and Blockchain Technologies on Banking and Financial Services. *Technology Innovation Management Review*, 2022, 12, 1/2.

50. Matviichuk, N., & Tesliuk, S. Main trends in the development of banking innovations in Ukraine. *Economic Journal of Lesya Ukrainka Volyn National University*, 2021, 1(25), pp. 79-87.

51. Pearce, P., Borkenhagen, M., & Gross, M. Digital banking redefined in 2021. *Deloitte Digital*. URL: <https://www.deloittedigital.com/content/dam/deloitte-digital/us/documents/offerings/offering-20200611-retail-banking.pdf>

52. Mastercard Study: 51% of Ukrainians are ready to use exclusively digital banking. URL:

<https://www.mastercard.com/news/eemea/uk-ua>

53. Karpov, O. Open banking in Ukraine: innovations and challenges for the financial system, 2022.

URL: <https://psm7.com>

54. Catalog of the best internet banking services in Ukraine, 2023. URL: <https://sp.minfin.com.ua/banks-online>

55. Prasad, A. Google predicts an increase in cyberattacks from Russia on Ukraine and NATO members in 2023.

URL: <https://forbes.ua/news/google-prognozue-zbilshennya-kiberatak-rosii-na-ukrainu-i-chleniv-nato-u-2023-rotsi-16022023-11778>

56. Statistics of the financial sector. Official website of the National Bank of Ukraine, 2023.

URL: <https://bank.gov.ua/ua/statistic/sector-financial>.

57. Ukrainians named the most expected functions they would like to see in digital banking (infographics), 2023. URL:

<https://news.finance.ua/ua/ukrainci-nazvaly-naybil-sh-ochikuvani-funkcii-yaki-hotily-b-bachyty-v-cyfrovomu-bankinhu-infohrafika>

58. Official data from OTP Bank. URL: <https://www.otpbank.com.ua/>

59. Blakey, D. Over 100 banking and payments experts share sector forecasts for 2023. Retail Banker International, 2022. URL:

<https://www.retailbankerinternational.com/analysis/100-banking-payments-experts-share-forecasts-for-2023/>

60. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

61. Catalog of the best internet banks. URL: <https://sp.minfin.com.ua/banks-online>



APPENDICES

Appendix A

Table A.1 Classification of RBS technology by types of information systems

No	RBS technology	Characteristics of IS
1.	PS-banking (PC-banking)	(client-bank systems can be included in this category). Client-bank is a special system that allows interaction with the bank based on the Internet. This is a DBO technology that involves installing the appropriate software (client part) on the client's computer. Connection to the corresponding server takes place via the Internet
2.	Internet banking (Internet banking)	the most convenient and progressive remote banking technology that appeared in the early 80s. 20th century. Since its appearance, it has quickly gained popularity in the global banking sphere, and the development of computer technologies has provided significant opportunities for the development and implementation of new ideas
3.	Mobile banking (mobile-banking)	a modern delivery channel for banking services; this is a DBO technology that involves installing the necessary software (client part) on the client's mobile phone. Connection to the corresponding server is carried out via the Internet. A full-fledged service assumes that a mobile phone is the same means of payment as a bank card. Mobile banking is generally only available to bank debit or credit card holders
4.	Telephone banking (phone-banking)	(sometimes the term telebanking is used) is one of the least popular, but still quite convenient types of service today. Provides generally the same opportunities as Internet banking, only through a call from the client to the bank's contact number (possibly a "hotline"). Phone banking is less productive than mobile banking
5.	SMS banking	is a type of telephone banking. It is suitable for quite primitive tasks: transferring funds, viewing balances, etc. As a rule, the possibilities of this type of service are very limited
6.	Video banking	a type of service that is not common on the Ukrainian market. It is an opportunity for interactive communication between the client and bank employees. Communication with the bank takes place with the help of special devices, "video kiosks", which work on protected communication channels. This type of service is widespread primarily in EU countries and the USA
7.	ATM banking	Services using ATMs and self-service banking facilities: cash deposit/withdrawal; payment for goods/services, telephone services, utility bills, fines, etc.)
8.	Investments on the Internet	is a type of electronic banking that allows customers to buy investments such as stocks, bonds and mutual funds online

Table B.1. List of basic remote banking services

Information services 1	Operational services 2	Auxiliary services 3
24/7 service without breaks or weekends, access from any computer connected to the Internet anywhere in the world	Execution of transactions online It has a mechanism of mutual authentication of the bank and the client; ensuring the protection of the client's operations through the use of passwords that are stored in the system in an encrypted version	The maximally simplified pre-registration (connection) procedure and often free help (mainly if calls are made from landline phones within Ukraine)
Information on movement and balances of funds on accounts with the possibility of various groupings and graphical presentation	Expansion of services for legal entities: issuance and circulation of online checks, letters of credit and other payment documents in which the bank plays a key role	Cross-selling: insurance policies, air and railway tickets
	Transfer of funds: intrabank, interbank, SWIFT	Assessment of creditworthiness, assigning a credit rating, establishing a credit limit
Information about current exchange rates and the dynamics of their fluctuations	Opening, replenishing, closing deposit accounts, using the client's Electronic Digital Signature (EDS) mechanism under all financial documents	Customization of the interface for the client: automatic payment of bills, quick top-up of the mobile phone
Information about available and new products and services of the bank	Repayment of loans	Loyalty programs that encourage the use of certain banking products and technologies, while providing discounts and bonuses.

Table B.2. Advantages and disadvantages of RBS for commercial banks and their clients

	Advantages	Disadvantages
Commercial banks	1) saving on the maintenance of front-office specialists and reducing the burden on it;	1) significant costs for the purchase or creation of the RBS system, its implementation and training of employees;
	2) implementation of the cost leadership strategy;	2) high risks of hacking and fraudulent attacks on the system;
	3) increase in income as a whole due to the growth of the client base, growth of account balances, obtaining additional commission income;	3) system maintenance costs, including communication channels with high throughput when serving a large number of clients;
	4) providing, in addition to traditional, qualitatively new banking products that meet the financial needs and expectations of clients;	4) it is necessary that a significant number of customers use the DBO, otherwise the system will not pay off and will not bring the proper effect;
	5) unification of work with customer documents, improvement of the CRM system;	5) the presence of risks associated with errors in the planning of costs for the implementation and maintenance of the system.
	6) competitive advantage in the fight for customers;	
Clients of banks	1) removal of temporal and spatial restrictions when carrying out banking operations;	1) the need to have special means for using the system (computer, etc.), which requires costs;
	2) satisfaction of customers' needs for new innovative products, a new level of comfort and ease of banking transactions;	2) the need to provide access to communication channels (Internet, etc.), the use of which is also associated with certain costs;
	3) more attractive conditions for DBO, for example, lower interest rates on loans;	3) the need to have a sufficient level of financial literacy and be a confident user of a computer (or other means) to successfully use the system;
	4) personalized offer of banking products, services, targeted advertising, etc.	4) the presence of risks related to the security of operations in the RBS system

Advantages and disadvantages of the "client-bank" system for
commercial banks and their clients

	Advantages	Disadvantages
Commercial banks	1) Saves the time of operators for receiving and processing customer documents	1) Requires costs for the purchase or creation of the system, its implementation and training of employees
	2) Makes it possible to unify work with clients' documents and provide them with various reference information	2) Requires maintenance costs (including communication channels with high bandwidth when serving a large number of clients)
	3) Acts as a powerful factor in the competition for customers	
	4) Allows receiving additional funds in the form of a fee for using the system by customers	
Clients of banks	1) Allows you to work with your accounts without leaving the office	
	2) Provides more complete protection of account information than fax or telephone	2) It often takes some time to retrain employees to work with electronic documents
	3) Allows you to receive various reference information from the bank in a single, connected form	3) As a rule, banks charge a fee for using such a system
	4) Allows the client to choose a bank without paying particular attention to territorial proximity	

Appendix D
Table D.1

Volumes of operations, billion hryvnias

Indicators	2019	2020	2021	2022	2023*	2023 p. To 2019, %	2023 to 2022, %
Transfers from card to card	762,6	945	1352	1835,3	1148,5	150,6	62,6
Transactions for payment of goods/services on the Internet	337,2	483,1	721,3	614,8	501	148,6	81,5
Transfer of funds from the card to a bank account (repayment of loans, replenishment of deposits)	152,4	158,5	118,6	71,5	82,9	54,4	115,9
Calculations for the use of payment terminals	513,4	595,1	878,7	896,6	1121,3	218,4	125,1
Operations in self-service devices	32,7	27	28,5	25,7	85,6	261,8	333,1
In total	1798,3	2208,7	3099,1	3443,9	2939,3	163,4	85,3

* for the 8th month of 2023 (submission of statistical reporting on transactions with payment cards is incomplete).

Table D.2

Number of operations, million units

Indicators	2019	2020	2021	2022	2023*	2023 to 2019, %	2023 to 2022, %
Transfers from card to card	473,8	654,4	894	748,7	579,9	122,4	77,5
Transactions for payment of goods/services on the Internet	727,9	1277,4	1826,9	1448,7	1051,1	144,4	72,6
Transfer of funds from the card to a bank account (repayment of loans, replenishment of deposits)	766,6	623,4	574,5	208,5	80,7	10,5	38,7
Calculations for the use of payment terminals	2133,2	2597,4	3686	2732,2	3504,9	164,3	128,3
Operations in self-service devices	65,6	58,6	58,5	56,3	196,1	298,9	348,3
In total	4167,1	5211,2	7039,9	5194,4	5412,7	129,9	104,2

Source: author's construction based on <https://bank.gov.ua/ua/news/all>

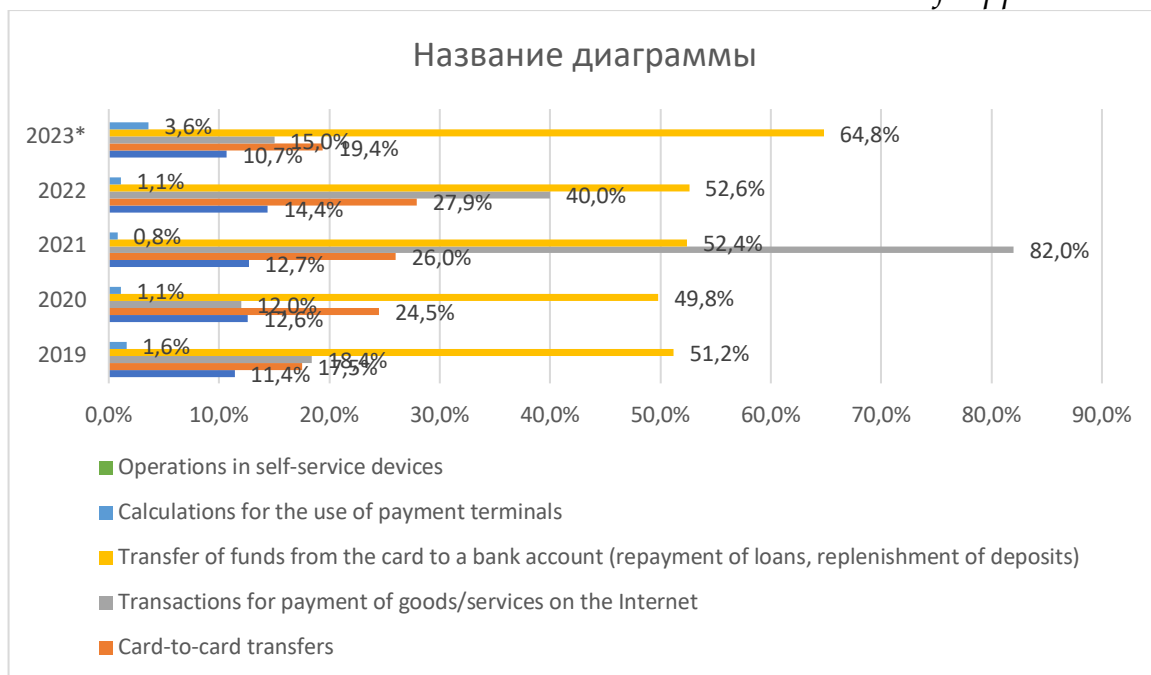


Fig.D.1 Structure of non-cash transactions by number when using payment cards in Ukraine for 2019-2023*, %

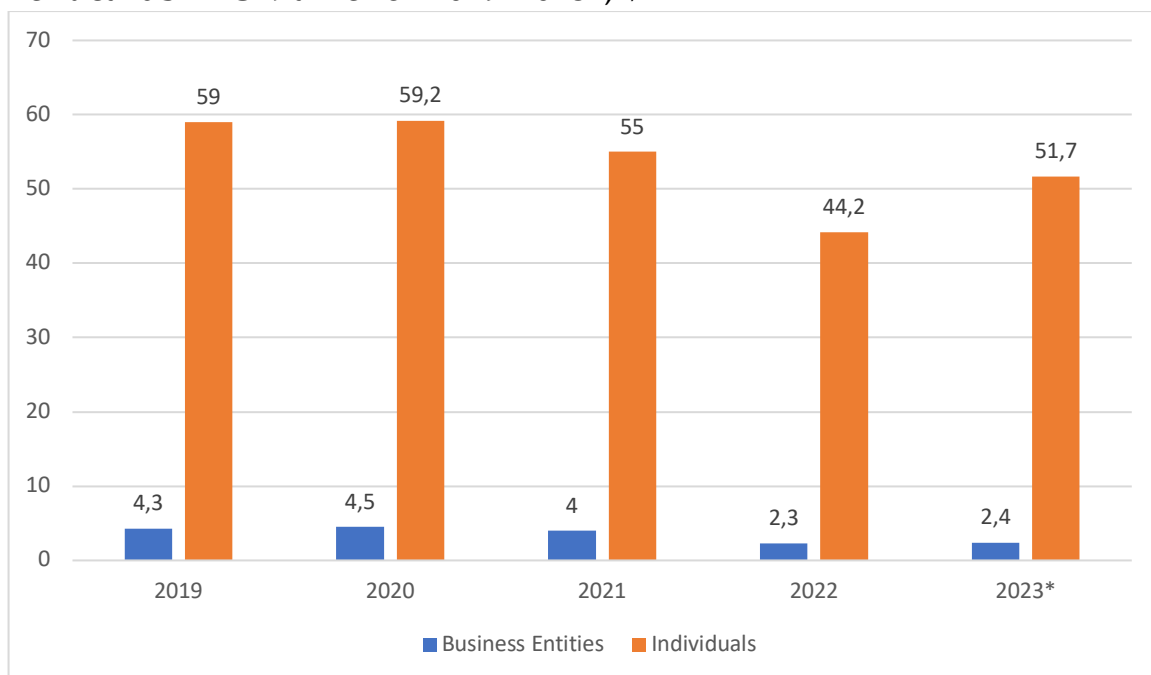


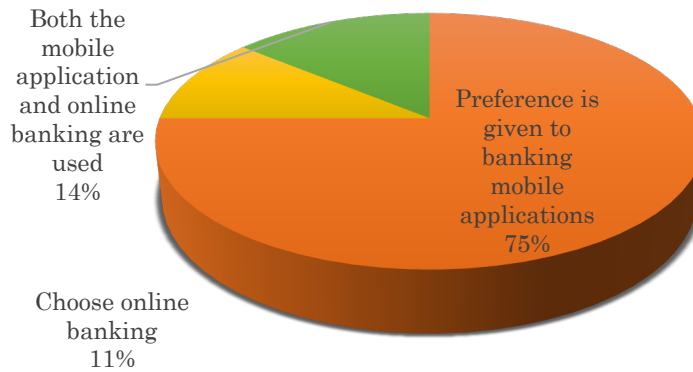
Fig. D.2. Number of clients using remote banking services in Ukraine from 2019 to 2023, million clients.

* the data are indicated for the period of 8 months of 2023 (the submission of statistical reporting on transactions with payment cards is incomplete).

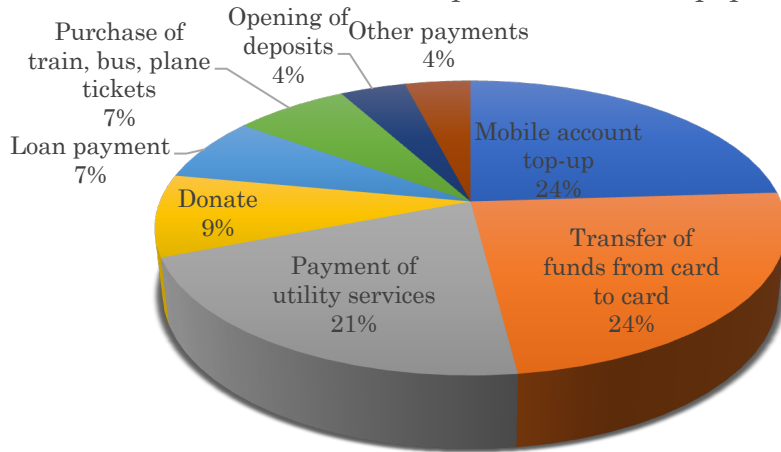
Source: author's construction based on <https://bank.gov.ua/ua/news/all>

Peculiarities of using bank mobile applications during martial law in Ukraine

Giving priority to the method of access to RBS



Predominant RBS operations in the population



The most expected RBS functions among Ukrainian users in 2024, %

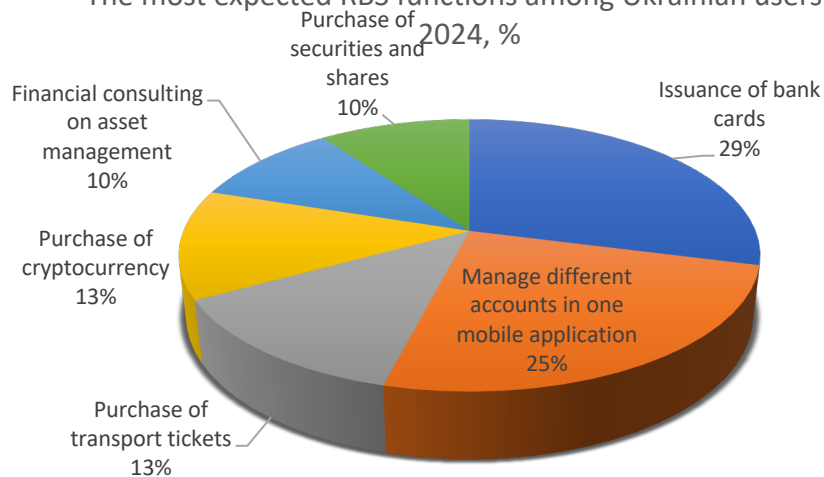


Table K.1

Tariffs for clients - individuals for operations and services in the
OTP Bank UA system

Operation	Tariff
Connecting and using the system	free
Repayment of a loan from a card of any bank or top-up of a card	free
Transfer within own accounts	Free, with a maximum transaction of up to 399,000 hryvnias/month
Transfers (P2P)	Up to UAH 1,000.00. - UAH 5
Mobile top-up	From UAH 1,000.01 to UAH 10.
Transfer to another bank	Free
Support of the purchase of OVDP	Up to UAH 10,000.00. - 2 hryvnias
The Bank provides an investment service for the purchase of securities	From UAH 10,000.01 - 0.5%, max. 500 hryvnias
The grace period for using the loan	0.15% of the total transaction amount
Withdrawal of credit funds in cash in Ukraine	0.15% of the total transaction amount

Source: official bank data

Table K.2.
The quality level of the OTP Bank JSC mobile application among competitors

Indicators	OTP Bank UA	Privat24	Oschad24/7	Mono	A-bank	Raiffeisen Online
1. Functionality						
Replenishment of mobile account without fees	+	-	+	+	-	-
Regulation of the size of the credit line, the volume of payments on the Internet	+	+	-	+	+	+
Issuance and repayment of the loan, payment in installments	+	+	-	+	+	+
Opening a deposit online	+	+	-	+	+	+
Ability to purchase bonds	+	-	-	-	-	-
Operations with securities	+	-	-	+	-	-
Garter of other cards of other banks	+	+	-	+	-	-
Ability to disable double conversion	+	+	-	+	-	-
Free transfers between accounts and transfers open in the Bank	+	-	-	+	-	-

2. Security						
The possibility of 3D secure	+	-	+	+	-	-
The possibility of changing the code word, financial number	+	+	-	+	+	+
Card reissuance with delivery to the post office	+	+	-	+	-	-
3. Level of digitization						
Possibility of appeal of the operation by the client	+	+	-	+	+	-
Confirmation of documents remotely	+	+	-	+	+	-
4. Customer support						
AI-powered Chatbot Help	+	+	-	+	+	+
The possibility of communication in convenient messengers Viber, Telegram, Facebook, as well as e-mail	+	+	+	+	+	+
Informative reference materials are freely available	+	+	+	+	+	+
sms/push notification or generation based on hardware token	+	+	+	-	+	+

Appendix L

Table L.1 Differences between OTP Bank cards

Tariff	OTP Tickets Travel Card	Mani na karmani
Loan amount	200 thousand hryvnias	30 thousand hryvnias
Interest rate	36.00 %	60.00 %
Commission for issuing credit funds	4.00 % + 6 грн	For free
Minimum monthly payment	5.00 %	7.00 %

Table L.2

Terms of OTP bank cards

Indicators	OTP Tickets Travel Card	Mani na karmani
Feature of use	with a grace period for non-cash transactions	free cash withdrawal of credit fund in Ukraine
Loan amount	From UAH 1,000 to UAH 200,000.	From UAH 1,000 to UAH 30,000.
Deposit interest	0.00% per annum on the balance of own funds.	
Interest rate	36.00% per annum	60.00% per annum
Monthly commission	Absent	
Grace period	Up to 55 days for non-cash transactions (until the 24th of the next month)	
Commission for issuing cash	1.00% - at OTP bank ATMs. 1.00 %, min. UAH 7 - at the OTP bank cash desks. 1.50% + UAH 10 - in other banks in Ukraine. 1.80% + UAH 40 - in other banks abroad.	1.00% - at OTP bank ATMs. 1.00 %, min. UAH 7 - at the OTP bank cash desks. UAH 5 - at the cash desks of retail outlets. 1.50% + UAH 10 - in other banks in Ukraine. 1.80% + UAH 40 - in other banks abroad.
Own funds	4.00% + UAH 6 - in Ukraine. 4.00% + UAH 32 - abroad.	Free - at all ATMs in Ukraine. 4.00% + UAH 32 - abroad.
Credit funds	For Free	
Minimum monthly payment:	20 hryvnias	
	UAH 0.00, USD 0.60. USA, Euro per month.	Absent.
Fee for issuing a card	The interest rate on the overdue payment amount, as well as on the unauthorized overdraft, is 36.00% per annum.	
Monthly subscription fee	A penalty is charged on the amount of the overdue payment in the amount of double the NBU accounting rate, but not more than 15.00% of the amount.	The interest rate on the overdue payment amount, as well as on the unauthorized overdraft, is 60% per annum.

SWOT-matrix of RBS services of OTP Bank in conditions of martial

law

<p>External environment</p> <p>Internal environment</p>	<p>Opportunities:</p> <ol style="list-style-type: none"> 1. Expanding the geography of service: Internet banking allows banks to provide services to customers in a large area, including remote and hard-to-reach regions. 2. Increasing the client base: Virtual channels increase the availability of banking services, which can lead to an increase in the client base. 3. Improved service: Internet banking allows you to provide convenient and fast access to banking services, including transfers and bill payments. 4. Cost reduction: Virtual transactions have the potential to reduce the bank's operating costs, as they do not require physical visits to branches. 5. Development of innovations 	<p>Threats:</p> <ol style="list-style-type: none"> 1. Competition: Other banks and financial institutions are also actively developing their Internet banking services, which may lead to competitive pressure. 2. Cyber Threats: The growing number of cyber attacks and fraudsters can increase the risk to online banking security and customer trust. 3. Low customer cyber security: Online banking users may not follow proper security measures such as strong passwords and two-factor authentication, leaving them vulnerable to cyber threats. 3. Clients may face problems accessing online banking if there is no Internet
<p>Strengths:</p> <ol style="list-style-type: none"> 1. Customers can easily access their bank accounts and perform financial transactions through Internet banking. 2. OTP Bank offers bonus programs for loyal customers, which may include discounts, cashback and other benefits. 3. Online services: The Bank provides a wide range of online services for convenient financial management, including payments, transfers and others. 	<p>Field of strengths and opportunities (1)</p> <ol style="list-style-type: none"> 1. Expansion of participation in the market of banking services 2. Attracting customers' attention to the services provided by the bank 3. Expansion of Internet services - access to the bank from anywhere in the world 4. Expanding the scope of work with private individuals and corporate clients 5. implementation of innovative solutions in this area 	<p>Field of strengths and threats (2)</p> <ol style="list-style-type: none"> 1. To keep customers from switching to a competitor by informing them about the high quality and reasonable price of our products. 2. Using the main advantages in relation to competitors: work experience and high reputation. 3. Reduction of the riskiness of operations by using the information base of customers
<p>Weaknesses:</p> <ol style="list-style-type: none"> 1. Weak geographic presence: Compared to some other banks, OTP Bank may have a limited network of branches and ATMs, making it less accessible to customers in certain regions. 2. Technical problems: Disabling the OTP Bank UA system for planned updates may lead to unavailability for customers at a certain time. 3. Dependence on the international parent bank: OTP Bank is a subsidiary of OTP Bank Plc. of Hungarian origin, which may affect his strategic decisions and financial stability. 4. Complexity of the registration procedure and imperfection of authentication 	<p>Field of weaknesses and opportunities (3)</p> <ol style="list-style-type: none"> 1 More active work of the marketing department to inform potential customers about the bank's services. 2. Reduction of loan interest due to a reduction in the cost of resources 3. Lowering the requirements for operational cashiers 	<p>Field of Weaknesses and Threats(4)</p> <ol style="list-style-type: none"> 1. The sudden entry of stronger competitors into the target market. 2. Improvement of the management system, its dynamism and flexibility, while maintaining the possibility of reducing risks due to large-scale resources 3. To attract professional personnel by increasing salaries and improving social security

Main Cybersecurity Threats in E-Banking under Martial Law Conditions

№	Threats to DBO cyber security	Features of threats
1.	Ransomware	Ransomware is a method of cybercrime where files are encrypted and users are locked out, and the criminals demand money to regain access to the system. Organizations affected by ransomware attacks may find that their systems will be damaged for a long period of time, especially if they do not have backups. Paying the ransom to these criminals also does not guarantee that access to your system will be restored.
2.	Constant risks from remote maintenance	Financial institutions have more potential cybersecurity vulnerabilities than ever before. Employees do not always have access to data on systems and networks controlled by the organization, so extra vigilance is required.
3.	Cloud cyber attacks	Banks must ensure that their cloud infrastructure is securely configured to protect against malicious hacks.
4.	Social engineering	Phishing, farming, vishing, etc. One of the biggest recent cyber threats to banking and finance is social engineering. People are often the most vulnerable link in the security chain – they can be tricked into providing sensitive data and credentials. This can equally affect both the bank's employees and its customers.
5.	Attacks on supply chains	An increasingly popular method for cybercriminals to distribute malware is to target a software vendor and then deliver the malicious code to customers and other members of the supply chain in the form of products or updates that appear to be legitimate at first glance. These attacks compromise distribution systems and allow cybercriminals to infiltrate the supplier's customer networks.

Source: summarized by the author

Table 1 Development of cyber security training in the conditions of JSC "OTP Bank"

Етапи тренінгу	Description of stages	A pattern of behavior
1. Simulation of a cyber attack	Organize a simulation of a cyber attack using a test environment. Use realistic scenarios covering different types of attacks.	scenario: Phishing attack on online banking. The actions of employees should be aimed at effective response and prevention of further risks.
2. Recognition of threats	Train staff to identify unusual activity and suspicious behavior online.	The first step is to note suspicious messages, e-mails or links that have arrived in the bank's mail, and which may indicate phishing. Report the suspicion to the bank's cyber security department and management.
3. Quick reaction	Identify specific steps that staff should take after detecting a cyber attack. Develop an action plan and communication protocols.	Do not open attachments or links in emails that may contain malicious content. Do not provide sensitive information, such as passwords or personal information, through untrusted channels.
4. Data security	Train staff to protect sensitive data during a cyber attack.	All suspicious messages should be collected and forwarded to the cyber security department for further analysis. If a detected phishing attack has affected banking systems, isolate the compromised objects to prevent further spread of the attack.
5. Recovery after an incident	Explain how to restore normal operation of systems after a cyber attack.	If there is a known customer base that may have been affected by a phishing attack, inform them of the possible risk and provide recommendations for changing passwords and strengthening the security of their accounts.
6. Cooperation with experts	Train staff to communicate with cybersecurity professionals and law enforcement.	Designation of responsible persons, familiarization with contact details of cyber security specialists
7. Knowledge testing	Conduct a test to check the level of mastery of the material.	Knowledge of terminology, technological aspects, incident recognition, reporting procedures. Practical lessons: Situational cases, Escape Room exercises for responding to incidents
8. Continuous training	Establish regular training and refresher skills in the field of cyber security.	After isolating the attack, analyze its methods and initial sources. Based on this analysis, develop strategies to prevent similar attacks in the future. Conduct employee training on phishing detection and actions in the event of an attack. Disseminate information about new types of phishing and updated protection methods among employees.
9. Analysis and improvement	Conduct training analysis and make improvements to improve training effectiveness.	If the attack became public information, provide timely information feedback and explanation of the situation to customers and the public.

Source: author's development

Table 2. Training plan for clear actions in the event of a phishing attack: actions of staff and customers

Plan for bank employees	A plan for the client
<p>1. Recognize phishing content: Check the sender: Make sure the email is sent from a legitimate source. Suspicious email addresses should be avoided.</p> <p>Check links: Do not click on links directly. Hover over them to see the URL before you jump.</p> <p>Suspicious attachments: Do not open files from unknown sources.</p> <p>2. Do not enter personal data: Never send personal information such as passwords, pin codes or card numbers via mail or email links.</p> <p>3. Contact information security: If you have any suspicions about a letter or message, notify the bank's information security department and give them the details of the attack.</p> <p>4. Do not distribute suspicious messages: do not send phishing messages to other bank employees.</p>	<p>1. Verification of the sender: Confirm that the email or message is from a legitimate source by checking the sender's email address or name.</p> <p>2. Don't send personal information: Never send personal information through mail or links in emails.</p> <p>3. Link Verification: Don't click on links directly. Hover over them to see the URL before you jump. Check the status of the site based on Google Safe Browsing</p> <p>4. Contact the bank: If you are suspicious of a message, contact the bank through other available means to confirm legitimacy.</p> <p>5. Change passwords and pin codes. If necessary, deactivate the payment card using online support or independently from the mobile application.</p> <p>6. Save evidence (save all messages, take screenshots)</p> <p>5. Notifying the bank of receipt of a phishing letter or message.</p>

Source: author's development

The main lead generation channels for activation of additional business processes of digital banking JSC "OTP Bank"

Lead generation channels	Bank website	Content	Groups, listings,	Social media, advertising	Outbound calls lead generation	referrals,
Number of responsible persons	2	1-2	Freelance	1	2-3	outsourcing,
Activity	SEO optimization, monitoring, landing pages, analytics	Blog, Article Comments, Quora, Reddit, Stack, Overflow,	websites	Facebook, LinkedIn, Instagram, Twitter, Ads	Outbound lead generation campaigns, Email marketing	Poll
Tools	Google Analytics, Ahrefs, SpyFu, Adbeat, Leadfeeder	Social Report (Publishing Tools)	1-2	Advertising campaign tools	Linked Helper, Dux Soup, Pipedrive, ActiveCampaign, MailChimp, Mailerlite	1
Campaign plans and strategic goals						

Source: author's development

Table P.1. Amounts of necessary investments to improve the remote banking service mechanism of JSC "OTP Bank"

Investments	2024	2025	2026	2027
1. Expanding the functionality of the mobile application	455,4	446,5	55,5	55,5
2. Marketing and advertising of the new mobile application	114,8	110,5	28,2	15,5
3. Training staff and customers to use the application	10,8	20,3	20,5	20,5
4. Development of an electronic identification system	22,8	12,5	5,6	5,6
5. Integration with the Diya system for electronic identification	22,8	0,5	0,5	0,5
6. Marketing and information campaign regarding the new registration method	8,4	1,2	0,5	0,5
7. Development of insurance cyber protection programs	86,7	25,3	18,5	18,5
8. Expansion of the range of services, including Unik-OTP youth cards	18,5	20,2	11,4	12,5
9. Promotion and lead generation through advertising in social networks	25,5	20,4	18,5	15
10. Development and implementation of a chatbot based on artificial intelligence and machine learning	2,8	0,8	0,5	0,5
11. Introduction of additional technical means of protection against cyber attacks	102,8	3,6	5,5	5,5
12. Implementation of personnel training programs (managed cyber security tools, motivational component of personnel)	1,5	2,1	0,5	0,5
together	872,8	663,9	165,7	150,6

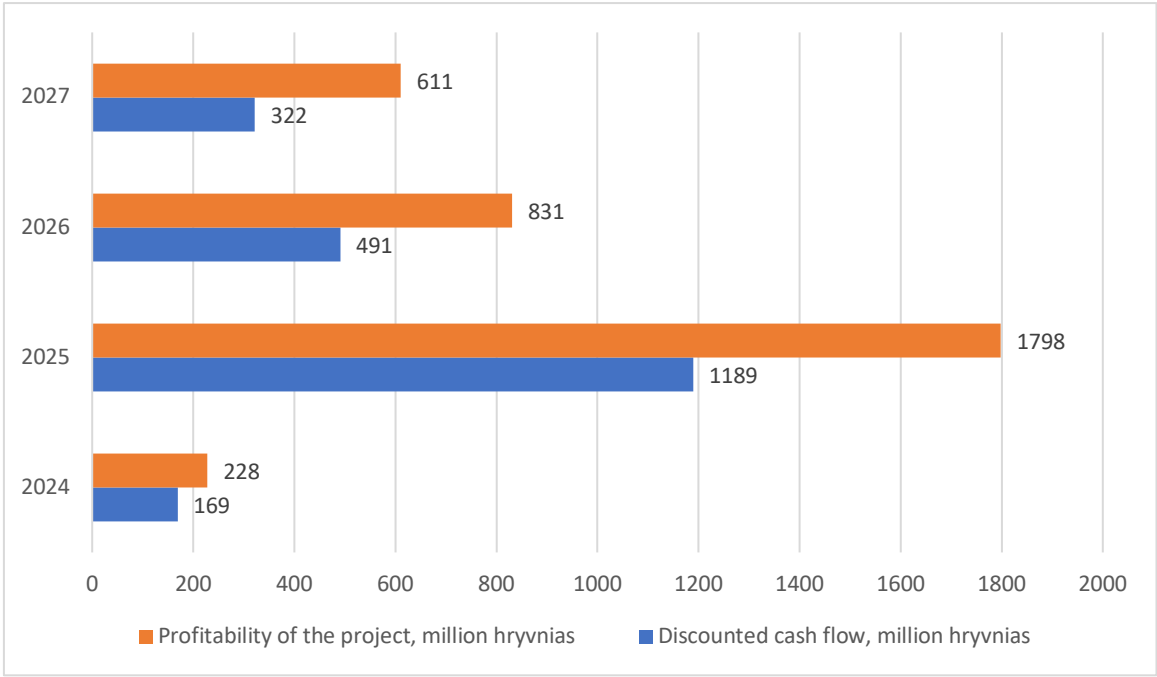


Fig. R.1. The value of cash flows of JSC "OTP Bank" from the implementation of the DBO development project in the current

JOINT STOCK COMPANY OTP BANK

**Separate Statement of Financial Position
for the Year Ended 31 December 2023
(In Ukrainian Hryvnias and in thousands)**

	Notes	31 December 2023	31 December 2022
ASSETS			
Cash and cash equivalents	4	10,827,171	4,749,260
Loans and advances to banks	5	21,491,993	21,720,592
Loans and advances to customers	6	24,861,899	29,892,900
Investments in securities	7	43,360,299	32,852,589
Derivative financial assets		-	3,246
Investments in subsidiaries, joint ventures and associates	8	139,143	139,143
Investment property		24,634	24,634
Current tax assets		40	5
Deferred tax assets	17	-	65,407
Intangible assets other than goodwill	9	486,795	362,306
Property plant and equipment	9	684,883	802,462
Other financial assets	10	114,674	330,426
Other nonfinancial assets	10	51,951	62,568
Total assets		102,043,482	91,005,538
LIABILITIES			
Due to other banks		15,211	231
Customer accounts	11	81,855,086	77,736,460
Derivative financial liabilities		22,758	9,233
Other borrowed funds		53	159
Current tax liabilities		2,683,009	119,500
Provisions:			
Provisions for loan commitments and financial guarantee contracts	24	246,958	301,643
Other financial liabilities	12	1,162,001	1,070,480
Other nonfinancial liabilities	12	162,478	137,164
Deferred tax liabilities	17	76,907	-
Total liabilities		86,224,461	79,374,870
EQUITY			
Statutory capital	22	6,186,023	6,186,023
Retained earnings		7,484,733	3,772,426
Share premium	22	405,075	405,075
Result from transactions with the shareholder	22	1,236,294	1,236,294
Other reserves		506,896	30,850
Total equity		15,819,021	11,630,668
Total equity and liabilities		102,043,482	91,005,538

Authorized for issue by management of JOINT STOCK COMPANY OTP Bank and signed on its behalf by:

 Volodymyr Mudryi, Chairman of the Management Board		 Natalia Diuba, Chief Accountant
19 April 2024		19 April 2024

The accompanying notes on pages from 8 to 93 form an integral part of these separate financial statements.

JOINT STOCK COMPANY OTP BANK

**Separate Statement of Profit or Loss
for the Year Ended 31 December 2023
(In Ukrainian Hryvnias and in thousands)**

	Notes	2023	2022
Interest Income:	13	12,121,526	8,787,828
Interest income calculated by using the effective interest rate	13	12,109,061	8,774,395
Other interest income	13	12,465	13,433
Interest expense	13	(3,480,867)	(1,981,446)
Net interest income (net interest expense)	13	8,640,659	6,806,382
Commission income	14	1,869,768	1,785,441
Commission expenses	14	(739,463)	(663,787)
Other income		91,475	128,973
Net gain (loss) from financial instruments at fair value through profit or loss		(102,552)	100,893
Net gain (loss) from operations with debt financial instruments at fair value through other comprehensive income		(24,491)	(7,847)
Net gain (loss) from trading in foreign currencies		378,182	713,690
Net gain (loss) from foreign exchange translation		206,885	70,226
Impairment gains and reversals of impairment losses (impairment losses) determined in accordance with IFRS 9	15	120,458	(5,658,273)
Other expense	16	(220,011)	(134,244)
Other gains (losses), including:		(129,729)	(100,474)
- Net loss on modification of financial assets		(129,729)	(100,254)
Employee benefits expense	16	(1,679,418)	(1,408,154)
Depreciation and amortisation expense	16	(341,058)	(341,116)
Other administrative and operational expenses	16	(647,867)	(565,299)
Profit (loss) before tax		7,422,838	726,411
Income tax expense (benefit)	17	(3,710,531)	(129,305)
Net profit (loss)		3,712,307	597,106
Earnings per share			
Weighted average number of outstanding ordinary shares		499,238	499,238
Basic and diluted earnings per share, UAH		7,436	1,196

Authorized for issue by management of JOINT STOCK COMPANY OTP Bank and signed on its behalf by:

 Volodymyr Mudryi, Chairman of the Management Board		 Natalia Diuba, Chief Accountant
19 April 2024		19 April 2024

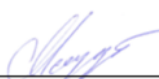
The accompanying notes on pages from 8 to 93 form an integral part of these separate financial statements.

JOINT STOCK COMPANY OTP BANK

**Separate Statement of Comprehensive Income
for the Year Ended 31 December 2023
(In Ukrainian Hryvnias and in thousands)**

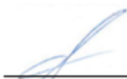
	Notes	2023	2022
Profit (loss)		3,712,307	597,106
Other comprehensive income			
Components of other comprehensive income that will not be reclassified to profit or loss, before tax			
Other comprehensive income - gains (losses) from investments in equity instruments		71	1,172
Components of other comprehensive income that will be reclassified to profit or loss net of tax			
Gains (losses) on financial assets at fair value through other comprehensive income, before tax		613,334	(41,983)
including:			
change in fair value of investments at fair value through other comprehensive income		202,824	(110,475)
change in allowance for expected credit losses on investments in debt instruments at fair value through other comprehensive income	24	410,510	68,492
Amount of accumulated gain / (loss), reclassified to profit or loss on disposal of investments at fair value through other comprehensive income		24,491	7,847
Income tax relating to items that may be reclassified subsequently to profit or loss	17	(161,850)	6,145
Total other comprehensive income that will be reclassified to profit or loss net of tax		475,975	(27,991)
Total other comprehensive income		476,046	(26,819)
Total comprehensive income		4,188,353	570,287

Authorized for issue by management of JOINT STOCK COMPANY OTP Bank and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board

19 April 2024




Natalia Diuba,
Chief Accountant

19 April 2024

The accompanying notes on pages from 8 to 93 form an integral part of these separate financial statements.

JOINT STOCK COMPANY OTP BANK

**Separate Statement of Cash Flows
for the Year Ended 31 December 2023
(In Ukrainian Hryvnias and in thousands)**

	Notes	2023	2022
Cash flows from operating activities			
Classes of cash receipts from operating activities			
Interest received		12,042,627	8,694,972
Commission income received		1,877,289	1,754,684
Net gain/(loss) from operations with financial instruments at fair value through profit or loss		(83,609)	113,546
Net gain/(loss) from operations with foreign currencies		378,182	713,690
Other cash receipts from operating activities (other income received)		91,947	140,785
Classes of cash payments from operating activities			
Interest paid		(3,473,023)	(1,994,258)
Commission expenses paid		(739,463)	(663,787)
Administrative expenses and other paid operating expenses, including:		(2,362,767)	(2,123,315)
Employee benefits expense		(1,517,150)	(1,437,346)
Other administrative and operational expenses		(625,606)	(551,505)
Other expense		(220,011)	(134,464)
Income taxes paid		(1,166,725)	(149,799)
Cash flows from (used in) operating activities before movements in operating assets and liabilities		6,564,458	6,486,518
Net (increase)/decrease in loans and receivables of banks		-	(379,871)
Net (increase)/decrease in loans and receivables		5,603,055	8,329,393
Net (increase)/decrease in other financial assets		214,559	(201,810)
Net (increase)/decrease in other nonfinancial assets		12,549	(3,696)
Net increase/(decrease) in due to other banks		15,211	(1,035)
Net increase/(decrease) in customer accounts		2,418,069	12,499,881
Net increase/(decrease) in other financial liabilities		(10,442)	(48,335)
Net increase/(decrease) in other nonfinancial liabilities		(12,535)	9,996
Net cash flows from (used in) operating activities		14,804,924	26,691,041
Cash flows from Investing activities			
Purchase of securities		(5,971,222,029)	(3,088,078,802)
Proceeds from sale and repayment of investments in securities		5,961,470,908	3,070,463,782
Purchase of property plant and equipment		(120,204)	(185,571)
Proceeds from sales of property plant and equipment		69,796	95,249
Purchase of intangible assets		(268,616)	(130,885)
Proceeds from sale of investment property		-	1,441
Net cash flows from (used in) investing activities		(10,070,145)	(17,834,786)

JOINT STOCK COMPANY OTP BANK

**Separate Statement of Cash Flows
for the Year Ended 31 December 2023 (Continued)
(In Ukrainian Hryvnias and in thousands)**

	Notes	2023	2022
Cash flows from financing activities			
Redemption of other borrowed funds		(579)	(17)
Payments on lease liabilities	12	(73,133)	(60,898)
Net cash flows from (used in) financing activities		(73,712)	(60,915)
Net increase (decrease) in cash and cash equivalents before effect of exchange rate changes		4,661,067	8,795,340
Effect of exchange rate changes on cash and cash equivalents		1,415,245	4,421,800
Effect of changes allowance on cash and cash equivalents	4	152,871	(126,713)
Net increase (decrease) in cash and cash equivalents		6,229,183	13,090,427
Cash and cash equivalents, at the beginning of the year	4	26,089,981	12,999,554
Cash and cash equivalents, at the end of the year	4	32,319,164	26,089,981

Authorized for issue by management of JOINT STOCK COMPANY OTP Bank and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board

19 April 2024




Natalia Diuba,
Chief Accountant

19 April 2024

The accompanying notes on pages from 8 to 93 form an integral part of these separate financial statements.

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Financial Position
for the Year Ended 31 December 2022
(In Ukrainian Hryvnias and in thousands)


	Notes	31 December 2022	31 December 2021
ASSETS			
Cash and cash equivalents	4	4,749,260	3,870,163
Loans and advances to banks	5	21,720,592	9,129,391
Loans and advances to customers	6	29,934,500	40,604,941
Investments in securities	7	32,855,937	14,631,671
Derivative financial assets		3,246	8,376
Investment property		24,634	26,075
Current tax assets		5	5,183
Deferred tax assets	15	65,407	68,847
Intangible assets other than goodwill	8	362,578	345,109
Property plant and equipment	8	805,721	953,430
Other financial assets	9	330,426	118,981
Other nonfinancial assets	9	66,239	80,838
Total assets		90,918,545	69,843,005
LIABILITIES			
Due to others banks		231	1,225
Customer accounts	10	77,064,900	56,427,453
Derivative financial liabilities		9,233	4
Other borrowed funds		159	176
Provisions:			
Provisions for loan commitments and financial guarantee contracts	23	301,643	300,334
Other financial liabilities	11	1,081,911	1,118,470
Other nonfinancial liabilities	11	139,628	137,788
Current tax liabilities		119,500	149,689
Total liabilities		78,717,205	58,135,139
EQUITY			
Issued capital	21	6,186,023	6,186,023
Retained earnings		4,331,655	3,810,958
Share premium	21	405,075	405,075
Result from transactions with the shareholder	21	1,236,294	1,236,294
Other reserves		42,293	69,516
Total equity		12,201,340	11,707,866
Total equity and liabilities		90,918,545	69,843,005

Authorized for issue by management of the Group and signed on its behalf by:


 Volodymyr Mudryi,
 Chairman of the Management Board

26 April 2023




 Natalia Djuba,
 Chief Accountant

26 April 2023

The accompanying notes on pages from 8 to 100 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK

**Consolidated Statement of Profit or Loss
for the Year Ended 31 December 2022
(In Ukrainian Hryvnias and in thousands)**

	Notes	2022	2021
Interest Income:	12	8,798,228	5,810,492
Interest income calculated by using the effective interest rate	12	8,784,795	5,780,825
Other interest income	12	13,433	29,667
Interest expense	12	(1,971,686)	(1,117,409)
Net interest income (net interest expense)	12	6,826,542	4,693,083
Commission income	13	1,785,293	1,989,779
Commission expenses	13	(663,639)	(700,555)
Other income		137,296	107,097
Net increase (decrease) from financial instruments at fair value through profit or loss		100,893	231,419
Net increase (decrease) from operations with debt financial instruments at fair value through other comprehensive income		(7,847)	183,338
Net increase (decrease) from trading in foreign currencies		713,690	301,288
Net increase (decrease) from foreign exchange translation		107,978	(218,288)
Impairment gains and reversals of impairment losses (impairment losses) determined in accordance with IFRS 9	14	(5,758,726)	(659,263)
Other expense		(134,244)	(122,095)
Other gains (losses)		(100,474)	(13,340)
- Net loss on modification of financial assets		(100,254)	(11,209)
Employee benefits expense	15	(1,442,494)	(1,365,398)
Depreciation and amortisation expense	15	(343,558)	(319,786)
Other administrative and operational expenses	15	(570,708)	(632,152)
Profit (loss) before tax		650,002	3,475,127
Income tax expense (benefit)	16	(129,305)	(605,620)
Net profit (loss)		520,697	2,869,507
Earnings per share			
Weighted average number of outstanding ordinary shares		499,238	499,238
Basic and diluted earnings per share, UAH		1,043	5,748

Authorized for issue by management of the Group and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board
 26 April 2023




Natalia Diuba,
Chief Accountant
 26 April 2023

The accompanying notes on pages from 8 to 100 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK


**Consolidated Statement of Comprehensive Income
for the Year Ended 31 December 2022
(In Ukrainian Hryvnias and in thousands)**

	Notes	2022	2021
Profit (loss)		520,697	2,869,507
Other comprehensive income			
Components of other comprehensive income that will not be reclassified to profit or loss, before tax			
Other comprehensive income - gains (losses) from investments in equity instruments, before tax		768	1,846
Components of other comprehensive income that will be reclassified to profit or loss net of tax			
Gains (losses) on financial assets at fair value through other comprehensive income, before tax		(41,983)	142,650
including:			
change in fair value of investments at fair value through other comprehensive income		(110,475)	209,643
change in allowance for expected credit losses on investments in debt instruments at fair value through other comprehensive income	23	68,492	(66,993)
Amount of accumulated profit / (loss), reclassified to profit or loss on disposal of investments at fair value through other comprehensive income		7,847	(188,680)
Income tax relating to items that may be reclassified subsequently to profit or loss	17	6,145	(12,299)
Total other comprehensive income that will be reclassified to profit or loss net of tax		(27,991)	(58,329)
Total other comprehensive income		(27,223)	(56,483)
Total comprehensive income		493,474	2,813,024

Authorized for issue by management of the Group and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board
 26 April 2023




Natalia Diuba,
Chief Accountant
 26 April 2023

The accompanying notes on pages from 8 to 100 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK

Notes to the Consolidated Financial Statements for the Year Ended 31 December 2022 (Continued) (In Ukrainian Hryvnias and in thousands)

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Cash Flows for the Year Ended 31 December 2022 (In Ukrainian Hryvnias and in thousands)

	Notes	2022	2021
Cash flows from operating activities			
Classes of cash receipts from operating activities			
Interest received		8,702,396	6,103,605
Commission income received		1,754,536	2,012,296
Net profit/(loss) from operations with financial instruments at fair value through profit or loss		113,546	223,047
Net profit/(loss) from operations with foreign currencies		713,690	301,288
Other cash receipts from operating activities (other income received)		161,119	238,911
Classes of cash payments from operating activities			
Interest paid		(1,984,381)	(1,071,678)
Commission expenses paid		(663,639)	(700,555)
Administrative expenses and other paid operating expenses, including:		(2,127,522)	(2,072,023)
Employee benefits expense		(1,437,346)	(1,315,765)
Other administrative and operational expenses		(555,712)	(635,542)
Other expense		(134,464)	(120,716)
Income taxes paid		(149,799)	(541,747)
Cash flows from operating activities before movements in operating assets and liabilities		6,519,946	4,493,144
Net (increase)/decrease in loans and receivables of banks		(379,871)	-
Net (increase)/decrease in loans and receivables		8,329,393	(14,068,505)
Net (increase)/decrease in other financial assets		(201,810)	(18,362)
Net (increase)/decrease in other assets		(3,696)	22,988
Net increase/(decrease) in due to other banks		(1,035)	1,234
Net increase/(decrease) in customer accounts		12,465,865	10,436,052
Net increase/(decrease) in other financial liabilities		(48,335)	60,543
Net increase/(decrease) in other liabilities		9,996	(7,084)
Net cash flows from operating activities		26,690,453	920,010
Cash flows from Investing activities			
Purchase of securities		(3,088,119,402)	(453,031,625)
Proceeds from sale and repayment of investments in securities		3,070,505,049	450,971,785
Proceeds from sales of property plant and equipment		95,265	4,666
Purchase of property plant and equipment		(185,771)	(288,955)
Purchase of intangible assets		(130,885)	(13,921)
Proceeds from sale of investment property		1,441	-
Net cash outflow to investing activities		(17,834,303)	(2,358,050)

JOINT STOCK COMPANY OTP BANK

Notes to the Consolidated Financial Statements
for the Year Ended 31 December 2022 (Continued)
(In Ukrainian Hryvnias and in thousands)

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Cash Flows
for the Year Ended 31 December 2022 (Continued)
(In Ukrainian Hryvnias and in thousands)

	Notes	2022	2021
Cash flows from financing activities			
Redemption of other borrowed funds		(17)	(91)
Payments on lease liabilities	9	(60,898)	(168,168)
Dividends paid		-	(1,200,000)
Net cash flows from financing activities		(60,915)	(1,368,259)
Net increase (decrease) in cash and cash equivalents before effect of exchange rate changes		8,795,235	(2,806,299)
Effect of exchange rate changes on cash and cash equivalents		4,421,905	(1,290,629)
Effect of changes allowance on cash and cash equivalents		(126,713)	(42,016)
Net increase (decrease) in cash and cash equivalents		13,090,427	(4,138,944)
Cash and cash equivalents, at the beginning of the year	4	12,999,554	17,138,498
Cash and cash equivalents, at the end of the year	4	26,089,981	12,999,554

Authorized for issue by management of the Group and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board

26 April 2023




Natalia Diuba,
Chief Accountant

26 April 2023


The accompanying notes on pages from 8 to 100 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK

**Consolidated Statement of Financial Position
for the Year Ended 31 December 2021
(In Ukrainian Hryvnias and in thousands)**

	Notes	31 December 2021	31 December 2020 (reclassified)	31 December 2019 (reclassified)
ASSETS				
Cash and cash equivalents	4	3,870,163	3,510,420	3,139,593
Loans and advances to banks	5	9,129,391	13,628,078	4,308,470
Loans and advances to customers	6	40,604,941	27,797,157	25,469,028
Investments in securities	7	14,631,671	12,507,619	10,844,079
Derivative financial assets		8,376	10,561	454
Investment property		26,075	27,857	28,152
Current tax assets		5,183	5,163	5,137
Deferred tax assets	15	68,847	76,544	38,747
Intangible assets other than goodwill	8	345,109	359,030	196,935
Property plant and equipment	8	953,430	825,999	565,546
Other financial assets	9	118,981	98,434	152,745
Other nonfinancial assets	9	80,838	115,144	79,919
Total assets		69,843,005	58,962,006	44,828,805
LIABILITIES				
Due to others banks		1,225	132	189,668
Customer accounts	10	56,427,453	47,337,814	35,094,301
Derivative financial liabilities		4	844	3,447
Other borrowed funds		176	267	378,133
Provisions for loan commitments and financial guarantee contracts		300,334	279,484	83,939
Other financial liabilities	11	1,118,470	1,057,087	783,241
Other nonfinancial liabilities	11	137,788	110,232	97,768
Current tax liabilities		149,689	81,304	84,827
Total liabilities		58,135,139	48,867,164	36,715,324
EQUITY				
Issued capital	21	6,186,023	6,186,023	6,186,023
Retained earnings		3,810,958	2,141,451	215,088
Share premium	21	405,075	405,075	405,075
Result from transactions with the shareholder	21	1,236,294	1,236,294	1,236,294
Other reserves		69,516	125,999	71,001
Total equity		11,707,866	10,094,842	8,113,481
Total equity and liabilities		69,843,005	58,962,006	44,828,805

Authorized for issue by management of the Group and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board

17 August 2022




Natalia Diuba,
Chief Accountant

17 August 2022

The accompanying notes on pages from 8 to 105 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK

**Consolidated Statement of Profit or Loss
for the Year Ended 31 December 2021
(In Ukrainian Hryvnias and in thousands)**

	Notes	2021	2020 (reclassified)
Interest income:	12	5,810,492	5,118,846
Interest income calculated by using the effective interest rate	12	5,780,825	5,099,019
Other interest income	12	29,667	19,827
Interest expense	12	(1,117,409)	(1,384,813)
Net interest income (net interest expense)	12	4,693,083	3,734,033
Commission income	13	1,989,779	1,683,913
Commission expenses	13	(700,555)	(567,027)
Other income		107,097	163,980
Net increase (decrease) from financial instruments at fair value through profit or loss		231,419	(402,922)
Net increase (decrease) from operations with debt financial instruments at fair value through other comprehensive income		183,338	79,306
Net increase (decrease) from trading in foreign currencies		301,288	692,833
Net increase (decrease) from foreign exchange translation		(218,288)	96,650
Impairment gains and reversals of impairment losses (impairment losses) determined in accordance with IFRS 9	14	(659,263)	(1,030,570)
Other expense		(122,095)	(78,219)
Other gains (losses)		(13,340)	(18,917)
Employee benefits expense	15	(1,365,398)	(1,184,725)
Depreciation and amortisation expense	15	(319,786)	(241,516)
Other administrative and operational expenses	15	(632,152)	(614,829)
Profit (loss) before tax		3,475,127	2,311,990
Income tax expense (benefit)	16	(605,620)	(385,627)
Net profit (loss)		2,869,507	1,926,363
Earnings per share			
Weighted average number of outstanding ordinary shares		499,238	499,238
Basic and diluted earnings per share, UAH		5,558	3,859

Authorized for issue by management of the Group and signed on its behalf by:

 Volodymyr Mudryi, Chairman of the Management Board 17 August 2022	 Natalia Diuba, Chief Accountant 17 August 2022
---	--

The accompanying notes on pages from 8 to 105 form an integral part of these consolidated financial statements.


JOINT STOCK COMPANY OTP BANK

**Consolidated Statement of Comprehensive Income
for the Year Ended 31 December 2021**


(In Ukrainian Hryvnias and in thousands)

	Notes	2021	2020
Profit (loss)		2,869,507	1,926,363
Other comprehensive income			
Components of other comprehensive income that will not be reclassified to profit or loss, before tax			
Other comprehensive income - gains (losses) from investments in equity instruments, before tax		1,846	(10,126)
Components of other comprehensive income that will be reclassified to profit or loss net of tax			
Gains (losses) on financial assets at fair value through other comprehensive income, before tax		142,650	149,042
including:			
change in fair value of investments at fair value through other comprehensive income		209,643	252,910
change in allowance for expected credit losses on investments in debt instruments at fair value through other comprehensive income		(66,993)	(103,868)
Amount of accumulated profit / (loss), reclassified to profit or loss on disposal of investments at fair value through other comprehensive income		(188,680)	(83,918)
Income tax relating to items that may be reclassified subsequently to profit or loss		(12,299)	-
Total other comprehensive income that will be reclassified to profit or loss net of tax		(58,329)	65,124
Total other comprehensive income		(56,483)	54,998
Total comprehensive income		2,813,024	1,981,361

Authorized for issue by management of the Group and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board

17 August 2022


Natalia Diuba,
Chief Accountant

17 August 2022

The accompanying notes on pages from 8 to 105 form an integral part of these consolidated financial statements.



JOINT STOCK COMPANY OTP BANK

Notes to the Consolidated Financial Statements for the Year Ended 31 December 2021 (In Ukrainian Hryvnias and in thousands)

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Cash Flows for the Year Ended 31 December 2021 (In Ukrainian Hryvnias and in thousands)

	Notes	2021	2020 (as reclassified)
Cash flows from operating activities			
Classes of cash receipts from operating activities			
Interest paid		(1,071,678)	(1,395,499)
Interest received		6,103,605	6,043,160
Commission income received		2,012,296	1,683,913
Net (increase)/decrease from operations with financial instruments at fair value through profit or loss		223,047	(412,639)
Net (increase)/decrease from operations with foreign currencies		301,288	692,833
Other cash receipts from operating activities (other income received)		238,911	120,704
Classes of cash payments from operating activities			
Commission expenses paid		(700,555)	(567,027)
Administrative expenses and other paid operating expenses, including:		(2,072,023)	(1,845,780)
Employee benefits expense		(1,315,765)	(1,144,668)
Other administrative and operational expenses		(635,542)	(633,366)
Other expense		(120,716)	(67,746)
Income taxes paid		(541,747)	(426,973)
Cash flows from operating activities before movements in operating assets and liabilities		4,493,144	3,892,692
Net (increase)/decrease in loans and receivables of banks		-	473,403
Net (increase)/decrease in loans and receivables		(14,068,505)	(2,566,411)
Net (increase)/decrease of derivative financial assets		2,185	(10,107)
Net (increase)/decrease in other financial assets		(20,547)	43,981
Net (increase)/decrease in other assets		22,988	(16,553)
Net increase/(decrease) in due to other banks		1,234	(189,987)
Net increase/(decrease) in customer accounts		10,436,052	8,998,468
Net increase/(decrease) of derivative financial liabilities		(840)	(2,603)
Net increase/(decrease) in other financial liabilities		61,383	120
Net increase/(decrease) in other liabilities		(7,084)	(161,318)
Net cash flows from operating activities		920,010	10,461,685
Cash flows from Investing activities			
Purchase of securities		(453,031,625)	(548,062,005)
Proceeds from sale of investments in securities		450,971,785	546,774,819
Proceeds from sales of property plant and equipment		4,666	34,551
Purchase of property plant and equipment		(316,797)	(108,904)
Purchase of intangible assets		13,921	(199,389)
Net cash outflow to investing activities		(2,358,050)	(1,560,928)

JOINT STOCK COMPANY OTP BANK


Notes to the Consolidated Financial Statements
for the Year Ended 31 December 2021
(In Ukrainian Hryvnias and in thousands)

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Cash Flows
for the Year Ended 31 December 2021 (Continued)
(In Ukrainian Hryvnias and in thousands)

	Notes	2021	2020
Cash flows from financing activities			
Redemption on other borrowed funds		(91)	(367,982)
Payments of lease liabilities	9	(168,168)	(147,237)
Dividends paid		(1,200,000)	-
Net cash flows from financing activities		(1,368,259)	(515,219)
Net increase (decrease) in cash and cash equivalents before effect of exchange rate changes			
		(2,806,299)	8,385,538
Effect of exchange rate changes on cash and cash equivalents		(1,290,629)	1,778,300
Effect of changes allowance on cash and cash equivalents		(42,016)	-
Net increase (decrease) in cash and cash equivalents		(4,138,944)	10,163,838
Cash and cash equivalents, at the beginning of the year	4	17,138,498	6,974,660
Cash and cash equivalents, at the end of the year	4	12,999,554	17,138,498

Authorized for issue by management of the Group and signed on its behalf by:


Volodymyr Mudryi,
Chairman of the Management Board

17 August 2022




Natalija Diuba,
Chief Accountant

17 August 2022

The accompanying notes on pages from 8 to 105 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK

**Consolidated Statement of Profit or Loss and Other Comprehensive Income
for the Year Ended 31 December 2020
(In Ukrainian Hryvnias and in thousands)**

	Notes	2020	2019
Interest income	4, 23	5,118,846	5,253,438
Interest expense	4, 23	(1,361,708)	(1,635,423)
Net interest income before allowance for expected credit losses on interest-bearing assets	4	3,757,138	3,618,015
Fee and commission income	6, 23	1,683,913	1,695,811
Fee and commission expense	6, 23	(506,379)	(392,952)
Net gain on foreign exchange and precious metals operations	23	296,674	176,917
Net gain on transactions with derivative financial instruments	23	89,887	164,169
Net gain on investments measured at fair value through other comprehensive income		79,306	43,502
Net loss on modification of financial assets		(18,917)	(12,884)
Charge of allowance for expected credit losses on interest-bearing assets	5, 23	(836,210)	(145,694)
Charge of allowance for expected credit losses on other operations		(202,707)	(46,447)
Other income	23	163,980	165,598
Net non-interest income		749,547	1,648,020
Operating income		4,506,685	5,266,035
Operating expense	7, 23	(2,194,695)	(2,041,548)
Profit before income tax		2,311,990	3,224,487
Income tax expense	8	(385,627)	(557,610)
Net profit for the year		1,926,363	2,666,877
Other comprehensive income/(loss) Items that may be subsequently reclassified to profit or loss: Change in fair value of investments measured at fair value through other comprehensive income		53,015	(3,284)
Other comprehensive income/(loss)		53,015	(3,284)
TOTAL COMPREHENSIVE INCOME FOR THE YEAR		1,979,378	2,663,593
Earnings per share			
Weighted average number of outstanding ordinary shares		499,238	499,238
Basic and diluted earnings per share, UAH		3,859	5,342

Authorized for issue by management of the Group and signed on its behalf by:

Volodymyr Mudryi,
Chairman of the Management Board

29 March 2021



Natalia Diuba,
Chief Accountant

29 March 2021

The accompanying notes on pages from 11 to 84 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Financial Position as at 31 December 2020 (In Ukrainian Hryvnias and in thousands)

	Notes	31 December 2020	31 December 2019
ASSETS			
Cash and balances with the National Bank of Ukraine	9	3,510,420	3,139,593
Due from banks	10, 23	13,628,078	4,308,470
Loans to customers	11, 23	27,797,157	25,469,028
Investments measured at fair value through other comprehensive income	12	6,606,201	3,631,783
Investments measured at amortized cost	13	5,901,418	7,212,296
Property and equipment and intangible assets	14	736,439	570,535
Right-of-use assets	15	448,590	191,946
Current income tax assets		5,163	5,137
Deferred income tax assets	8	76,544	38,747
Investment property		27,857	28,152
Other assets	16, 23	224,139	233,118
TOTAL ASSETS		58,962,006	44,828,805
LIABILITIES			
Due to banks and other financial institutions	17, 23	399	567,801
Customer accounts	18, 23	47,337,814	35,094,301
Lease liabilities	19	450,684	174,425
Current income taxes payable		81,304	84,827
Other liabilities	20, 23	996,963	793,970
TOTAL LIABILITIES		48,867,164	36,715,324
EQUITY			
Share capital	21	6,186,023	6,186,023
Share premium	21	405,075	405,075
Other additional capital	21	1,236,294	1,236,294
Revaluation reserve for investments measured at fair value through other comprehensive income		125,999	71,001
Retained earnings		2,141,451	215,088
TOTAL EQUITY		10,094,842	8,113,481
TOTAL LIABILITIES AND EQUITY		58,962,006	44,828,805

Authorized for issue by management of the Group and signed on its behalf by:

Volodymyr Mudryi,
Chairman of the Management Board

29 March 2021



Natalia Diuba,
Chief Accountant

29 March 2021

The accompanying notes on pages from 11 to 84 form an integral part of these consolidated financial statements.

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Cash Flows for the Year Ended 31 December 2020 In Ukrainian Hryvnias and in thousands

	Notes	2020	2019
CASH FLOWS FROM OPERATING ACTIVITIES			
Interest received		6,043,160	4,843,858
Interest paid		(1,372,394)	(1,563,618)
Fee and commission income received		1,683,913	1,695,811
Fee and commission expense paid		(506,379)	(392,952)
Net gain on foreign exchange and banking metals operations		200,024	234,233
Net gain on transactions with derivative financial instruments		80,170	84,424
Other income received		120,704	177,171
Operating expense paid		(1,929,533)	(1,775,680)
Cash flows from operating activities before movements in operating assets and liabilities		4,319,665	3,303,247
Changes in operating assets and liabilities:			
Decrease/(increase) in due from banks		473,403	(483,132)
Increase in loans to customers		(2,566,411)	(4,077,017)
Decrease/(increase) in other assets		17,321	(68,134)
(Decrease)/increase in due to banks and other financial institutions		(189,987)	187,026
Increase in customer accounts		8,998,468	10,126,857
(Decrease)/increase in other liabilities		(163,801)	160,849
Cash inflow from operating activities before income tax		10,888,658	9,149,696
Income taxes paid		(426,973)	(206,813)
Net cash inflow from operating activities		10,461,685	8,942,883
CASH FLOWS FROM INVESTING ACTIVITIES			
Purchase of property and equipment and intangible assets		(308,293)	(198,841)
Proceeds on sale of property and equipment, intangible assets, and investment property		34,551	11,964
Purchase of investments measured at fair value through other comprehensive income		(39,510,646)	(36,760,827)
Proceeds on sale and repayment of investments measured at fair value through other comprehensive income		36,924,819	34,291,919
Purchase of investments measured at amortized cost		(508,551,359)	(112,055,301)
Proceeds on repayment of investments measured at amortized cost		509,850,000	108,521,000
Net cash outflow from purchase of an entity		-	(60,151)
Net cash outflow to investing activities		(1,560,928)	(6,250,237)

JOINT STOCK COMPANY OTP BANK

Consolidated Statement of Cash Flows for the Year Ended 31 December 2020 (Continued) (In Ukrainian Hryvnias and in thousands)

	Notes	2020	2019
CASH FLOWS FROM FINANCING ACTIVITIES			
Proceeds on borrowings from international financial institutions	17	-	367,935
Repayment of borrowings from international financial institutions	17	(367,982)	-
Repayment of lease liabilities		(147,237)	(154,803)
Net cash (outflow to)/inflow from financing activities		(515,219)	213,132
Effect of changes in foreign exchange rates on cash and cash equivalents		1,778,300	(758,703)
Net increase in cash and cash equivalents		10,163,838	2,147,075
Cash and cash equivalents, at the beginning of the year	9	6,974,660	4,827,585
Cash and cash equivalents, at the end of the year	9	17,138,498	6,974,660

Authorized for issue by management of the Group and signed on its behalf by:

Volodymyr Mudryi,
Chairman of the Management Board

29 March 2021



Natalia Diuba,
Chief Accountant

29 March 2021

The accompanying notes on pages from 11 to 84 form an integral part of these consolidated financial statements.

Joint-Stock Company OTP Bank

Consolidated Statement of Profit or Loss and Other Comprehensive Income for the Year Ended 31 December 2019 In Ukrainian Hryvnias and in thousands

	Notes	2019	2018
Interest income	4, 24	5,253,438	4,133,371
Interest expense	4, 24	(1,635,423)	(1,226,343)
Net interest income before allowance for expected credit losses on interest bearing assets	4	3,618,015	2,907,028
Fee and commission income	6, 24	1,695,811	1,445,122
Fee and commission expense	6, 24	(392,952)	(297,109)
Net gain on foreign exchange and precious metals operations	24	176,917	152,056
Net gain on transactions with derivative financial instruments	24	164,169	164,224
Net gain on investments measured at fair value through other comprehensive income (FVTOCI)		43,502	5,570
Net loss on modification of financial assets		(12,884)	(20,320)
Impairment losses on interest bearing assets	5, 24	(145,694)	(393,928)
(Provision)/recovery of provision on other operations		(46,447)	4,344
Other income	24	165,598	97,632
Net non-interest profit		1,648,020	1,157,591
Operating profit		5,266,035	4,064,619
Operating expense	7, 24	(2,041,548)	(1,662,895)
Profit before income tax		3,224,487	2,401,724
Income tax expense	8	(557,610)	(427,414)
Net profit for the year		2,666,877	1,974,310
Other comprehensive (loss)/income			
Items that may be subsequently reclassified to profit or loss:			
Change in fair value of investments measured at fair value through other comprehensive income		(3,284)	65,465
Other comprehensive (loss)/income		(3,284)	65,465
Total comprehensive income for the year		2,663,593	2,039,775
Earnings per share			
Weighted average number of outstanding ordinary shares		499,238	499,238
Basic and diluted earnings per share, UAH		5,342	3,955

Authorized for issue by management of the Group and signed on its behalf by:

Tamas Hak-Kovacs,
Chairman of the Management Board

26 March 2020



Natalia Diuba,
Chief Accountant

26 March 2020

The accompanying notes on pages from 11 to 77 form an integral part of these consolidated financial statements.

Joint-Stock Company OTP Bank

Consolidated Statement of Financial Position as at 31 December 2019 *In Ukrainian Hryvnias and in thousands*)

	Notes	31 December 2019	31 December 2018
ASSETS			
Cash and balances with the National Bank of Ukraine	9	3,139,593	2,320,458
Due from banks	10, 24	4,308,470	2,507,127
Loans to customers	11, 24	25,469,028	22,059,052
Investments measured at fair value through other comprehensive income	12	3,631,783	1,102,220
Investments measured at amortized cost	13	7,212,296	3,677,428
Property and equipment and intangible assets	14	570,535	478,898
Right-of-use assets	15	191,946	-
Current income tax assets		5,137	127,402
Deferred income tax assets	8	38,747	177,315
Investment property		28,152	39,381
Other assets	16, 24	233,118	267,857
TOTAL ASSETS		44,828,805	32,757,138
LIABILITIES			
Due to banks and other financial institutions	17, 24	567,801	441
Customer accounts	18, 24	35,094,301	26,855,632
Lease liabilities	19	174,425	-
Current income taxes payable		84,827	-
Other liabilities	20, 24	793,970	646,259
TOTAL LIABILITIES		36,715,324	27,502,332
EQUITY			
Share capital	21	6,186,023	6,186,023
Share premium	21	405,075	405,075
Other additional capital	21	1,236,294	1,236,294
Revaluation reserve for investments measured at fair value through other comprehensive income		71,001	67,683
Retained earnings/(Accumulated deficit)		215,088	(2,640,269)
TOTAL EQUITY		8,113,481	5,254,806
TOTAL LIABILITIES AND EQUITY		44,828,805	32,757,138

Authorized for issue by management of the Group and signed on its behalf by:

Tamas Hak-Kovacs,
Chairman of the Management Board

26 March 2020

Natalia Diuba,
Chief Accountant

26 March 2020


The accompanying notes on pages from 11 to 77 form an integral part of these consolidated financial statements.

Joint-Stock Company OTP Bank

Consolidated Statement of Cash Flows for the Year Ended 31 December 2019 (Continued) In Ukrainian Hryvnias and in thousands

	Notes	2019	2018
Cash flows from financing activities			
Proceeds on borrowings from international financial institutions		367,935	-
Repayment of lease liabilities		(154,803)	-
Net cash inflow from financing activities		213,132	-
Effect of changes in foreign exchange rates on cash and cash equivalents		(843,799)	(206,328)
Net increase/(decrease) in cash and cash equivalents		2,147,075	(1,058,747)
CASH AND CASH EQUIVALENTS, at the beginning of the year	9	4,827,585	5,886,332
CASH AND CASH EQUIVALENTS, at the end of the year	9	6,974,660	4,827,585

Authorized for issue by management of the Group and signed on its behalf by:


Tamas Hak-Kovacs,
Chairman of the Management Board

26 March 2020


Natalia Diuba,
Chief Accountant

26 March 2020

The accompanying notes on pages from 11 to 77 form an integral part of these consolidated financial statements.

Scientific edition

Viktoriia Kostiuk, Olha Faichuk, Oleksii Muravskyi

**MECHANISM FOR THE IMPLEMENTATION OF REMOTE
BANKING SERVICES IN THE CONTEXT OF MODERN
CHALLENGES AND THREATS**

MONOGRAPH

ISBN 978-9916-752-10-4

Publisher
Teadmus OÜ
Tallinn, Estonia
teadmus.org

Signed for printing: 2024 November 04
Conditional Printed sheets 10,5