Economic Affairs, Vol. 68(Special Issue), pp. 881-886, May 2023
DOI: 10.46852/0424-2513.2s.2023.34

AESSRA

Review Paper

Cyber Security of the System of Electronic Payment of the National Bank of Ukraine

Nataliia Vyhovska[1*], Iryna Voronenko[2], Anastasiia Konovalenko[3], Vita Dovgaliuk[1] and Iryna Lytvynchuk[1]

[1]Department of Finance and Digital Economy, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
[2]Department of Information Systems and Technologies, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
[3]Department of Economics and Business, Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia, Ukraine

[*]Corresponding author: vyhovska-nata@ukr.net (**ORCID ID:** 0000-0001-7129-6169)

Received: 21-12-2022 **Revised:** 07-04-2023 **Accepted:** 29-04-2023

ABSTRACT

In the world of today, cases of cyber attacks on banking systems have become more frequent. The aim of this research is to develop methodical and practical recommendations how to eliminate threats of oversight of payment systems, stabilize the protection of participants and users of the payment portfolio of banking institutions against misinformation and fraud. The research proposes a synergistic cyber security model of the SEP of NBU, taking into account the securitization of the payment portfolio of banking institutions in the financial market to prevent threats and meet the needs of participants and users in banking services. The article analyzes the chronology of attacks on the information resources of the NBU and the banking system during the period of martial law in Ukraine, and presents fraudulent targeted attacks "using eidetic of banking institutions of Ukraine. The criteria for the level of cyber security of the SEP of NBU are recommended. The research concludes with a determination of the reference state bank of Ukraine, which has the best combination of the level of securitization of the payment portfolio of banking institutions and the protection of active information resources. The practical significance of this research lies in providing recommendations aimed at improving the stability of cyber security in the SEP of NBU, thereby ensuring the safety of cash transactions in the digital economy.

HIGHLIGHTS

- Necessity of stabilization of cyber security in the System of Electronic Payment of the National Bank of Ukraine (SEP of NBU) in the banking sector is a relevant issue.

Keywords: Banking sector, payment portfolio, state regulator, digital economy, cash transactions.

In the conditions of aggravation of threats to the economy of Ukraine, the problem of protecting national interests, in particular the protection of the electronic payment system of the banking sector, is becoming especially relevant. The banking sector relies on external regulatory mechanisms to protect the national currency, manage financial capital, and handle cyber attacks and fraud. Without proper safeguards, this could result in financial losses and destabilize the country's financial system.

There is no cyber security of the electronic payment system in the non-banking sector. However, subjectively determined threats have two main forms of manifestation: violence (physical influence) and disinformation (information influence). Financial threats often manifest as an attempt by criminals or fraudsters to destroy payment systems and appropriate financial resources through actions that

How to cite this article: Vyhovska, N., Voronenko, I., Konovalenko, A., Dovgaliuk, V. and Lytvynchuk, I. (2023). Cyber Security of the System of Electronic Payment of the National Bank of Ukraine. *Econ. Aff.*, **68**(Special Issue): 881-886.

Source of Support: None; **Conflict of Interest:** None

appear to be legal and/or economically justified. In the payment systems of the banking sector, there is a conflict of interests, which is disguised as the optimization of information media to accelerate the flow of financial resources through electronic payments. Therefore, the immediate protection of payment transactions in the network of banking institutions is the result of the electronic resources regulator's timely response to fraud and misinformation regarding the legality of financial flows between users of payment systems.

The problems of managing financial instruments of payment systems in the flow of settlement operations were examined by the scientists A. Abramova (2021), A. Dadoukis *et al.* (2021), B. Issina *et al.* (2022), who methodologically defined an analytical synthesis between the cyber security of the information space of banking institutions and the national security regulators of the state regarding the protection of clients' interests. The scientists P. Huo and L. Wang (2022), I. V. Voronenko and N. A. Klymenko (2022), M. Peihani (2022), A. Shabbir *et al.* (2022) shaped the concept of financial security of the banking sector and experimentally verified all its provisions regarding hedging the risks of the electronic payment system, connected with the strategic orientations of the development of the state's economy.

This research aims to develop the methodical and practical recommendations for the stabilization of cyber security of the SEP of NBU, which, in the conditions of cyber attacks, eliminates the threat of oversite payment systems, protects the participants and users of the payment portfolio of banking institutions against misinformation and fraud.

MATERIALS AND METHODS

A methodological approach for determining the level of cyber security of the banking service hierarchy of participants and users of the SEP of NBU has been proposed. It includes building an integrated model of confidentiality, integrity, authenticity, and reliability of banking services, assessing the probability of threat impacts on information security, oversite security of payment systems, and SPPB, and determining indicators of the protection of banking information resources. The approach aims to ensure the cyber security of the SEP of NBU (Forcadell *et al*. 2020; Trofymenko *et al*. 2019; Voronenko *et al*. 2022). Data from Table 1 is used to determine the weighting coefficients α_i, that determine the conditions for the manifestation of the *i*-th threat.

Table 1: Selection of weighting coefficients α_i for the manifestation of the *i*-th threat and its occurrence in the hierarchy of banking services for participants and users of the SEP of NBU

Weighting coefficients a_i	Conditions of manifestation of the threat
0.067	The threat appears no more than once every 5 years
0.133	The threat appears no more than once a year
0.2	The threat appears no more than once a month
0.267	The threat appears no more than once a week
0.333	The threat appears every day

At the next stage, based on the results of a comprehensive assessment of threats to objects IS, OSPS, SPPB in the model hierarchy of banking services of participants and users of the SEP of NBU – indicators of the protection of banking information resources are determined under the condition of oversite payment systems and the payment portfolio of banking institutions on the financial market to ensure cyber security of the SEP of NBU.

The proposed cyber security methodology by the NBU's SEP increases the protection of banking information resources and addresses hybrid threats such as disinformation and fraud. It also prevents ineffective actions in securing payment portfolios in the financial market. The methodology uses a mathematical toolkit to evaluate the cost-efficient integration of payment systems in the banking sector with open communication channels, while ensuring integrity, confidentiality, authenticity, and reliability of banking information resources. The toolkit also evaluates the functionality of the system of electronic payments.

RESULTS

The cyber security of NBU's SEP is essential in protecting the payment space at macro-, meso-, and microlevels. At the macro level, it warns

users of payment transfer services of cyber-attacks, monitors credit and investment flows, and integrates Fintex-technologies into the payment potential of the state, ensuring profitability and liquidity of banking institutions (Forcadell *et al*. 2019; Horna *et al*. 2022; Trusova and Chkan, 2021). However, payment systems in banking institutions face significant threats due to the high volume and size of operations, affecting payment instruments, delivery systems, communication, clearing, settlement mechanisms, and the economy as a whole.

The National Bank of Ukraine is urging regulators to protect the banking sector's information resources in cyberspace, as it directly influences the functioning of payment systems. The interaction between the National Bank and banking institutions in adopting innovative payment systems expands the functional capabilities of the national space of payment systems and its participants (Trusova *et al.* 2021b). However, outdated payment system innovations contribute to the development of the interbank periphery, consolidating its subordinate position in relation to the center. This poses threats of a depository, investment, credit, operational, systemic nature, and a decrease in liquidity in the participants of the system, which are overseen by the banking sector's regulatory body (Trusova *et al*. 2021a).

To minimize cyber-attacks, the National Bank of Ukraine (2022) determines target orientations for participants and users of their payment systems through banking institutions. This is done by analyzing threats to the interbank periphery of payment systems, anticipating deviations from expected results, and introducing Fintex-innovations that optimize payment portfolios with maximum threat protection. These innovations address credit, operational, liquidity, technological, and informational threats in the SEP of NBU's space (Nehrey *et al*. 2022).

Thus, The National Bank of Ukraine preparation for a cyber-attack in 2022 stabilized the functioning of the SEP, limiting the risks of settlement operations for participants and users of payment systems, both domestically and internationally. This was crucial for preserving the liquidity of Ukrainian banks and maintaining the country's currency capital. Despite the ongoing war, innovative banking services for individuals and legal entities were fully restored, and the SEP processed an average of 1.4 million payments worth 10.3 billion EUR daily. However, the SEP has the potential to process ten times more documents daily than in the current war period, according to the National Bank of Ukraine (2022).

In 2022, the National Bank of Ukraine implemented a more flexible security policy which included measures such as key management, remote access and use of cloud systems. Despite threats from DDoS-attacks and encryption viruses, there were no security breaches in the System of Electronic Payment. However, the use of cloud technology requires a certain level of maturity from their providers, and Ukrainian legislation is not fully harmonized with cloud service providers (The Network Readiness Index, 2019). The NBU recommends the use of cloud technology by banking institutions, but emphasizes the importance of being responsible and complying with financial monitoring and information disclosure regulations. The most popular banking services from 2020-2022 were payment cards, QR-payments, internet banking and mobile banking, with averages of 83%, 81%, 74% and 53% respectively (National Bank of Ukraine, 2022; National Cyber Security Index, 2022; World Development Indicators, 2022).

Thus, based on the results of the assessment of the threats to the payment systems of banking institutions of Ukraine, considering their impact on the level of cyber security of the SEP NBU, it can be concluded that in 2022, the most cyber-attacks were conducted against the payment systems "Google Pay" and "Monobank". During the I-IV quarters of 2022, the level of influence of threats of these payment systems on the integrated level of cyber security of the SEP of NBU ranged from 0.516 to 0.235 (payment system "Google Pay") and from 0.644 to 0.131 (payment system "Monobank"), which is due to the high level of cyber-attacks on credit and deposit security information resources (from 0.504 to 0.22 in payment system "Google Pay" and from 0.637 to 0.1 in payment system "Monobank"), a high level of fraud in money transfer information resources (from 0.608 to 0.15 in payment system "Google Pay" and from 0.647 to 0.134 in payment system "Monobank"), as well as threats to the information security of payment systems in general (from 0.644 to 0.329 in payment

system "Google Pay" and from 0.645 to 0.143 in payment system "Monobank").

A high level of threats of cyber attacks was observed on the national payment system "Prostir", in particular, in the I-II quarter of 2022 – from 0.301 to 0.104(threat level to credit and deposit security), from 348 to 0.25 (threat level to money transfers), from 0.326 to 0.214 (threat level of QR-payments), as well as in the I-IV quarters of 2022 – from 0.421 to 0.301 (level of information security threats) technological and information security. Such dynamics provoked the blocking of payments through the "Prostir" payment system, which lowered the cyber security level of the SEP of NBU from 0.301 to 0.122, respectively.

Thus, to measure the securitization of payment portfolios and protection of active information resources for various banks, the primary threat for JSC "Ukrgasbank" and JSC "Ukreximbank" is cyber attacks on Fintex-innovations, money transfers, and QR-payments. For JSC "Oschadbank" and JSC CB "Privatbank" it is pricing policies affecting active information resources of Fintex-innovations. The level of securitization and protection of payment portfolios and active information resources can be calculated using a formula, which considers the measures taken to ensure cyber security in the SEP of NBU, particularly in Fintex-innovations (Yehorycheva, 2011):

$$I_{fSPPB} = \frac{RL}{(PC + LC)}, \quad \ldots(1)$$

where, I_{fSPPB} – the level of securitization of the payment portfolio and protection of active information resources of the banking institution to ensure the cyber security of the SEP of NBU, taking into account Fintex-innovations; *RL* – recovered loss in the field of Fintex-innovation in the event of a cyber-attack on information resources; *PC* – preventive costs incurred by the bank in the field of Fintex-innovation to protect information resources in the event of a cyber attack; *LC* – liquidation costs incurred by the bank in the field of Fintex-innovation in the event of a cyber attack on information resources. The paired linear regression model, where the mean value of the dependent variable is considered as a function of one independent variable (x), is presented in formula:

$$\hat{y}_x = f(x) \quad \ldots(2)$$

The regression equation is reduced to the estimation of its parameters. For this, the method of least squares was used, that allows for obtaining parameters in which the sum of squares of the deviations of the actual values of the resulting characteristic (y) from the theoretical ones ($\hat{y}_x$) is minimal. The closeness of the connection of the studied phenomena is estimated by the linear pair correlation coefficient (r_{xy}) for linear regression (–1≤1):

$$r_{xy} = \frac{\text{cov}(x, y)}{\sigma_x \sigma_y} \quad \ldots(3)$$

where, $cov(x,y)$ – is the covariance of signs x and y, respectively; σ_x σ_y– variances x and y.

Thus, the cyber security level of NBU's System of Electronic Payment relies on the "current level of SPPB" of JSC CB "Privatbank". Securitizing the payment portfolio of the state banking institution can protect the pricing of services and maintain information resource activity against credit security threats. This also considers the costs associated with restoring Fintex-products following a cyber-attack. The process of "management of SPPB" focuses on managing the price policy of information resources of credit security with the coordination of the cost mechanism of the digitalization of Fintex-innovations, preventing a cyber attack on Fintex-products, and thus, allows for stabilizing the level of cyber security of the SEP of NBU.

The study identified JSC CB "Privatbank" as the reference state bank with the best combination of securitization of the payment portfolio and protection of active information resources while meeting requirements in areas such as "current level of SPPB", "management of SPPB", and "level of awareness of SPPB". The model developed in the study uses mathematical descriptions of components and functions to calculate the level of cyber security of the System of Electronic Payment of NBU, reflecting the essential properties of protecting Fintex-innovation information resources in case of cyber-attacks. The study also found a correlation between the increasing indicator of SPPB of JSC

CB "Privatbank" and the level of cyber security of the National Security Service of NBU, with graphs illustrating the intensity of the relationship. (Formulae (30-32) (ISO/IEC 27001, 2022).

DISCUSSION

The issue of stabilizing cyber security of electronic payment system of the NBU SEP in the event of an aggravation of the problem of cyber attacks has been considered by many scientists in their scientific works. In particular, the article by A. Bahuguna *et al.* (2020) focuses on the country-level cyber security posture assessment and analyzes the practices involved in this process. The authors emphasize the need for a collaborative and coordinated effort between government agencies, private sector organizations, and international partners to effectively assess and improve a country's cyber security posture. The proposed framework could serve as a useful tool for policymakers and cyber security practitioners to identify areas of strength and weakness in a country's cyber security posture and develop appropriate strategies to address them.

The group of scientists T.M. Eisenbach *et al*. (2022) develop this proposal. They highlight the need for financial institutions and regulators to continue to invest in cyber security measures and improve their ability to detect and respond to cyber threats. The article provides a pre-mortem analysis of the potential consequences of a systemic cyber attack on the financial system of the United States, using a combination of scenario analysis and stress testing. The authors consider various scenarios, such as a disruption of the payment system, a loss of confidence in financial institutions, and a widespread data breach. The described experience may be used in developing recommendations for avoiding cyber attacks on the banking system of Ukraine.

In turn, A. Javed *et al*. (2022) in their article propose to develop a real-time cyber attack forecasting model using security analytics. The authors suggest a framework that incorporates different types of data sources, including network traffic data and cyber threat intelligence, to predict future cyber attacks. The study finds that it can provide a more accurate and efficient approach to early detection and response to cyber threats. The security analytics could play a significant role in predicting and preventing cyber attacks, especially when used in real-time.

The article by N.V. Trusova *et al*. (2021) points on credit-investment activity of banks in Ukraine, with a particular emphasis on the impact of financial globalization, risks, and stabilization. The study aims to analyze the dynamics and structure of credit investments in Ukrainian banks, as well as to identify the factors that affect their stability. The authors argue that banks need to adopt more effective risk management strategies to improve their stability and resilience in the face of changing market conditions. This idea can be seconded for the reason that credit investments in Ukrainian banks have grown significantly over the past few years, but at the same time, they have become riskier due to increased competition, reduced interest rates, and the impact of global economic factors.

In conclusion, various scientific works have discussed the need for stabilizing the cyber security of NBU's SEP in the event of cyber attacks, as digitalization has increased the complexity and scope of risks faced by commercial banks. To mitigate these risks, new and innovative risk management strategies are necessary.

CONCLUSION

Thus, ensuring the balance of the money supply should be carried out on the basis of the effective use of tools for the protection of information resources in the electronic payment system, by strengthening in the monetary policy of banking institutions the security of money transfers, the cost of services for Fintex-products that simplify QR-payments for participants and users of payment systems. One of the tools that the SEP participants can use as a factor in the formation of a moderate structural deficit of liquidity in banking institutions to control cyber-attacks on payment systems is the monetary regulator of mandatory requirements. It provides for improvement of the SEP of NBU criteria by differentiating the amount of reserve money in the bank deposits by target orientation; reducing the amount of required reserves by the amount of long-term investment loans provided at the expense of self-generated resources, the amount of purchased of Interior State bond loans (ISBL) and deposit

certificates of the NBU; introduction of accrual and payment of interest on the amount of required reserves in the payment portfolio of banking institutions in order to increase the efficiency of payments and transfers of the participants of the SEP of NBU.

At the same time, this tool in the monetary and credit regulation of banking institutions does not belong to the number of operational ones, but is used only in the conditions of the occurrence of systemic and structural disproportions and the instability of the functioning of the information resources of the banking sector in the event of the threat of a cyber-attack on new payment systems. Therefore, it is expedient to transform this tool of monetary influence from the list of tools for the operational functioning of the SEP of NBU to the category of tools for long-term and structural influence on strengthening protection against threats of macro-financial destabilization in the payment system.

REFERENCES

Abramova, A. 2021. The risk system of commercial banks in conditions of digitalization. *Probl. and Prosp. of Econ. and Manag.*, **4**(28): 186-193.

Bahuguna, A., Bisht, R.K. and Pande, J. 2020. Country-level cybersecurity posture assessment: Study and analysis of practices. *Inf. Sec. J.*, **29**(5): 250-266.

Dadoukis, A., Fiaschetti, M. and Fusi, G. 2021. IT adoption and bank performance during the COVID-19 pandemic. *Econ. Let.*, **204**: 109904.

Eisenbach, T.M., Kovner, A. and Lee, M.J. 2022. Cyber risk and the U.S. financial system: A pre-mortem analysis. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf (Last Accessed on 19th April, 2023).

Forcadell, F.J., Aracil, E. and Ubeda, F. 2019. The influence of innovation on corporate sustainability in the international banking industry. *Sust.*, **11**(11): 3210.

Forcadell, F.J., Aracil, E. and Ubeda, F. 2020. The impact of corporate sustainability and digitalization on international banks' performance. *Glob. Pol.*, **11**(S1): 18-27.

Horna, C.J., Toro, L. and Regalado-Pezua, O. 2022. Silver bank: Vulnerability and risks during cyberattacks. *Emer. Emerg. Mark. Case Stud.*, **12**(1): 1-33.

Huo, P. and Wang, L. 2022. Digital economy and business investment efficiency: Inhibiting or facilitating? *Res. in Inter. Bus. and Fin.*, **63**: 101797.

ISO/IEC 27001. 2022. https://www.iso.org/isoiec-27001-information-security.html (Last Accessed on 19th April, 2023).

Issina, B., Bekzhanova, S., Ananiev, S. and Kenzhekeeva, A. 2022. Prospects for the development of digital economy in the Republic of Kazakhstan. *AIP Conf. Proc.*, **2449**: 040001.

Javed, A., Lakoju, M., Burnap, P. and Rana, O. 2022. Security analytics for real-time forecasting of cyberattacks. *Soft.: Pract. and Exp.*, **52**(3): 788-804.

National Bank of Ukraine. 2022. https://bank.gov.ua/ (Last Accessed on 19th April, 2023).

National Cyber Security Index. 2022. https://ncsi.ega.ee/ncsi-index/ (Last Accessed on 19th April, 2023).

Nehrey, M., Voronenko, I.V., Salem, A.B.M. 2022. Cyber security assessment: World and Ukrainian experience, pp. 335-340. *In:* 2022 12th International Conference on Advanced Computer Information Technologies. IEEE, Ruzomberok.

Peihani, M. 2022. Regulation of cyber risk in the banking system: A Canadian case study. *J. of Fin. Reg.*, **8**(2): 139-161.

Shabbir, A., Shabir, M., Javed, A.R., Chakraborty, C. and Rizwan, M. 2022. Suspicious transaction detection in banking cyber-physical systems. *Comp. & Elect. Eng.*, **97**: 107596.

The Network Readiness Index: Towards a future-ready society. 2019.https://networkreadinessindex.org/wp-content/uploads/2020/03/The-Network-Readiness-Index-2019-New-version-March-2020.pdf (Last Accessed on 19th April, 2023).

Trofymenko, O., Prokop, Y., Loginova, N. and Zadereyko, O. 2019. Cybersecurity of Ukraine: Analysis of the current state. *Ukr. Inf. Sec. Res. J.*, **21**(3): 150-157.

Trusova, N.V. and Chkan, I.O. 2021. Payment systems in Ukraine and risks of their functioning. *Bus. Inf.*, **1**(516): 257-263.

Trusova, N.V., Hryvkivska, O.V., Melnyk, L.V., Gerasymova, O.V. and Tereshchenko, M.A. 2021b. The risks of payment systems of banking institutions of Ukraine. *Univ. J. of Acc. and Fin.*, **9**(4): 637-652.

Trusova, N.V., Melnyk, L.V., Shilo, Z.S. and Prystemskyi, O.S. 2021a. Credit-investment activity of banks of the Ukraine: Financial globalization, risks, stabilization. *Univ. J. of Acc. and Fin.*, **9**(3): 450-468.

Voronenko, I.V. amd Klymenko, N.A. 2022. Innovative development in the context of digitalization: Assessment and priorities. *Ekon. ta Derzh.*, **2**: 38-45.

Voronenko, I.V., Nehrey, M., Laptieva, A., Babenko, V. and Rohoza, K. 2022. National cybersecurity: Assessment, risks and trends. *Int. J. of Emb. Syst.*, **15**(3): 226-238.

World Development Indicators. 2022. https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on (Last Accessed on 19th April, 2023).

Yehorycheva, S.B. 2011. Methodological principles of organization of innovation process in commercial banks. *Bul. of the Nat. Bank of Ukr.*, **1**: 53-57.