та підтримці кібербезпеки. Застосовуючи новітні технологічні розробки та досягнення, банківські організації мають можливість не тільки підвищувати свою операційну ефективність, але й задовольняти потреби клієнтської бази.

Список використаних джерел

1. Як банки адаптуються до воєнних реалій за допомогою хмарних технологій. URL: https://fintechinsider.com.ua/yak-banky-adaptuyutsya-do-voyennyh-realij-za-dopomogoyu-hmarnyh-tehnologij/ (дата звернення 29.01.2025).

2. Український фінтех у 2024 році: ключові цифри та факти. URL: https://fintechinsider.com.ua/ukrayinskyj-finteh-u-2024-roczi-klyuchovi-czyfry-ta-fakty/ (дата звернення 29.01.2025).

3. Blockchain technology market share forecast worldwide in 2021, by use case. Statista. URL: https://www.statista.com/statistics/982566/worldwide-top-use-cases-blockchain-technology-by-market-share (дата звернення 30.01.2025).

Oleksii Melnyk
Postgraduate Student (PhD)
Dmytro Motornyi Tavria State Agrotechnological University
Zaporizhzhia, Ukraine

SECURITY OF THE BANKING SYSTEM BASED ON THE METASPACE OF FINTECH SERVICES

The banking system intervenes in all sectors of the economy, serves non-cash payments, carries out storage of funds and credit servicing of clients through national and foreign exchange flows. Its mechanism of functioning in Ukraine depends on external regulators of protection of the national currency, capitalization and distribution of financial capital on electronic payment media, which are characterized by a high level of cyberattacks and threats of fraud. In the absence of protective information resources, this can lead to loss of financial flows when servicing users in the payment landscape of

banking institutions, and, accordingly, radically destabilize the financial system of the state as a whole.

The danger in the banking system is subjectively caused by financial threats, which often manifest themselves as an attempt by criminals or fraudsters to destroy payment systems and appropriate financial resources through actions that are given the appearance of legal and (or) economically justified. Therefore, in a multi-space payment system there is a conflict of interest between decentralized finance of the metaspace, which is disguised in information carriers to accelerate the flow of financial resources, and centralized regulatory levers of settlement operations in the interbank market. Their instant protection in the banking system network is carried out on the basis of FinTech service tools, which react with intense speed to new payment systems emerging in banking services. These circumstances force the banking sector to integrate into the digital economy by introducing mobile applications, contactless payments for online lending, the use of artificial intelligence for electronic transactions of venture financing, credit investment in the real sector of the economy [2].

The adaptation of the banking system to decentralized macro-financial regulators using the state's reform policy should be combined in the functions of FinTech services to eliminate contradictions in the diversified multifunctional structure of payment systems formed on the Blockchain technology platform. On the one hand, Blockchain technologies centralize, and on the other hand, decentralize the system of a public registry of cryptocurrency based on cryptographic algorithms for combining the capital of investment and credit institutions with the maximum increase in the profitability of financial transactions, forming electronic wallets in the interbank market. The effective combination of Blockchain technologies and FinTech services as tools for intensifying the development of the metaspace in the interbank system allows you to translate all possible payment registers into an electronic distribution form of investment and financial flows in the currency industry market and activate financial chains in the capital market [1].

The constant increase in the influence of metaspace tools on the cyberspace of the banking system protects it from threats of cybernetic origin, developed at the global level by international institutions, and laid down in the national strategy of banking policy of

each state. The inclusion of Blockchain technologies and FinTech services in the Internet network 24/7 to preserve the confidentiality of information resources of the banking system prevent cybercrime with the aim of illegally seizing financial flows. The harmonious interaction of metaspace financial tools in the segment of banking products is combined with the phenomenon of their virtualization at the level of private-public partnership, which is based on daily technological achievements, the growth of the share of electronic money in payments, online trading, online banking, mobile financial services, etc. [3].

From a single security perspective of the banking system, the level of the banking service hierarchy for participants and users of the NBU SEP is determined based on a comprehensive assessment of threat objects in the metaspace of FinTech services, taking into account Blockchain technology tools. This methodology allows for a formal assessment of the security of the oversight of payment systems (SOPS) and the security of the payment portfolio of banking institutions (SPPB). The assessment platform includes: building an integrated holistic model of FinTech regulators when changing the parameters of information resources in order to identify potential threats to SOPS and SPPB objects in the interbank market and ensure the stable functioning of the NBU SEP.

However, cyberattacks on the banking system have serious negative consequences for users and consumers of payment systems, which depend on the integrity of the functioning of FinTech regulators, which are divided into two types (ISA/IEC 62443; ISO/IEC 27001): the first type is mandatory FinTech regulators to meet the requirements for protecting the financial resources of banking institutions; the second type is recommended FinTech regulators to meet the requirements for protecting the information resources of the NBU's SEP [4].

Blockchain is a decentralized (in the classical sense) system of a public registry of information and financial resources, based on cryptographic algorithms and containing data on all previously conducted banking and payment system transactions.

Schematically, the structure of the blockchain looks like this: each transaction is encoded with a special set of characters and forms a hash. The set of hashes is also encoded and forms a new hash. The set of hashed hashes is also encoded and forms a

block. Each change in the hash or block causes a change in the hashes of the previous ones, which determines the reliability of the system for servicing information resources of the banking system in the input languages of FinTech regulators [5].

From the position of virtualization of centralized and decentralized Blockchain spheres, the focus of their action is modified at the request of the objects of protection, and since their functionality when conducting transactions for electronic operations enables only partial security of the objects under study, therefore, to increase the level of protection of banking transaction servicing, aggregate hashed registers must interact with FinTech regulators as a holistic platform of a secure banking system.

References

1. Barr M.S., Harris A., Menand L., Xu W. Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion. *Center on Finance, Law & Policy*. 2020. Vol. 1-28. http://dx.doi.org/10.2139/ssrn.3664790.

2. Doran N.M., Bădîrcea R.M., Manta A.G. Digitization and financial performance of banking sectors facing Covid-19 challenges in central and eastern European countries. *Electronics (switzerland)*. 2022. Vol. 11(21). P. 3483. https://doi.org/10.3390/electronics11213483.

3. Huo P., Wang L. Digital economy and business investment efficiency: Inhibiting or facilitating? *Research in International Business and Finance*. 2022. Vol. 63. doi: https://doi.org/10.1016/j.ribaf.2022.101797.

4. Laitsou E., Kargas A., Varoutas D. Digital Competitiveness in the European Union Era: The Greek Case. *Economies*. 2020. Vol. 8(4). P. 85. https://doi.org/10.3390/economies8040085.

5. Naderi E., Pazouki S., Asrari A. A remedial action scheme against false data injection cyber attack sin smart transmission systems: Application of thy ristor-controlled series capacitor (TCSC). *IEEE Transaction son Industrial Informatics*. 2022. Vol. 18(4). P. 2297-2309. https://doi.org/10.1109/TII.2021.3092341.