АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

ЗБІРНИК МАТЕРІАЛІВ
II МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«НАУКОВИЙ ВИМІР ОСМИСЛЕННЯ ТА ПОШУКУ ОПТИМАЛЬНИХ МОДЕЛЕЙ РОЗВИТКУ УКРАЇНИ: МАРКЕТИНГОВИЙ, ЕКОНОМІЧНИЙ, ФІНАНСОВИЙ, УПРАВЛІНСЬКИЙ ТА ПРАВОВИЙ АСПЕКТИ»
(19 БЕРЕЗНЯ 2025 РОКУ, М. КИЇВ, УКРАЇНА)

КАФЕДРА МАРКЕТИНГУ

КИЇВ – 2025

НАУКОВИЙ ВИМІР ОСМИСЛЕННЯ ТА ПОШУКУ ОПТИМАЛЬНИХ МОДЕЛЕЙ РОЗВИТКУ УКРАЇНИ: МАРКЕТИНГОВИЙ, ЕКОНОМІЧНИЙ, ФІНАНСОВИЙ, УПРАВЛІНСЬКИЙ ТА ПРАВОВИЙ АСПЕКТИ : збірник матеріалів ІІ Міжнародної науково-практичної конференції, м. Київ, 19 березня 2025 р. Київ: Академія праці, соціальних відносин та туризму / За заг. ред.: Н.В. Писаренко, В.Б. Сухомлин, – Київ. 2025. 378 с.

Викладено матеріали доповідей учасників конференції, в яких розглянуто проблематику маркетингових, економічних, фінансових, управлінських та правових пошукових моделей майбутнього розвитку України.

Для науковців, фахівців, викладачів закладів вищої освіти, здобувачів вищої освіти всіх рівнів.

Рекомендовано Вченою радою Академії праці, соціальних відносин та туризму
(протокол № 8 від 25.03.2025 р.)

За виклад, зміст і достовірність матеріалів відповідальні автори
Матеріали друкуються мовами оригіналу: українська, англійська

СЕКЦІЯ 4. СУЧАСНІ ТЕНДЕНЦІЇ ІННОВАЦІЙНОГО РОЗВИТКУ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ ТА ЕКОНОМІЧНОЇ БЕЗПЕКИ

SECTION 4. CURRENT TRENDS IN INNOVATIVE DEVELOPMENT IN THE CONTEXT OF FINANCIAL AND ECONOMIC SECURITY

Matsuka V.,
PhD in Economics, Associate Professor,
Associate Professor of the Department of Management and Finance
Horbashevska M.,
PhD in Economics, Associate Professor,
Associate Professor of the Department of Management and Finance,
Mariupol State University,
Kyiv, Ukraine

FINANCIAL TRANSACTION SECURITY MANAGEMENT USING BIOMETRICS

In today's financial environment, characterized by the rapid development of digital technologies, the issue of transaction security is becoming particularly relevant. Traditional authentication methods, such as passwords and PIN codes, are gradually losing their effectiveness due to the growing threats of cyber fraud. In this context, biometric technologies are becoming a key tool for increasing the level of financial security, as they provide unique identification of the user based on physical or behavioral characteristics.

The purpose of the study is to analyze the use of biometric technologies in financial security management, determine their effectiveness, potential risks, and development prospects.

The introduction of biometrics into the financial sector not only helps increase payment security, but also optimizes risk management processes, which makes this topic relevant.

Biometric authentication is becoming an important tool in ensuring the security of financial transactions, in particular due to its ability to provide a high level of accuracy and convenience for users. Various types of biometrics are used to verify identity, making the authorization process simple and reliable [5].

Fingerprints are one of the most common identification methods used in mobile banking and payment systems.

Facial recognition – provides fast and convenient authentication, used in financial applications and ATMs.

Voice identification – used to verify identity during telephone financial transactions.

Iris scanning is one of the most accurate methods that provides a high level of security.

Behavioral biometrics – analyzes typing style, screen touch rhythm, and other unique features of user behavior.

Principles of operation and role of artificial intelligence:

Biometric systems work based on the analysis of the user's unique physical or behavioral characteristics [4].

For identification, the data is compared with previously saved templates.

Artificial intelligence (AI) improves identification accuracy, reduces false positives, and detects fraudulent activity.

Machine learning algorithms are able to adapt to changes in users' appearance and analyze anomalies in financial behavior.

The use of AI in biometric systems contributes to faster and more secure processing of financial transactions.

Biometrics combined with artificial intelligence is a key trend in the financial sector, allowing for increased payment security and improved user experience.

Security management of biometric financial systems.

Implementation and risk management.

The implementation of biometric systems requires a comprehensive approach: technology integration, data protection, and risk management.

Main threats: biometric data leakage, fraud with "fake" biometric samples, cyberattacks.

Risk management methods: use of multi-factor authentication, data encryption, decentralized storage of biometric templates [1].

Constant monitoring and updating of security systems are key to reducing vulnerabilities.

Regulation and security standards (GDPR, PSD2)

GDPR (General Data Protection Regulation, EU) – regulates the storage and use of biometric data, requires users to obtain consent and ensure their right to delete information [2].

PSD2 (Second Payments Directive, EU) – obliges financial institutions to use strong authentication.

(SCA), which includes biometrics as one of the security methods.

Compliance with international standards such as ISO 27001 (information security) and FIDO2 (passwordless authentication) is essential for financial institutions [3].

Security management of biometric financial systems requires a comprehensive approach that combines technological, legal, and economic aspects.

Risks of biometric systems (hacking, privacy).

Biometric data compromise – leaked fingerprints or facial scans cannot simply be "changed" like a password, making them a valuable target for hackers.

Artificial forgery of biometric identifiers – the development of deepfake technologies allows for the creation of realistic fake faces and voices.

Privacy and regulatory requirements – storing biometric data raises questions about compliance with personal data laws (GDPR, CCPA).

Physical limitations – damaged fingerprints, changes in appearance, or a hoarse voice can cause problems with identification.

Trends: blockchain, artificial intelligence, passwordless payments

Blockchain for biometric data protection – decentralized technologies allow biometric templates to be stored in an unchangeable form without centralized servers.

Artificial Intelligence to Improve Accuracy – AI analyzes user behavioral patterns, which increases the accuracy of biometric authentication.

Passwordless payments – biometrics are gradually replacing traditional passwords, simplifying financial transactions (e.g. PayPal Passkey, Google Pay Face Authentication).

Multi-biometrics – combined identification methods (e.g. facial recognition + behavioral biometrics) increase the level of security.

Biometrics reduce fraud risks due to the uniqueness of user characteristics. The main threats are data leakage and counterfeiting, so encryption and blockchain are important for protection. It is important to comply with standards such as GDPR and PSD2 to protect data. The implementation of biometrics reduces security costs, increases transaction efficiency and user trust. Further research and improvement of security standards are needed.

References:

1. Directive (EU) 2015/2366 of the European Parliament and of the Council On Payment Services in the Internal Market (PSD2). 2015. URL: https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng (accessed 10 March 2025).

2. European Union. General Data Protection Regulation (GDPR). 2016. URL: https://gdpr-info.eu/ (accessed 10 March 2025).

3. FIDO Alliance. FIDO2: A New Standard for Passwordless Authentication. 2020. URL:

https://fidoalliance.org/fido2/ (accessed 10 March 2025).

4. Müller M.M., Dittmann J. Biometric Security: Fundamentals, Applications, and Case Studies. 2019. Wiley-IEEE Press.

5. Patel S., Sharma A. Advances in Biometrics: Systems and Applications. Springer. 2020.

Sheludko Sergii,
Ph.D. (Economics), Associate Professor,
State Tax University,
Irpin, Ukraine

FOREIGN EXCHANGE RESERVES DEPLOYMENT AND UKRAINE'S FINANCIAL SECURITY IN TERMS OF WARTIME CHALLENGES

In the context of unprovoked military aggression against Ukraine, the effectiveness of managing its financial security is directly contingent upon the ability to maintain an adequate level of international liquidity. Relevant measures encompass not only the attraction and rational allocation of international financial assistance but also the optimization of existing resource utilization, restructuring of external debt, and effective foreign exchange oversight. Thus, international liquidity, typically a routine objective of financial policy during periods of economic growth, elevates to a priority of state financial security in times of crisis.

When examining the deployment of foreign exchange reserves in the context of aligning state financial security management with wartime challenges, two key aspects warrant attention. First, are actual reserves being inadvertently used to facilitate further outflows of foreign currency assets into non-institutional savings? Second, does the structure of reserves remain adequate in terms of their intended applications?

The answer to the first question lies in identifying a clear relationship between the dynamics of foreign exchange interventions and the flow of foreign currency from the domestic market into informal savings (Fig. 1).
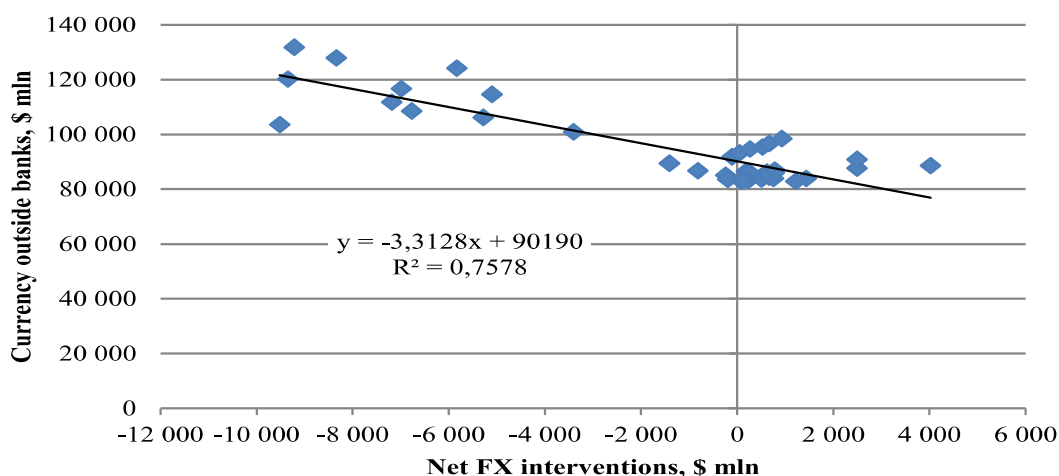

Fig. 1. Dependence of foreign cash outside the banking system on net FX interventions in Ukraine, 2015 – 2024Q3
Calculated based on [4]

An ordinal graphical analysis of the trend depicted in Fig. 1 demonstrates a relatively robust linear relationship (with a 75% level of determination) between informal cash currency savings and the net foreign exchange interventions of the National Bank of Ukraine (NBU). At a neutral level of