







“The use of biometric technologies for bank transaction security management against the background of the international experience: Evidence from Ukraine”

AUTHORS	Mykola Kurylo  Alyona Klochko  Nataliia Volchenko  Nataliia Klietsova  Anna Bolotina 
ARTICLE INFO	Mykola Kurylo, Alyona Klochko, Nataliia Volchenko, Nataliia Klietsova and Anna Bolotina (2021). The use of biometric technologies for bank transaction security management against the background of the international experience: Evidence from Ukraine. <i>Banks and Bank Systems</i> , 16(2), 47-58. doi: 10.21511/bbs.16(2).2021.05
DOI	http://dx.doi.org/10.21511/bbs.16(2).2021.05
RELEASED ON	Tuesday, 11 May 2021
RECEIVED ON	Wednesday, 17 March 2021
ACCEPTED ON	Wednesday, 05 May 2021
LICENSE	 This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Banks and Bank Systems"
ISSN PRINT	1816-7403
ISSN ONLINE	1991-7074
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”



NUMBER OF REFERENCES

34



NUMBER OF FIGURES

2



NUMBER OF TABLES

0

© The author(s) 2021. This publication is an open access article.



BUSINESS PERSPECTIVES



LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine
www.businessperspectives.org

Received on: 17th of March, 2021

Accepted on: 5th of May, 2021

Published on: 11th of May, 2021

© Mykola Kurylo, Alyona Klochko,
Nataliia Volchenko, Nataliia Klietsova,
Anna Bolotina, 2021

Mykola Kurylo, Doctor of Law,
Professor, First Vice-Rector, Sumy
National Agrarian University, Ukraine.

Alyona Klochko, Doctor of Law,
Associate Professor, Head of the
International Relations Department,
Sumy National Agrarian University,
Ukraine. (Corresponding author)

Nataliia Volchenko, Ph.D. in
Economics, Associate Professor,
International Relations Department,
Sumy National Agrarian University,
Ukraine.

Nataliia Klietsova, Ph.D. in Economics,
Associate Professor, International
Relations Department, Sumy National
Agrarian University, Ukraine.

Anna Bolotina, Ph.D. Student, Law
Faculty, International Relations
Department, Sumy National Agrarian
University, Ukraine.



This is an Open Access article,
distributed under the terms of the
[Creative Commons Attribution 4.0
International license](https://creativecommons.org/licenses/by/4.0/), which permits
unrestricted re-use, distribution, and
reproduction in any medium, provided
the original work is properly cited.

Conflict of interest statement:

Author(s) reported no conflict of interest

Mykola Kurylo (Ukraine), Alyona Klochko (Ukraine), Nataliia Volchenko (Ukraine),
Nataliia Klietsova (Ukraine), Anna Bolotina (Ukraine)

THE USE OF BIOMETRIC TECHNOLOGIES FOR BANK TRANSACTION SECURITY MANAGEMENT AGAINST THE BACKGROUND OF THE INTERNATIONAL EXPERIENCE: EVIDENCE FROM UKRAINE

Abstract

In view of the expanding range of banking services in Ukraine, the issue of introducing innovative means of protecting consumers against illegal actions in the field of banking becomes relevant. This paper aims to determine the effectiveness of biometric technologies for customer identification during banking transactions, the legality of their use, and to identify areas for the development of state policy focused on the legal use of biometric data in order to protect the rights and legitimate interests of individuals and legal entities. Based on analysis and systematization of scientific publications and regulatory framework, it was found that a potential direction for banks to implement the customer focus concept in their services to establish the appropriate level of security is the use of biometric technologies that ensure the proper storage of personal data. The summarized information on the actual application of biometric identification methods in the banking sector allows stating that the factors stipulating the criminal offenses using biometric data can be neutralized by the subjects of counteracting such offenses and through effective legal remedies. Contradictions arising between the state of regulatory support and the actual needs for the use of biometric technologies in the field of banking in Ukraine decelerate the use of effective security tools with a high degree of reliability in the banking sector. It is concluded that further implementation of biometrics in the banking sector in Ukraine requires a comprehensive approach and consideration of the best world practices.

Keywords

biometric technologies, banking institutions,
identification, legal support, security, criminalization

JEL Classification

G21, G23, K14, F52

INTRODUCTION

Improving security of banking transactions is one of the priority tasks to be solved by organizational measures by the subjects of countering criminal offenses in the banking sector. In addition to law enforcement agencies, executive authorities, the central body of state power, state collegial and advisory bodies, territorial offices of the National Bank of Ukraine and other entities, these subjects in Ukraine include Ukrainian banks and their branches (top management, officers and employees of banking institutions, security services of banking institutions). Banks develop new highly effective means to protect bank customers from unauthorized access to bank accounts, one of which is the use of biometric technologies for customer identification. Biometric identification of a person in the field of banking, on the one hand, will reduce the time of bank transactions, and customer au-

thentication with these technologies does not require memorization of personal identification numbers (hereinafter – PINs) to identify the legal cardholder, which makes it quite user-friendly. In addition to the above, alternative ways of biometric technologies can be used to combat money laundering, bank card fraud that uses bank transactions and criminal offenses committed by management, officials and other staff of banking institutions. There arises a need to analyze the possibility, feasibility and prospects of biometric technologies used by banking institutions as an identification management tool for a wide range of services. Due to the fundamental importance of security issues for ensuring sustainable operation of the banking sector, innovative technologies, including biometrics, occupy a special place in the bank's customer protection system.

1. LITERATURE REVIEW

Currently, biometrics is becoming widespread, and its use in various spheres of public life is increasingly successful. Biometric technologies allow easy access to medical services, office buildings and certain types of banking services. Biometric technologies have the capability to become a unique method for personal verification and secure identification activities in banking institutions (Bielski, 2000). In recent years, a significant number of financial institutions have recourse to biometric technologies to enhance security. In particular, Deutsche Bank, Mars National Bank, Barclays and HDFC Bank, Mountain America Credit Union, National Payments Corporation of India, and Wells Fargo financial corporation (Worldvision, 2015). It should be noted that Resolution 2396 (2017) adopted by the UN Security Council at its 8148th meeting held on December 21, 2017 authorizes the states to collect biometric data in order to identify and stop movement of terrorist militia, especially those returning from a conflict zone. The responsible use of biometrics contributes to strengthening the capacity of Member States' border-control and law-enforcement agencies to prevent the movement of terrorists. Developing and maintaining technical tools to manage biometric data can be very complicated. Governments should also analyze the human right implications of this technology and use it in line with their international legal obligations (United Nations, 2017). Development of biometric technologies in banking is stipulated with the dynamic development of mobile technologies. In particular, modern smartphones widely apply the technologies that use a camera for the face and iris identification. However, this raises issues related to efficiency, security and risks of biometric technologies in banking now and in the near fu-

ture in Ukraine. Kuznichenko et al. (2018) made comparative assessment of the regulatory and legislative measures in Ukraine and foreign countries concerning

consumers' protection against illegal actions in the banking sphere. There is the risk associated with confidentiality and privacy if biometric signature gets misused or stolen. In this regard, organizations should determine the level of security needed for their specific application: low, middle or high (Lysecki, 2006). Today, banks are gradually introducing ATMs equipped with fingerprint scanners to replace digital passwords. In theory, this increases confidentiality, since the password can be easily stolen by any interested parties. On the other hand, however, inadequate protection of the bank's fingerprint database can lead to their loss and result in a theft of customer biometric data (United States Supreme Court, 1977). Some issues of identification by biometric parameters were the subject of research carried out by scientists and practitioners; however, it did not extend to the application of biometric technologies in banking. In particular, as Serbin states, the use of biometric technologies enabled a "revolution" in the financial systems of many countries. Specifically, now you can pay online for goods and services, conduct online bank transactions, etc. with your fingerprint (Serbin, 2019). Anil K. Jain understands a person's biometric characteristics as his/her measurable physical characteristic or personal behavioral trait. The author states that identification of a person is carried out during a check of the person's biometric characteristics with the identity of a registered user (Jain & Ross, 2008). Moreover, Jain, Griess, and Connell investigated methods of biometric identification of computer system users aimed at ensuring protection of confidential information, including the image of signatures (Jain

et al., 2002). Tatarchenko and Tymoshenko hold on to the opinion that biometric technologies are the methods of obtaining human biometric characteristics. In biometric systems, a human personality is the identifying feature. This type of identification and authentication is based on the procedure of reading the presented biometric feature of the user and comparing it with the previously obtained sample (Tatarchenko & Timoshenko, 2002). According to Koval and Zlepko, biometric identification is a way of identifying an individual by certain specific biometric features (identifiers) that are specific to a particular person (Koval et al., 2019, p. 104). Maznychenko refers the means of identification (user recognition by the presented identifier) and authentication (validation of the identified user) to the classic mechanisms of information security of computer networks and user access control (Maznychenko, 2017, p. 238). Ivanov focuses on dynamic methods of biometric identification, among which special attention is paid to the dynamics of handwriting and keystroke pattern (Ivanov, 2000, pp. 3-9). The current state and prospects for the biometric technology development were the subject of research by Golubev and Gabrielyan (2004). Uniqueness of biometric characteristics of a person and high efficiency of biometric technologies for the needs of information protection is confirmed by Dvoryankin. In particular, as the scientist proves, the peculiarity of identification by biometric parameters relies upon their uniqueness. The chance of two people with the same features is very low (for example, the chance that two different people will have the same fingerprints on the same fingers of one hand is equal to 1 per 24 million, which is almost zero) (Dvoryankin, 2003).

Biometric technologies are being gradually but consistently introduced into the banking system of Ukraine. This process cannot be called simple, as it is accompanied by certain problems arising due to the gaps in legal regulation in relation to the use and storage of biometric data and absence of responsibility for unauthorized actions made to them. It is obvious that modern processes in the banking sector are mainly based on use of digital technologies, including those for ensuring constant remote access of customers to the bank services. This has become especially important during the COVID-19 pandemic. The

COVID-19 pandemic conditions have become a completely new factor that required prompt and adequate level of threat measures (Koval & Luchenko, 2020). In particular, the National Bank of Ukraine called the citizens for the limited use of cash during payments for the quarantine period. The need for social prudence necessitates the transition to non-cash payments, contactless and mobile payments with smartphones (Kirovograd Regional State Administration, 2020). Therefore, digitalization and biometrics in the banking sector are interrelated notions, because biometric technologies are used exactly in the context of digitalization (Kirovograd Regional State Administration, 2020). To minimize losses, banking institutions and other financial services firms have shifted their focus away from traditional authentication (passwords, PINs and magnetic stripes) to the biometric technology. This is because face, fingerprint and voice-recognition technologies are much better suited to greater convenience and security for the growing number of channels used in modern banking – in-person, Internet, smartphone, over the phone, etc. (AWARE, 2019).

According to a study conducted in Ukraine in January 2020, the international payment system Visa predicts rejection of the use of classic passwords and a gradual transition (over the next five years) to biometric technologies. 67% of respondents think that this method of access is faster (Interfax Ukraine, 2020). The reliability rating of user identification methods, according to Fabrizio Ward survey for Visa, shows that the fingerprint use is the most trusted method among Ukrainians. 89% of respondents noted this method of identification. Although the question may be controversial, given that 87 and 83% (not much less) of respondents noted that retinal scans and the use of a one-time password are the safest methods, respectively. Scanning of the vein pattern was considered the safest by 78% of respondents, and face scanning – 73% (Interfax Ukraine, 2020).

Customers of Ukrainian banks (PrivatBank, Raiffeisen Bank Aval, Oshchadbank, UKRSIB-BANK and other banks of the TOP 15 trust rating in the current year of 2021) can log in to mobile applications of the respective banks by fingerprint (Touch ID) or face recognition technology (Face

ID). On Android and iOS devices that support this technology, payments can be confirmed in a similar way.

In August 2020, PrivatBank launched the first in Ukraine 260 biometric payment POS-terminals with FacePay24 technology, which allow for payments for purchases using identity. By the end of the year, PrivatBank had installed 7,700 biometric POS-terminals. To use the 'payment service', you need to install an updated Privat24 application on your smartphone and activate FacePay24 payment, take three selfies from different angles and attach a bankcard. To make a payment in the Android PAX POS-terminal, you need to select the payment by face identification after entering the amounts on the terminal, look at the front camera of the terminal and tap 'pay'. After confirming the transactions with the PIN of the selected card, the purchase will be paid (PrivatBank, 2021).

Mastercard, in partnership with PrivatBank, is implementing the first in Ukraine customer verification project based on behavioral biometrics. The new solution is provided by NuDetect, a transparent user verification platform from NuData. With NuDetect, it will be possible for online banking and the Privat24 mobile application to test customers by their unique behavior in interaction with the devices or applications. The solution analyzes hundreds of signals, including device characteristics, passive biometrics, and behavioral features. Then it compares them with the user's behavior in the past. The solution provides unobtrusive continuous authentication, it is invisible and does not require prior registration. A user does not need to perform any additional actions other than those he/she normally performs when using his/her account. Behavioral data from such interactions are analyzed in real time to provide a reliable assessment of user risks; this helps the companies to prevent potential invasions and attacks. Identifying information is not stored and the data will never be available to hackers (Kovalenko, 2019).

Fingerprint payment was a pilot project launched as part of Kyiv Music Festival in 2018. It was implemented by Privatbank together with VISA payment system with 10 scanners. The bank is counting on the further interest of small business and the spread of this technology everywhere (Uteka, 2018).

Among the mechanisms of biometric data protection in Ukraine, technology and legal mechanisms could be distinguished. The technology mechanism of biometric data protection in Ukraine is characterized by the use of special software and devices, introduction of limited access to media and sources that store the relevant information.

The legal mechanism for the protection of biometric data in Ukraine is under development. Theoretically, it is supposed to provide for transparent legal regulation of the collection, use and protection of biometric data of citizens. The processes of European and Euro-Atlantic integration of Ukraine should be bound with the political, economic and security aspects of further development of the country (Nesterenko & Bohatyrova, 2019). Some individual issues of collecting, using and processing biometric data are covered in certain regulations of Ukraine, in particular, the Civil Code of Ukraine, the Law of Ukraine "On Information", the Law of Ukraine "On the Unified State Demographic Register and Documents Confirming Ukrainian Citizenship, Identify a Person or His/Her Special Status", the Law of Ukraine "On the Legal Status of Foreigners and Stateless Persons", the Law of Ukraine "On Personal Data Protection", and the Law of Ukraine "On Refugees and Persons Requiring Additional or Special Protection". Some of the regulations in Ukraine are only indirectly related to the introduction of biometric technologies in banking; however, they focus on the establishment of a national system for collecting biometric data (parameters) to ensure primarily economic well-being and human rights, and national security. In particular, the Guideline on the procedure for recording biometric data (parameters) of foreigners and stateless persons by officials of the State Migration Service of Ukraine, its territorial bodies and territorial subdivisions (hereinafter the Guideline) (Ministry of Internal Affairs of Ukraine, 2018). According to the above Guideline, biometric data (parameters) of persons are entered and kept in the internal information systems of the Ministry of Internal Affairs, the State Migration Service, the Ministry of Foreign Affairs, the State Border Service, the Ministry of Defense, National Police, the Foreign Intelligence Service, and the State Security Service of Ukraine. The national sys-

tem of collecting biometric data (parameters) of persons is created, first of all, to identify a foreigner and a stateless person entering or leaving Ukraine, control over compliance by these persons with the rules of stay in Ukraine. In the same context, the resolution of the Cabinet of Ministers dated December 27, 2017 No. 1073 approved the Regulation on the National System of Biometric Verification and Identification of Citizens of Ukraine, Foreigners and Stateless Persons (Cabinet of Ministers of Ukraine, 2017).

It should be noted that none of the above regulations contains the procedure for collecting, using and storing biometric data for the needs of banking, since its operation is determined by a certain specificity, customer focus, the need to provide the most convenient services and the need to preserve information and money of bank customers.

2. GENERALIZATION OF THE MAIN STATEMENTS

Banking institutions around the world are actively implementing biometric technologies and using various biometric identification methods – from iris or fingerprints scanning, signature recognition to the corporate use of biometric technologies. This trend is also seen in Ukraine; however, as analysis has shown, biometric identification methods are mostly tested and their further implementation in banking requires a comprehensive approach. In Ukraine, there is a need to strengthen both technology and legal mechanisms to protect biometric data used for banking. The processes related to the use of biometric identification methods in the banking sector of Ukraine are characterized by certain features, in particular, absence of a unified legal regulation of collecting biometric data acceptable for the banking sector in Ukraine. The current legal framework in Ukraine is focused primarily on the issues of biometric verification and identification of citizens of Ukraine, foreigners and stateless persons for their stay in Ukraine and abroad. These are biometric identification documents, which are fitted with the appropriate electronic media for biometric data of the document holder.

Review of the current legislation of Ukraine reveals the lack of attention of the legislative power to the protection of biometric personal data in banking activities and lack of liability for unauthorized actions with such data. For example, the citizens of Ukraine have two types of biometric passports: internal (an ID card) and travel passports are fitted with electronic chips with the owner's biometric data. The purpose of the introduction of such passports was the need to ensure protection to the society from any manifestations of international terrorism and criminal offenses. However, at the same time, the consequences of unauthorized actions with biometric personal data can be socially dangerous, regardless of the source from which they were obtained illegally. Currently, the legislative power does not see any signs of public hazard in such actions, ignoring the trends in the public relations development and all the sufficient grounds for criminalization. Therefore, the level of enforcing liability for unauthorized actions with biometric personal data is unacceptable. In the applicable Criminal Code of Ukraine, the relevant actions are qualified under Art. 182 "Violation of privacy" and Art. 361 "Unauthorized interference in the operation of computers, automated systems, computer or telecommunication networks" of the Criminal Code of Ukraine. Beside these provisions of the law, liability for certain actions that constitute unauthorized use of biometric personal data and bring socially dangerous consequences of data arises under Articles 188-39 "Violation of legislation related to personal data protection", Article 188-40 "Failure to comply with legal requirements of the Commissioner of the Verkhovna Rada of Ukraine for Human Rights" of the Code of Administrative Offenses of Ukraine.

It should be noted that the level of biometric technologies introduced in the banking sector of Ukraine is low. The tendencies of gradual rise could be seen in testing various methods of biometric identification in banking institutions. One of the factors complicating the process of biometrics implementation by the banks is the lack of technical capabilities. For example, an agreement on comprehensive banking services for individuals of PJSC "State Savings Bank of Ukraine" sets forth that the mobile application/mobile device of the remote banking system can use the follow-

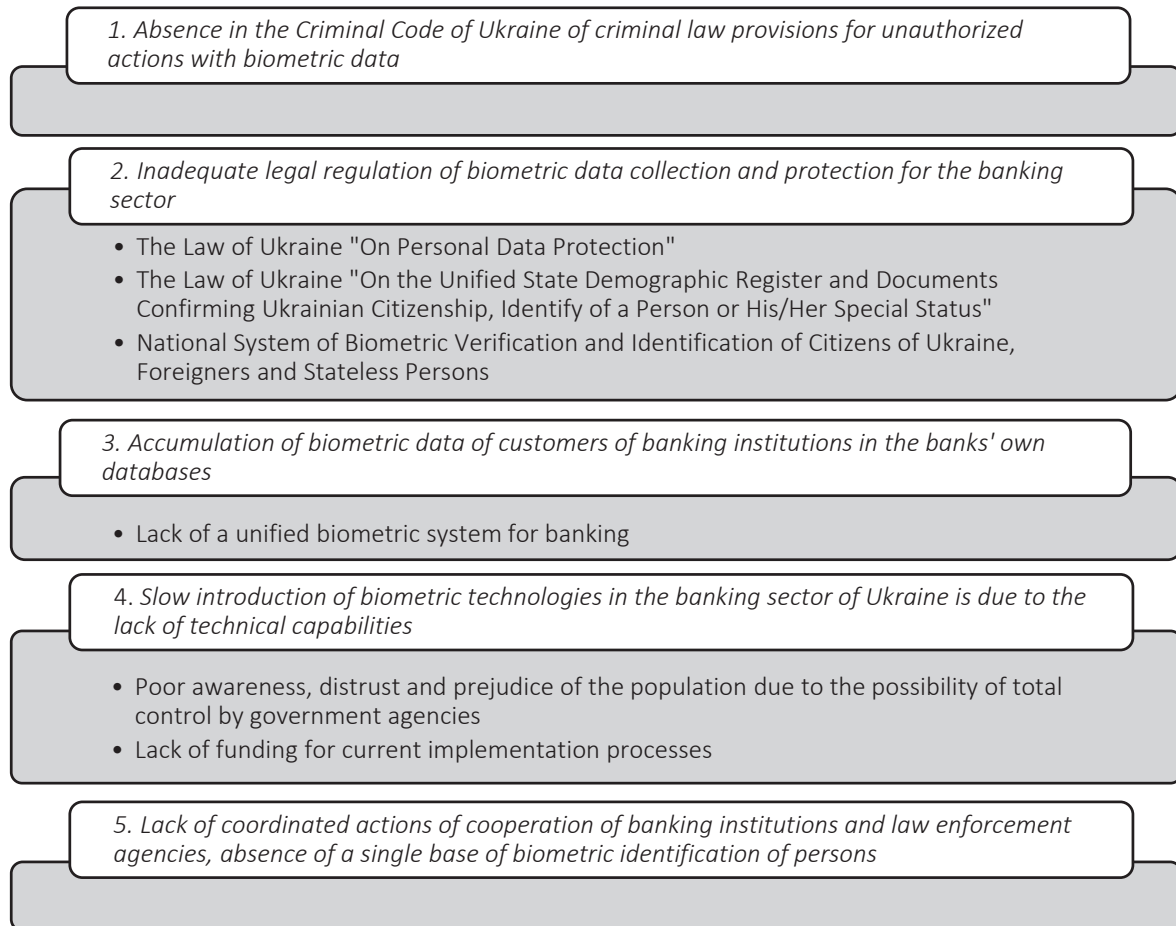


Figure 1. Factors hindering the introduction of biometric technologies in the field of banking in Ukraine

ing technologies of biometric customer identification: Touch ID (and similar) – fingerprint(s) scanner, including developed by Apple; Face ID (and the like) – a face scanner, including developed by Apple. Biometrics can be used subject to technical implementation (State Savings Bank of Ukraine, 2018). A summary of some of the factors hampering the implementation of biometric technologies in the banking system of Ukraine is presented in Figure 1.

In particular, the development of mobile biometrics in different countries of the world is associated with the needs for mobile banking operations. In Ukraine, biometric technologies are mostly used to identify a person for cash withdrawal in an ATM, or when a person calls to a banking institution, uses online banking and mobile banking for online transactions. In the field of banking, biometric technologies are currently used in remote

customer service (identification in call-centers using voice biometric identification). Voice biometrics is a technology that examines human voice characteristics and enables customer identification. Voice biometrics consists of a voice receiver, a voice modulator, a voice recorder, appropriate biometric software, and a voice database. Unlike other biometric technologies, voice biometrics allows to verify a person at a considerable distance. A customer sends a voiceprint and a face image to the bank to create a template for further identification. The next time you call the call-center, a biometric customer voice template is automatically created. This method of biometric identification is currently widely used in banking institutions in Russia and Belarus.

Biometric identification methods are also used in operations with ATMs and self-service terminals, in particular: cash withdrawals from ATMs with

a mobile device using biometric technologies, sensors integrated into ATMs, biometric plastic cards with fingerprint sensors. UBS analysts consider that biometric payment cards could cover a 15% share of the card market within the following five years. The Swiss bank informs that an increasing demand of fingerprint sensor cards will drive USD 5 billion in revenue by 2026 (Finextra, 2021). The customers of the Postal Savings Bank of China take part in large-scale testing of the digital currency of the Central Bank (CBDC) and use personal biometric cards. The best offer that the Ukrainian banks can currently make to their customers is a smart card (or a chip card), which is fitted not only with a magnetic stripe, but also with a microprocessor. Such a chip card allows its holder to pay for purchases without producing any documents, even outside Ukraine; to purchase any goods by approaching the card to the terminal using a PayPass or payWave chip; to pay for any goods without a PIN (in case of a Mastercard, the amount should not exceed UAH 500, and in case of a VISA – UAH 1,500). Potentially the fastest development of biometric technologies is observed in China. The rate of biometrics market expansion here is about 15%. The Ministry of Public Security has been collecting biometric data of citizens for almost 10 years. Introduction of electronic identification cards, which seems to increase online security, allows identifying a user on the Internet. Such cards are built into chips, smart cards, including official documents like a residence permit, a social or a bank card.

Japan is actively using biometrics in the banking sector, which is of research interest in this study. Japanese bank Ogaki Kyoritsu Bank is gradually moving to biometric customer identification both in branches and in ATMs. A new approach is to scan the vein pattern on the palms.

The examples of effective biometrics implementation can be found in the practice of various institutions, including law enforcement and security agencies. For example, in 2016, the Georgetown University reported on the creation of a database of the law enforcement authorities in the United States that contained data taken from about 120 million people with a face identification technology. Innovative biometrics technologies used by US national security systems include DNA testing and cloud services.

The European biometrics market is not inferior in its development to the American one. Germany can be called the “pioneer” of the biometrics use in Europe, as it was the first to introduce a travel document with complete biometric data. In addition to a passport, German citizens have electronic identity cards. Foreign nationals at German airports are identified by electronic passports using EasyPASS eGate terminals. This technology was implemented based on a government order and cost EUR 30 million.

In general, biometric technologies are actively used for the purchase of goods, for instance, mobile payments, payments to the operator using biometric terminals or a mobile device without a card. In particular, the state-owned bank Privatbank, in cooperation with Visa, launched FacePay24 biometric payment technology in Ukraine for the use in retail chains. To use the “face payment” service, the updated Privat24 application should be installed on your smartphone with FacePay24 activated. After that, you need to take three photos of your face from different angles and bind your Visa bank card to your face image to pay for any goods by looking at a special camera in the tablet located next to the cash register (Epravda, 2019). Eye scanning is also used successfully in banking. Bank customers get access to their bank accounts by looking at the smartphone camera. Eye-scanning is performed by the iris, retinal vessels and the pattern of vessels on the whites of eyes. Modern smartphones use iris scanning. Due to the eye-scanning technology, millions of Americans have access to their bank accounts by merely looking at their phones (Roberts, 2016).

For banking institutions with a large staff, a reliable mechanism for control of access to information is important. Multifactor authentication is supplemented with Face ID, thus confirming the user’s identity before accessing the system. The use of biometric authorization in corporate systems allows you to authenticate employees in the workplace, authenticate the employees working from home, account the working hours, control visitors, and provide access to storage and access to the safes. Biometric technologies are successfully used for banking access control and management systems.

Summarized sample data of the international experience of biometric technologies introduced in payment systems allow one to state that biometrics in banking is a separate trend in the world market. PayPal, an international electronic payment system, has partnered with electronics manufacturers Lenovo and Intel to enable remote user authentication on personal computers using a fingerprint when making payments. This project is being implemented in collaboration with Synaptics, the developer of biometric technologies (Central Bank of the Russian Federation, 2018). Synaptics helps users get the most out of their devices through an extensive portfolio of human interface solutions that enable elegant, intuitive user experiences (Synaptics, n.d.). The Ukrainian Privatbank uses only the customer's signature on the tablet to confirm the transaction at the cash desk. This indicates that most biometric technologies used by foreign countries for the banking system of Ukraine are currently not available, but it is advisable to use them in the near future.

3. DISCUSSION

The development of biometric technologies of personal identification is due to the growing number of information objects and flows that need protection from unauthorized access in the field of banking, in particular, personal identification systems, access control systems, information security, check-in of visitors and accounting of working hours, electronic payments. However, the contradictions arising from the lack of legislative instruments to ensure their use and the actual demand in banking lead to their slow implementation and poor awareness of bank customers about the possibilities of biometric methods of identification. The security level of biometric data correlates with their protection level. Therefore, according to Brihynets, it is expedient to store them distributed in different places and to ensure a multilevel method of authentication to grant access rights (Brihynets, 2019). Individual biometric identifiers (fingerprints, voice or signature of a person) can be forged using various methods. Some of the methods used by criminals to obtain bank customers' biometric data include unauthorized interference with the operation of computers or automated systems where the relevant data are accumulated,

conspiracy with the employees of banking institutions who have direct access to biometric data of individuals. Resonant leaks of human biometric data include the following criminal acts: in 2018, the leakage of screenshots from the passport database of Nova Poshta customers was reported, leaks of data from Morrisons supermarket chains (resulting in a fine of 10.5 thousand pounds), British Airways (paid a fine of 183 million pounds), in March 2019 the criminals stole information about the owners of Toyota and Lexus cars, data about Mastercard users leaked in August 2019 (Brihynets, 2019). In Ukraine's banking sector, there are all grounds for further implementation of biometric technologies. This is due, in particular, to its high criminalization level, which can be minimized by a comprehensive approach to regulatory and legal support of biometric technologies applied in banking.

First of all, there is a need to create a Unified Biometric System for the banking sector's needs. Similar models of such systems operate successfully in some foreign countries. Adoption of the Law of Ukraine "On Digital Banking Technologies" will promote determination of the legal status of biometric data, as well as the procedure for their use and storage. Currently in Ukraine, to carry out banking activities in accordance with the applicable law, banks process personal data of individuals, namely the employees of a banking institution, retail customers, legal entities – authorized persons of customers, counterparties. The Bank processes personal data in the following personal databases: customers' personal database, employees' personal database, and counterparties' personal database. Obviously, this process is necessary to reduce the risk of admission of unscrupulous persons to banking activities, preserve information and minimize abuse of all subjects of banking relations. Biometric technologies, as compared to identification by means of the access password, are characterized by high reliability, and the base of technical decisions is already developed for them at the present stage of informatization. To enter data into the unified biometric system, a user should first register in it with the help of a bank employee, and provide their biometric data such as a voice record and a face image. After these procedures, user data are entered into the unified biometric system. At the next stage, the user will have access

to remote services of the banking institutions that work with this system. However, it should be emphasized that the implementation of a full-fledged biometric identification system for a banking institution requires significant investment.

Also, there is a need in Ukraine to establish a special executive body to regulate the processes related to person identification with biometric data, and it will have the following authorities:

- ensuring the conformity of technological and information means for the processing of biometric personal data for identification purposes;
- development and approval of verification methods for authenticity of biometric personal characteristics of individuals and their biometric data stored in a unified biometric system;
- establishment of the procedure for processing biometric personal characteristics for identification purposes;
- determination of the requirements for technical and information means for the processing of biometric personal data for identification purposes, etc.

Biometrics provides identification of a person by his/her features, which are unique: eye features, fingerprints, voice, signature, face size and shape, hand shape, etc. Each of these characteristics is unique in its own way. New methods of biometric technologies, such as scanning the vein pattern, palms, are gradually gaining popularity in the field of banking in Ukraine. Improving existing biometric technologies and developing new ones, for example, with the masking elements in biometric data, is one of the topical and promising areas for building up effective security components of banking in Ukraine.

The proposed set of legislative instruments expressed as proposals on establishment of a Unified Biometric System for the needs of banking, adoption of the Law of Ukraine “On Digital Banking Technologies” and formation of a special executive body, also allowed us to state the need for criminal protection of public relations arising

in connection with illegal actions with biometric data of citizens. Findings of the study allowed for proposals to supplement the Criminal code of Ukraine with a criminal law provision concerning “Unauthorized use of biometric personal data” in the following formulation:

- 1) Unauthorized use of biometric personal data, which has led to serious consequences, shall be punished with a fine of two hundred to five hundred non-taxable minimum incomes or personal restraint for up to five years, or imprisonment for up to three years, deprivation of the right to hold certain positions or engage in certain activities for the term of up to three years or without such term.
- 2) The same acts committed by an official or by prior conspiracy by a group of persons, or if they have led to serious consequences, shall be punished with a fine of five hundred to one thousand non-taxable minimum incomes or imprisonment for a term of two to five years, with deprivation of the right to hold certain positions or engage in certain activities for the term of up to three years or without such term.

The method of counteracting criminal offenses is stipulated with the development of scientific research and modern knowledge about the ways of committing acts resulting from the development of public relations, as well as those that may result from gaps in legislation. The set of legal mechanisms for the protection of biometric data for the needs of the Ukrainian banking sector, which should be implemented, is illustrated in Figure 2.

Criminalization is one of the criminal legal means for combating criminal offenses; it is a kind of a preventive measure aimed at minimizing their manifestations in the society. Crime prevention is a combination of economic, ideological, legislative, social, cultural, educational and other actions aimed at mitigating, eliminating or neutralizing the conditions and causes of crime (Klochko et al., 2020). Criminalization of the illegal use of biometric personal data against his/her will is aimed at neutralizing criminogenic factors in the banking sector, which is stipulated with the need to build public trust to biometric technologies for their further introduction in the banking system.

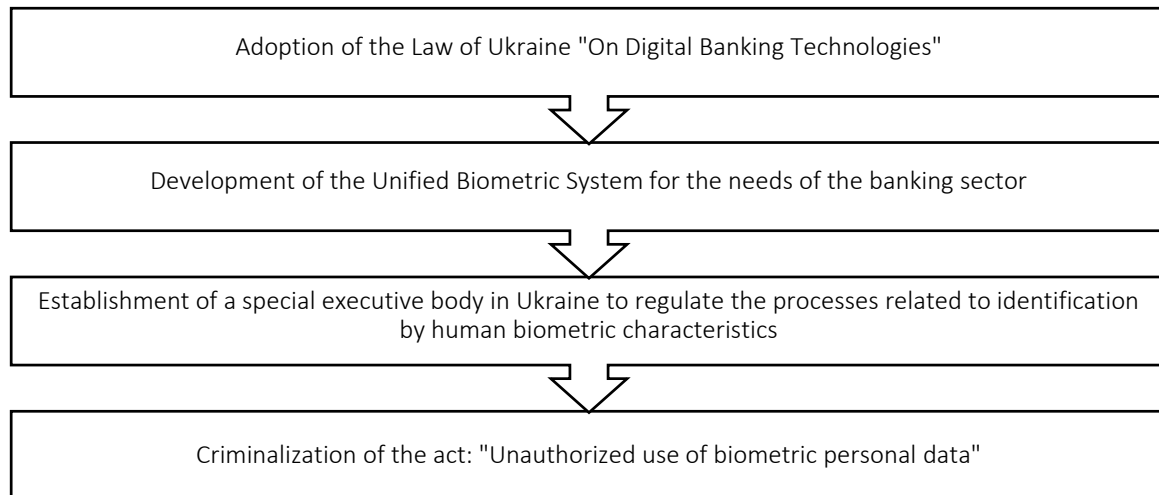


Figure 2. A set of legal mechanisms to be implemented for protecting biometric data for the needs of the Ukrainian banking sector

Appropriate legal regulation of the use of biometric technologies in Ukraine will promote their development by strengthening the confidence of bank customers, as well as competition of biometric algorithms in the presence of unified standards and requirements.

CONCLUSION

The idea of using biometric technologies to identify customers in banking operations can be very successfully implemented in the banking system of Ukraine. Some biometric identification technologies are already being actively tested in the banking sector. At present, bank customers distrust the introduction of biometric banking technologies due to personal beliefs and fear of being subject to total control by government agencies and services. However, citizens are gradually realizing the benefits of biometric authentication methods. The results of the study confirm that biometric technologies entail probable theft of biometric samples of a person and their subsequent illegal use. However, it should be noted that despite certain risks, the benefits of using biometric technologies are much higher, which is confirmed by the best practices of many countries (USA, Germany, China). Systems that combine several different types of biometric identification, combined types of authentication, in particular, hardware and biometric technologies, can provide maximum protection for banking operations. However, the widespread introduction of biometric technologies in the field of banking in Ukraine is possible with appropriate legislative regulation of the biometric system.

AUTHOR CONTRIBUTIONS

Conceptualization: Mykola Kurylo, Alyona Klochko.

Data curation: Anna Bolotina.

Formal analysis: Nataliia Klietsova.

Funding acquisition: Alyona Klochko, Nataliia Volchenko, Anna Bolotina.

Investigation: Mykola Kurylo, Alyona Klochko, Nataliia Volchenko.

Methodology: Alyona Klochko, Nataliia Klietsova.

Project administration: Mykola Kurylo, Nataliia Volchenko, Nataliia Klietsova, Anna Bolotina.

Resources: Nataliia Volchenko.

Writing – original draft: Alyona Klochko, Anna Bolotina.

Writing – reviewing & editing: Mykola Kurylo, Nataliia Klietsova.

REFERENCES

1. AWARE. (2019). *How financial institutions secure mobile banking with biometric technology*. Retrieved from <https://www.aware.com/blog-securing-mobile-banking-biometric-technology/>
2. Bielski, L. (2000). Time to start biometrics. *American Bankers Association Banking Journal*, 92(10), 54-59.
3. Brihynets, S. (2019). *Biometrychni dani: zbir i zakhyst u Yevropi, SShA ta Ukraini [Biometric data: collection and protection in Europe, USA and Ukraine]*. Yurydychna Hazeta – Legal Newspaper. (In Ukrainian). Retrieved from <https://yur-gazeta.com/publications/practice/inshe/biometrychni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html>
4. Cabinet of Ministers of Ukraine. (2017). *Pro zatverdzhennia Polozhennia pro natsionalnu systemu biometrychnoi veryfikatsii ta identyfikatsii hromadian Ukrainy, inozemtsiv ta osib bez hromadianstva [On approval of the Regulation on the national system of biometric verification and identification of citizens of Ukraine, foreigners and stateless persons]* (Decree No. 1073). (In Ukrainian). Retrieved from <https://zakon.rada.gov.ua/laws/show/1073-2017-%D0%BF#n12>
5. Central Bank of the Russian Federation. (2018). *Obzor mezhdunarodnogo rynku biometrycheskikh tekhnologiy i ikh primeneniye v finansovom sektore [International market overview biometric technologies and their application in the financial sector]*. (In Russian). Retrieved from https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf
6. Dvoryankin, S. V. (2003). *Recheyaya podpis [Speech signature]* (184 p.). Moscow: RIO MTUSI. (In Russian).
7. Epravda. (2019). *Pryvatbank zapustyv tekhnolohiiu oplaty tovariv oblychchiam [Privatbank has launched the technology of paying for goods by face payment]*. (In Ukrainian). Retrieved from <https://www.epravda.com.ua/news/2019/09/13/651594/>
8. Finextra. (2021). *UBS: Fingerprint cards will generate \$5bn in bank revenues by 2026*. Retrieved from <https://www.finextra.com/news-article/37498/ubs-fingerprint-cards-will-generate-5bn-in-bank-revenues-by-2026>
9. Golubev, G. A., & Gabrielyan, B. A. (2004). *Sovremennoye sostoyaniye i perspektivy razvitiya biometrycheskikh tekhnologiy [The current state and prospects for the development of biometric technologies]*. *Neyrokomp'yutery. Razrabotka, Primeneniye – Neurocomputers. Development, Application*, 10, 39-46. (In Russian). Retrieved from <http://neurocomp.ru/sovremennoe-sostoyanie-i-perspektivy-razvitiya-biometrycheskix-tekhnologij/>
10. Ignatovich, A. O. (2016). *Metody pidvysychennia efektyvnosti komponentiv bezpeky kompiuternykh system z vykorystanniam maskuiuchykh elementiv tekstovykh ta biometrychnykh danykh [Methods to increase the effectiveness of computer systems security components by using masking elements of text and biometric data]* (Ph.D. Thesis). (In Ukrainian). Retrieved from <https://lpnu.ua/sites/default/files/2020/dissertation/1508/dissihnatovycho.pdf>
11. Interfax Ukraine. (2020). *Visa prohozuie vidmovu platizhnoi industrii vid paroliv i perekhid do biometrii v naiblyzhchi piat rokov [Visa promises to the payment industry view of passwords and changes to biometrics in the next five years]*. (In Ukrainian). Retrieved from <https://ua.interfax.com.ua/news/economic/660747.html>
12. Ivanov, A. I. (2000). *Biometrycheskaya identifikatsiya lichnosti po dinamike podsoznatelnykh dvizheniy [Biometric personality identification based on the dynamics of subconscious movements]*. Izdatelstvo Penzenskogo gosudarstvennogo universiteta – Penza State University Press. (In Russian). Retrieved from <https://search.rsl.ru/ru/record/01000671435>
13. Jain, A. K., & Ross, A. (2008). Introduction in Biometrics. In A. K. Jain, P. Flynn, & A. Ross (Eds.), *Handbook of Biometrics* (pp. 1-22). Springer. Retrieved from https://link.springer.com/chapter/10.1007%2F978-0-387-71041-9_1
14. Jain, A. K., Griess, F. D., & Connell, S. D. (2002). On-line signature verification. *Pattern Recognition*, 35, 2963-2972. Retrieved from http://biometrics.cse.msu.edu/Publications/Signature/JainGriess-Connell_OnlineSignature_PR02.pdf
15. Kirovograd Regional State Administration. (2020). *Nadannia bankivskykh posluh pid chas karantynu [Provision of banking services during quarantine]*. (In Ukrainian). Retrieved from <http://www.kr-admin.gov.ua/start.php?q=Aktualno/Ua/1404201/14042001.html>
16. Klochko, A., Kvasha, O., Zahynei, Z., Logvinenko, M., & Kurylo, M. (2020). Combating crime in the banking sector as a method for ensuring its stability (evidence from Ukraine). *Banks and Bank Systems*, 15(1), 143-157. [http://dx.doi.org/10.21511/bbs.15\(1\).2020.14](http://dx.doi.org/10.21511/bbs.15(1).2020.14)
17. Koval, L. G., Zlepko, S. M., Novitsky, G. M., & Krekoten, E. G. (2019). *Metody i tekhnolohii biometrychnoi identyfikatsii za rezultatamy literaturnykh dzherel [Methods and technologies of biometric identification by results of literary sources]*. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriya: tekhnichni nauky – Scientific notes of TNU named after VI Vernadsky. Series: technical sciences*, 30(2), 104-112. (In Ukrainian). Retrieved from http://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf
18. Koval, N., & Luchenko, D. (2020). Non-tariff barriers: Ukrainian practice under conflict with Russia and COVID-19. *Lex Portus*, 4, 56-76. <https://doi.org/10.26886/2524-101X.4.2020.3>
19. Kovalenko, E. (2019). *Mastercard i PryvatBank zapustiat pershyi v Ukraini proekt povedinkovoi biometrii [Mastercard and*

- PrivatBank launch the first behavioral biometrics project in Ukraine*. (In Ukrainian). Retrieved from <https://www.mastercard.com/news/europe/uk-ua/розділ-новин/прес-релізи/uk-ua/2019/veresen/mastercard-i-приватбанк-україні-поведінкової-біометрії/>
20. Kuznichenko, Y., Frolov, S., Zhuravka, F., Yefimov, M., & Fedchenko, V. (2018). Regulatory assessment of the bank market risk: international approaches and Ukrainian practice. *Banks and Bank Systems*, 13(4), 73-84. [https://doi.org/10.21511/bbs.13\(4\).2018.07](https://doi.org/10.21511/bbs.13(4).2018.07)
 21. Lysecki, S. (2006). *Federal facial recognition project raises privacy fears*. Itbusiness. ca. Retrieved from <https://www.itbusiness.ca/news/federal-facial-recognition-project-raises-privacy-fears/9130>
 22. Maznichenko, N. I. (2017). Pidvyshchennia zakhyshchenosti informatsiinykh resursiv kompiuternykh system na osnovi systemy identyfikatsii korystuvachiv [Improving the security of information resources of computer systems based on the system of user identification]. *Aktualni pytannia suchasnoi nauky – Current issues of modern science*, 236-246. (In Ukrainian). Retrieved from https://dSPACE.nlu.edu.ua/bitstream/123456789/14290/1/Maznichenko_236-246.pdf
 23. Ministry of Internal Affairs of Ukraine. (2018). *Pro zatverdzhennia Instruksii pro poriadok fiksatsii biometrychnykh danykh (parametriv) inozemtsiv ta osib bez hromadianstva posadovymy osobamy Derzhavnoi mihratsiinoi sluzhby Ukrainy, yii terytorialnykh orhaniv i terytorialnykh pidrozdiliv* [About the statement of the Instruction on the order of fixing of biometric data (parameters) of foreigners and stateless persons by officials of the State migration service of Ukraine, its territorial bodies and territorial divisions] (Order No. 944). (In Ukrainian). Retrieved from <https://zakon.rada.gov.ua/laws/show/z1428-18#n14>
 24. Nesterenko, K. O., & Bohatyrova, M. O. (2019). Reforming of public administration in Ukraine in the context of the European integration. *Lex Portus*, 6, 52-65. (In Ukrainian). <https://doi.org/10.26886/2524-101X.6.2019.4>
 25. PrivatBank. (2021). *Pryvat-Bank zapustyv pershi v Ukraini biometrychni pos-terminaly* [PrivatBank has launched the first biometric pos-terminals in Ukraine]. (In Ukrainian). Retrieved from <https://privatbank.ua/news/2020/8/10/1270>
 26. Roberts, J. J. (2016). *Eye-Scanning Rolls Out at Banks Across U.S.* Fortune. Retrieved from <https://fortune.com/2016/06/29/eye-scanning-banks/>
 27. Serbin, J. (2019). Koduvannia tila [Body coding]. *Yurydychna Haze-ta – Legal Gazette*. (In Ukrainian). Retrieved from <https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/koduvannya-tila.html>
 28. State Savings Bank of Ukraine. (2018). *Dohovir kompleksnoho bankivskoho obsluhovuvannia fizychnykh osib* [Complex Banking Agreement Service of Individuals]. (In Ukrainian). Retrieved from https://www.oschadbank.ua/sites/default/files/2019-01/DKBO_100119.pdf
 29. Synaptics. (n.d.). *Enhancing the user experience. Products*. Retrieved from <https://www.synaptics.com/products>
 30. Tatarchenko, N. V., & Timoshenko, S. V. (2002). Biometricheskaya identifikatsiya v integrirovannuh systemah bezopasnosti [Biometric identification in integrated security systems]. *Spetsialnaya tehnika – Special technique*, 2, 2-7. (In Russian). Retrieved from <https://docplayer.ru/27367654-Tatarchenko-niko-lay-valentinovich-timoshenko-svetlana-vyacheslavovna-biometricheskaya-identifikaciya-v-integrirovannyh-sistemah-bezopasnosti.html>
 31. United Nations. The Security Council. (2017). *Resolution No. 2396*. Adopted by the Security Council at its 8148th meeting, on 21 December 2017. Retrieved from https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf
 32. United States Supreme Court. (1977). *Whalen v. Roe* (No. 75-839). Retrieved from <https://caselaw.findlaw.com/us-supreme-court/429/589.html>.
 33. Uteka. (2018). *V Ukraini zapustily platezhi za vidbytkamy paltsiv* [Ukraine has launched payments for fingerprints]. (In Ukrainian). Retrieved from <https://uteka.ua/ua/publication/news-14-delovye-novosti-36-v-ukraine-zapustili-platezhi-po-otpechatkam-palcev>
 34. Worldvision. (2015). *Biometrics in the banking sector*. (In Ukrainian). Retrieved from <https://worldvision.com.ua/ua/articles/biometriya-v-bankovskoy-sfere>