SECURITY SYSTEM FOR BANKING INDUSTRY BASED ON BIOMETRICS

Maksym Slatvinskyi[1], Nataliia Gvozdej[2]

[1]Ph.D. (Economics), Associate Professor, Head of Department of Finance, Accounting and Economic Security, Pavlo Tychyna Uman State Pedagogical University, Uman, Ukraine, e-mail: ms@udpu.edu.ua, ORCID: https://orcid.org/0000-0003-4096-2901

[2]Ph.D. (Economics), Associate Professor of Department of Finance, Accounting and Economic Security, Pavlo Tychyna Uman State Pedagogical University, Uman, Ukraine, e-mail: gvozdej@ukr.net

With the development of banking technologies, new banking products, and services the development of systems for protecting banking operations from possible risks is becoming increasingly important. The spread of hacker attacks on banking institutions and bank customer accounts, fraud with payment cards, credit fraud, etc. is the main reason for the introduction of various protection systems and finding the best ways to prevent and eliminate risks in the banking industry. Therefore, the issue of security systems for banking operations is not only relevant but also a vital condition for the proper functioning of Ukraine's economy.

Banking operations are a fundamental factor in the functioning of the banking system. Despite the importance of ensuring their security for the improvement and development of banks, there is no uniform approach to determining the security of banking operations. The security of banking operations is not singled out in the holistic direction of development of economic science but is only a supplement to the doctrines of banking security in general.

Many Ukrainian and foreign scientists have been engaged in theoretical and practical research on the problem of the formation and management of the bank's financial and economic security system. Leading economists such as Yaremenko S., Bukin S., Kirichenko O., Gamza V., Tkachuk I., Mezhokh Z., Yermoshenko M., Sorokivska Z., Zubok M., Alaverdov A., Kril Ya., Baranovskyi O., Kamlyk M. have made a significant contribution into issues of bank's financial and economic security systems.

The scientific researches mostly reveal the general principles of the formation and management of financial and economic security, but there are not enough scientific works that would consider the protection of banking operations. The use of methods and means of protection of banking operations can give impetus to improving the financial and economic security of banks in general.

Management of financial and economic security of banks depends on the economic policy, the efficiency of state institutions, the legal support of these institutions, their existing financial potential, and compliance with NBU standards, etc. [1–5].

The financial and economic security of the banks is one of the most important components of its successful operation and competitiveness in the financial services market. To effectively counter existing and potential threats and create conditions for the safe operation of the banks, a system of its comprehensive protection must be created.

The protection of the banking industry should be understood as processes aimed at protecting banks from the influence of individuals and legal entities, which is associated with violations of the law, as well as compensation for possible or affected by this activity economic or other damages [6].

The security system is a target subsystem of the bank management systems and strategic management, a set of methods, processes, and resources required for the implementation of security management based on security policy [7].

Thus, the system of financial and economic security of the bank is a combination of elements (security of material resources, financial security, information security, and personnel security) and their interconnections. The purpose of this system is to protect the bank against threats and counter them.

Klekov O. emphasized that constructing the security system occurs through the setting of appropriate tasks.

They include:

– protection of the legitimate interests of the bank and its employees;

– prevention of offenses and criminal encroachments on the property and staff of the bank;

– timely detection of real and potential threats to the bank, measures to neutralize them;

– identification of internal and external causes and conditions that may contribute to causing the bank, its employees, customers, and shareholders material, intellectual and other damages, interfere with their normal activities [8].

At the same time, the form of security organization is the external expression of its content.

Banks' security structures should be based on the bank resource capabilities, modelling the risks of possible threats and uncertainties in banking and related activities, and optimizing chosen solutions.

In this regard, O. Stayer proposed to divide all the principles of economic security of the bank into three levels:

– interaction level – legality, independence and responsibility, competence, coordination, confidentiality, complexity, separation, equivalence, preventive and reactive measures;

– operation level – economic expediency, continuity, purposefulness, differentiation, objectivity, interdisciplinary approach, control;

– self-development level – adaptation, integration, constant development, scenario modelling, variability, reflexes [9].

According to O. Stayer, this will provide a better understanding of the need to manage these principles in ensuring the bank`s economic security, which depends on the effectiveness of the bank`s management and professionals to avoid possible threats and eliminate harmful effects of certain negative components of the external and internal environment.

Thus, the financial and economic security of the bank is ensured through the setting of appropriate tasks and in compliance with important principles. In the interaction of these tasks and principles, it is possible to form a system of financial and economic security, which is aimed at measures to protect and prevent threats to banking.

At the same time, the state of financial and economic security of Ukrainian banks shows that the existing security systems operate only in the mode of protection against threats, not countering them, and mostly provide standard measures that are not always effective. Bank security measures are limited to the activities of security departments directly without extending security functions to other departments of the bank. The main disadvantage of the organization of banking security systems is that the main focus is on identifying violations in banks, rather than preventing them.

Aiming to develop a comprehensive system of economic security, which would solve these problems in banks, S. Yaremenko [10] established its organizational and methodological principles. She considered the organization of a comprehensive system of economic security of the bank as a certain process that has a certain structure of interrelated measures. Each of the measures is basic for the next and forms a certain basis for the creation, formation, and development of a security system. The process of organizing a comprehensive system of economic security is based on a certain information base, which consists of: results of an analysis of bank threats, decisions of the bank manager on security, legal norms of current legislation on banking protection, main tasks of the bank and its possibilities to create a comprehensive system of economic security.

S. Yaremenko also considers the formation of financial and economic security of the bank as a complex process aimed at the development, satisfaction, and protection of the interests of the bank, which has a corporate character. That is, the management process, according to S. Yaremenko, should be organized through the impact on the conditions and factors that ensure the development and security of the bank as a corporate interest.

And the protection of security interests in terms of process management involves maintaining the necessary level of protective capabilities of entities through the formation of their economic, intellectual, physical, and other potentials in

accordance with the needs of security and the conditions in which it performs its functions [11].

However, banks will not cope with the qualitative formation of the system of financial and economic security on their own. According to Z. Sorokivska, first of all, it is necessary to strengthen the state regulation of the banking industry for forming a high-quality and comprehensive bank's financial and economic security system. In particular, it is necessary to develop an effective mechanism for refinancing commercial banks, to impose severe sanctions on those banks that do not comply with basic prudential rules, provide inaccurate information, to make banking information more transparent, to strengthen the level of banking supervision by the National Bank of Ukraine. With these measures, it is necessary to improve the methodological basis for assessing the level of compliance with the bank`s financial security. To do this, it is required to intensify the development and implementation of new methods and technologies for processing and analyzing information to assess and ensure the bank`s financial security [12].

Thus, the formation of a bank`s financial and economic security should be based on the principles of financial and economic security, according to which its objectives will be set. Based on these objectives, organizational and methodological principles will be developed, which will be used by banks as a basis for ensuring their effective and high-quality security system. Compliance with the prudential rules by banks is important for the qualitative formation of their financial security system.

Security of banking operations is not less interesting, as concerns the essence of the banking business and is directly related to the bank and personnel security. The technology of staff violations and the use of the current order and rules, shortcomings and violations in the bank in the personal interests of bank staff or its owners, as well as in the interests of competing banks and organizations, crime and bureaucracy is of particular interest.

Regarding the systems of protection of banking operations, the direction of protection against credit risks has most scientific publications. Scientific articles cover only long-known and generally accepted truths and do not introduce anything new. The works of economists, general legislative provisions are cited, and those methods of protection that are well-known and currently ineffective are described. The system of protection of banking operations does not have a holistic and comprehensive study.

Thus, the security of banking operations is less explored by economists. Most information about the banking operations protection systems can be found in popular scientific and journalistic articles, on the websites of banks, but not in authoritative scientific works. General conclusions and duplication of well-known information, the secrecy of most information and statistics for studying the banking security systems

is a problem for the development of an independent and thorough direction in economic thought.

The level of banking fraud is growing rapidly in the process of developing electronic technologies, expanding the functionality of payment cards and remote banking channels (RBC). Nowadays, Internet banking is becoming very popular, which is a convenient way to use banking services, but also has many dangers. There are the following main risk groups for e-banking users: key/screen logging – capturing entered logins and passwords from the screen or keyboard; SMS interception; theft of an electronic digital signature (EDS) key; phishing (infecting a computer with spam on behalf of well-known brands); malware on the computer; malware on the phone; remote hostile computer control; transaction substitution (MIM / MIB – technologies "man in the middle", "meeting in the middle", "loss in the middle", "man in the browser") [13].

These risks are to varying degrees relevant to the RBC of individuals and businesses. 95% of banks use a one-time password via SMS to authenticate individual users. This message with a one-time password is easy to use, but it has serious drawbacks:

- one-time password eliminates only a small part of modern attacks;
- sending each SMS is costly for the bank.

Ideally, for more secure remote payments, individuals should focus on different authentication tools for different transaction limits: SMS with a password for small payments, more secured OTP generators – for large amounts [14].

For customers who use more than 10 SMS with OTP per month, it is much more convenient (and cheaper for the bank) to get a hardware OTP generator or a similar mobile application for smartphones.

95% of banks use EDS (Electronic Digital Signature), and the key is stored on unprotected storage media (hard drive, flash drive, optical disk). This technology sometimes allows attackers to steal the EDS key and password to it. This information will be enough for the hacker to transfer money from the bank customer's account. The following mechanisms allow to avoid it [15]:

1. Secure USB-compatible authorization token (can be as a smart card) for generating and storing an EDS key.

The main advantage of the certificate is that the EDS key is generated directly inside the token, so the key cannot be copied or extracted from there. But the problem is that users very often leave the token connected to the PC, allowing an attacker (or virus that infects the user's PC) to create and sign unauthorized payments on the user's PC.

2. One-time password generators (OTP) to the available EDS.

Additional protection can be provided by various types of OTP generators (SMS with OTP, OTP keychains, or mobile applications). Their main advantages are no need to connect to the PC, no software to install; can be used in parallel the generator for RBC of individuals, and also for the protection of transactions on corporate cards; more secure authorization schemes can be implemented (simple OTP, then OTP with binding to receipt banking information) [13].

It is a completely different situation when the security of the RBC is threatened by bank insiders. Among the typical mistakes of the financial institutions – failure to comply with the procedure for dismissal of a staff member who has the keys to access the domains. In this case, according to the legislation of Ukraine, it is necessary to change all passwords of the login system, having previously deprived the dismissed employee of access to its administration. Experience shows that the reverse order of such a process can lead to the leakage of insider information and as a consequence – to the theft of funds from customer accounts [16].

According to the statistics of the authoritative Bureau of Statistical Research GfK, in 2014, cybercriminals attacked 57 banks, during which they tried to illegally transfer 116 million UAH from the accounts of businesses and 11 million UAH – from the accounts of individuals [17]. However, over 70% of such attempts were in vain – account holders had blocked the funds on the card after notification of suspicious transactions.

You can freeze your funds and chargeback within one to two business days from the date of the online transaction to the value date. Thus, the bank customer has not enough time to notice the illegal discarding of money from his account and block it. Since not every customer checks the account balance every day, the chances of seeing an unauthorized money transfer in time are higher in customers who are connected to SMS banking.

It is difficult to prove the illegality of the transaction. The mechanism of such a procedure is not legally registered, so legal entities – victims of hackers apply to specialized law firms, which involve law enforcement agencies in the investigation and collect evidence. According to the experience of the Ukrainian Bureau of Interpol, the investigation process may take several years, especially in the case of international transactions.

Thus, the modern development of banking technologies for transaction protection focuses on the development and improvement of RBC (remote banking). Internet banking, SMS banking, and others are new technologies that significantly reduce the risk of fraud of bank employees and save time and money for bank customers. Banks implement new technologies of information security (for example EDS – electronic digital signature, etc.). But each new technology has its advantages and disadvantages.

The human factor is one of the most important factors in the security of banking operations. Entrepreneurs have bank accounts, as it has become a vital necessity in our time. According to a study conducted by marketing and sociological research company GfK Ukraine commissioned by Ukrainian Interbank associations of members of EMA payment systems [17], Ukrainian payment card holders need more information on modern efficient ways to prevent themselves from being robbed by cybercriminals.

According to the survey, 11 % of payment card users could not name any method of protection, and other respondents said that they know only 1-2 ways to protect against fraud. The main methods of protection were traditional: 52 % of respondents know about the need not to tell anyone the PIN code of the card; 22 % – do not pass the card to other people; 14 % – do not store the PIN code with the card, including not writing it on the card [17].

At the same time, modern and effective means of protection for most payment card users remain largely unknown: only five percent or less of respondents were able to name a significant part of them without prompting.

Respondents explain the non-use of modern means of protection by the lack of information on their purpose and conditions: for example, a minority of respondents know the fact that setting limits on transactions is a way to minimize financial losses in the result of fraud.

A small part of bank customers is informed that the limits can be increased quickly by calling the bank's contact center or through the Internet Banking system. Ignorance of the possibility of rapid change of limits is the main barrier to the use of this mean of protection.

The SMS banking is perceived by most holders as a source of information about the receipt of funds on the card (91 %), and not as a tool to stop fraudulent transactions: less than half of users chose the option “to contact the bank in case of theft or other fraud and block the card” (44 %). At the same time, 94 % of respondents say that the card should be blocked in case of theft or loss, and only 58 % believe that this should be done when receiving an SMS about a transaction that the cardholder did not do [17].

Among the rules for the safe use of payment cards, which require additional explanations from banks, respondents named: setting limits on transactions; connection of SMS notifications; informing bank employees when leaving abroad; re-issuance of the payment card after returning from abroad; regular change of PIN code; counting of money near an ATM immediately after receipt; storage of documents confirming banking operations [17].

Based on research data and bank information on protecting the accounts from criminals, we can highlight the most important security measures when banking:

keeping in a secret from third parties PIN code, prevention of personal data disclosure when paying for online purchases, using an ATM pay attention to the absence external devices on it, email and messenger users need to check financial offers from their acquaintances by contacting them by voice.

Thus, the human factor is one of the main factors that provokes threats in the banking market. A person can provide the greatest protection for his/her bank account, following the rules of security and being careful and cautious, while banking security systems are more focused on information and computer systems.

The creation and implementation of the latest technologies for the protection of banking operations is a continuous process characterized by truly progressive qualitative and quantitative characteristics. The implementation of new methods of authentication for access to a bank account is one of the most dynamic and promising areas of development of the bank`s security systems.

Having researched the market of the new technologies and innovative ideas, we have singled out those innovations, the implementation of which could be started in Ukraine and get incredibly positive results.

The banks of City have been testing a new customer authentication system – comparing the customer's appearance with his/her photos on social networks.

A software called Perceive, which uses biometric parameters for authorization, was developed by experts from Socure, based in New York. The system evaluates the image from bank customer`s smartphone and determines his identity. And for additional verification it uses his profiles on social networks such as Facebook, Twitter, and LinkedIn. After verification, the system either approves the payment or activates an alarm.

Socure noted that this technology is already used by several American banks in the fight against card fraud – although still at the testing level.

Earlier, MasterCard announced the launch of testing the system of using fingerprints and selfies to confirm online payments. Testing has been conducted in some European countries and the United States.

Some US banks use a new way to verify customers: now instead of passwords and signatures to confirm the transaction is enough to take a selfie on a smartphone.

The USAA was the first American financial institution to offer its customers to install a special application on their smartphone that allows them to use selfies for authentication when conducting banking transactions. This bank launched this service in test mode in December 2014. And since January 2015, more than 100 thousand customers of the credit institution in Florida have been able to use the new service.

Another American bank – WellsFargo began to offer its customers to take eye selfies. Instead of passwords and signatures, the credit institution's customers can install a special application EyeVerify on their smartphones, which studies the

structures of the sclera and pupil of the client's eye, compares the data entered into the database and verifies the person when performing banking operations.

The British bank Halifax has tested a new system for authenticating its customers through heart rate monitoring, which allows depositors to access their account without entering additional codes and passwords. The bank's experiment is based on the fact that the pattern of each person's heart rate is as individual as fingerprints or an iris. To authenticate it, the bank customers will be provided with a special bracelet that will connect to the carrier's home computer and confirm its identity, opening access to online banking.

Vietnam's joint export-import commercial bank Eximbank has started installing biometric ATMs in the country. Customers of such ATMs are authenticated by fingerprints. Users of Eximbank ATMs do not need to remember and enter a PIN code for their cards. Any transactions with funds on the current account are carried out with the touch of a finger. However, given customers concerns that the innovation could lead to a surge in crime, the Eximbank administration notes that fingerprint scanners can detect if a hand is alive, and will not give access to financial transactions if the finger is cut off.

However, the security of fingerprint recognition authentication has been compromised. Research company SRLabs easily bypassed the fingerprint scanner of the Samsung Galaxy S5 smartphone, using a copy of the fingerprint and toner. SRLabs experts note that the ease of hacking is a very serious threat to the user of data because Samsung has decided to use fingerprints to protect the information in the payment system PayPal. Thus, by stealing the phone and breaking its scanner, criminals have the opportunity to seize all the information from the cards, thereby making purchases without problems, as well as send money anywhere without the knowledge and consent of the real owner. The situation is complicated by the fact that the smartphone does not require a password after rebooting – all the security of the mobile device and the data stored on it depends solely on the scanner, which was broken in a few minutes.

Thus, the latest technologies of biometric authentication by recognition of facial features, fingerprints, hand data, and heart rate have a real basis for implementation in the banking systems of different countries. During testing, the novelties impress with the level of speed of information processing, reliability, and data protection and client`s funds from illegal encroachments.

Biometric systems are currently forming a new generation of information security. By biometrics we mean the technology of identification of a person that uses the physiological parameters of the subject (DNA code, fingerprints, iris, facial image, voice tone, etc.) for authentication [18].

For the banking system, the introduction of biometric data as a means of authentication will be an outpost for the formation of an integrated banking protection system. If the traditional systems of the first generation have such features as unambiguity and consistency of the identification parameter, the parameters of the new generation systems, which are biometric systems, depend on many factors and are always variable. In traditional systems (PIN, magnetic card) anyone has access because the system expects the correct code, not a specific person. Therefore, the loss or theft of the key – allows unauthorized access to data. The absence of this disadvantage in biometric systems provides some significant advantages, as it uses unique identifiers specific to a particular person. The algorithm for authentication in the first-generation systems typically much simpler than biometric authentication systems.

Due to the development and spread of biometric technologies, they have been actively used in many areas related to the protection of access to confidential information, material values, when crossing the state border, etc. Biometric technologies are widely used in banking security, investment, as well as retail, public order, health care, recently it has been actively used in social services. Shortly, biometric technologies will take leading positions in many areas of personal authentication, used separately or used in conjunction with smart cards, keys, and signatures [19].

Currently, the most common biometric systems by type of biometric parameters are fingerprints, hand geometry, facial images, iris.

Fingerprint recognition authentication [20]. According to this method, you need to get an image of the papillary pattern of one or more fingers. Then this image is processed, during which are detecting its characteristic features, such as lines branching, ending, or crossing (Fig. 1). For each feature, except its type, the relative positions and other parameters are also stored, for example, for the endpoint of the line – its direction. The set of such data features and their characteristics forms a template of human biometric characteristics (HBC).

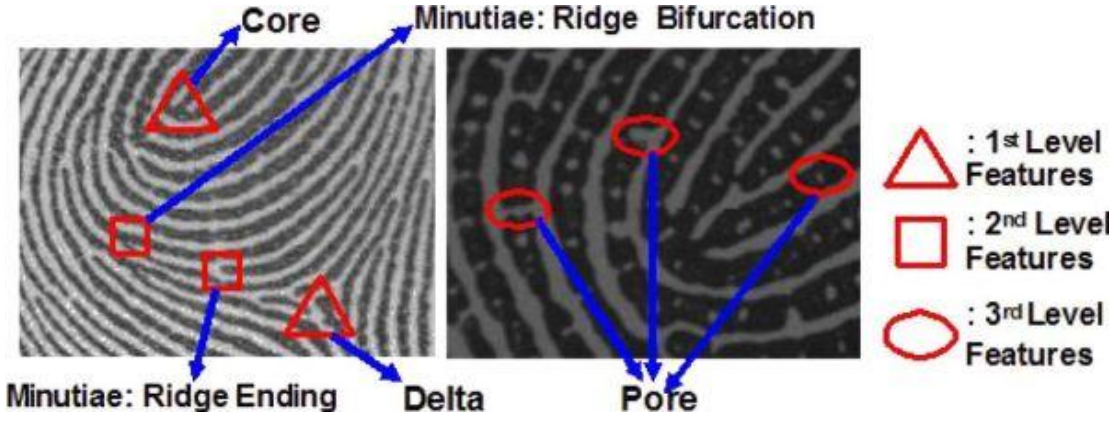

Fig. 1. Fingerprint recognition [21]

When authenticating a person, a comparison of the obtained fingerprint template with previously obtained ones is used. At a certain level of compliance, a conclusion is made about the identity of the templates and there is verification or identification of the submitted fingerprint. This method is the most common in the world. It is used both in business life, for example, access to a computer system, and in everyday life, for example, for door locks. The advantages of this method are relative cheapness and high efficiency, ease of use, ease of installation, compactness of form. It should be noted that dactyloscopy authentication in terms of applicability and affordability from a financial point of view surpasses all other technologies (Table 1).

Table 1. Comparison of biometric methods of personal authentication

Measured parameters	FRR	FAR	Cost (average), USD
Drawing of covers of fingers, hands	0.05	10-6	200
Drawing of blood vessels of the fundus	0.01	10-9	5000
Drawing of blood vessels of the hand	0.05	10-4	2000
Drawing of iris	0.05	10-5	2000
Hand geometry	0.02	10-3	500

Disadvantages of this method include insufficient resistance to forgery of the fingerprint and external factors – scanner contamination or finger cleanliness.

Handshape recognition authentication [20]. This method is based on the geometry of the human hand. Receive several silhouettes of user`s hand using illuminated diodes, and construct the three-dimensional image of hand (Fig. 2).

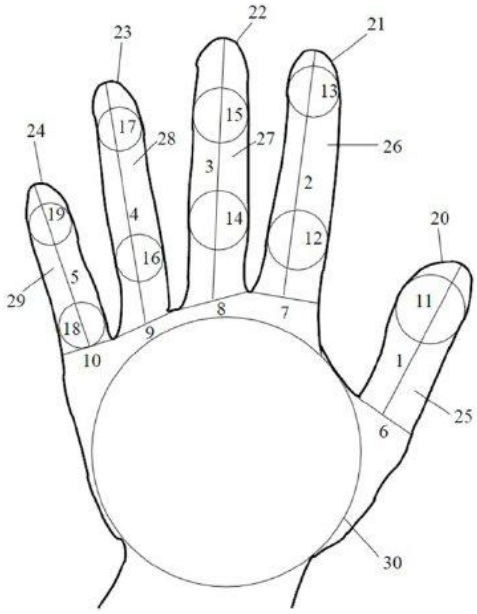

Fig. 2. Hand geometry and 3D hand gestures [22]

For each of them compute the vector of values. All vectors of traits of one person are combined into a separate class. The traits of the reference image are the average values of the traits of the whole class, i.e. determine its center. The initial

traits are modified by computing new ones or reduced by bringing to a lower number. And, thus, a hand pattern is formed based on the sample. The resulting image is transferred to a class of original or modified features compared with the standard. Advantages of the method: there are no requirements for the cleanliness of the hand, its temperature, and humidity. Disadvantages: bulkiness of devices, low resistance to counterfeiting [23].

Iris recognition authentication [20]. The iris is also a unique HBC. To scan it, a portable camera with specialized software is enough that allows you to capture the image of the part of the face from which the image of the eye is extracted. From the image of the eye, in turn, stands out the drawing of the iris, which builds a digital code for person recognition (Fig. 3). The advantages of this method are a high degree of recognition, non-contact scanning method, small database volume that is typical for most biometric systems, and a small number of errors of the first and second type (Table 1). Disadvantages include the high price of the devices and some inconveniences for users due to the need to focus.

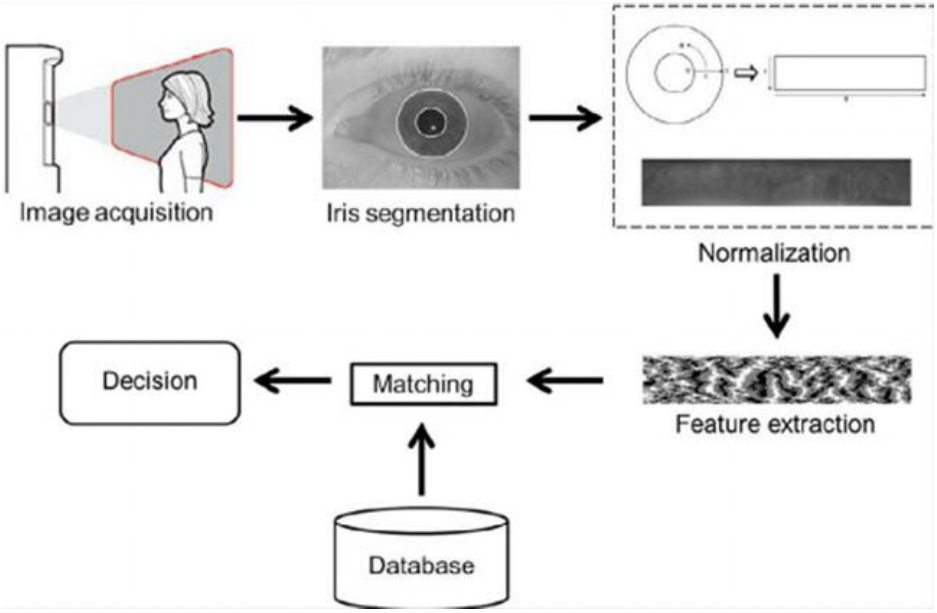

Fig. 3. Iris recognition process [24]

Voice recognition authentication [20]. Voice is one of the traditional ways to identify a person. Since this method is non-contact and does not require much effort, work is underway to create voice locks and systems to restrict access to information. Interest in this area is also associated with forecasts of the widespread introduction of voice interfaces. The principle of operation is based on the following: each burst of the voice signal corresponds to some fragment of speech. It can be a single letter, a combination of them, or a short word. Fragmentation is followed by the digitization of fragments according to frequency indicators (Fig. 4).

Advantages of the method: the usual method of recognition, low cost, non-contact. Disadvantages: high level of errors of the 1st and 2nd type, high sensitivity to interference, which causes the need for a specialized soundproof room for recognition, the possibility of unauthorized interception of the phrase. The quality of recognition depends on many factors, such as intonation, speech rate, disease, and psychological state of the source, etc. [23].

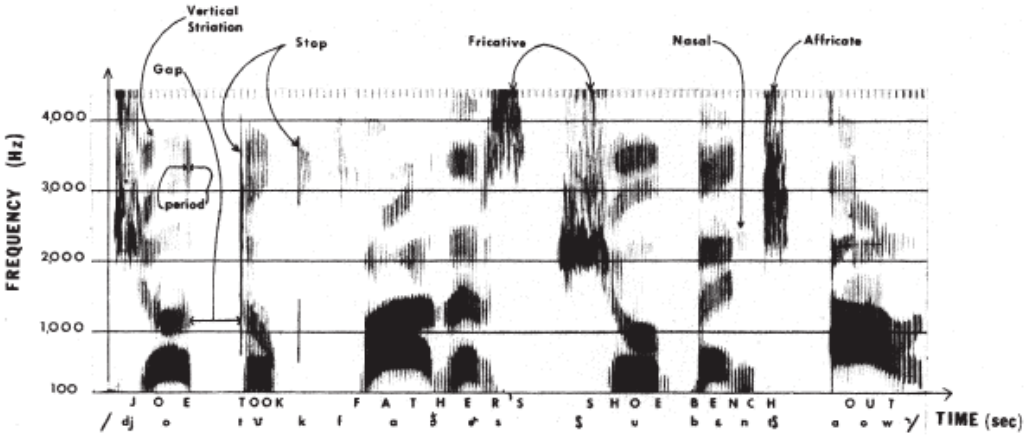

Fig. 4. Voiceprint [25]

Each of the types of biometric authentication is characterized by certain features that depend on the requirements for ease of use, cost, and accuracy of the method. Accuracy contains three components:

− FRR (False Rejection Rate) – the rate of erroneous denial of access – access is denied to the user registered in the system; called “error of the 1st type”;

− FAR (False Acceptance Rate) – the rate of erroneous tolerance that takes into account the cases of providing the access to an unauthorized user by the system – the percentage threshold that determines the probability that one user can be mistaken for another; called “error of the 2nd type”;

− the probability that the system will not be able to make any decisions is called “error of the 3rd kind” [26].

Usually, there is a balance between errors of the first and second type in a biometric system, while the number of false-positive operations is reducing the probability of false-negative operations is increasing and vice versa. It is possible to increase both indicators of reliability only by the fundamental improvement of biometric techniques.

Errors of the third type are similar to errors of the second type – the user is denied access because the system could not recognize it. However, the nature of these errors is different. It is not related to defects in recognition algorithms, but it is related to external causes. For example, non-recognition of a person who has lost or for some reason could not present the necessary HBC for the verifying: cut or burn a finger, runny nose, etc.

Biometric authentication methods provide the idea directed on complex consideration of internal characteristics of biometric systems and their external displays, most visibly revealing advantages of biometrics in comparison with other technologies. The list of these advantages is obvious: person identification instead of the password or the material carrier, impossibility to refuse actions confirmed by biometric identifiers, the identifiers are inseparable from a particular person and cannot be lost, stolen or exchanged. So that this list does not remain a declaration, we consider a specific example of the consequences of the use of other technologies.

An analysis of Jerome Kerviel's € 5 billion loss to Societe Generale found that the trader had borrowed the passwords of his colleagues and traded under their names, manipulated the banking information system, deleted transaction details and then recovered them. These actions do not exhaust the list of Kerviel offenses, but the above is enough to conclude the serious shortcomings of the system of user authentication and management of their access to information resources [23].

In addition to the fundamental aspects, business customers are also interested in the economic benefits of implementing biometric systems, and it should be expressed in specific indicators. Techniques based on ROI (Return on Investment) analysis are often used to determine them, and calculations are already being made for biometrics.

According to the consulting company Nucleus Research, which specializes in analyzing the payback of information technologies, the adoption of a biometric system in banks leads to savings of 800 USD per year per employee. The method of calculating ROI is to estimate the effect, which is expressed in a decrease in operating costs, an increase in the number of customers, and (or) an increase in attendance, etc. Analyzing the activities of biometric payment systems, experts found (according to CNN Money) that the use of biometrics halves the transaction costs and increases attendance stores with biometric banking terminals by 15 % [27].

ROI indicators can be interpreted in terms of the effect of saving time and increasing productivity, accuracy, and transparency of payments. The direct relationship between saving time and increasing economic efficiency can be traced to examples of the use of biometrics for customer service. Thus, already in the first stages of testing biometric payment terminals, the time of entering information about the payer was reduced to 1-2 seconds (when using a fingerprint scanner), and the turnover provided by these biometric terminals increased by 30 %.

Thus, the rapid development of information technologies, the need to use local and global communication networks increase attention to information security issues. The vast majority of information security systems focus on the use of biometric features. The use of biometric features to protect banking operations will give a powerful development of the bank's security systems. In turn, this will minimize all types of risks for individuals and corporate customers and the banks as a whole.

Thus, as a result of studying the prospects of using the new technologies to improve the bank's security systems we formed the following conclusions.

1. According to the analyzes of the theoretical essence of the bank`s security systems, we can argue that banking security is not enough studied by economists. Most information about the bank`s security systems can be found in popular science and journalistic articles, on the websites of banks, but not in authoritative scientific works. General conclusions and duplication of well-known information, the secrecy of most information and statistics to study the bank`s security systems are a problem for the development of an independent and thorough direction in economic thought.

2. As a result of the research of modern banking security methods, it is revealed that the modern development of banking technologies of protection of operations is focused on RBS (remote banking service) development and improvement. Internet banking, SMS banking, and others are new technologies that significantly reduce the risk of fraud of bank employees and save time and money for the bank's client. Banks are introducing new technologies to protect information from attackers (EDS – electronic digital signature, etc.). But each new method has its advantages and disadvantages. The human factor is one of the main factors that provokes threats in the banking market. Bank`s security systems are more focused on information and computer systems. But the greatest protection of their funds in bank accounts can be done by the person himself, following the rules of security, and being careful and cautious in using his/her bank account.

3. Searching for ways to increase efficiency and improve the system of protection of banking card transactions, it was found that the rapid development of information technologies, the need to use local and global communication networks increased attention to information security. The vast majority of information security systems focus on the use of biometric features. Therefore, we propose a new approach to the organization of protection of banking operations – the use of biometric technologies to identify unique human traits that are not susceptible to counterfeiting. The adoption of biometric ATMs, readers of biometric information in banking operations, minimizes the risks associated with cyberattacks, fraud with payment cards. and will increase the level of a bank`s security as a whole. The use of biometric features in Ukraine to protect banking operations will strongly develop a bank`s security system, increase public confidence in banks. The adoption of the latest technologies of biometric authentication by face, fingerprints, hand data, and heart rate have a real basis for implementation in the banking systems of different countries, including the banking system of Ukraine. During testing, the novelties impress with the level of speed of information processing, reliability, and protection of client data and funds from illegal encroachments. The ratio of the cost of adopting biometric authentication systems to their benefits allows us to say that the biometric

systems of banking operations protection are liquid and profitable. Therefore, due to the unique and effective development, in a short period, we will have a complete reformatting of the banking security in Ukrainian and world markets.

References:

1. Slatvinskyi, M. (2014) Economic security in the investment area: countering threats [Jekonomicheskaja bezopasnost' v investicionnoj sfere: protivodejstvie ugrozam]. *Proc. Int. Conf.* "*The global economic dynamics as a stress factor of socio-political processes, cycles, crisis and conflicts".* Euro-Mediterranean Academy of Arts and Sciences (Athens), The University of Educational Management (Kyiv). Athens, Greece. pp. 264-268. [In Russian]
2. Slatvinskyi, M. (2015) Institutional imperatives of investment policy as a basis of economic security [Instytucijni imperatyvy investycijnoyi polityky yak osnova ekonomichnoyi bezpeky]. *Economic Bulletin: a collection of scientific papers [Ekonomichnyi visnyk: zbirnyk naukovykh prats]*. Uman, Ukraine: FPE Zhovtyi O. O. Vol. 9. pp. 56-61. [In Ukrainian]
3. Slatvinskyi, M. (2015) The growth of capitalization of banking institutions as a basis for the development of investment processes [Zrostannia kapitalizatsii bankivskykh ustanov yak osnova rozvytku investytsiinykh protsesiv]. *Proc. 5 Int. Conf. "Priorities of development of the national economy of Ukraine: strategy and prospects" ["Priorytety rozvytku natsionalnoi ekonomiky Ukrainy: stratehiia i perspektyvy"]*, 28 September. Uman, Ukraine: Vizavi. pp. 32-34. [In Ukrainian]
4. Slatvinskyi, M. (2017) Banking system as a factor in forming the investment security of the business environment [Bankivska systema yak chynnyk formuvannia investytsiinoi bezpeky biznes-seredovyshcha]. *Proc. Int. Internet Conf. "Financial regulation of changes in the Ukraine`s economy" ["Finansove rehuliuvannia zrushen u ekonomitsi Ukrainy"]*, Mukachevo. 21-22 March. Mukachevo: Mukachevo State University. pp. 442-444. [In Ukrainian]
5. Slatvinskyi, M. (2016) The model of multilevel protection as a basis for effective risk management of financial institutions [Model bahatorivnevoho zakhystu yak osnova efektyvnoho ryzyk-menedzhmentu finansovykh ustanov]. *Economic Bulletin: a collection of scientific papers [Ekonomichnyi visnyk: zbirnyk naukovykh prats]*. Uman, Ukraine: FPE Zhovtyi O. O. Vol. 10. pp. 120-122. [In Ukrainian]
6. Il'jasov, S. (2006) Security management in the banking sector of the region [Upravlenie bezopasnost'ju v bankovskoj sfere regiona]. *Money* & *Finance*. No. 5. p. 46. [In Russian]
7. Baranovskyi, O. (2014) *Philosophy of security [Filosofiia bezpeky]*. *Vol. 2. Security of financial institutions [Bezpeka finansovykh instytutiv]*. Kyiv, Ukraine: UB NBU. [In Ukrainian]
8. Kliekov, O. (1997) *Banking security [Bankivska bezpeka]*. Kyiv, Ukraine: Blits-Inform. [In Ukrainian]
9. Shtaier, O. (2011) Directions of ensuring and basic components of bank`s economic security [Napriamy zabezpechennia ta osnovni skladovi ekonomichnoi bezpeky banku]. *European Vector of Economic Development***.** No. 2. p. 266. [In Ukrainian]
10. Yaremenko, S. (2010) *Ensuring banks` economic security [Zabezpechennia ekonomichnoi bezpeky diialnosti bankiv]*. Ph.D. Thesis. Kyiv, Ukraine. [In Ukrainian]
11. Yaremenko, S. (2011) Complex system of bank's economic security and its management [Kompleksna systema ekonomichnoi bezpeky banku y upravlinnia neiu]. *Finance, accounting and audit*. Vol. 17. pp. 211-213. [In Ukrainian]
12. Sorokivska, Z. (2011) On the issue of financial security of the bank in the global economic crisis [Do pytannia finansovoi bezpeky banku v umovakh svitovoi ekonomichnoi kryzy]. *Ekonomichnyy analiz*. Vol. 8. Part 1. p. 407. [In Ukrainian]
13. Riznyk, N., Vorobiova, I. (2008) Assessment and ways to ensure the economic security of the bank [Otsinka ta shliakhy zabezpechennia ekonomichnoi bezpeky banku]. *Ekonomichni Nauky. Seriia "Oblik I Finansy". Zbirnyk Naukovykh Prats. Lutskyi Natsionalnyi Tekhnichnyi Universytet*. Vol. 5 (20). Part 2. [In Ukrainian]
14. Osipova, M. (2012) On the concept of banking in the Russian Federation [O ponjatii bankovskoj dejatel'nosti v Rossijskoj Federacii]. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii = Izvestiya of Irkutsk State Economics Academy*. No. 2. pp. 161-166. [In Russian]
15. Remote banking: ways to protect transactions [Dystantsiine bankivske obsluhovuvannia: sposoby zakhystu tranzaktsii]. Available at: http://www.bankchart.com.ua/rko/statti/distantsiyne_bankivske_obslugovuvannya_sposobi_zahistu_tranzaktsiy (Accessed: 18 July 2020). [In Ukrainian]

16. Bukin, S. (2003) Bank security [Bezopasnost' banka]. *Bankovskie tehnologii*. No. 9. pp. 44-47. [In Russian]
17. GfK Ukraine (2014) *Fraud and literacy in the use of payment instruments: a view of Ukrainian consumer [Shakhraistvo ta hramotnist u sferi vykorystannia platizhnykh instrumentiv: pohliad ukrainskoho spozhyvacha]*. Available at: http://www.gfk.com/ua/news-and-events/press-room/pressreleases/Pages/ema_research_release.aspx. (Accessed: 27 July 2020). [In Ukrainian]
18. Lysenko, A. (2004) The use of biometrics for personal identification [Zastosuvannia biometrychnykh system dlia identyfikatsii osoby]. *Bulletin of Taras Shevchenko National University of Kyiv. Legal Studies*. No. 60/62. p. 87. [In Ukrainian]
19. Mytsko, A., Paramud, Ya. (2014) *Face recognition software service with using 3D sensor PrimeSense Carmine 1.08 [Prohramnyi servis rozpiznavannia oblych z vykorystanniam 3D sensora PrimeSense Carmine 1.08]* Available at: http://eom.lp.edu.ua/sntk/doc/spr2014/mytsko.doc (Accessed: 27 July 2020). [In Ukrainian]
20. *Russian biometric portal* (2016). Available at: http://www.biometrics.ru/ (Accessed: 04 August 2020)
21. Zhang, D., Liu, F., Zhao, Q., Lu, G., Luo, N. (2011) *Selecting a Reference High Resolution for Fingerprint Recognition Using Minutiae and Pores*. IEEE Trans. on Instrumentation and Measurement, 60 3 863 871.
22. Bulatov, Y., Jambawalikar, S., Kumar, P., Sethia, S. (2002) Hand Recognition System Using Geometric Classifiers. *DIMACS Workshop on Computational Geometry*. (14-15 November 2002). Piscataway, NJ. Pp. 14-15
23. Romanov, V., Haleliuka, I., Klochan, P. (2010) Technologies of personal authentication on biometric characteristics [Tekhnolohii autentyfikatsii osoby za biometrychnymy kharakterystykamy]. *Computer Means, Networks and Systems = Kompiuterni Zasoby, Merezhi ta Systemy*. No. 9. p. 54. [In Ukrainian]
24. Thakkar, D. (2017) *An Overview of Biometric Iris Recognition Technology and Its Application Areas.* Available at: https://www.bayometric.com/biometric-iris-recognition-application/ (Accessed: 04 August 2020)
25. *Voice Print Analysis Services.* (2016) Available at: https://www.drdennistanner.com/Voice%20Print%20Analysis.htm. (Accessed: 05 August 2020).
26. Marčelja, S. (1980). Mathematical description of the responses of simple cortical cells. *Journal of the Optical Society of America*. 70(11). Available at: http://dx.doi.org/10.1364/JOSA.70.001.297. (Accessed: 24 July 2020)
27. *Nucleus Research* (2005). ROI Evaluation Report. Available at: http://nucleusresearch.com/. (Accessed: 05 August 2020).