European Journal of Business Startups and Open Society

Vol. 3 No. 4 (April - 2023): EJBSOS

http://innovatus.es/index.php/ejbsos

Improvement of the Banking Information Protection System

Valiev Azizbek Mutalibdzhanovich
BFA

Abstract: this article gives an idea of the improvement of the information security system in the country's commercial banks and provides an analysis of information security. In addition, it describes the work carried out to improve the information security system in commercial banks, and the reforms carried out by the government, as well as information security considerations that contribute to its development.

Key words: banking, information security, information space, cybersecurity, electronic payments, automated system.

Introduction

Today, as a result of the rapid development of remote services and online sales in the process of globalization of the world market, there is an opportunity for customers to freely use these services from anywhere on Earth. In particular, in the Republic of Uzbekistan, the use of electronic payment services via the internet is becoming increasingly popular. As globally, the development of remote banking services, along with the penetration of advanced digital technologies into our society, there is an increasing number of financial fraud in relation to users of the services of banking and payment organizations over the internet. To date, no violations have been recorded in electronic payment systems in the Republic, but there are cases of illegal embezzlement of funds by using the opportunities created to transfer electronic payments to users for selfish purposes and entering into their trust using methods of social engineering in relation to customers. Today the whole world lives in a complex environment, where information has become the most powerful weapon thanks to the revolution of digital technologies. This factor, in turn, requires each state to form mechanisms to ensure information security and protect users from existing cyber threats. After all, the current rapid globalization indicates that this issue is becoming extremely relevant in the process of building an informatized society.

Analysis of literature on the topic. It is devoted to the study of the information security system as an element of economic security in commercial banks as a key factor in research y. Baliyan, R.Mardanov, I.Of The Year, M.Lagazio,, N.Sheriff, M. The works of Cushman and other economists reflect various aspects of the banking information security system.

Problems of the information security system for achieving the goals of financial development of commercial banks D. Shinder, E. Titte, E.Markova, P.Williams, R.Tuchila, V.The developments of Pelyh and others are dedicated. Some issues of the development of the banking information security system and the creation of conditions for its effective use are discussed by economists of our country Z.Mamadiyarov, H.Abulqasimov, A. Also considered in the works of dusmukhamedov and others.

In the scientific work of the above-mentioned authors, insufficient attention was paid to the development of the banking information security system and the formation of a strategy for ensuring

information security, taking into account the effective use of its effective use. Therefore, the development and effective use of the banking information security system is one of the urgent issues.

Research methodology. This article gives an idea of the improvement of the information security system in the country's commercial banks and provides an analysis of information security. In addition, it describes the work carried out to improve the information security system in commercial banks, and the reforms carried out by the government, as well as information security considerations that contribute to its development. Systematic analysis, generalization, and abstract-logical thinking were used during the study of the subject along with general economic methods.

Analysis and results. Currently, measures are being implemented in our country to increase the popularity of financial services, expand the penetration of banks into the regions and ensure the provision of the same type of services in all settlements.

On the basis of modern service solutions to the banking system, it is required to widely introduce information technologies, financial technologies, to ensure the level of information security, as well as to take operational measures to reduce the influence of the human factor in the provision of financial services.

One of the main goals of the central bank is to develop and strengthen the banking system of the Republic, as well as to ensure that the payment system is betokhtov and functioning effectively. One of the most important conditions for the implementation of this goal is the adequate and necessary provision of information security in the organizations of the banking system of the Republic of Uzbekistan, that is, in most cases it consists in determining the level of information security of the automated banking system (ABT), banking technological processes (payment, data, etc.).

The peculiarity of the banking system is that the consequences of the occurrence of negative situations in the work activities of individual organizations lead to the rapid development of the system crisis in the payment system, affect the income of customers and owners. The occurrence of incident cases in Information Security increases the chances of significant damage to the organizations of the banking system. Therefore, the threat to the information assets of the organizations of the banking system, that is, the danger to information security, expresses the Real danger posed to the organization.

The reputation and competitiveness of the bank depends on its information security. A high level of information security of a credit institution allows you to minimize the following risks:

- risk of leakage of information constituting official/commercial/banking secrets;
- risk of destruction and loss of valuable information;
- risk of using incomplete or distorted information in banking activities, including making management decisions;
- risk of spreading information in an external environment that threatens the bank's reputation.

The features of banking information systems are that they are:

- storage and processing of large amounts of information on the financial condition and activities of individuals and legal entities
- have the tools to carry out operations with financial consequences
– it is impossible to close them completely, since they must meet modern requirements for the level of service (online banking system, network of ATMs connected to common communication channels, etc.).(Figure 1)

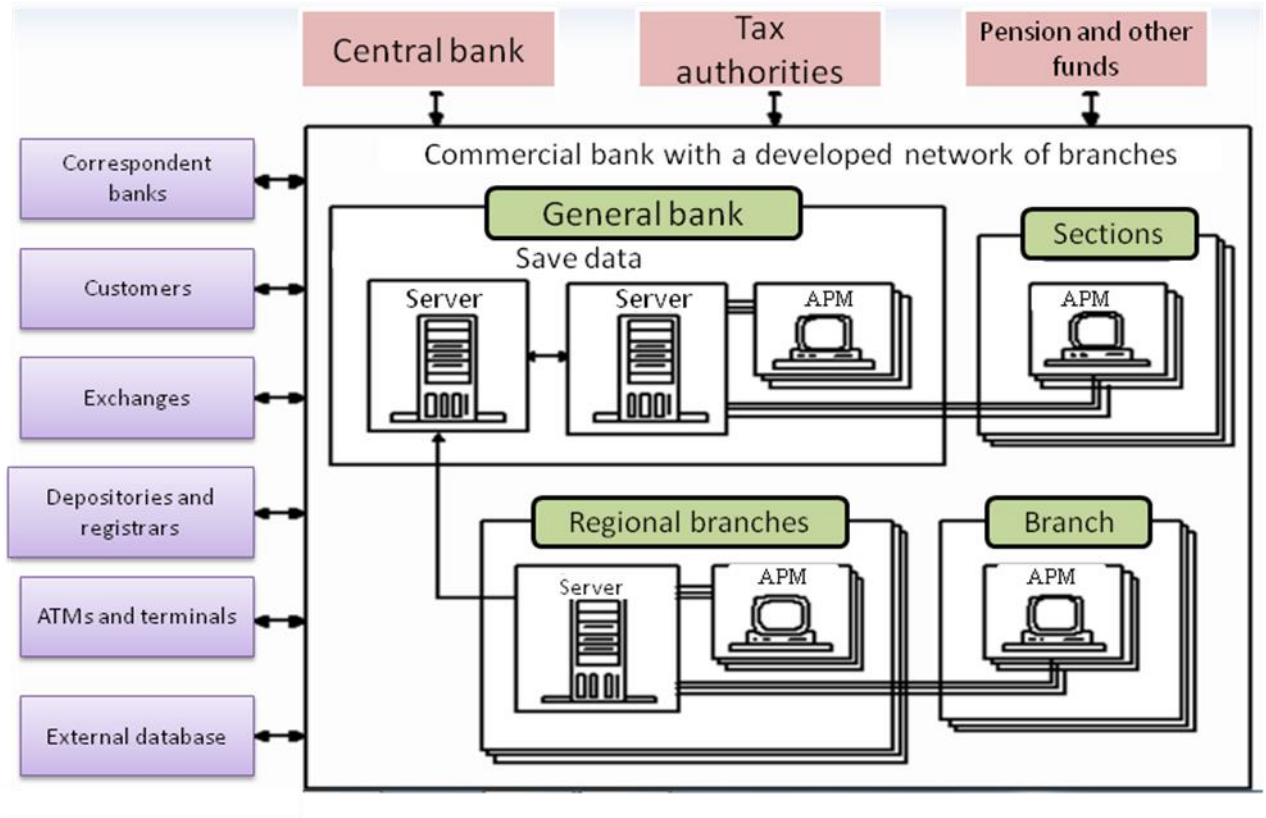

Figure 1. The procedure for ensuring bank information security[1]

The following works are carried out in ensuring the banking information security system:

- systematization and analysis of the data obtained for the development of analytical conclusions on the criticality of the identified information security problems, assessment of the degree of damage caused by the use of vulnerabilities;

- development of recommendations on the elimination of vulnerabilities identified in the target systems of the organization and the shortcomings of Information Security;

- the recommendations under development should include information on organizational and technical measures that the client must carry out in order to increase the level of security.

Bank information systems and databases contain confidential information about bank customers, the status of their accounts and various financial operations.

The need to maintain the information security of this information is obvious, but without the rapid and timely exchange of information, as well as without processing, the banking system will fail. For this reason, a whole is needed that protects bank data and ensures the confidentiality of the customer base.

The sequence of measures to protect this data can be shown as follows:

* evaluation and development of confidential information;

* equip the facility to carry out protection;

* control over the effectiveness of the measures taken.

The Bank can fully carry out its activities only if there is an internal data exchange and a reliable security system. Information security equipment of banking facilities can take various forms.

[1] Compiled by the author

Access to Bank information is protected by an identification system, that is, using passwords or electronic keys. Working with employees using the banking system involves conducting briefings and monitoring the fulfillment of the necessary requirements.

Strict accounting of channels and servers, as well as measures to ensure the technical protection of information and the security of the bank, provides for the protection of backup copies, uninterrupted power supply of equipment containing valuable information, restriction of access to safes and protection against leakage of information.

To analyze the effectiveness of the measures taken, it is necessary to keep a record that records the effectiveness of those used in the bank.

Despite the large number of opportunities for hacking and the spread of information, it is quite possible to ensure the safety of bank data and their confidentiality.

Modern methods have made it possible to improve the cryptography system, as well as implement such a measure as an electronic digital signature (eds). It serves as an analogue of a handwritten signature and is directly associated with an electronic key stored in the owner of the signature. The key consists of two parts: open and closed, and is protected by a special code.

In general, the security system is a continuous process of identification, analysis and control. There are a number of basic principles that ensure the information security of the bank:

* timely detection of problems;

• ability to predict development;

* relevance and effectiveness of the measures taken.

It is also important to note the importance of careful and regular work with employees, since ensuring information security largely depends on the qualitative and accurate fulfillment of the requirements imposed by the security service.

In recent years, as a result of the penetration of the digitization process in the banking industry, the system of ensuring information security of the bank has also been changing. In this case, the main focus is on the immediate study of the demand for digital products and its implementation (sound recognition of biometric technologies, fingerprint recognition, face recognition, etc.).) aims to develop strategies in different approaches to providing to bank customers. The main issue of drawing up a digital banking strategy is the need for banks to pay attention to the remote, convenient and low cost of new banking services, as well as to pay special attention to the information security system.

It can be seen that the number of users of remote banking services in our country has increased especially sharply in the last two years (Figure). This can be explained by two cases, firstly, an increase in the volume of banking products through digitalization in commercial banks, and secondly, an increase in demand for digital banking products in the context of a pandemic. Taking into account the above circumstances, banks today require putting the system of ensuring their disaffection in the right way.

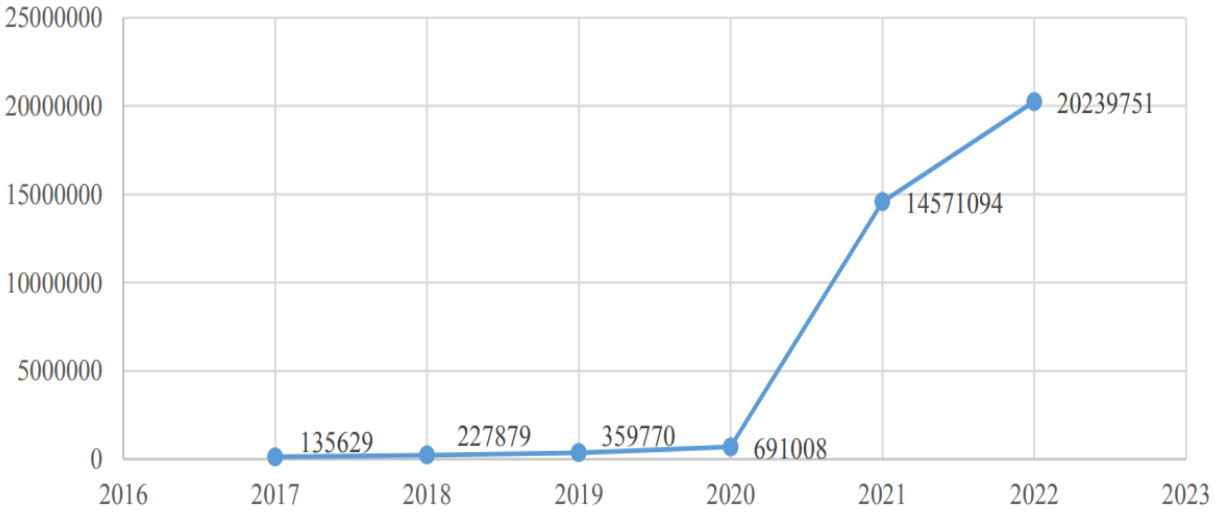

Figure 2. Number of users of remote banking services[2]

To date, ensuring information security is one of the urgent problems, the solution of which requires special attention. In this regard, there is a need to create appropriate organizations that are responsible for the organization and implementation of work aimed at ensuring the protection of information.

It is no secret that banks in the Asia-Pacific region are increasingly becoming targets of hackers and cybercriminals. This makes financial institutions in the region pay more attention to the security of their information networks. A sociological survey, which interviewed 150 bank employees conducted by Robert Half International, showed that employees of Singapore banks take the performance of their duties seriously. 70% of the top managers of Singapore banks surveyed commented on the growth of cyber threats. For comparison: among employees of Hong Kong banks, this figure was 60 percent, in Japan-42 percent. During the survey, respondents were asked to express their opinion on cloud technologies and share plans for their implementation and use. A survey of top managers of Singapore banks showed that 36% of them do not use cloud technologies, since they do not believe in their security; 24 percent are concerned about the security and integrity of data, while 18 percent of the transition to the use of cloud technologies is hampered by a lack of understanding the internal structure of the cloud environment. At the same time, 44% of top managers said that they did not plan to use cloud technologies in the near future.

Conclusions and suggestions.

The following recommendations were made on improving the information security system in commercial banks of the country and on the analysis of Information Security.

1. Based on the experience of foreign countries, the banking system of our country is one of the most sensitive areas of the national economy of any country to innovation and the ever-changing architecture of the socio-economic system. This is explained by the dualism of the economic interests of the banking institution in the conditions of digitalization. On the one hand, the formation of the digital economy is a strong focus for the qualitative evolution of the product portfolio, with the possibility of offering personalized products and services to retail and corporate customers.

2. Globalization and integration in the field of intellectual activity contribute to the development and modernization of the banking system of our country as a whole, which, on the one hand, the prospects for the further development of possible functionality and credit organizations,

[2] https://cbu.uz/oz/statistics/buleten/592793/compiled by the author based on his data

on the other hand, constantly require the search for ways to minimize the information security risks of commercial banks associated with the

3. Today, the implementation of unsystematic measures aimed at increasing the level of information security cannot provide the required level of protection. To understand the priority of measures aimed at increasing the level of information security, it is necessary to develop and apply a mechanism for managing the risk of Information Security. Such effective risk management allows banks to concentrate efforts and direct them to protect the bank from dangerous threats with minimal costs.

List of used literature

1. Shinder D.L., Tittel E. Scene of the Cybercrime: Computer Forensics Handbook BookReader. Available at: http://bookre.org/reader?file=495251 (accessed 23.03.2022).
2. Markova E.A. Ugolovno-pravovaja harakteristika hishhenija, sovershaemogo s ispol'zovaniem jelektronnyh sredstv platezha. Diss. dokt. jur.nauk [Criminal-legal characteristics of theft committed using electronic means of payment dis.. cand. jurid] – Saint-Peterburg, 2022. – P. 251.
3. Williams P., Organized Crime and Cybercrime: Synergies, Trends, and Responses Crime Research. Available at: http://www.crime-research.org/ library/ Cybercrime.htm (accessed 23.03.2022). Tuchila, R. Servicii bancare prin Internet. E-finance Romania, 2000.
4. Pelyh V.YA. Finansy 4.0 kak ideya cifrovoj transformacii finansovoj sfery. Mir ekonomiki i upravleniya. 2020. № 20. S. 134 – 148.
5. Mamadiyarov, Z. (2021). Analysis of factors affecting remote banking services in the process of bank transformation in Uzbekistan. Financial and credit activity: problems of theory and practice, 1(36), 14-26.
6. Абулқосимов Ҳ.П. Iktisody havfsizlik. //Tashkent. The academy. 2006., Dusmukhametov A. Information protection by the method of establishing horizontal and vertical restrictions on access to information resources // Customs Bulletin of Uzbekistan. - 2019. - №2. С. 46-50.
7. Йохан Балийон. Modern trends in the field of information security of banks // Banking. 2014. No. 10. pp. 60-63., Mardanov R.H., Ilyin I.V. Information security standards in the banking system // Bulletin of the Ufa State Aviation Technical University. 2013. Т. 17. № 7. С. 55–60.