Methodological Aspects of the Bank's Information Security

Askarjon Khujamurodov

Senior Teacher at Tashkent State University of Economics, Tashkent City, Republic of Uzbekistan

Zilola Jumanova

Master's Student at Tashkent State University of Economics, Tashkent City, Republic of Uzbekistan

Abstract- **The article describes the methodological aspects of the information security of the bank. The author substantiates that the information security of banks has connections with the general information and computerization of banking. In addition, were discussed the trends of crimes and their classification in the banking sector.**

Keywords- Internet, information security, bank, electronic payments, plastic cards, computer networks, economic crime.

I. INTRODUCTION

As you know, from the time of their appearance, banks have invariably aroused criminal interest. And this interest was associated not only with the storage of funds in credit institutions, but also with the fact that important and often secret information about the financial and economic activities of many people, companies, organizations and even states was concentrated in banks.

Today, in connection with the general information and computerization of banking activities, the importance of information security of banks has increased many times over. Even 30 years ago, the object of information attacks was data on bank customers or on the activities of the bank itself. Then such attacks were rare, the circle of their customers was very narrow, and the damage could be significant only in special cases. Currently, as a result of the ubiquitous spread of electronic payments, plastic cards, computer networks, the rapidly growing popularity of services provided to customers via Internet technologies, the funds of both banks and their customers have become the object of information attacks. Anyone can make an attempt to steal - you just need a computer connected to the Internet. Moreover, this does not require physically entering the bank, you can "work" and thousands of kilometers from it.

For example, in August 1995, 24-year-old Russian mathematician Vladimir Levin was arrested in Great Britain, who, using his home computer in St. Petersburg, managed to find the keys to the banking security system of one of the largest American banks, Citibank, and tried to withdraw large sums from his accounts. According to the Moscow representative office of Citibank, until then, no one has succeeded. Citibank's security service found out that they tried to steal $ 2.8 million from the bank, but the controlling systems discovered this in time and blocked the accounts. But Vladimir Levin managed to steal only 400 thousand dollars. for which he went to England, where he was arrested.[1]

II. LITERATURE REVIEW

Some local economists, as well as Khodiev B. Y. [2], Mus-tafakulov Sh. I., [3] and others proposed evaluation methodology for integrated assessment of production capacity management, which is based on qualitative and effective indicators of production capacity management. Methodology for assessment the efficiency of production capacities management at textile enterprises were investigated by B. O. Tursunov in other works [4], but they have not investigated problems of influence of the Covid-19 pandemic coronavirus of the world economy.

III. ANALYSIS AND RESULTS

The computerization of banking activities has made it possible to significantly increase the productivity of the bank's employees, introduce new financial products and technologies. However, progress in crime technology was no less rapid than the development of banking technologies.[5]

Currently, most of the crimes in this area are associated with the use of automated information processing systems of the bank (ASOIB). Consequently, when creating and modernizing ASOIB, banks need to pay close attention to ensuring its security.[6]

It is this problem that is now the most urgent and, alas, the least studied. If in ensuring physical and classical information1 security, well-established approaches have long been developed (although development is taking place here as well), then in connection with frequent radical changes in computer technologies, the security methods of ASOIB require constant improvement and updating. As practice shows, there are no complex

computer systems that do not contain errors. And since the ideology of building large ASOIB regularly changes, fixing the found errors and "holes" in the security systems is not enough for long, since the new computer system brings new problems and new errors, an adequate restructuring of the security system is required.[7]

This problem is especially relevant in Russia. In Western banks, software (software) is developed specifically for each bank, and the ASOIB device is largely a trade secret.

Classical information security is understood as a system of separation of access rights to information, measures to protect against eavesdropping, prevention of leaks by personnel and other measures not directly related to ASOIB.[8]

Distribution of "standard" banking packages, information about which is widely known, which facilitates unauthorized access to banking computer systems. Moreover, firstly, the reliability of the "standard" software is lower due to the fact that the developer does not always have a good idea of the specific conditions in which this software will have to work, and secondly, some Russian banking packages did not meet the security conditions. For example, early versions (which are still operated in small banks) of the most popular Russian banking package required a personal computer to have a floppy drive and used a key diskette as a security tool. Such a solution, firstly, is technically unreliable, and secondly, one of the security requirements of ASOIB is to close the drives and input-output ports in the computers of employees who do not work with external data.

For banks (unlike other businesses), information security is critical. We should not forget about the development of banking information technologies (IT), since it is these technologies that largely determine the bank's information security system.(Fig.1)

The first trend is an increase in the value of economic parameters when making decisions on the choice of projects. The presented scheme shows that in 80% of cases the formal justification for starting a technological project is the parameters of the return on investment or the payback period of the project.

Other trends relate to the changing role of the bank's IT department. The data presented illustrates that the majority of respondents report an increase in collaboration with business units. Also noted are such changes as increased centralization and control, focus on business results and the introduction of new technologies and solutions. Only about 10% of the respondents note the absence of any changes.

Recently, there has been a significant increase in the share of third-party services, organizations are increasingly using outsourcing. At the same time, they strive to transfer practically all non-key business functions to outside organizations. Today, on average, 28% of IT budget funds go to third-party solution and service providers, which cannot but affect security in general. About 40% of respondents note that they have transferred (in whole or in part) to other suppliers such their technological functions as development, support and operation of applications.

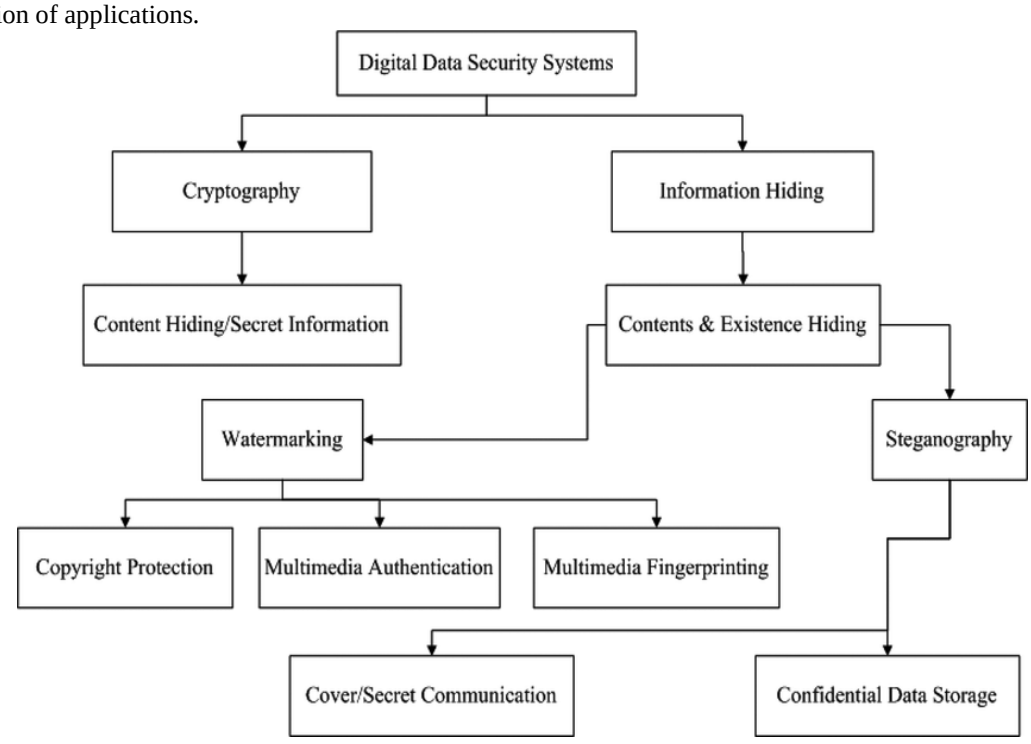

Fig.1. Classification of information security systems.

Another significant trend in information technology management is the increase in the speed of decision-

making when purchasing IT solutions: the vast majority of all decisions in this area are made in less than three months.

As you can see from the above, an IT strategy cannot be drawn up without an understanding of the business strategy and must be based on it. It is advisable to draw up a strategic plan in the form of two documents - a long-term strategy and a short-term one. A long-term strategy is drawn up for 3-5 years and includes the corresponding tasks and goals, a short-term one - for a period of 1 to 3 years.

Both documents should be updated regularly. For a long-term document, this can occur on a semi-annual basis, for a short-term document, on a quarterly basis. All updates are made in close collaboration with business managers and are coordinated with the top management of the organization.

Fig.2. IT strategy.
Source: https://bitco3.com/en/topics/it-strategy/

The IT strategy is approved by the senior management of the bank based on the results of joint preliminary study of the heads of IT and business units. Such work is possible within the framework of the meetings of the information technology (or technical) committee of the bank.

Also the most important element of strategic planning is execution control. The strategy should not be a declarative document, and the main way to achieve this is to control its implementation, including by the top management of the bank, the information technology committee.

According to statistics, most of the crimes against banks are committed using insider information. In this regard, it is necessary to pay constant attention to ensuring information security in the field of work with personnel.

With the development and expansion of the scope of application of computer technology, the acuteness of the problem of ensuring the security of computer systems and protecting the information stored and processed in them from various threats is increasing. There are a number of objective reasons for this.[9]

Today, the problem of protecting computer systems is becoming even more significant in connection with the development and spread of computer networks. Distributed systems and systems with remote access have brought to the fore the issue of protecting processed and transmitted information.

The availability of computer technology, and primarily personal computers, has led to the spread of computer literacy among the general population. This, in turn, has caused numerous attempts to interfere with the work of state and commercial, in particular banking, systems, both with malice and out of purely "sports interest." Many of these attempts have been successful and have caused significant damage to the owners of information and computing systems.

To a large extent, this applies to various commercial structures and organizations, especially those who, by the nature of their activities, store and process valuable (in monetary terms) information that also affects the interests of a large number of people. In banks, when it comes to electronic payments and automated account management, this information is in some way money.

It is rather difficult to create a holistic picture of all protection possibilities, since there is still no unified theory of computer systems protection. There are many approaches and points of view on the methodology of its construction. Nevertheless, serious efforts are being made in this direction, both in practical and theoretical terms, the latest achievements of science are used, and advanced technologies are involved. Moreover, leading

companies in the production of computers and software, universities and institutes, as well as large banks and international corporations are engaged in this problem.

There are various options for protecting information - from a security guard at the entrance to mathematically verified methods of hiding data from acquaintance. In addition, we can talk about global protection and its individual aspects: protection of personal computers, networks, databases, etc.

It should be noted that there are no completely secure systems. We can talk about the reliability of the system, firstly, only with a certain probability, and secondly, about protection from a certain category of violators. Nevertheless, penetration into a computer system can be foreseen. Defense is a kind of competition between defense and attack: the one who knows more and provides effective measures wins.

Organization of ASOIB protection is a single set of measures that must take into account all the features of the information processing process. Despite the inconvenience caused to the user during work, in many cases, protective equipment may be absolutely necessary for the normal functioning of the system. The main disadvantages mentioned include:

1) additional difficulties in working with most protected systems;

2) increase in the cost of the protected system;

3) additional load on system resources, which will require an increase in working time to perform the same task due to slower access to data and operations in general;

4) the need to attract additional personnel responsible for maintaining the health of the protection system.

It is difficult to imagine a modern bank without an automated information system. The computer on the desk of a bank employee has long become a familiar and necessary tool. The connection of computers with each other and with more powerful computers, as well as with computers of other banks is also a necessary condition for the successful operation of a bank: there are too many operations that must be performed within a short period of time.

Computer systems, which no modern bank can do without, are a source of completely new, previously unknown threats. Most of them are due to the use of new information technologies in banking and are characteristic not only of banks. It should be remembered that in many countries, despite the increasing role of electronic processing systems, the volume of transactions with paper documents is 3-4 times higher than with their electronic counterparts.

The level of automation equipment plays an important role in the bank's activities and, therefore, directly affects its position and income. Increased competition between banks leads to the need to reduce the time for making settlements, increase the range and improve the quality of services provided.

The less time it takes for settlements between the bank and clients, the higher the bank's turnover and, consequently, the profit will become. In addition, the bank will be able to react more quickly to changes in the financial situation. A variety of bank services (first of all, this relates to the possibility of non-cash payments between the bank and its customers using plastic cards) can significantly increase the number of its customers and, as a result, increase profits.

Several facts can be cited to confirm this thesis:

• Losses of banks and other financial institutions from impacts on their information processing systems amount to about $ 3 billion. in year;.

• The volume of losses associated with the use of plastic cards is estimated at $ 2 billion. per year, which is 0.03-2% of the total volume of payments, depending on the system used;

• $ 27 million pounds were stolen from the London branch of Union Bank of Switzerland;

• 5 million marks stolen from Chase Bank (Frankfurt); the employee transferred the money to a Hong Kong bank; they were taken from a large number of accounts ("salami" attack), the theft was successful;

• $ 3 million - Bank of Stockholm, the theft was committed using the privileged position of several employees in the bank's information system and was also successful.

To protect themselves and their customers, most banks take the necessary protection measures, among which the protection of ASOIB is not the last. It should be borne in mind that the protection of ASOIB bank is an expensive and complicated undertaking. For example, Barclays Bank spends about $ 20 million to protect its automated system. annually.

In the first half of 1994, the Datapro Information Services Group conducted a mail poll of randomly selected information systems managers. The purpose of the survey was to clarify the state of affairs in the field of defense. 1,153 questionnaires were received and the following results were obtained:

1) about 25% of all violations are natural disasters;

2) about half of the systems experienced sudden power or communication interruptions, the reasons for which were artificial;

3) about 3% of systems experienced external violations (penetration into the organization's system);

4) 70-75% - internal violations, of which:

- 10% were committed by offended and dissatisfied employees-users of ASOIB bank; - 10% - committed out of selfish motives by the personnel of the system; - 50-55% - the result of unintentional errors of personnel and / or users of the system as a result of negligence, negligence or incompetence.

These data indicate that the most common violations, such as attacks by hackers or theft of computers with valuable information, do not occur, but the most common ones arising from everyday activities. At the same time, it is deliberate attacks on computer systems that bring the greatest one-time damage, and measures to protect against them are the most complex and costly. In this regard, the problem of optimizing the protection of ASOIB is the most urgent in the field of information security of banks.

There are two aspects that set banks apart from the rest of the commercial systems:

1. Information in banking systems is "live money" that can be received, transferred, spent, invested, etc.
2. It affects the interests of a large number of organizations and individuals.

Therefore, the information security of a bank is a critical condition for its existence. As a result, banking systems are subject to increased requirements regarding the security of storage and processing of information. Domestic banks will also not be able to avoid the fate of total automation for the following reasons:

- increased competition between banks;
- the need to reduce the time for making calculations;
- the need to improve the service.

In the United States, Western Europe and many others that have faced this problem for a long time, a whole industry for the protection of economic information has now been created, including the development and production of secure hardware and software, peripheral devices, scientific research, etc.

IV. CONCLUSIONS

The field of information security is the most dynamic area in the development of the security industry as a whole. While physical security has a long tradition and well-established approaches, information security constantly requires new solutions. computer and telecommunication technologies are constantly being updated, and more and more responsibilities are placed on computer systems.

Statistics show that the vast majority of large organizations have a plan with information access rules as well as a disaster recovery plan. The security of electronic banking systems depends on a large number of factors that must be taken into account at the design stage of this system. Moreover, for each separate type of banking operations and electronic payments or other methods of exchanging confidential information, there are specific security features. Thus, the organization of the protection of banking systems is a whole range of measures that should be taken into account both general concepts, but also specific features.

It is obvious that the automation and computerization of banking (and money circulation in general) continue to grow. The main changes in the banking industry over the past decades are associated precisely with the development of information technologies. It is possible to predict a further decrease in the turnover of cash and a gradual transition to non-cash payments using plastic cards, the Internet and remote terminals for managing the account of legal entities.

Proceeding from the fact that the factors that determine the trends in the development of crime in the field of information technology, in the near future may not undergo significant changes, obviously, one should not expect radical changes in the criminal situation in the information sphere.

REFERENCES

[1]. Jung, Ki-Hyun & S.Ramakrishnan,. (2019). Cryptographic and Information Security Approaches for Images and Videos. 10.1201/9780429435461.

[2]. Khodiev, B. Y. & Mustafakulov, Sh.I., Tursunov, B.O., Sigidov, Yu., Khavrova, K.S. (2019). Methods for control efficiency evaluation of the prodcution capacities. Astra Salvensis, Supplement no. 1, 499–521. https://doi.org/10.5281/zenodo.3666484

[3]. Mustafakulov, Sh. I., Zarova, E. V., Tikhomirova, A. N., & Tursunov, B. O. (2019). Research of efficiency of use of production capacity at the enterprises of textile industry on the basis of methods of multivariate statistical analysis: On the example of Namangan Region of the Republic of Uzbekistan. Journal of Advanced Research in Dynamical and Control Systems, 11(7), 886–899. Retrieved from https://doi.org/10.5281/zenodo.3756255

[4]. Tursunov, B. O. (2019). Methodology for assessment the efficiency of production capacities management at textile enterprises. Vlakna a Textil, 26(2), 74–81. https://doi.org/ 10.5281/zenodo.3756262The special role of exports in the growth of the economy. // J. Economic Review, No. 10,2005.

[5]. Khujamurodov, A. (2018). Trends of development of the Uzbekistan stock market and analysis of influencing factors. Бюллетень науки и практики, 4, (1), 242-247

[6]. Khujamurodov AJ (2018) Analysis of development of the infrastructure of the stock market in Uzbekistan and the methodology of its estimation. ISJ Theoretical & Applied Science, 05 (61): 168-176.

[7]. Khujamurodov AJ (2019) Economic Essential of Stock Infrastructure and Features of Its Development. Asian Journal of Technology & Management Research (AJTMR) ISSN: 2249 –0892 Special Issue–2, Sep -2019
[8]. Khujamurodov, A.J., Jahongirov, R.J. (2020) Peculiarities of corporate strategy and risk prevention in joint stock companies. «Актуальные научные исследования в современном мире» ISSN 2524-0986. 59 (част 3), 21-25.
[9]. Khudjamuratov, A., Rejabbaev, S. (2020). Development and formation of the securities market in Russia. International Journal of Scientific & Engineering Research. ISSN 2229-5518, 1559-1563.