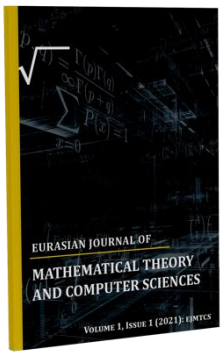
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 7.906 www.in-academy.uz



PROBLEMS OF PROVIDING INFORMATION SECURITY OF THE CREDIT ORGANIZATION

Sadikov Sh.M.
Kobiljanov Sh.N.
Professor of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi. Independent researcher of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
https://doi.org/10.5281/zenodo.13326873

ARTICLE INFO

Received: 09th August 2024
Accepted: 14th August 2024
Online: 15th August 2024

KEYWORDS

External threat, internal threat, credit organization, complex system, security system, criminological, banking resources, intangible resources, protection objects.

ABSTRACT

This article examines internal and external threats in banking systems, existing security problems in practice, researches the goals and tasks of ensuring the security system of credit organizations, defines the main tasks that arise in the creation of a security system, examines the elements of the criminal internal infrastructure, also the main threats in banking information systems are studied.

Legal, organizational and management, special, social-psychological, regulatory, technical, preventive and promotional measures aimed at qualitative implementation of the protection of the banking institution from external and internal threats by analyzing the foreign and local experience of ensuring security in the banking sector requires the need to create a comprehensive security system of the credit organization that performs its functions on an integrated basis. The main principle of creating such a system should be to ensure a certain level of security for the credit organization with the minimum cost of the organizational and technical measures implemented for this purpose and the protective means used.

In practice, the creation of such a security system is associated with solving a wide and diverse set of problems (Fig. 1).

In order to organize work in each of the above areas, to clearly formulate their final goals, to ensure the necessary sequence of solving problems, to determine all the important consequences and interdependence of each particular solution. a modern way of formalizing information appropriate to the level of threats is needed.

The problems of credit organization security and their solution is to use the currently widespread concept form should be created based on the credit organization's security concept, based on scientifically based views on determining the main directions, conditions and procedures for practical solutions to the problems of protecting the banking institution from illegal actions and unfair competition.

The concept, goals and objectives of the complex system of credit organization security, principles of its organization, operation and legal support, types of external and internal security threats to the banking institution and its protected financial, material and information

resources, as well as the main way of developing this system determines its directions, including legal, organizational and engineering-technical protection. It should include a systematic description of the types of threats (illegal attacks), defining the functions of the participants that ensure bank security, and a set of methods and tools for protecting the property and infrastructure of the credit organization.

The concept should be developed for the long term and take into account the interests of the owners, management, employees and customers of the credit organization.

In this regard, it is possible to formulate the main requirements for the organization of a comprehensive security system of a credit organization:

– it should have dynamic, flexible and upgradeable system features;

– its goals and structure, forces and means, directions of activity, forms and methods must change depending on the change of the internal and external situation, ensuring the necessary security situation.

In practice, the organization of such a system should be based on the fact that there is no absolute protection system and it is impossible to reduce threats to absolute zero and elimination of threats for each specific situation.

Objects protected from potential threats and illegal encroachments include:

Financial and material resources are the assets of the credit organization, which include cash, securities (including own funds and borrowed funds), property rights to objects of banking activity (collateral and others), also includes buildings, structures, warehouses, technical equipment and other means.

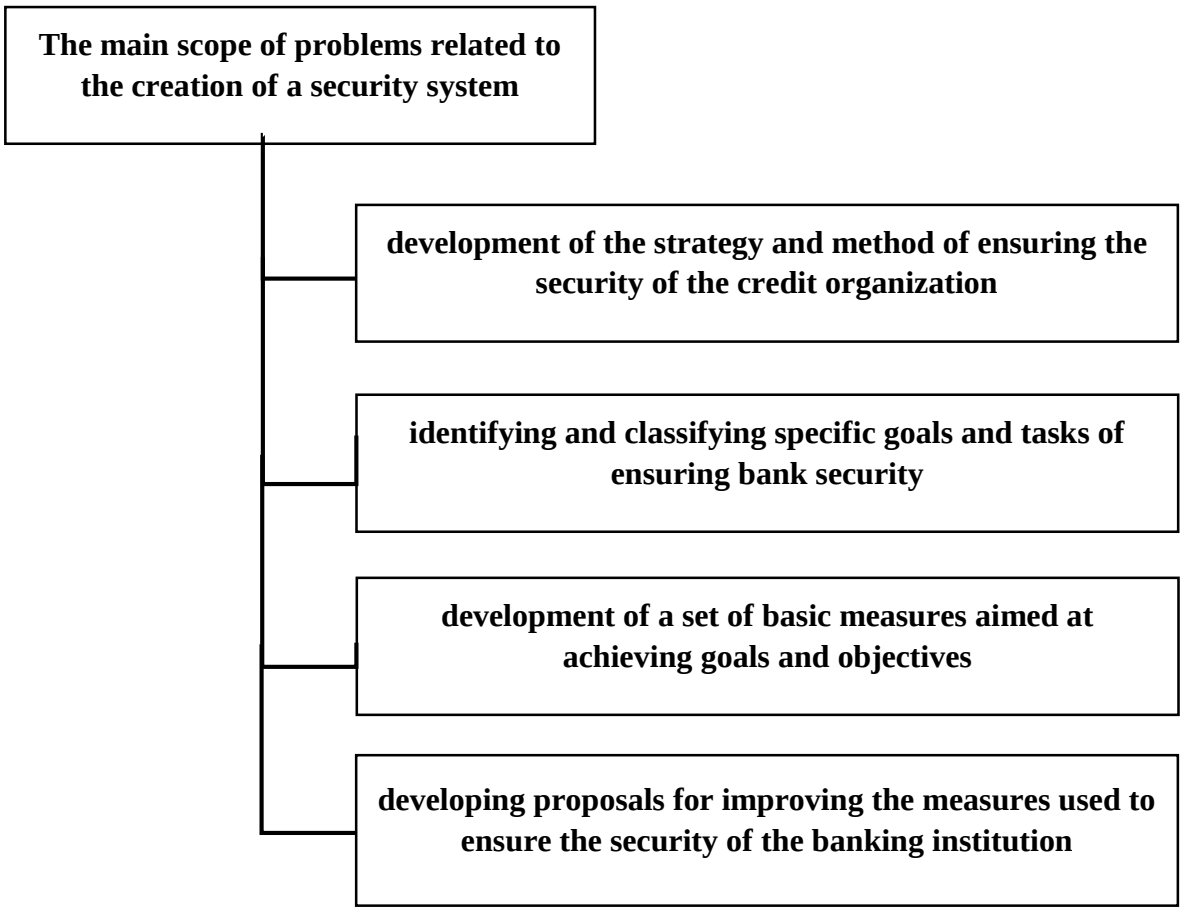


Figure 1. The main tasks that arise when creating a security system.

The main threats to the material resources of the credit organization are theft, fraud, misappropriation or embezzlement, robbery, robbery, extortion, etc.

The concept of “financial and material resources” also includes the infrastructure of a credit organization, which means the totality of property, legal, organizational elements and the stability of relations between them, which ensures the creation and stable operation of a banking institution.

In banking theory, it is accepted to separate internal and external infrastructure elements.

Among the criminologically significant internal infrastructure elements, the most important are:

– Legislation and other legal norms defining the organization of a credit organization and its operation;

– internal rules for the implementation of bank operations and protection of bank interests;

– banking management procedure (accounting, reporting, creation of an analytical database, computer processing of data based on modern communication systems).

includes elements such as information and personnel, intangible goods (the bank's business and its business relations with partners) important for ensuring the security of the credit organization.

The main threat to the credit organization's infrastructure is the destruction of its elements.

Information resources - separate documents and their arrays, that is, large-scale information used by the credit organization to make effective management decisions, to adopt new technologies and markets, as well as to take preventive measures in unfavorable situations. The information resources of the credit organization are formed by creating, collecting and purchasing documented information about facts, events and situations related to the banking sector. For this purpose, computer technologies and means of communication (information objects) that provide information processing, storage and transmission are involved.

The main threats to informatization objects, both in the field of traditional document exchange and in the field of the latest information technologies, are:

– illegal collection and use of information;

– unauthorized access to information resources;

– of information (false information, concealment or distortion of information), violation of information processing technologies.

Human resources are the employees of the credit organization. The intensity, types and goals of possible criminal attacks on employees of a banking institution depend on the functional duties and powers of each employee.

The main threats to the human resources of the credit organization are the threats, extortion and extortion of the employees of the banking institution by a criminal group or competitors and forcing them to engage in criminal activities.

Intangible resources are the credit organization's business reputation and its business relationships. The main threat to them is unfair competition in order to limit the activities of the credit organization or remove it from the banking services market (distribution of defamatory false information materials, involvement in malicious projects, destruction of customer relations, etc.).

All objects that can be subjected to security threats or illegal attacks have different levels of potential vulnerability in terms of material or moral damage. Based on this, they should be qualified in terms of vulnerability (danger), risk level.

In the classical classification of protection objects: human-information - material values, the main priority is, of course, focused on ensuring the safety of the employees of the credit organization. Currently, due to the wide development of modern banking information and payment technologies, information is taking second place from the point of view of security. In addition, this applies not only to information containing banking or commercial secrets, but also to public information, because it becomes "vulnerable" during processing with the help of computer technologies, so that the information is corrupted or lost. q can be, which in turn can have the most negative consequences for the credit organization.

Subjects of legal relations in solving the security problem of the credit organization:

– as the owner of resources created, purchased and collected at the expense of state budget funds, as well as state information resources;

– the Central Bank and its regional institutions implementing the monetary policy of the country;

– the owner of financial and informational resources constituting official, commercial or banking secrets of a credit organization as a legal entity;

– other legal entities and individuals participating in the activity of the credit organization, including partners and clients in financial relations (state authorities, executive bodies, law enforcement agencies, organizations and firms involved in providing various services, including security, service personnel, etc.);

– credit organization's security department and in some cases private security structures involved in solving security problems.

For the effective operation of the comprehensive security system of the credit organization, not only the professional experts of the security department, but also all the bank employees must actively participate in the measures to protect the bank structure. Establishing close cooperation between the security department and other departments of the credit organization is the key to successfully combating external and internal threats.

References:

1. Sadikov Sh.M., Ma’lumotlar bazasida ma’lumotlarni tashkil etishning modellari, International Scientific and Technical Conference “Digital Technologies: Problems and Solutions for Practical Implementation in an Industry” on April 27-28, 2022. B. 241-243.
2. I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker. “Security threats to critical infrastructure: The human factor”. The Journal of Supercomputing, vol. 74, no. 10, pp. 4986-5002, 2018.
3. Климович В.П. Финансы, денежное обращение и кредит: Учебник 2006

4. Ross Anderson “Security Engineering: A Guide to Building Dependable Distributed Systems” 2012

5. Sadikov Sh.M., Korporativ tarmoqda ma’lumotlar bazasiga bo‘ladigan tarmoq hujum turlari, International Scientific and Technical Conference “Digital Technologies: Problems and Solutions for Practical Implementation in an Industry” on April 27-28, 2022. B. 244-246.3