GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 8 August (2024)

BASIC PRINCIPLES OF ORGANIZING A COMPLEX SYSTEM OF ENSURING THE SECURITY OF A 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

ABSTRACT

In this article, a complex system of ensuring information security in a credit organization is proposed, the complex system includes several stages, in which each stage, each component is covered in sequence.

Keywords: Complex system, complexity, continuity, activity, legitimacy, validity, economic compatibility, equality, interaction, flexibility, planning, purposefulness.

INTRODUCTION

The correct organization and effective operation of the complex system of ensuring the security of the credit organization (Fig. 1). We will consider them below.

1. Complexity

There are various ways of breaching the security of the credit organization . This is due to the presence of many channels through which attackers can affect the protection objects . Therefore, it is necessary to use different measures, methods and means of protection at the same time.

This principle implies the perfection of protective measures against all forms of external and internal threats to the security of the credit institution, which is the result of the uncertainty of the security process due to the presence of many objective and subjective factors.

In this regard, activities in many areas of ensuring the security of the credit organization are being carried out at the same time:

- ensure safety of personnel, material and financial resources from possible threats by all available legal means, methods and measures;
- information resources during their availability, processing (changing) and at all technological stages of their use, in all operating modes;

Complexity is achieved through:

- ensuring the appropriate security regime of the credit organization;
- organization of special proceedings aimed at protecting information constituting banking and commercial secrets;
- personnel selection and placement activities;
- extensive use of technical security and information security tools;
- full description of information-analytical activity.

Is realized by a combination of legal, organizational and engineering-technical measures.

2. **Timeliness**

It includes the implementation of measures to ensure the security of the credit organization in a timely manner , including the development of a comprehensive security system based on analysis and analysis both in the entire banking sector of the credit organization and in its separate segments in the initial stages of defining tasks, external and internal threats to the security of the banking structure, as well as developing effective preventive measures and suppressing attacks on its legal interests.

3. Continuity

To ensure the comprehensive security of the credit organization , it should be taken into account that attackers are constantly looking for opportunities to bypass protective measures, and for this, resort to legal and illegal methods.

4. Activity

It is necessary to protect the interests of the credit institution with sufficient determination through the extensive use of security forces and means and non-standard protection measures.

5. Legality

Development of a comprehensive security system of the credit organization based on the federal legislation in the field of banking, information and information protection, private security activities and other regulatory documents on security approved by state administration bodies within the scope of their powers, detection and prevention of violations must be carried out using authorized methods.

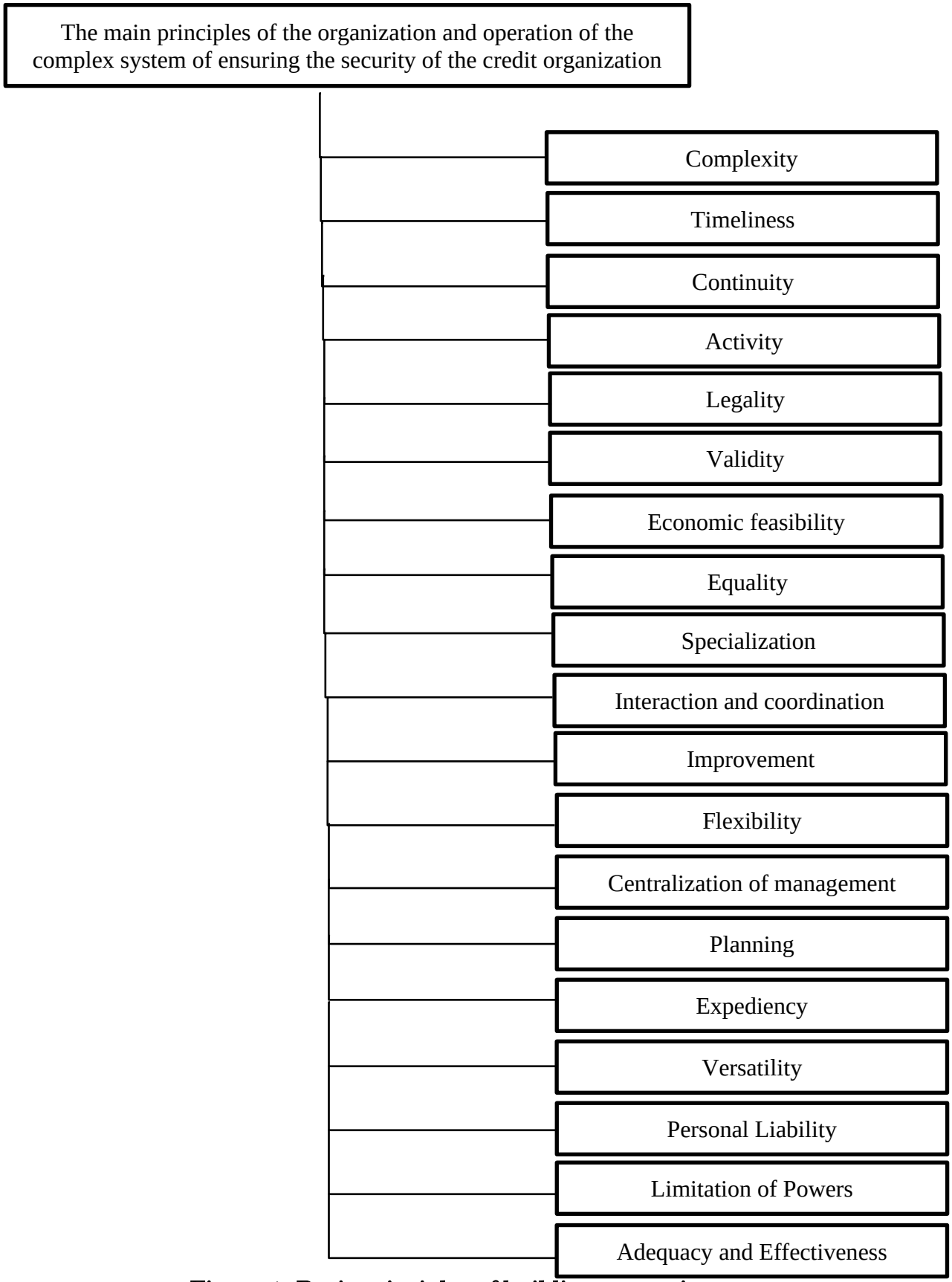

Figure 1. Basic principles of building a security system

6. Validity

The implemented measures and means of protection must be implemented at the current level of science and technology development, be justified in terms of the specified level of security and meet the specified requirements and standards.

7. Economic feasibility

Maintaining a comprehensive security system of the credit institution should be less than the amount of damage caused by any external and internal threats ("Effectiveness - cost" criterion).

8. Equality

The strongest and most effective protection measures should be taken against the most dangerous threats that can cause the greatest financial, material and moral damage to the credit organization. With a local decrease in threat, the protective power decreases accordingly.

9. Specialization

For a specific type of security activity, have practical work experience and have a state license for the right to provide services in this field, to develop and implement protection measures and tools. is appropriate. The use of technical means and the implementation of security measures should be carried out by professionally trained specialists of the credit organization's security department, its functional and service departments.

10. Interaction and coordination

To ensure the security of the credit organization are clear cooperation of all interested departments and services, third-party specialized organizations in these areas, coordination of their efforts to achieve the set goals, as well as coordination of activities with state management bodies and the law. should be implemented on the basis of integration with the protection authorities.

This principle aims to create a comfortable internal and external security environment. The first is achieved through the trust relationship between the employees of the security department and the employees of the credit organization. At the same time, it is necessary to ensure that the staff understand the need to help the security unit . The bank security system should not be perceived by employees as a means of monitoring them. It is much more difficult for attackers to act in an environment of trust.

A favorable external environment is achieved by establishing cooperation with interested organizations and individuals.

11. Improvement

The complex system of ensuring the security of the credit organization must be constantly improved based on the experience of its use, changes in economic intelligence methods and tools, regulatory and technical requirements, the emergence of new technical protection tools, taking into account the domestic and foreign experience gained.

12. Flexibility

The credit organization's comprehensive security system must be flexible , that is, it allows to develop this system without fundamentally destroying technical protection complexes and to introduce new modes of their operation.

13. Centralization of management

Centralized management of the credit organization's comprehensive security system should be in accordance with uniform organizational, functional and methodological principles.

14. Planning

To ensure the security of the credit organization should be implemented on a planned basis by developing detailed action plans to ensure the security of all necessary components of the bank structure.

15. Expediency

Only specific objects of protection are protected in the credit organization.

16. Versatility

To ensure the security of the credit organization should block the paths of all external and internal threats, regardless of the possible location.

17. Personal Liability

Each employee of the credit organization is personally responsible for fulfilling the security requirements within the limits of their authority and relevant instructions. In this case, a comprehensive security system should be built so that the range of persons who can become offenders with any violation of it is clearly known or minimized. This facilitates the investigation of an emergency situation, encourages the conscientious performance of official duties, and prevents potential attackers from unauthorized actions.

18. Limitation of Powers

This principle applies to the employees of the credit organization and the means of information protection and processing. This includes the access problem.

The probability of disclosure of a bank secret should be proportional to the number of persons who are aware of it. No one should be exposed to confidential information unless required to perform their job duties .

The second component of this principle is the need to prohibit physical access to especially vulnerable areas of persons who are not required to stay there due to the type of activity.

The third component defines the minimization of the functional responsibilities of employees and any means through which customer actions are performed. For example, a computer must have minimum software (software) that ensures the functional activity of an employee in data processing . Otherwise, there are additional opportunities for unauthorized actions.

19. Adequacy and Effectiveness

The financial, material, informational and other resources of the credit organization requires the efforts of highly qualified specialists and depends on many factors. The scope of the adopted security measures must correspond to the existing threats, otherwise the protection system will be economically ineffective .

Excessive security measures should not be abused. This will tire and annoy the employees of the credit organization, which can undermine the idea of the need to maintain security at the required level and, as a result, make the work of the security department ineffective. In addition, extreme measures hide the object of protection and even provoke aggressive actions. It is important to identify, analyze and forecast possible threats to the banking institution as part of the development of the concept and the creation of a complex system of ensuring the security of the credit organization, taking into account objectively existing external and internal conditions that affect the security situation. plays Its results should be used to justify, select and implement protective measures that threaten the security of the credit institution .

REFERENCES

1. P. K. Paul and P. S. Aithal. “Database security: An overview and analysis of current trend”. International Journal in Management and Social Science, vol. 4, no. 2, pp. 53-58, 2019.
2. Sadikov Sh.M. “Analysis of existing vulnerabilities in information reception, processing and transmission systems in a distributed database” In volume 21, of. Eurasian Journal of Engineering and Technology(EJET) Belgium, August, 2023, ISSN(E): 2795-7640
3. Bozarov Farhod “Bank faoliyati avtomatlashtirilgan axborot tizimlari va texnalogiyalari” 2021
4. 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
5. Ross Anderson “Security Engineering: A Guide to Building Dependable Distributed Systems” 2012.