THE MECHANISM BASED ON AN IMPROVED RISK MODEL OF USE RESTRICTION

Kobiljanov Sh. N.
Independent researcher at Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract:
This in the article commerce banks information in systems use restriction in the process risks assessment and to manage aimed at improved dynamic risk model offer is being used . use management models main their weaknesses static to the character ownership , risks between dependency enough at the level into account not being able to and extreme situations assessment of opportunity limitedness analysis This is done . problems eliminate to grow risk probability for the purpose and damage level to time related change , inter-risk correlation , optimal allocation of resources , tail risk (VaR) and CVaR) analysis and of the system again recovery level into account recipient complex approach working is issued . Offer commercial model banks information in systems use restriction mechanism dynamic in case organization information safety increase and from resources effective use opportunity gives .

Keywords : information security , commerce banks , use limitation , risk model , dynamic risk, VaR , CVaR , extreme risks.

In recent years, the activities of commercial banks have been deeply integrated into digital technologies, and banking information systems have become the main infrastructure for managing financial transactions, processing customer data and making strategic decisions. The concentration of large amounts of confidential and sensitive information in these systems makes them an attractive target for cybercriminals. As a result, the issues of restricting access to information systems and effective risk management remain the most important components of a bank's information security policy.

Traditional access control models often use rigid rules and a static permission system. This approach defines the relationship between users and resources at a given point in time, but does not adequately account for the changing risks over time, the emergence of new threats, and the dynamic updating of the system state in the real environment. Especially in commercial banks, the simultaneous occurrence of different types of risks, their interdependence, and their complex effects make security management even more complex.

Therefore, it is important to organize the process of restricting access in modern banking information systems not only on the basis of strict rules, but also through a risk-based approach. In a risk-based approach, a user's access to the system is determined not only by his

role or level, but also by the current risk situation, the probability of the threat and the level of possible damage. This allows making the access restriction mechanism more flexible and effective.

This article develops a dynamic and comprehensive risk model to improve the process of restricting access to information systems of commercial banks. This model is aimed at analyzing risks over time, taking into account interdependencies between risks, optimally distributing resources, and strengthening protection mechanisms for extreme situations.

Problems of restricting access in information systems of commercial banks

Information systems of commercial banks have a complex hierarchical structure, which includes different levels of users, information resources and services. The authority of each user in the system must be clearly defined, since incorrect or excessive permissions can pose a serious threat to information security.

The following problems are observed in the current use restriction mechanisms:

static risk assessment;

failure to take into account the interrelationships between risk types;

lack of a mechanism for optimal allocation of resources in conditions of limited resources;

insufficient analysis of rare but highly damaging extreme events;

the complexity of assessing the level of system recovery after security incidents.

These problems create the need to improve the process of limiting access in commercial banks to meet modern requirements.

Conceptual foundations of the improved dynamic risk model

The proposed improved risk model involves organizing the process of restricting access based on an integrated approach. The main idea of the model is not to simply assess risks once, but to monitor and manage them dynamically.

The model is based on the following key principles:

Dynamics - the probability of risk and the level of damage change over time.

Complexity - risks are analyzed not in isolation, but in interrelationships.

Flexibility — decisions to restrict use are updated in line with the current risk situation.

Optimization - increases the efficiency of resource use.

Stability - preparedness for extreme situations and emergencies will be strengthened.

Stages of an improved risk model

Time-dependent analysis of risks

In the improved model, the risk probability and the level of damage are considered as a function of time. This approach allows us to take into account the dynamic nature of threats to banking information systems. For example, the level of damage may change over time as the probability of cyberattacks increases or as new technologies are introduced.

Taking into account risk interdependence

The emergence of one risk in banking information systems can increase other risks. For example, human factor errors lead to the activation of technical risks. Therefore, the improved model uses inter-risk correlation coefficients to more accurately assess the overall risk level.

Optimal resource allocation

The resources allocated to ensure information security are not always unlimited. The proposed model provides for the distribution of resources allocated to security measures in accordance with the level of risk. This will help to effectively use the financial and technical capabilities of the bank.

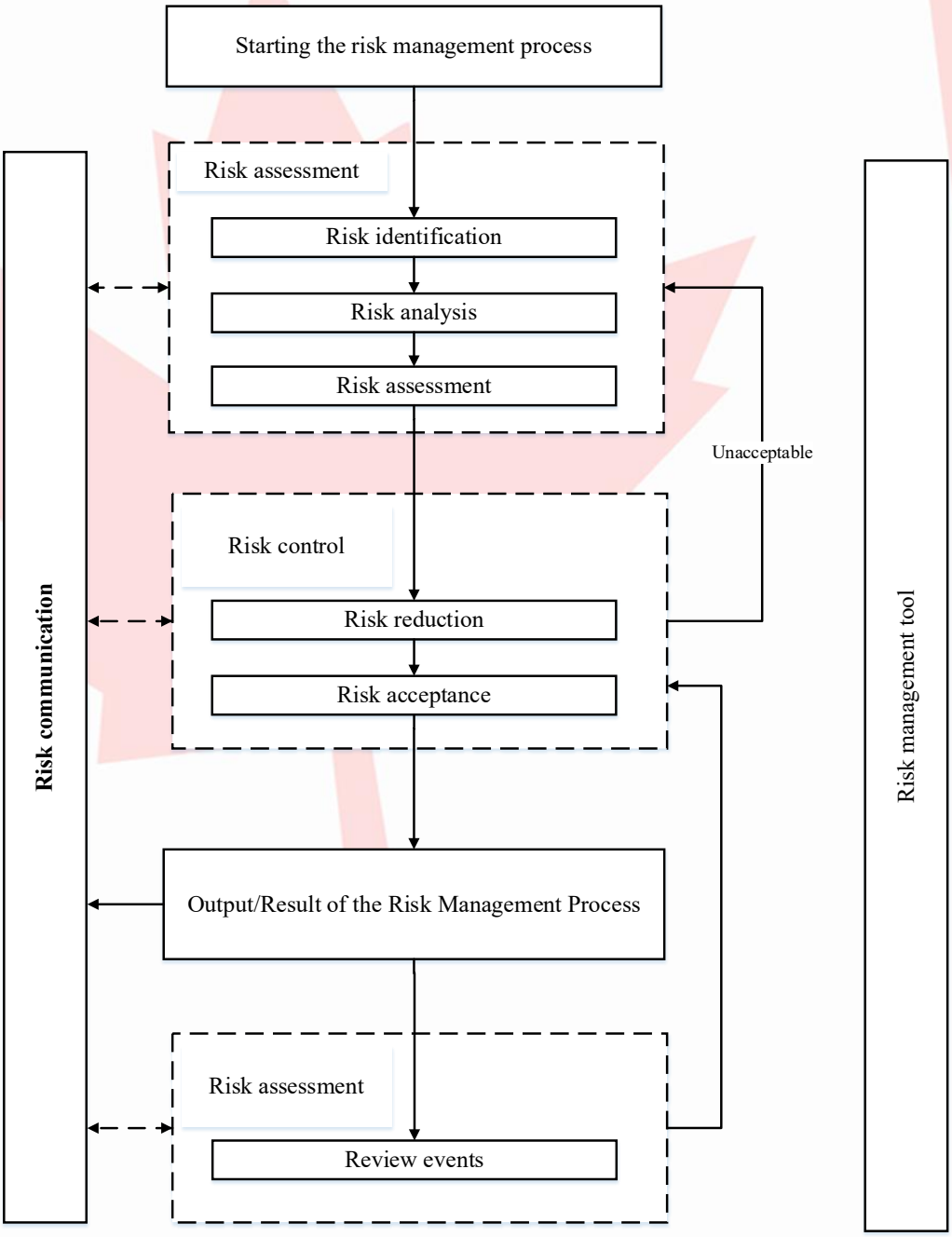

Figure 1. Example structure of a usage restriction mechanism based on Extreme risk analysis

Rare but very damaging events are the most dangerous for banking information systems. The model uses VaR and CVaR methods to assess such events. These methods determine the probability of extreme risks and the amount of potential damage.

Assessing efficiency and recovery rate

Once risk management measures are implemented, it is important to assess their effectiveness. The proposed model analyzes the level of risk reduction, resource utilization efficiency, and system resilience through separate indicators.

Figure 1 depicts the general structure of the mechanism for restricting access to the information system of commercial banks, based on an improved risk model. In this mechanism, the user, information resources, risk assessment module, decision-making unit, and monitoring system work in an interconnected manner.

As shown in the figure, the request from the user is first analyzed in the risk assessment module. This module passes information to the decision-making block, taking into account the current risk level, user profile and the level of importance of the resource. As a result, a dynamic decision is formed to allow or deny access.

Advantages of the improved model

The proposed model has a number of advantages over current usage restriction methods:

the ability to assess risks in real time;

anticipate and prepare for extreme situations;

rational use of resources;

increase the level of information security;

ensuring the stability of banking information systems.

In conclusion, the use of an improved dynamic risk model in the process of restricting access to information systems of commercial banks is an effective tool for ensuring information security. This model allows for a comprehensive and dynamic analysis of risks, optimization of resources, and strengthening of protection mechanisms for extreme situations. As a result, the reliability and stability of bank information systems are significantly increased.

References

1 Behl A., Behl K. Cybersecurity and cyberwar: What everyone needs to know. - Oxford: Oxford University Press, 2020. - 312 p.

2ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. - Geneva: International Organization for Standardization, 2022. - 68 p.

3 NIST SP 800-30 Rev.1. Guide for conducting risk assessments. – Gaithersburg: National Institute of Standards and Technology, 2022. – 95 p.

4Aven T., Zio E. Globalization and risk analysis: How risk analysis needs to be enhanced to be useful in a globalized world // Reliability Engineering & System Safety. - 2020. - Vol. 191. – P. 106–113.
5 Böhme R., Laube S., Riek M. Improving cyber risk management: A value-at-risk based approach // Journal of Cybersecurity. - 2021. - Vol. 7, No. 1. – P. 1–15.
6Hubbard DW, Seiersen R. How to measure anything in cybersecurity risk. – Hoboken: John Wiley & Sons, 2022. – 432 p.
7Kshetri N., Voas J. Cybersecurity economics: A comprehensive overview // IEEE Computer. - 2021. - Vol. 54, No. 8. – P. 6–10.
8Shameli-Sandy A., Aghababaei-Barzegar R., Cheriet M. Taxonomy of information security risk assessment // Computers & Security. - 2021. - Vol. 109. – P. 102–119.