IMPROVED DYNAMIC RISK MODEL TO RESTRICT USE IN INFORMATION SYSTEMS OF COMMERCIAL BANKS

Kobiljonov 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 management for improved dynamic risk model offer The current risk models statics , types of risk between dependency enough at the level into account not being able to and extreme tail risk assessment of opportunity limitedness This is determined by shortcomings eliminate to grow for the purpose to time associated risk probability and damage level into account recipient functions , inter-risk correlation coefficients , optimal allocation of resources mechanism , VaR and CVaR to the methods based extreme risk analysis and risk again recovery level assessment stages working is issued . Offer commercial model banks information in systems risks dynamic observation , effective management and use restriction mechanisms optimization opportunity gives . From the model use information safety increase, resources reasonable use and emergency to the circumstances preparation to strengthen service does .

Keywords: information security, commerce banks, use limitation, risk model, dynamic risk, VaR, CVaR, tail risk, resources optimization.

In the digital economy, information systems of commercial banks have a highly complex and multi-component structure, which ensure the processing of financial transactions, customer data and strategic information in a centralized environment. The stability and reliability of such systems directly depend on the level of information security, and one of the pressing issues is the effective organization of access restriction mechanisms. In particular, the rapid development of cyber threats, the emergence of new attack vectors and risks associated with the human factor increase the need for a comprehensive and dynamic assessment of risks in banking information systems.

Many risk models used in practice are static in nature, limited to assessing the probability of risk and the level of damage at a given point in time. This approach cannot fully reflect the changes in risks over time in real environments, the interaction between risk types, and the likelihood of extreme events. As a result, decisions to restrict access may be insufficiently justified or lead to inefficient use of system resources[1].

Therefore, improving the process of restricting access to information systems of commercial banks through a risk-based approach is of significant scientific and practical importance. An improved risk model should take into account not only individual risks, but also their interdependence, time-dependent changes, and rare but highly damaging events. In this case, the optimal allocation of risk mitigation measures in conditions of limited resources is also an important task.

This article proposes a six-step approach to improve the existing risk model of access restriction. This approach includes taking into account the dynamic nature of risk, identifying correlations between risks, optimizing resources, performing tail risk analysis based on VaR and CVaR methods, assessing the effectiveness of risk management, and determining the level of system recovery. The proposed model allows ensuring security, stability, and efficiency simultaneously in the process of access restriction in information systems of commercial banks[2].

To eliminate the shortcomings of the risk model of access management in the information system and increase the effectiveness of the protection system, it is necessary to introduce one or two parameters into the model and optimize the existing calculations based on the characteristics of the information systems of commercial banks. After that, the improved model can be used in the process of restricting access in the information system of commercial banks. The proposed model should be more dynamic and complex than the current one and should be able to analyze various risks simultaneously. The improved risk model of restricting access in the information system is based on the risk model of access management and is implemented in the following manner [3, 4].

First stage. The variability of risk is taken into account. It is clear that the risk and level of damage change over time. For example, the probability or level of damage of a cyberattack on the information system of commercial banks may change depending on new technologies and types of risk. This requires the addition of time-dependent functions:

$$R(t) = \sum_{i=1}^{n} (P_i(t) * Z_i(t)) \quad 1$$

Here:

$P_i(t)$- the time-dependent probability of risk.

$Z_i(t)$-the time-dependent damage level of the risk.

Second stage. The relationship between risk types is taken into account. Each risk is not analyzed in isolation, but rather is studied in relation to other risks. For example, errors by employees of commercial banks can increase cyber risk. To take this into account, it is

necessary to take into account the correlation between risk types. To calculate this relationship, the cross-risk coefficient can be used:

$$R_{general} = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}(P_i(t) * Z_i(t)) * (P_j(t) * Z_j(t)) \quad 2$$

Here:

p_{ij}- icorrelation coefficient between risk and .j

$P_i(t)$ and $Z_i(t)$– ithe time-dependent probability of the risk.

$P_j(t)$ and $Z_j(t)$– j- the time-dependent damage level of the risk.

Third stage . Implement optimal resource allocation. Optimal resource allocation is necessary for the measures used to reduce risk (for example, Firewall, network monitoring, etc.). In addition, it is necessary to take into account the limitations of resources. For this, a resource allocation model is used or the optimal resource allocation can be calculated using the Lagrangian method [5] :

$$\max_{R_{reduced}} \sum_{i=1}^{n} (P_i(t) * Z_i(t)) \text{ (subject to resource constraints)} \quad 3$$

This takes into account the need for the maximum amount of resources and how they should be distributed.

The key stage in improving the model is the fourth stage. This stage is absent in the current model, and it is by introducing this stage that it will be possible to eliminate some of the shortcomings of the current model mentioned above and to limit its use.

Step Four . A “Tail Risk” analysis of the risk is performed. “Tail risk” refers to events that are very rare but have a significant impact (for example, extreme cases of cyberattacks). For this type of risk, VaRthe (Value at Risk) and CVaR(Conditional Value at Risk) methods can be used. VaRcalculates the maximum loss of the risk over a certain period of time:

$$VaR_{\alpha} = \text{quantity}(R_{distribution}, \alpha) \quad 4$$

Here α, it represents the probability level of the risk in the range of 95 percent to 99 percent. CVaRis used to assess how high the damage can be and VaRclearly shows the average damage value for risk situations above . Accordingly, restrictions are imposed on the use of information system users of commercial banks in the information system or the use of resources in the information system.

Step Five. An assessment of the effectiveness of risk management is carried out. To assess the effectiveness of risk management strategies, efficiency and profitability ratios $R_k$can be calculated. Here, the effectiveness of the risk management process is calculated using the following formula.

$$S_{efficiency} = \frac{R_{managed}}{R_{final}} \quad 5$$

Here:

$R_{managed}$- managed (reduced) risk level.

R_{final}- final risk level.

The profitability ratio takes into account the resources spent to reduce risk:

$$R_k = \frac{R_{reduced}}{\text{Resources spent}} \quad 6$$

Based on this, the efficiency and profitability coefficient are determined and the sixth stage is implemented. In the sixth stage, the main attention is paid to the issue of restoring data lost in the system as a result of the risk. The level of recovery of lost data allows us to calculate the level of recovery of the risk.

Sixth stage. The risk recovery rate is calculated. In addition to risk analysis and management, the system recovery rate is also very important. For this, it is necessary to calculate the recovery time and probability of recovery of lost data in the information systems of commercial banks.

$$R_{restoration} = P_{restoration} * T_{restoration} * \alpha \quad 6$$

Here αis the coefficient indicating the efficiency of recovery.

Summarizing all the calculations above, the final risk in the improved risk model for restricting access to the information system of commercial banks is expressed in the following form[6].

$$R_{final} = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}(P_i(t) * Z_i(t)) * (P_j(t) * Z_j(t)) + \sum_{i=1}^{n}\left(P_i(t) * Z_i(t)\right) +$$

$$+ \sum_{i=1}^{n}(P_{reduced} + Z_{reduced}) + VaR_\alpha + CVaR + R_k \quad 3.17$$

The improved risk model in the process of restricting access to the information system of commercial banks allows for dynamic monitoring, analysis and management of risks in the information system of commercial banks, and allows for optimization of resources in the information system, increased efficiency, and assessment of risks in the process of restricting access to the information system, i.e., a protection mechanism for extreme situations.

References

1 Behl, A., & Behl, K. (2020). Cyberwar and information warfare. Oxford University Press.
2 Hubbard, D. W., & Seiersen, R. (2021). How to Measure Anything in Cybersecurity Risk. Wiley.
3 NIST. (2020). Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev.2).
4 ISO/IEC 27005:2022. Information security risk management.
5 Aven, T. (2021). Risk assessment and risk management: Review of recent advances. Reliability Engineering & System Safety.
6 McNeil, A. J., Frey, R., & Embrechts, P. (2022). Quantitative Risk Management: Concepts, Techniques and Tools. Princeton University Press.