MATHEMATICAL MODEL OF USE RESTRICTION

Irgasheva D. Ya.
Director of the Network center for retraining and Professional Development of Pedagogic Personnel at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, DSc, Professor

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

Abstract:
This article considers the issues of mathematical modeling of the process of restricting access in information systems of commercial banks. In the study, users of banking information systems, system resources, roles and access rights are identified as the main parameters, and the relationship between them is described through formal mathematical expressions. An approach to using an access rights matrix to express users' rights to use resources is proposed. Also, a mechanism for managing user rights is developed based on the role-based access control (RBAC) model. The thesis highlights the general structure of algorithms for granting access rights and checking access restrictions in information systems of commercial banks, and justifies their importance in ensuring information security. The proposed mathematical models and algorithms serve to prevent unauthorized access in banking information systems, strictly control user rights, and increase the overall security level of the system.

Keywords: commercial banking information system, access restriction, access control, mathematical model, user, resource, role, access rights, RBAC model, information security.

Access restriction systems in the information system of commercial banks serve to provide access and management rights to information and system resources of employees, customers, system administrators and other system users of the organization, who are considered system users. Usually, the mathematical hardware of the systems used to solve such a task is the same, and according to the architecture of the system and functional components, the access rights of users to a particular resource in the systems are organized based on the user's role, task or other parameters. The mathematical model of access restriction is used to accurately represent these processes, optimize access control in the information system and ensure information security [1].

The mathematical model of usage limitation is based on four main parameters, which are:

- information system users (F);
- resources in the information system (R);
- roles in the information system (R′);
- access rights (K).

Users (F) − are individuals who log in to the system in order to use the information and resources available in the information system of commercial banks, and all of these users are system users with a unique ID number and personal identifier and authenticator information. $F = \{f_1, f_2, \ldots f_i\}$Expressed as a set of all users in the information systems of commercial banks, f_i −it indicates the user who has the right to access the information system .i −

Resources (R)- is information that can be used by users of the information system of commercial banks. Examples of this type of information include resources such as bank accounts, credit history of customers, or transaction times. $R = \{r_1, r_2, \ldots r_j\}$It is the main resource of the information system j −, expressed as a set of resources in the information system of commercial banks r_j −[2] .

Roles (R′) are different roles of users in the process of restricting access to the information system of commercial banks. Each role allows access to a specific resource in the information system of commercial banks or the use of a resource. Examples of roles in the information system of commercial banks include roles such as bank employee, customer or system administrator. The total number of roles in the information system of commercial banks $R' = \{r'_1, r'_2, \ldots r'_k\}$is expressed in the form of a set of roles.

Access rights (authorizations) (K)- access rights (authorizations) in the process of restricting access in the information system of commercial banks represent the authority (ability) of a user or role to access a specific resource in the system. Set of access rights $K = \{k_1, k_2, \ldots k_l\}$in the information system of commercial banks Each access right $k_l$allows a user to use a specific resource (e.g., read, write, or delete)[3].

Based on these parameters, the mathematical model used in the process of restricting access to the information system of commercial banks uses a matrix to represent the access or use rights of system users to resources in the system. This matrix Krepresents the access rights$F \times R$ can be formulated as a two-dimensional matrix of dimensions . Where k_{ij} - i −chi j −represents the user's access (or permission) to resource chi, the matrix looks like this:

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1j} \\ k_{21} & k_{22} & \dots & k_{2j} \\ \dots & \dots & \dots & \dots \\ k_{i1} & k_{i2} & \dots & k_{ij} \end{bmatrix} \quad 1$$

$k_{ij} = 1$ –in which case $f_i$the user $r_j$is considered to have the right to access (use) the resource.

$k_{ij} = 0$ –in which case $f_i$the user $r_j$is considered not to have the right to access (use) the resource.

This matrix represents the authority (access) of users to use resources in the system in the process of managing access in the information system of commercial banks, that is, it is an expression indicating which resources in the system a user is allowed to use or not. In the information system of commercial banks, there are such types of users who are not bank employees, but bank customers, who need to use the system and use the services offered by the bank. In such cases, access control using role-based methods of restricting access is much more effective. In this case, permission to use resources in the system is not carried out by checking the use of resources separately for each client connected to the system, but a role is assigned to the user depending on his status when permission to use the system is obtained. For example, one of the roles, such as client or admin, is assigned. Depending on the roles assigned to the user, it is determined which resources in the information system of commercial banks are allowed to use. Therefore, in order to implement the above calculations based on roles and apply them in the process of restricting access, it is necessary to perform the following calculations. As a result, in the information system of commercial banks, by applying a role-based access control system, user access rights to resources are controlled through roles. Each user is assigned a specific role, and resources and rights corresponding to each role are determined [4] .

In the mathematical model of this process, the access rights of roles to resources are expressed as follows:

R_f — user f_i- a set of resources;

R_r —r'_k a set of resources that belong to a role.

If a user f_i 's role $r'_k$is based on , their access rights $K(f_i)$are calculated as follows:

$$K(f_i) = \bigcup_{r'_k \in R_{f_i}} K(r'_k) \quad 2$$

Here, R_{f_i}user f_i represents one or more roles of $K(r'_k)$- and - represents the access rights (authorizations) to all resources in that role.

There are two main types of algorithms based on a mathematical model of the process of restricting access to an information system based on these calculations, which are as follows:

- Algorithm for granting access rights to the information system of commercial banks;

- Algorithm for checking access restrictions to the information system of commercial banks [5] .

The implementation of these two algorithms in the information system of commercial banks, in turn, allows for full control over all users in the system and not granting unauthorized powers to users in the system, as well as constant control over the roles and powers assigned to roles belonging to all users in the system. The algorithm for granting access rights to the information system of commercial banks, in turn, protects users from incorrect granting of access rights when logging in to the system, and the second algorithm, which works as a separate module for each user who successfully logs in to the system, directs the access restrictions to the information system of commercial banks to the algorithm for checking access restrictions. This, in turn, serves to increase the reliability of the protection mechanism.

References

1 Stallings W., Cryptography and Network Security: Principles and Practice. – Pearson Education, 2020.
2 Bishop M. Computer Security: Art and Science. – Addison-Wesley, 2019.
3 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.
4 Ross Anderson “Security Engineering: A Guide to Building Dependable Distributed Systems” 2012.
5 O.Y. Rashidov, I.I.Alimov, I.R.Toymuhamedov, R.R.Tojiyev, “Pul, kredit va banklar” Toshkent 2011.