Journal of Siberian Federal University. Engineering & Technologies 8 (2014 7) 959-965
~ ~ ~

УДК 004.4.056.57

Access Matrix as a Passive Element in the Protection of Information Resources

Igor Z. Krasnov*
Siberian Federal University
79 Svobodny, Krasnoyarsk, 660041, Russia

Received 11.10.2014, received in revised form 03.11.2014, accepted 05.12.2014

In this work the author considers a problem of management of access to information resources of the enterprises. Formulates the purposes of a control system of access. Defines interrelation of the purposes of information security and available threats of safety. Suggests to use an access matrix as a passive element of protection of information resources. Formulates tasks which need to be solved in any control system of access. Sets a task of a redundancy exception when carrying out measures of information resources protection. Offers a formation technique of an access matrix. Describes procedure of information categorization, risk groups identification, formation of access profiles, fixing of access rights in organization regulating documents.

Keywords: access matrix, information resources, information protection.

Матрица доступа как пассивный элемент защиты информационных ресурсов

И.З. Краснов
Сибирский федеральный университет
Россия, 660041, Красноярск, пр. Свободный, 79

В данной статье автор рассматривает проблему управления доступом к информационным ресурсам предприятий. Формулирует цели системы управления доступом. Определяет взаимосвязь целей защиты информации и имеющихся угроз безопасности. Предлагает использовать матрицу доступа как пассивный элемент защиты информационных ресурсов. Формулирует задачи, которые необходимо решать в любой системе управления доступом. Ставит задачу исключения избыточности при проведении мер защиты информационных ресурсов. Предлагает методику формирования матрицы доступа. Описывает процедуру категорирования информации, выявление групп риска, формирование профилей доступа, закрепление прав доступа в регламентирующих документах организации.

Ключевые слова: матрица доступа, информационные ресурсы, защита информации.

* Corresponding author E-mail address: bk_24@bk.ru

Nowadays information security is determinant of organization robust performance and stability. Main information protection activity is concentrated on information resources protection from the perspective of human resource which have an access to main actives of organization.

Clear definition of term "information security" is one of the basic condition in effective information security system constructing. Information security system should include access control which based on information resources categorization and division of user access rights. Information system obviously should constructed taking into account needs of categorization and access control. This needs could be taken from analysis and "configuring" work processes. Business process in organization frequently not have optimal construction, so there are some access points where information with different privacy levels is mixed. This situation lids to vulnerability which significantly reduces the effectiveness of information security system or high costs of security.

Goal of information security includes: elimination or significant reduction of the possibility of harm to subjects which interests are at risk when object of information security is used, material damage, moral or accidental or intentional damage, ensuring confidentiality of commercial secret, personal information and saving IS financing stability [1].

Information security system construction starts at the level of defining of organization business processes.

Fig. 1 demonstrates an interrelation of information security goals and security threats in the development, implementation, modification and exploitation of IS.

The main goal of access control system is such rules definition that every subject in IS consists with well-defined information resource.

This tasks should be solved for this goal:

- Determine critical resources (consist confidential information or processing it) which is used in organization business process.
- Estimate the result situation of existing users access rights to resources with access matrix.
- Identify redundant access rights.
- Construct the result access matrix which consist of access matrix for business process level and access matrix for personal access right of every user in the organization (this matrix should be a part of information security policy).
- Create access profiles for managers, top managers and specialists of every division.
- From time to time inspect users for fair use of entrusted information resources (control results, identify and analysis a deviation, identify reasons of deviation).

For solving this tasks organization should audit access system to compatibility with security standards.

Permission matrix use provide organization to use access matrix (permissions table). There is a fragment of example access matrix (Table 1): strings is subjects identifiers which have access rights in the IS and rows – objects (information resources). Every element can include name and size of provide resource, access rights (read, wright, etc.), link to other IS which specify access rights, link to access management program.

Internal audit is taken for real state value identification of resources access system. Internal audit should include a division audit of access rights to information an program resources between organization users. This type of audit have tasks:

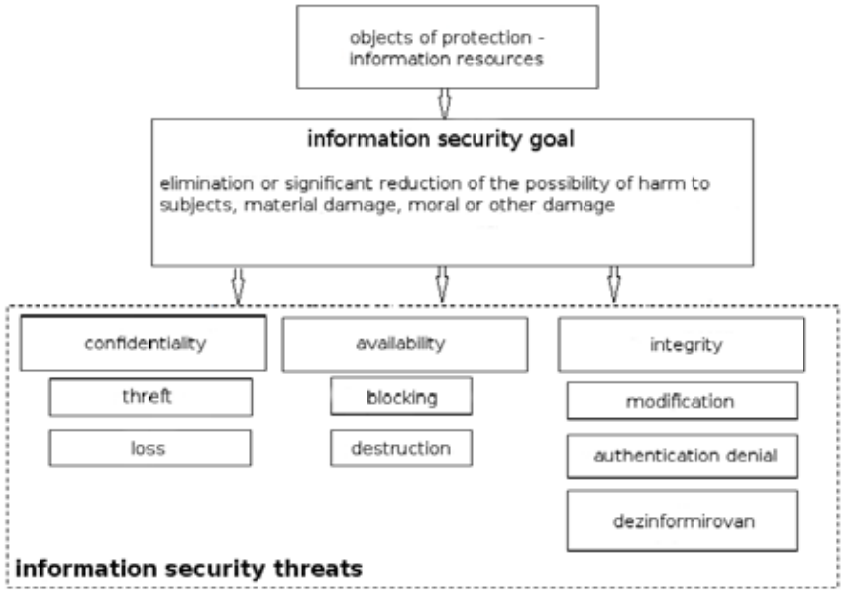

Fig. 1. An interrelation of information security goals and security threats

Table 1. Fragment of permission matrix

Subject	Dir d:\Heap	Program prty	Printer
User 1	cdrw	e	w
User 2	r		w from 9:00 to 17:00

c – create, d – delete, r – read, w – write, e – execute.

- compatibility evaluation of access rights division system with modern information security standards;
- risk analysis of threats possibility to IS outsources;
- development of information secure organizational-administrative documents in inspection borders;
- setting tasks to IT-staff for provide information security in inspection borders;
- taking part in teaching staff to use and service IS in terms of information security;
- result compatibility evaluation of access rights division system with chosen information security standard after implementation of information security measures.

According to GOST R ISO/IEC 27001 [2, 3], first of all organization should determine the approach to risk assessment. Author is considering only qualitative approach to risk assessment in this article because numerical damage from threat implementation and probability of implementation (numerical approach) should be evaluated by a special commission.

On the first step organization should identify and evaluate risks. It means:

- to identify assets and owners of this assets;
- to identify risks of this assets;

Table 2. Possible risks

Assets threat	Impact of threat implementation	Possible damage	Processing option
Using rights of the authorized user	Loose of information confidentiality and integrity	high	avoid the risk
Unauthorized reading, copying information	Loose of information confidentiality by direct reception of confidential information	high	Avoid the risk
Plugging in the removable media	Confidential information leak, computer viruses and scumware infection	high	avoid the risk
Disinformation	Loose of database and information resources integrity and availability	high	reduce the risk
Unauthorized modification of the access rights	Loose of information confidentiality and integrity by modification of access rights to read/write	high	reduce the risk
IS management interception	Loose of information confidentiality and integrity and availability by deletion, modification of system resources	high	reduce the risk

- to identity an impact of threat implementation in case of information confidentiality, integrity or availability loss;
- evaluate risks;
- to determine if risk is acceptable or requires processing.

If it is necessary to division access rights between structural divisions or users their functionality should be identified at the first step. Using interviews with top-management like a base organization should make a table with to columns:

- Division/post
- Functionality

Investigation resources description

Categorization (classification) of information should be made for purposes of division access rights to it. The main goal of categorization is to ensure that information security is on the appropriate level. Access categories (confidential levels are demonstrated in Table 3) and their protection measures should consider collective use of information or limiting access to it, demage to organiztion if information unauthorized accessed or broken.

Information owner is responsible for categorization access to his part of it for example to document, to data file or volume and he is responsible for periodically check this category.

Information assets describing make sure thy have effective protection and it can be useful for the labour protection, insurance or financial matters (asset management). So organization should identify their assets in view of their relative value and importance. Uses this information it is possible to ensure the desired protection levels which corresponding with value and importance of assets. Every asset should be clearly identified and classified in terms of information security, their owners should be clearly defined. Standard R R ISO/IEC 27002:2005 (“Information technologies. Security methods. Practical rules of information security management”) defines the following types of assets:

- information assets;

Table 3. Protected information categories in the organization

№	Category	Abbreviation	Definition
1	Confidential information	CI	Information which have value to the organization. Access to this information is restricted lawfully and based on local normative acts of the organization. Confidential information could consist: personal data, official secrecy, secrecy, utility model or industrial design.
2	Information for internal use	IIU	All internal information which circulates in the organization network, loss of this information have no serious consequences. This information could not be confidential by low but access to it should be limited.
3	Public information	PI	Information which could not be confidential by low and information for public access.

- software assets;
- physical assets;
- services (human capital).

Inventory consist of valued assets list definition. This process usually is performed by the assets owners. The term "owner" define persons and parts which have responsibilities for management, development, maintenance, use and protection of assets. This responsibilities should be approved by a top-management.

For the example of access matrix compilation research with an Active Directory was made. Access groups to directories (with access rights), programs, Internet and e-mail was created. Every user in this groups have their own rights in his division.

There can be only two access levels: reading – only right to view resource contents without rights to change or delete, modification – rights to change and delete the resource.

It is important to understand that in every division there are users with different access rights. So this matrix should be a three-dimensional object where the third dimension is consist of division users rights.

The intersection of a row and a column shows if anyone in this department has an access right to this resource:

" " – no access

"p" – only read access

"m" – modification

There is two risk groups when access matrix is compiled:

- Users groups who shared resource for common goals.
- Wide access rights to resources of one or two users – this situation should be considered one more time.

The logical inconsistency of divisions functionality and resource assignment should be identified. Access rights redundancy should be identified because it rises up the probability of leakage through the fault of employees.

The result matrices should be compiled with the heads of divisions because they are owners of the resources and know which employee needs to have access rights.

Table 4. Access profile

Resouce	Rights (read/modification)
Chief accountant	
G:\out_buh\Common	m
G:\out_buh\Audit	m
G:\Sap	r
G:\Katalog\dogovora	m
1C Accounting “Outsource-Accounting”	-
External E-mail	-
General Director deputy	
G:\IT\Audit	m
G:\out_buh\Common	m
G:\KT\Buh	m
G:\Sap	r

Redundancy rights consist differences between the initial and final matrices and they are unnecessary in IS. Redundancy rights rises up the leakage probability of confidential information. Access profile gives minimal access rights for every appointment which is necessary for employee duties. You can look at access profile in table 4.

Access profiles pros:

- excludes unreasonable requests to access rights “just in case”;
- increases an efficiency of consideration of access rights applications from informatization divisions;
- simplifies a procedure of approval access rights with information security division;
- optimizes an procedure of assigning new user access rights. So the probability of employees downtime while rights are assigning and financial damage reduced.

Requirements for ensuring control of logical access should be documented according to GOST R ISO/IEC 27002:2005. The main goal of this measures is not only regulate users actions but establish a responsibility for a rule violations.

After approving of access division rights by information security policy and establishing a responsibility activity regulations in accordance with the access matrix should be embedded.

Conclusion

A developed method of access control was embedded in a number of real objects of region informatization. This allowed to reduce the information security risks.

References

[1] *Andrianov V.V., Marshmallows S.L., Golovanov V.B. etc.* Providing business information security. M.: Alpina Publisher, 2011.

[2] *Baldin K.V.* Risk management. M.: Penguin Books, 2006.

[3] *Astakhov A.M.* The art of managing information risk. M.: DMK Press, 2010.

[4] *Repin V.* Business Processes. Modeling, implementation, management. M.: Mann, Ivanov and Ferber, 2013.