УДК 004.492.2

Improvement of distributional model of resource usage in terms of informational security

Godla A., advisor Gubenko N.
Donetsk national technical university
anastasiia.godla@mail.ru

Abstract

Godla A., Gubenko N. "Improvement of distributional model of resource usage in terms of informational security" *The main purpose of the paper is the improvement of the model of the distribution and use of resources, allocated to information security. A comparative analysis of information security and risk assessment systems in conditions of small business was held and the model of shared access to resources was proposed.*

Keywords: Information security, risk analysis, threats, losses, risk management, risk assessment

Introduction

Nowadays, ensuring of the necessary level of information is a serious problem in the area of informational security. It requires organizational activities and the usage of specific tools and methods for its solution. At present companies become increasingly dependent on information systems and services, and therefore more vulnerable to security threats. By this reason it is very important to provide stable object functioning, preventing threats to its security, theft of funds, distortion, diversion, and destruction of company's information [1].

One of the principal elements of the scientific and methodological basis of protection is the model of informational security processes. The grounds for its construction are environment of the models and common aims of informational security. The main problem that could occur in the creation of the model of protection system is the estimation of the needed allocated resources for the required level of protection [2].

As the basis for this paper a model of allocation and use resources for the protection of information offered by G.G. Grezdov was chosen. Due to reliable mathematical foundation this model gives an opportunity to develop an effective security system.

Model of distribution and use of resources allocated to informational security

The process of data protection is the process of interaction of threats that affect the information, and information security, which prevent their collision [3].

The distributional model of using resources is based on the capabilities of the enemy and the defending side. The threat model and the estimates of losses model are also used. Due to the basis of economic feasibility, the costs on protection must not exceed the estimated damage from security violation.

Analysis of the selecting model of information security

Distributed attack is an enemy's action or related actions sequence of the enemy, which use the vulnerability of the defense. In order to prevent this, method should consider the question of counter information security system to distributed attacks.

There should be a choice in the model between different options of building integrated system of information protection. The problem is to work out such a system that could be changed in terms of the existing situation.

This model should consider the fact that the losses related to decreased productivity caused by the use of information security depend on the distribution of information security. Thus, funds that could be allocated by the defenders for data protection should also depend on the distribution of information security and can be obtained after a special calculation.

The chosen model and selected principles do not provide a common approach of forming information security of state or military and commercial secrets. This approach is only relevant to the problems of small business.

Analysis and risk assessment. Risk management

Information security – is the protection of information and supporting infrastructure from accidental and intentional action of natural or artificial character, which can result in damage to

the owners and users of information, and supporting infrastructure in general.

In the information security the analysis of information risks of the company and management of information risks are very important. Today we have a common approach to ensure regime of information security that is used in many countries.

According to Petrenko S.A., regardless of the size of the company and its specific information systems, the efforts for providing of information security regime generally consist of the following stages:

- the definition of information security policy;
- setting boundaries, which are intended to support the regime of information security;
- risk assessment;
- selection of countermeasures and risk management;
- selection of controls and management to ensure regime of information security;
- certification of information security management systems for compliance with safety standards.

A set of minimum requirements for information security regime form the basic level of information security and usually it is enough for the standard projects. For such level of defense it is possible to use a number of standards and specifications, which have a minimum of the most likely threats, such as viruses, unauthorized access etc. To neutralize threats countermeasures must be taken. The choice depends on the likelihood of their realization and sensitivity of the resources.

Sometimes the baseline requirements for information security regime are not enough. Threats and vulnerabilities could lead to the devastating consequences and it is important to make additional high requirements. In this case it is vital to determine the value of the used resources, to identify the vulnerability of resources, to calculate the probability of threats, to evaluate the potential damage from the attacks and to estimate the economic losses. Besides this the higher level of security should also provide the higher standards of confidentiality too.

It could be concluded that there are some common stages in the creation of the method of the informational security for the common use and the higher level of security. In the second variant some special steps should be added and the accuracy level should be increased.

Nowadays in many small businesses risk management is not so popular among their other priorities. According to the Stephen Townsend a survey that was taken place at America's Small Business Summit in May 2010 shows that business owners distribute their strategies for the importance in the following order [5, 6]:

- marketing and sales;
- managing cash flow;
- attracting financing;
- attracting and retaining employees;
- identifying and managing insurable risks;
- compliance with federal and state regulations;
- protecting against litigation and lawsuits.

No wonder that priorities connected with earning money are on the top of the list. Small companies are interested on staying in business and they don't want to spend their money on extra personnel that would work with the information security. IT security countermeasures are not ideal yet and that is why small business should prepare to manage risk rather than try to eliminate it.

In the conditions of small business an idea of development security policies could be solved with the help of special informational security programs. Usage of these programs could influence effectively on the saving of those money which earlier businessman spent earlier on elimination of the consequences of attacks on informational property [7].

These programs provide:

- model of the information system in terms of information security;
- tools for compiling the list of threats and assessment of their probability;
- techniques to assess the value of resources;
- choice of countermeasures and the analysis of their effectiveness;
- analysis options for constructing protection, the creation of reports [8].

There should be a strategy for risk management of different classes. Such approaches are possible:

- reducing risks: many risks can be reduced through the use of simple and cheap countermeasures;
- risk aversion: certain classes of the risk can be avoided with the help of the imposition of a Web server of organization outside of the local network;
- the changing of nature of risk: if it is impossible to evade the risk or reduce it effectively, it is better to take insurance;
- risk taking: the specialist should know the residual value risk as it is usually impossible to reduce it to a very small value.

As a result of taking into account the risks a control model should be established [8].

Methods for the information security risk assessment process in terms of small business

There is a great number of programs that are dealing with the security risk assessment process. Here are some of them:

- RA2 art of risk;
- vsRisk;
- RiskWatch;

- COBRA;
- РискМенеджер etc.

But in terms of using such kind of programs in small companies best results with less money expenses could be achieved with the OCTAVE-S and CRAMM.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation SM) is a number of tools, techniques, and methods for risk-based information security strategic assessment and planning.

These methods are founded on the OCTAVE criteria. OCTAVE-S was developed due to the needs of small companies with a staff no more than 100 people. OCTAVE-S based on the same criteria but it is based on the special approaches of small organizations.

This method has some notifications that are vital to consider before using it:

- for the analysis of the information security of the small business this method requires a team of specialists who already worked in the current field and has real knowledge about different spheres of its actions;
- OCTAVE-S has narrow specialization and works only in certain areas because it is considered that small business constantly inspect the field and there is no ability to study and interpret the results of vulnerability tools [9].

CRAMM-CCTA Risk Analysis & Management Method – a method of analysis and risk management. There are several versions of the method focused on requirements of the Ministry of Defense, civilian government agencies, financial institutions, private sector organizations.

The method is implemented in specialized software, customized to different areas with the help of "profiles".

Current version CRAMM 5 corresponds to BS 7799 (ISO 17799).

CRAMM risk analysis consist of the identification and calculation of risk-based assessments, assigned resources, vulnerabilities, threats and resources.

CRAMM risk control is the identification and selection of countermeasures in order to decrease the risks to acceptable levels.

Risk analysis significantly reduces the complexity of the implementation of all phases of the method. Use of applications is appropriate during internal and external audit of information security. The use of software requires highly skilled analyst, quite a long period of training and experience in the application [10].

Improvement of the model of distribution and use of resources allocated to informational security

Thus, the analysis shows that for the developing of the effective, integrated information security system the following changes should be made:

- identify the resistance of the protection system to the distributed attack. During the formation of a threat model it is important to pre-build the model of distributed attacks;
- determine the vulnerability of the object of protection. The risk assessment of information system security of each precious resource is determined not only by the analysis of threats, acting on a specific resource, but with the help of vulnerabilities through which these threats can be realized. This could be done by the conducting of audit of the information system. It is necessary to form a model of vulnerability while building the model of distributed attack.

It is also important to mention that the usage of resources in Resource distribution model could be based on E-NET models for distribution, access and use of resources by security levels and groups (ENLG) by Nikolai Todorov Stoianov, Veselin Tsenov Tselkov [11].

The principle of interaction in the model is that any group consists of users and resources with the maximum access level. Any user can interact only with that resources which level is lower or equal to the user's level. Moreover, resources must belong to the same group.

According to this model the functional possibilities for user are:

- request for access (Ident);
- analysis of user rights (CheckAuthorities);
- identification of security level (IdentLevel);
- receiving list of groups (ListGroups);
- selecting group (SelectGroup);
- receiving list of resources (ListResources);
- selecting resource (SelectResource);
- using resource (UseResource);
- saving log file (LogFile);
- exit from the system (Quit).

Therefore, it becomes possible to reduce the risk of unauthorized usage of computer resources because of the verification of users' access to the right resources.

On the figure 1 the sequence diagram is presented. In the table 1 the main stages and steps of ENLG model are shown that are giving clear explanation of the discussed here method.

Годла А.С., Губенко Н.Є.
Донецький національний технічний університет

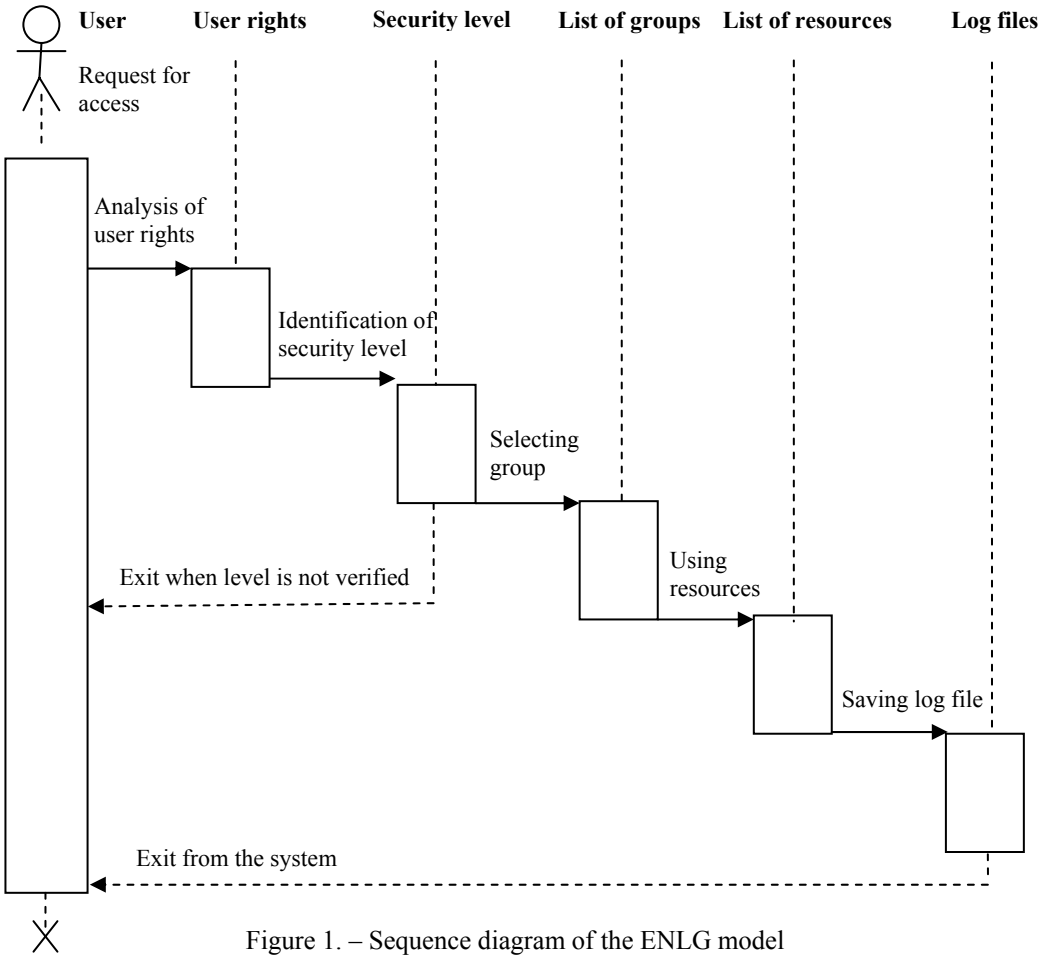

Figure 1. – Sequence diagram of the ENLG model

Table 1. – Chart of ENLG model

Stage / Steps	request for access	analysis of user rights	identification of security level	receiving list of groups	selecting group	receiving list of resources	selecting resource	using resource	saving log file	exit from the system
Step 1	X									
Step 2		X								
Step 3			X							
Step 4										X
Step 5				X						
Step 6					X					
Step 7						X				
Step 8							X			
Step 9								X		
Step10									X	
Step11										X

Conclusions

Models of information security processes are the main elements of the scientific and methodological basis of protection. The basis for their construction is common aims of information security and the environment in which the protection is running.

Nowadays in many small companies, risk management is given little attention but in the nearest future it is expected to be raised due to the money savings.

In condition of small business an idea of development security policies could be solved with the help of special security risks programs such as CRAMM and Octave-S.

In order to understand the infrastructure it is vital to make a risk assessment, analysis of risk situations or full audit of the company.

The proposed changes can improve the model and reduce the probability of the threat to confidentiality, integrity and availability of data. In other words, it becomes possible to reduce the risk of unauthorized usage of computer resources.

References

1. Цымбалова А.А., Губенко Н.Е. Анализ модели использования ресурсов с точки зрения информационной безопасности. Информационные управляющие системы и компьютерный мониторинг – 2011 [Текст] / Материалы II Всеукраинской научно–технической конференции студентов, аспирантов и молодых учёных. – Донецк: ДонНТУ – 2011. – С. 292 – 295.
2. Корнеев Д.В. Обобщенная модель системы защиты ресурсов распределения вычислительной сети [Электронный ресурс] http://admin.smolensk.ru/virtual/expo/html/tesis.htm (14.05.12).
3. Гроздов Г.Г. Модифицированный способ решения задачи нормирования эффективной комплексной системы защиты информации автоматизированной системы [Текст] / Г.Г. Гроздов; монография. – К.: ДУІКТ, 2009. – 32 с.
4. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность [Текст] / Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.
5. Managing Risk: It's Not Just for Big Business, Stephen Townsend, IS 8930 Information Security Administration, Summer 2010,7/14/2010 [Electronic resource]: http://stephendtownsend.com/wordpress/wp-content/uploads/2010/12/Stephen_Townsend_ResearchPaper2.pdf (25.04.12).
6. Business Wire. 2010. Risk Management a Low Priority for Small Business Owners, Travelers Survey Finds. Market Watch. [Electronic resource]: http://www.marketwatch.com/story/risk-management-a-low-priority-for-small-business-owners-travelers-survey-finds-2010-06-08 (14.05.12).
7. Issues in Informing Science and Information Technology Volume 5, 2008. Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises: A Research Agenda. [Electronic resource]: http://www.informingscience.us/icarus/journals/iisit/publications (30.05.12).
8. JetInfo, информационный бюллетень, вып. 1(68)/1999; [Текст]/М.: Джет Инфо Паблишер
9. Software Engineering Institute Carnegie Mellon [Electronic resource]: http://www.cert.org/octave/octaves.html (30.05.12).
10. IT Expert [Electronic resource]: http://www.itexpert.ru/rus/ITEMS/77-33/index.php (10.05.12).
11. Nikolai Todorov Stoianov, Veselin Tsenov Tselkov; E-net models for distribution, access and use of resources in security information systems [Electronic resource]: http://arxiv.org/abs/1011.3148 (25.04.12).

Годла А.С., Губенко Н.Є.
Донецький національний технічний університет