ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse48942020.pdf
https://doi.org/10.30534/ijatcse/2020/48942020

Models and Methods of Corporate Information Protection System

Karimov Madjit[1], Ganiyev Abdulkhalil[2], Sayfullaev Sherzod[3]
[1]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan, dr.mmkarimov@rambler.ru
[2]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan, ganiyev_ab@mail.ru
[3]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan, sherzodsay@gmail.com

ABSTRACT
This article examines the models and methods of protection of information security systems, in particular, the model of building a corporate information security system, the model of security analysis in the absence of intrusive threats in information systems and the three-tier model of information security systems. As a result of the analysis of corporate information protection systems, models and recommendations for improving the efficiency of the information protection system are proposed.

Key words: Information security system, three-tier model, security analysis model, information security standards, protection.

1. INTRODUCTION

The main goal of any information security system is to ensure the sustainable functioning of an object: to prevent threats to its security, to protect the legitimate interests of the information owner from unlawful encroachments, including criminal acts in the considered sphere of relations provided for by the Criminal Code of the Republic of Uzbekistan, to ensure normal production activities of all divisions object. Another task comes down to improving the quality of services provided and guarantees of security of property rights and interests of clients.

2. MODELS

This requires:

– classify information as limited access (official secret);

– predict and timely identify security threats to information resources, causes and conditions that contribute to the infliction of financial, material and moral damage, disruption of its normal functioning and development;

– create conditions for functioning with the least probability of implementation of security threats to information resources and causing various types of damage;

– create a mechanism and conditions for a prompt response to threats to information security and manifestations of negative trends in functioning, effective suppression of encroachments on resources based on legal, organizational and technical measures and means of ensuring security;

– create conditions for the maximum possible compensation and localization of damage caused by unlawful actions of individuals and legal entities, and thereby weaken the possible negative impact of the consequences of a breach of information security.

When performing work, you can use the following model for building a corporate information security system (Figure 1), based on the adaptation of the General Criteria (ISO 15408) and risk analysis (ISO 17799). This model complies with special regulatory documents on ensuring information security adopted in the Republic of Uzbekistan, the international standard ISO/IEC 15408 "Information technology - security methods - criteria for assessing information security", the ISO/IEC 17799 standard "Information security management" and takes into account the development trends of domestic regulatory framework on information security.

The presented model of information security is a combination of objective external and internal factors and their influence on the state of information security at the facility and on the safety of material or information resources.

The following objective factors are considered:

– information security threats characterized by the likelihood of occurrence and the likelihood of implementation;

– vulnerabilities of an information system or a system of countermeasures (information security systems) that affect the likelihood of a threat;

– risk is a factor reflecting the possible damage to an organization as a result of the implementation of a threat to information security: information leakage and its misuse (the risk ultimately reflects probable financial losses - direct or indirect).

To build a balanced information security system, it is planned to initially conduct a risk analysis in the field of information security. Then determine the optimal level of risk for the organization based on the specified criteria. The information security system (countermeasures) must be built in such a way as to achieve a given level of risk.

The proposed methodology for conducting analytical work allows you to fully analyze and document the requirements related to ensuring information security, avoid costs for unnecessary security measures that are possible with a subjective risk assessment, assist in planning and implementing protection at all stages of the life cycle of information systems, and ensure that work is carried out in a short time, provide a justification for the choice of countermeasures, evaluate the effectiveness of countermeasures, compare various options for countermeasures.

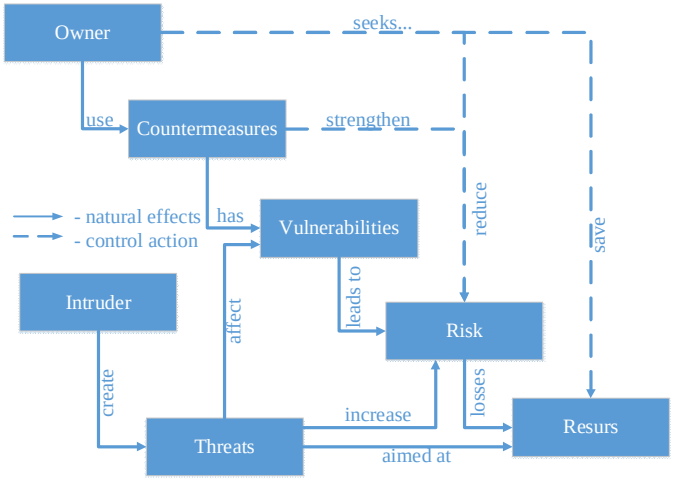

Figure 1: Model of building a corporate information security system

During the work, the boundaries of the study should be established. To do this, it is necessary to allocate the resources of the information system, for which risk assessments will be obtained in the future. In this case, it is necessary to separate the resources under consideration and the external elements with which interaction is carried out. Resources can be computer hardware, software, data, as well as information resources - individual documents and separate arrays of documents, documents and arrays of documents in information systems (libraries, archives, funds, data banks, other information systems). Examples of external elements are communication networks, external services, etc.

The analysis of IS security in the absence of malicious factors is based on the model of interaction of the main IS components shown in Figure 2 [4, 11-12].

When building the model, the relationships between resources will be taken into account. For example, the failure of any equipment can lead to loss of data or failure of another critical element of the system. Such relationships determine the basis for building a model of an organization from the point of view of information security (IS).

This model, in accordance with the proposed methodology, is constructed as follows: for the allocated resources, their value is determined, both from the point of view of the possible financial losses associated with them, and from the point of view of damage to the organization's reputation, disorganization of its activities, non-material damage from disclosure of confidential information etc. Then the relationship of resources is described, security threats are identified and the probabilities of their implementation are estimated.

On the basis of the constructed model, it is possible to reasonably choose a system of countermeasures that reduce risks to acceptable levels and have the highest cost efficiency. Part of the system of countermeasures will be recommendations for conducting regular reviews of the effectiveness of the protection system.

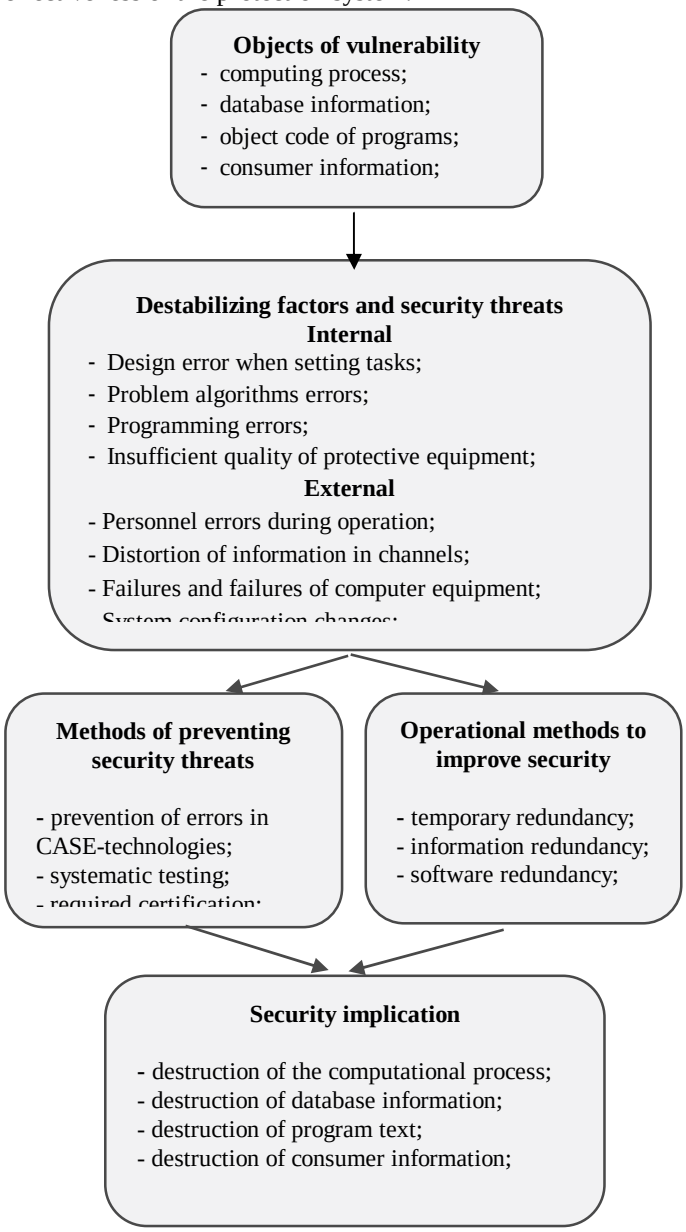

Figure 2: Model for analyzing the security of information systems in the absence of malicious threats

Ensuring increased requirements for information security involves appropriate measures at all stages of the life cycle of information technology. These activities are planned after the completion of the risk analysis stage and the selection of countermeasures. An obligatory part of these plans is the periodic verification of the compliance of the existing IS regime with the security policy, certification of the information system (technology) for compliance with the requirements of a certain security standard.

A schematic of the three-edge model of the ISS for N = 3 is shown in Figure 3.

Upon completion of the work, it will be possible to determine the measure of security assurance of the information environment, based on the assessment with which the information environment of the object can be trusted. This approach assumes that a large guarantee follows from the use of great effort in the safety assessment.

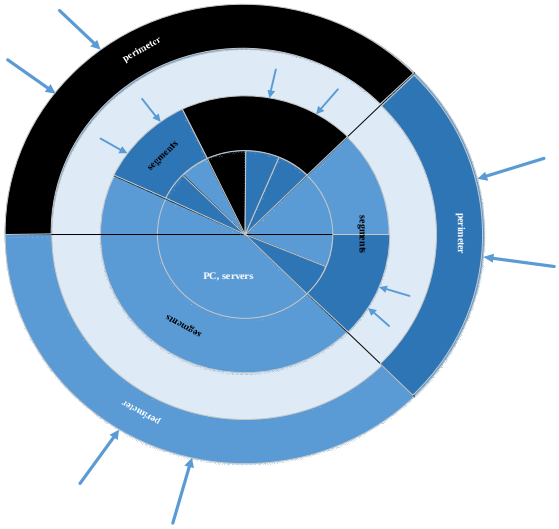

Figure 3: Three-line model of the ISS (arrows indicate external and internal threats)

The adequacy of the assessment is based on the involvement in the assessment process of a larger number of elements of the information environment of the object, the depth achieved through the use of more projects and descriptions of execution details in the design of the security system, rigor, which consists in the use of a larger number of search tools and methods aimed at detecting less obvious vulnerabilities or to reduce the likelihood of their presence.

To improve, develop and increase the efficiency of the information security system (ISS), it is necessary to develop and apply methodological support related to solving particular problems of system design and information security management, in particular, the development of an ISS model - obtaining a description of an organized set of software and hardware protection means, taking into account the potential sources of threats as fully as possible [2, 5-8].

Protection model is a formalized or non-formalized description of a complex of software and hardware and organizational protection measures, which is the basis for the development of an information protection system [3, 9, 10].

Based on the analysis of all possible channels of unauthorized access to the information environment of the corporate information system segment and in accordance with the above basic principles of building a security system, a three-edge model of the information security system is proposed.

The first line is the perimeter of the protected object - a set of functional subsystems, including the means and mechanisms of systemic protection against external threats of an intruder and potentially destructive influences of a remote user; the second frontier is a set of functional subsystems for protecting the network segment from potentially possible intersegment and remote attacks; the third line includes a set of functional subsystems that protect the information environment of a separate personal computer, server.

Thus, the ISS model includes three components: a perimeter protection model of a protected object, a network segment protection model, a PC and server protection model.

3. CONCLUSION

The proposed method for the formation of a rational modular structure of the information security system is based on the three-edge protection model.

Such an organized systematic ordering of information is a means of its subject organization, which ensures the process of using information about possible threats to the information environment and the necessary barriers corresponding to them, which reduces the level of uncertainty when deciding on the composition of the information security system.

The purpose of this model is to obtain information from the user about his preferences and, using certain procedures, to order the compared alternative implementations of barriers by means of a multi criteria comparative analysis of information about protection means.

REFERENCES

1. A. V. Artemov. **Information security. Course of lectures** https://tech.wikireading.ru/12985, 2019
2. I. V. Mashkina. **Information security. Management in the segment of corporate information system based on intelligent technologies** // DSc Dissertation, 2005
3. V. V. Domarev. **Security of information technologies. System approach.** - Kiev: LLC TID DS, 2004. - 992 p.
4. **Information systems and technologies in Economics and management** [electronic resource] https://www.intuit.ru/studies/courses/3627/869/lecture/31761, 2018

5. A. V. Alekseev. **Intelligent systems for making design decisions** / A. V. Alekseev, A. N. Borisov. - Riga: Zinatne, 1997.
6. A. V. Andreychikov. **Development of the intellectual system of socio-economic forecasting and decision-making in conditions of uncertainty** / A. V. Andreychikov, O. N. Andreychikova // Information technologies. - 1999. - № 2. - 14-22 p.
7. A. V. Lukatsky. **Detection of attacks.** - Saint Petersburg: BHV-Petersburg, 2003. - 608 p.
8. A. A. Malyuk. **Information security and methodological bases of information protection: textbook. manual for universities** / Malyuk A. A.-M: Hotline-Telecom, 2005. - 280 p.
9. A. A. Polovinkgm. **Automation of search design** / ed. by A. A. Polovinkin. - Moscow: Radio and communications, 1981.
10. V. Jakimets. **Investigation of the Morphological Space of Systems Variants.** - P. 80-110. II ASA, Laxenburg, Austria, 1981.
11. A. A. Emelyanov, E. Y. Avksentieva, S. Y. Avksentiev, N. N. Zhukov. **Applying Neurointerface for Provision of Information Security**, *IJATCSE*, Volume 8 No. 6, pp. 3277 – 3281, 2019 https://doi.org/10.30534/ijatcse/2019/97862019
12. Marilou O. Espina, Arnel C. Fajardo, Bobby D. Gerardo and Ruji P. Medina. **Multiple Level Information Security Using Image Steganography and Authentication,** *IJATCSE*, Volume 8 No. 6, pp. 3297 - 3303, 2019 https://doi.org/10.30534/ijatcse/2019/100862019