Applying intelligent methods of risk analysis in information communication systems

Maria Maslova*

Information security department of Sevastopol State University, Russia

Abstract. In the modern world there is a constant growth of information and information technologies, a risk-oriented approach to managing information security of information and communication systems of companies seems increasingly promising. But apart from development, there are threats and risks that affect both the image and the financial component of companies. Therefore, one of the main tasks is to assess, analyze and prevent the risks of information security in information communication systems using modern methods in conjunction with the use of intelligent analysis methods.

1 Introduction

At this stage of development in the field of information, information systems and technologies, the process of constant development and improvement in various fields of human activity is under way. Therefore, one of the tasks in this direction is protecting these systems to ensure their effective functioning through certain methods of threat identification and information risks. Information and communication systems are among the most sensitive to reliable and safe operation of information systems. Information security (IS) is definitely an integral part of the modern society. Therefore, the companies of the information and communication industry should be well equipped with a wide range of means of providing IS, which should be automated, it should increase controllability and at the same have disaster recovery. And only then the company will operate in a stable, continuous mode of operation of all processes. But because of the constant increase in the level of information security risks, old methods for determining risks in IT systems companies use now are no longer able to cope, as they are modified over time, and there is a need to constant improvement of search and protection methods.

2 Research objects and experimental methods

The subject of the study was methods for assessing risks in information and communication systems:

1) Existing methods;
2) Method of intelligent data analysis.

* Corresponding author: mashechka-81@mail.ru

3 Methods of risk identification and analysis in information and communication systems

For companies, the main task is to obtain optimal technologies of assessment, risk analysis with maximum efficiency, so it is necessary to choose and apply the best methods of protection, analysis and determination of risks in information communication systems. The integration of telecommunications and information technologies into a single industry - information communications - is a global trend oriented towards the development of the telecommunications network and the expansion of the number of global information services based on it.

The most complex modern information structures, focused on large companies, are information communication systems using a large number of computers, client-server architecture, server specialization, etc. At the same time, databases consist of their large volumes of data [1].

The security requirements for infocommunication systems are established by methodically identifying security risks, with which decisions are already made and tools are used to reduce risks. Currently, software systems are used to identify, analyze and control information security risks, for example, RiskWatch, CRAMM, SISSI, RISAN, COBRA, MINIRISK, OCTAVE, FRAP, Microsoft, GRIF, AvanGard [2]. These methods mainly collect primary data on user actions, conduct their automated analysis (taking into account the security policy) and perform the necessary actions, such as: restricting user rights, informing administrators, etc. [3].

These methods have some drawbacks:

– they are intended mainly for large companies;

– highly qualified auditors are needed to work with them;

– the high cost of a license (from $ 2,000 to $ 10,000) per user;

– based mainly on the qualitative and quantitative method, which leads to a decrease in efficiency;

– knowledge bases are formed on a subjective assessment and they must be constantly updated (very time-consuming and financially expensive);

– constant modification of attacks (it is necessary to constantly improve and complicate the means of defense);

– the presence of delayed counteraction.

To identify dependencies in large volumes of data, it is necessary to apply intelligent data analysis. It can also reveal hidden, non-obvious and existing relationships, explore complex processes and detect fragments with homogeneous properties and create promising information protection systems. At the same time, intelligent data analysis is not used as an independent solution - it is used in combination with traditional algorithms due to the imperfection of modern intelligent methods which find hidden patterns, classify objects, but do not reveal the reason for their choice to the operator [4, 5].

4 Conclusion

Existing methods of risk assessment and analysis were reviewed, from which it is clear that in the field of information security of information and communication systems, risk assessment is very important, because companies suffer huge financial losses due to poor quality assessment of risks associated with the implementation of IS threats. Therefore, it is necessary to go one step further, for this it is necessary to apply the existing methods of risk management risk assessment and analysis as a source of information for making decisions, together with intelligent data analysis methods, to improve them, removing existing limitations and shortcomings, while creating a self-developing system of risk analysis.

Reference

1. Kolesnikov A. V., Maslova M.A. Usovershenstvovanie vozmozhnostej komp'yuternogo parka kafedr fakul'teta informacionnyh tekhnologij VUZa za schet ispol'zovaniya terminal'noj arhitektury i tekhnologii «tonkij klient// Perspektivy razvitiya informacionnyh tekhnologij: sbornik materialov HXIII Mezhdunarodnoj nauchno-prakticheskoj konferencii / Pod obshch.red. S.S. CHernova.– Novosibirsk: S. 126 – 132, Sekciya 8, (2015)
2. nCircle Vulnerability Scoring System. [Elektronnyj resurs]/Rezhim dostupa: https://habr.com/ru/company/pt/blog/266485/
3. Pugin, V.V., Gubareva, O.YU. Obzor metodik analiza riskov informacionnoj bezopasnosti informacionnoj sistemy predpriyatiya. T-comm Seriya: Telekommunikacii i transport. M: №6, (2012)
4. Gubareva Ol'ga YUr'evna Ocenka riskov informacionnoj bezopasnosti v telekommunikacionnyh setyah // Vestnik VUiT, №2 (21), (2013)
5. Dyuk V. A., Samojlenko A. P. DataMining: uchebnyj kurs // SPb.: Piter, 53s, (2001)