DOI: https://doi.org/10.5281/zenodo.12542140

UDC: 334.025

MODELING RISK ASSESSMENT BY THE METHOD OF HIERARCHY ANALYSIS WHEN USING CLOUD IT SERVICES TECHNOLOGY

Shirinov Laziz Toxirovich

Tashkent university of information technologies named after Muhammad al-Khwarizmi, PhD student

E-mail: shirinovlaziz05@gmail.com

Annotation. *The article discusses the modeling of risk assessment using hierarchical analysis methods when using cloud IT services technology, in particular the Functional model for assessing the risks of using cloud IT services and technology technology for assessing the risks of using cloud technologies.*

Keywords: *cloud technologies, risk assessment, hierarchy analysis method, methods, models, assessment, risks, services, cloud computing.*

МОДЕЛИРОВАНИЕ ОЦЕНКИ РИСКОВ МЕТОДОМ ИЕРАРХИЧЕСКОГО АНАЛИЗА ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ОБЛАЧНЫХ ИТ-СЕРВИСОВ

Аннотация. *В статье рассматривается моделирование оценки рисков с использованием методов иерархического анализа при использовании технологии облачных ИТ-сервисов, в частности функциональная модель оценки рисков использования облачных ИТ-сервисов и технологическая технология оценки рисков использования облачных технологий*

Ключевые слова: *облачные технологии, оценка рисков, метод иерархического анализа, методы, модели, оценка, риски, сервисы, облачные вычисления.*

BULUTLI IT-SERVISLAR TEXNOLOGIYASIDAN FOYDALANISHDA IERARXIYA TAHLILI USULI BILAN RISKLARNI BAHOLASHNI MODELLASHTIRISH

Annotatsiya. *Maqolada bulutli IT-servislari texnologiyasidan foydalanishda ierarxik tahlil usullaridan foydalangan holda risklarni baholashni modellashtirish, xususan, bulutli IT-servislaridan foydalanish riskini baholashning funksional modeli va bulutli texnologiyalardan foydalanish riskni baholashning texnologiyasi ko‘rib chiqildi.*

Kalit so‘zlar: *bulutli texnologiyalar, risklarni baholash, ierarxik tahlil usuli, usullar, modellar, baholash, risklar, servislar, bulutli hisoblash.*

Introduction

At the moment, there are several methods for assessing risks from the introduction of information technologies and software products created on their basis. These include: risk model Octave, Cramm, Risk Watch. In the case of a private cloud, these models can be used to manage risk with a number of adjustments. However, if a private cloud is owned by an organization and physically exists within its jurisdiction, then it is possible to abstract from the idea of the cloud and consider that the company does not use it. When using a private cloud, the organization’s employees can be considered a client, and the organization itself a service provider [3]. They can also serve as the basis for creating a new model that can satisfy the emerging need. It is important to note that none of the existing models for assessing information technology risks is completely suitable for the case of cloud computing, because None of them take into account the specific interaction model inherent in cloud environments. This specificity lies in the possibility of remote access to the services provided. In this regard, it becomes necessary to consider the following possible risks:

- the adverse consequences of poor data management;
- unjustified maintenance costs;

- financial or legal problems of the supplier;
- operational problems or supplier downtime;
- problems of data recovery and confidentiality;
- general security problems;
- attacks on the system from outside.

Modeling risk assessment methods

The author proposes the following additive model for assessing the risks of using cloud IT services based on factor analysis. Before proceeding with the calculation of the risk assessment model, the following several steps must be completed [1].

Step 1. Segmentation of data based on its importance. NASA's Jet Propulsion Lab recently began its own cloud computing research. Research was carried out in the field of navigation among data with different levels of access and security. Their team mapped their cloud research into a chart, plotting different data sets according to security requirements for each slice. Then the JPL team began working with information in accordance with the diagram - from public data to secret ones.

Step 2. Determine how much information needs to be protected through outsourcing. If we initially determine what part of the data we want to leave on storage resources and what part of it will go to the cloud system, the process of organizing data safety will be organized much better than others. Of course, in this case, part of the responsibility for the level of data security falls on the employees who directly work with these resources.

If the company has an advanced security team, great; if not, it's easy to outsource this task. This is money that will truly be well spent. It would be optimal to combine these two methods and include third-party audit and code revision in this process. Cloud service providers are beginning to realize that having strong security is a good way to differentiate themselves from other providers, since most of them do not think about actually protecting the information hosted on their services from unauthorized access. To resolve such situations, it is necessary to establish dialogue and

understanding between the cloud service provider and the company department that is responsible for risk management.

Step 3: Shortlist cloud providers to evaluate. It is worth evaluating suppliers based on an overall view of their capabilities, with the caveat that the deeper the risk management department attempts to understand the infrastructure of the supplier being reviewed, the greater the responsibility it may assume to the organization. And at the same time, if the cloud supplier cannot provide a level of scaling commensurate with the company's needs, information security problems will arise regardless of the supplier's initial promises.

Step 4. Write a detailed description of the provider. Here are four main criteria that characterize suppliers:

1) safety: confidence that the supplier and subcontractors will comply with all applicable laws;

2) compensation: how the supplier and its subcontractors will compensate the company for damage in the event of information leaks;

3) Liability: It is the supplier's responsibility to notify the company of information leaks and to cover the costs of foreseeable leaks, in accordance with relevant laws, including possible third party claims arising from the leak;

4) audit: suppliers whose services are considered the most exposed to risks are required to conduct and pay for third-party audits.

Through this process, service providers that pose too many risks can be identified.

Step 5. Agreeing on the contract and special conditions. The language of the standard contract and service level agreements should be specific when describing your security requirements. It makes sense to learn to stick to your line in negotiations with suppliers when it comes to the right to ownership of information, to the point that if the relationship with a supplier is broken, the company gets all its data back, even if this data needs to be delivered on disks.

Step 6: Monitor the performance of the supplier's risk management program and observe the results of audits of the firms supporting it. A number of firms have created a process dedicated to ongoing supplier assessment. They (firms) should also contract with third party auditors to use their services whenever required.

Step 7. Launch the prototype with data images. Security goes hand in hand with availability and reliability. Security features such as scanning can themselves be a performance hit - you need to ensure that all security systems are in place and working during tests. The system must survive poor performance at any time when some process can cause it to crash or freeze. It is necessary to be able to recover the system from these errors. But leaving them can cause problems in the security system.

While the risk of hacking is always present, the real risk when outsourcing any function—whether it's a cloud service or not—is understanding the level of control that has been lost and what the consequences might be.

Step 8: Perform penetration testing. At this final stage, the organization uses its internal experts or information consultants to hack the system using publicly available tools. These consultants can also be helpful in resolving system vulnerabilities they find [2].

In Figure 1 shows the designed functional SADT model using BPwin. This model represents a risk assessment system in the form of a simple component - one block and arcs that depict interfaces with functions outside the system.

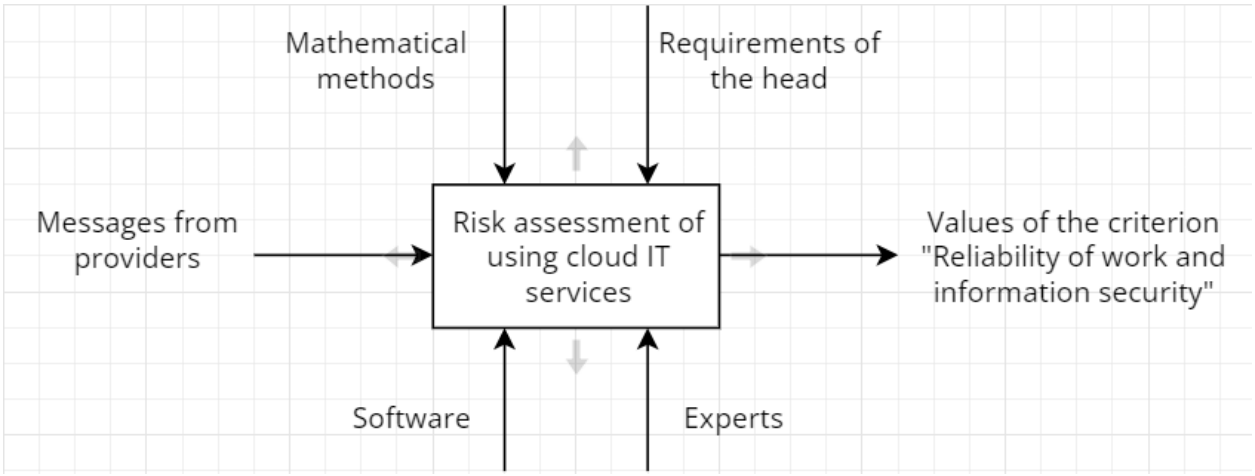

Fig. 1. Functional model for assessing the risks of using cloud IT services

Recently, there has been a widespread belief that modern cloud technologies can significantly reduce costs, and today many companies are increasingly moving their enterprise systems and business applications to the cloud. This is evidenced by the results of the second annual Cisco Cloud Watch study [5].

From the point of view of the use of information technology, the cloud is understood as a network of computers that ensures the operation of certain software and provides the user with the opportunity to work with these software products for a fee.

From a security point of view, cloud technologies have such positive qualities as fault tolerance and safety of data placed in a virtual environment. However, we should not forget that the cloud is not a panacea for all problems, so we must be realistic and always take precautions and protection measures to avoid unpleasant cases that occur in the cloud in the same way as on the ground.

Having studied the experience of using cloud technologies to organize the work of an enterprise, we can identify different types of risks [4]:

- legal;
- operating rooms;
- informational;
- technical.

Each group of identified risks can include its own factors. For example, the group of technical risks includes the level of reflection of all types of liability in concluded contracts and financial guarantees, bankruptcy or takeover of the provider, control of the provider, the extent to which the provider uses laws and regulations applicable to the field of cloud computing. Operational risks include restrictions on the use of software configurations and its updating in accordance with industry changes, the possibility of losing the uniqueness of business processes of a particular organization when using the same data processing algorithms implemented in the accounting program. The main factors of information risks are the security and confidentiality of data processed in the program, the possibility of the developer refusing to further

develop the program, the possibility of becoming dependent on the cloud service provider, the reliability of resource sharing between different cloud users, access to third party data and attacks on the system from outside [6].

Risk assessment technology is a process of step-by-step identification of the most suitable cloud service provider and includes the following steps [7]:

- decomposition of the problem into a hierarchy;
- constructing a matrix of paired comparisons;
- calculating the vector of local priorities, the largest eigenvalue of pairwise comparison matrices, the consistency index and consistency relations;
- calculation of global priorities.

At the first stage, the problem is presented in a hierarchical form (figure). At the highest level is the provider that provides cloud technologies with the least risk. The second level contains the types of risks, and the third level contains cloud providers that must be assessed against the risks of the second level.

Conclusion

It should be noted that within this method there are no general rules for forming the structure of the decision-making model. This is a reflection of the real decision-making situation, since there is always a whole range of opinions for the same problem. The method allows us to take this circumstance into account by constructing an additional model to reconcile different opinions by determining their priorities. Thus, the method allows you to take into account the “human factor” when preparing a decision. This is one of the important advantages of this method over other decision-making methods.

The considered method can serve as a superstructure for other methods designed to solve poorly formalized problems, where human experience and intuition are more adequately suited than complex mathematical calculations. The method provides convenient means of accounting for expert information for solving various problems.

REFERENCES

1. 8 steps to secure cloud systems // Information Security / Information security. – 2013. – No. 1. – P. 28–29.

2. Maslov A.V., Grigorieva A.A. Mathematical modeling in economics and management: textbook - Yurga: Publishing house of the Yurga Technological Institute (branch) of Tomsk Polytechnic University, 2007. - 264 p.

3. Moskalenko A. Cloud and mobile: What can save the Russian IT market? // InLine group, 01/24/2013, [Electronic resource]. – Access mode: http://www. inlinegroup.ru/events/press-releases/5635.php (date of access: 04/08/2013).

4. Razumnikov S.V. Analysis of existing methods for assessing the effectiveness of information technologies for cloud IT services [Electronic resource] // Modern problems of science and education. – 2013 – No. 3. – P. 1. – Access mode: www.science-education. ru/109-9548.

5. Razumnikov S.V. Using the linear programming method to assess the effectiveness of using cloud IT services // Privolzhsky Scientific Bulletin. – 2013. – No. 7(23). – pp. 43–45.

6. Moiseeva, T. M. Technology for assessing the risks of using cloud technologies / T. M. Moiseeva // Economic and legal prospects of society, state and consumer cooperation: collection. scientific Art. international scientific-practical Internet conference, Gomel, March 31, 2017 / Bel. trade and economics the university will consume. co-op; under. scientific ed. Zh. Ch. Konovalova, T. S. Alekseenko. – Gomel, 2017. – pp. 216–219.

7. Malin, A. S. Research of control systems / A. S. Malin, V. I. Mukhin. – M.: Publishing house. House of State University Higher School of Economics, 2005. – 399 p.