Risk Management for Information Security of Corporate Information Systems Using Cloud Technology

A.D. Kozlov, N.L. Noga
V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences
Moscow, Russia
alkozlov@ipu.ru

***Abstract*—Risk management technique using the methods of fuzzy logic to ensure information security of corporation's information systems with cloud technologies is offered.**

Keywords—information security, cloud technologies, threat, vulnerability, damage, risk, fuzzy logic, linguistic variable, risk management, information resources control.

I. INTRODUCTION

The natural desire to improve the economic efficiency and competitiveness of the company (corporation) pushes it to use the principles of lean production. In the market conditions, the winner is the one who can produce more and at the least cost. The saturation of the market has led to a reassessment of the role of product quality and services, including information services. Any business is a set of people, business processes, resources. Lean manufacturing is aimed at improving the efficiency of business processes, which include information systems, especially corporate distributed systems.

Any process can be described within: costs; time and characteristics of the services or products that result from the process; quality of the services or products produced; risks associated with the process. If the company is not itself a provider of information services for external consumers, and is only a consumer of these services to meet their internal needs, such a thing as a quality triangle, acquires a simple form: efficiency (quality of services), the cost of services and the risks associated with the process of obtaining information services. In these simple coordinates becomes an attractive model of the information system based on the use of "cloud" technologies that can significantly reduce the cost, especially for the creation of its infrastructure [1].

In short, the cloud technology is a model of building an information system, when one or more necessary for the creation and operation of information system functions are performed (provided) by a third-party contractor, as a service (service). It is clear that the appearance of a third party corporate information system (service provider) in the system of functioning increases the risks of information security by decreasing information resources control. How to assess and minimize these risks?

Typically, the following two basic techniques are used to ensure information security in distributed enterprise information systems. The first is based on the verification of compliance of the components of the corporate information system using cloud technologies, mandatory requirements of standards and regulatory documents, as well as the verification of the security of all parts of the system against current threats (ISO/IEC 18045 and ISO/IEC 15408). The second is based on the assessment and management of information security risks. The relevance and necessity of the second method are steadily increasing due to the increasing role of information technologies in the processes of the functioning of corporations as economic entities with access to the international market. At the same time, the tasks are solved to identify the possibility of implementing threats and calculating possible damage, to identify actual threats, to reduce the permissible level of risk, etc. In a broad sense, risk assessment consists of the evaluation of threats, vulnerabilities, and damage that occurs during their implementation. The risk analysis procedure involves modeling the situation of adverse conditions, taking into account all sorts of internal and external factors (we call them to input parameters), characterizing the risk as such. A detailed description of the risk analysis procedure can be found in ISO/IEC 27002, where the following scheme is proposed during the risk analysis:

- the position of an information system in the initial state with an assessment of the size of the expected damage from violations of information security in a given period is considered;
- assessment of the impact on the reduction of risks of the proposed means and security measures with an assessment of their value.

The ideas of risk management had for the first time arisen in the 70th last century when the Clements-Hoffman model had been presented [2]. The disadvantage of this model is the lack of accounting for the cost of the implemented protection means, as well as the correspondence of this cost to the possible damage in the implementation of a specific threat. At the same time, it is not always feasible to search for all possible attacks of the offender. Moreover, there are always new ways to influence the information system.

978-1-5386-4924-4/18/$31.00 ©2018 IEEE

Therefore, if it is impossible to protect against all threats, then it is necessary to solve the problem of selection of only actual threats. The authors propose to solve the problem of filtering threats using the mechanism of attack trees. So the severity of the vulnerability is estimated using the procedure of the calculator, described below.

So, let us dwell on the methodology of information security risk assessment, based on the use of fuzzy logic and fuzzy set theory, which allows taking into account the uncertainties inherent in the information systems. The concept of fuzzy sets was proposed by L. Zadeh [3] in the late sixties of the last century. When considering the concept of a set in their work, they proposed the following assumption: the function of belonging of an element to a set can take any values in the interval [0; 1]. Such sets he called fuzzy. Various logical operations were introduced on these sets. Also, the concept of a linguistic variable, whose values are fuzzy sets, was introduced. A linguistic variable is a variable that is difficult to quantify using mathematical language. For example, such concepts as a professional information security violator and hacker-a lover of clear boundaries of their knowledge do not have, and it is not possible to describe them mathematically accurately.

II. INFORMATION SECURITY RISKS

We will divide the process of information security risk management of the Corporation into several stages;

- identification (or inventory) of the Corporation's information assets;
- determination of the list of current threats;
- definition of the list of vulnerabilities;
- risk analysis and assessment;
- processing of risks, identification of residual risks.

Identification of assets is carried out by expert evaluation of the value of assets. The value of each asset is determined by the value of the damage that can be caused to the Corporation in the event of loss of asset security properties such as privacy, integrity, availability. A linguistic variable is an introduced-the value of an asset, and an assessment of the value of each asset for each of the above security properties is carried out. It is proposed to place the data of the evaluation in tabular form (see Table I).

TABLE I. VALUATION OF ASSETS

	The level of values	**The value of an asset (in CONV. units))**	**The boundaries of the term "Value of the asset.»**
1	Negligible	0 - 5000	0-0,20
2	Low	5001 - 50000	0,21-0,40
3	Average	50001 - 300000	0,41-0,60
4	High	300001 - 1000000	0,61-0,80
5	Critically high Above	Above 1000001	0,81-1,00

To get the total value of an asset, you must select the maximum value from the values obtained for each security property. For example, the value of one asset by security properties: confidentiality - 0.4, integrity – 0.35, and availability – 0.7. Then the total valuation of the asset is max(0,4, 0,35, 0,7) = 0,7. At the next stage, to determine the list of current threats, we consider only those assets whose total value is not less than 0.5.

In the process of modeling threats to the security of information in the information system of the Corporation formed a lot of relevant threats to the system in the form of their formal description. The analysis results determine actual threats to information security:

- potential for information security violator, for example, calculated by the algorithm given in [4];
- possible vulnerabilities of the information system using vulnerability data banks, for example [5];
- various options for implementing information security threats using information security threat databases, for example [6];
- consequences (amount of damage) of threats to information security.

Thus, any threat to the security of information in the information system of the Corporation can be represented as a function:

T = T (*potential of the offender, vulnerabilities, variant of realization of the i-th threat, assets, volume of damage*).

To determine the implementation of the I-th threat, you can use the technique of attack trees [4]. Attack trees are built to visualize a variety of options for both information and technical impact on the information system and represent a graphical representation of the conditions that lead to an unwanted event, which is located on the top of the tree.

For each possible threat for a particular system, a tree of attacks is built. The top of such a tree is the implementation of a data security threat. To reach the top of the tree, the information security intruder must meet many conditions at various levels of the system, called intermediate nodes of the attack tree. The Fig.1 shows an example of the choice of the variant of implementation of the threat of changing the settings of the means of information protection in the cloud. One of the variants of realization of the threat of substitution settings will be the following path: $\{B_{2.1}, B_{1.1}, B_0\}$, where IPF – information protection facilities.

The weak point in building attack trees is scalability. If the system has an extremely complex structure, then to simplify the analysis and minimize the time of building attack trees, it is necessary to carry out the detail at the lower levels only for the actual options for the implementation of the threat for a particular system. The degree of relevance of the threat implementation option naturally depends on both the likelihood that the offender will use this way and the degree of possible damage caused by the consequences of the threat.

The level of vulnerability risk is estimated by the CVSS assessment method (Common Vulnerability Scoring System - General vulnerability assessment system). The method of

assessment is implemented by the Calculator procedure [7], where the level of risk of vulnerability is set within limits specified in Table II.

Fig. 1. An example attack tree for the threat is realization change settings of IST.

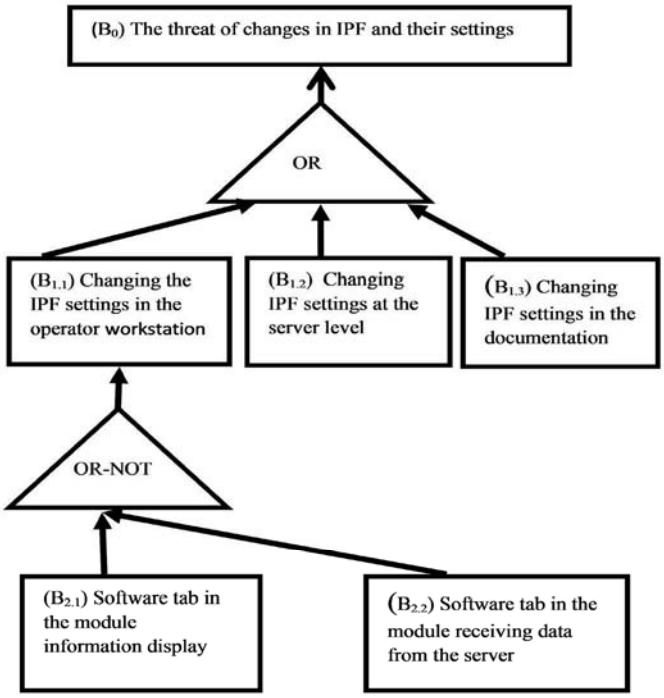

TABLE II. LEVEL OF VULNERABILITY RISK

Severity vulnerabilities, by following the CVSS calculator			
Low: [0; 3,9]	Average: [4; 6,9]	High: [7; 9,9]	Critical: 10

To assess the consequences of the threat implementation through a specific vulnerability, we will introduce a linguistic variable "Impact Assessment" (see Table III).

TABLE III. INFLUENCE ASSESSMENT

Level of influence	Influence. Description of the damage	The boundaries of the term " influence assessment.»
Minor	Minor effect. Recovery actions are not required	0-0,25
Average	An asset can be recovered fairly quickly	0,26-0,50
Serious	Asset requires a fairly serious and long-term recovery	0,51-0,75
Critical	An asset is destroyed and cannot be repaired	0,76-1,00

Let V be a variant of threat realization. Let's call it relevant if there is a probability P ($P|P \neq 0$) threat realization for the information system (for example data-center) use of option V by the offender with an appropriate assessment of the attack potential. Let the implementation of the threat can lead to damage. Then

$$V_{ij} = \{P_{ij}, \text{damage}_i\},$$

where i is the number of the considered information security threat in the information system; j is the number of the possible implementation of the considered information security threat in the system.

The probability of the i-th threat realization by the j-th variant – P_{ij}, is calculated based on the assessment of the intruder potential calculated by the algorithm given in [4], as well as the presence and level of the vulnerability risk, contributing to the threat realization by the determined way.

Let us now consider the linguistic variable "threat probability" (or "threat level") and determine the boundaries of its term, thus linking assets, vulnerabilities, and threats (see Table IV).

TABLE IV. THE PROBABILITY OF THE THREAT.

Probability level	A frequency of threat occurrence	The boundaries of the term "Probability of threat.»
Low	Missing. For new assets, the probability of threat execution is low	0-0,33
Average	Once or twice a year. For new assets, the probability of threat execution is average	0,34-0,66
High	For new assets, the probability of threat execution is high	0,67-1,00

To determine the damage (or level of damage) caused by a single threat, build Table V, the cells which indicate the level of damage or financial loss at a qualitative level. The level of damage is understood as the possible consequences for the information system of the Corporation in the event of various information security incidents and, by and large, is a multi-criteria value (financial losses, inability to perform work on the Corporation's contracts, data compromise, etc.).

The production rules corresponding to table 5 are defined, for example, as follows:

- *IF* the value of the asset is "negligible" *AND* the probability of a threat is "low", *THEN* the damage is "insignificant";
- *IF* the value of the asset is "high" *AND* the probability of a threat is "low", *THEN* the damage is "average",

etc. all other rules.

Further, by analogy, tables are built, and other linguistic variables are introduced into consideration according to other criteria of information security risks of the system.

TABLE V. ASSESSMENT OF THE DAMAGE.

The level values	Level of the probability of threats		
	Low	*Average*	*High*
Negligible	Negligible	Low	Low
Low	Low	Low	Average
Average	Low	Average	Average
High	Average	Average	High
Critical high	High	High	Critical high

In this case, a sequence of tables that link different elements in the risk analysis process is used. Thus, the level of risk can be represented as a function of *R = R(threat level, vulnerability level, damage level)* or

$$R = p(T)p(V)D, \quad (1)$$

where *p(V)* is the probability of using the vulnerability, *p(T)* is the probability of the threat realization through the given vulnerability and *D* is the value of the damage from the threat realization.

The task of identifying residual risks requires further investigation and is not considered in this report.

It should be noted that there are many different methods of information security risk analysis both at the qualitative level, for example, OCTAVE, FRAP, and in quantitative terms, for example, Risk Watch, as well as in the mixed version, for example, CRAMM or Microsoft.

III. FEATURES OF RISKS WHEN USING CLOUD TECHNOLOGIES

The methods mentioned above do not take into account the features that appear when using cloud technologies for the construction of distributed corporate information systems.

Stages of creation, operation, modernization of corporate information systems can be represented as a specific set of business processes. For example, in the operation of the information system (integrated): collection, transmission, processing, storage of information; providing access to information resources to users; administration, technical support of hardware and software, etc.

All these business processes can be performed on their own, or receive services from third-party providers. Depending on the set of services received, there are different "cloud" models.

According to the service model: Iaas-Infrastructure-as-a - Service (infrastructure as a service); PaaS-Platform-as-a - Service (platform as a service); SaaS-Software-as-a – Service (software as a service); BPaaS-Business Process-as-a-Service (business processes as a service), etc.

By the deployment model, "clouds" are divided into private and public.

As it can be seen from the short list of models - cloud technologies are one of the types of outsourcing.

At the same time, the more services the company receives from the outside, the less (lower) the degree of control over its information assets.

Almost everyone uses smartphones (communicators) in everyday life. Many have faced the problem of losing contacts for one reason or another, and when system software developers (Android, IoS) offer to store contacts in the "cloud", and then naturally they agree to this, as it increases the reliability of storing contacts, and also simplify the migration of data from one smartphone to another. However, by agreeing to the storage of contacts in the extraterritorial "cloud" users lose control over the possible use of their contacts by third parties. For example, personal data stored from Facebook in 2016.

Of the 14 principles of management formulated by Jeffrey K. Liker [8], six relate to the human factor in varying degrees. When creating and operating information systems, it is often the "human factor" that can be the key when choosing technical solutions. So when assessing risks, it is necessary to take it into account.

The company (corporation) receiving the service from a third-party supplier cannot affect the recruitment of this supplier, professionalism, training, dedication (corporation), the ability to work in a team of their employees. All influence is limited to the choice of the supplier. The more people who are not bound by specific obligations to the owner of information resources have direct or indirect access to these resources, the more difficult it is to control.

In order to ensure the possibility of assessing the risks associated with the use of cloud technologies in distributed information systems, we will introduce an indicator – the coefficient of the level of the information resources control – K_c. It can take values from 1 (processing data on a stand-alone computer by the owner of the information) to 0 (storing data in an extraterritorial anonymous "cloud").

Some values of this coefficient are given in Table VI as an example.

TABLE VI. THE RATIO OF THE LEVEL OF INFORMATION RESOURCES CONTROL

Received service from an external provider	K_c
Private cloud	
Operator services	0.95
Equipment rental	0.9
Administration	0.8
Public cloud	
Data storage services (if you have a contract with the provider)	0.9
Services data warehouse in the cloud extraterritorial	0.5
Full data center infrastructure services, including administration, subject to contract	0.75
Provision of ready-made services for business processes	0.7
Information security services	0.8

In the case of receiving several services from the coefficients of the control level, the coefficient with the minimum value is selected.

Then the level of risk from (1) taking into account the coefficient of the level of the information resources control can be represented as (2):

$$R_1 = \frac{p(T)p(V)D}{K_c}. \qquad (2)$$

Risk assessment based on fuzzy logic methods and fuzzy set theory, taking into account the uncertainties arising in any corporate information system, can be implemented using the Fuzzy Logic Toolbox package of MATLAB system [9].

It should be noted that the graphical interface of the package allows to view graphs of the risk dependence on various input parameters, for example, the threat probability.

IV. CONCLUSION

Thus, the presented approach to information security risk assessment allows:

- to assess the level of risk concerning the corporate information system located in the " cloud»;
- assess the level of risk, both generally and by various criteria (e.g., the risk of loss of access to data as a result of international sanctions for political reasons, financial risk, the risk of compliance with various regulations and legislation, etc.);
- to decide on the possibility of using specific models of deployment of corporate information systems;
- make decisions on the use of third-party providers for the creation and operation of corporate information systems, as their elements, and systems in general.

The proposed approach can be useful for medium and small businesses with a distributed branch network.

REFERENCES

[1] V.N. Lebedev, N.L. Noga, “Security and assessment of the economic feasibility of using "cloud" technologies in corporate information systems." Proceedings of the XXVI all-Russian conference "Information and information security of law enforcement." M. Academy of management of the Ministry of Internal Affairs of Russia, 2017. pp.99-104.

[2] L. Hoffman, “Modern methods of information protection” / / Trans. with English. M. Soviet radio, 1980. 264 p.

[3] L.A. Zadeh., “Fuzzy sets”. Information and Control, Vol. 8, pp. 338-353. (1965).

[4] A.D. Kozlov, V.L. Orlov, “Methods and means of information security of distributed corporate systems." M. IPU RAS, 2017. 156 p.

[5] “A database of information security threats. The list of threats." URL: http://www.bdu.fstec.ru/threat.

[6] “A database of information security threats. List of vulnerabilities." URL: http://www.bdu.fstec.ru/vul.

[7] “CVSS calculator”, version 3. URL: http://www.bdu.fstec.ru/calc, 2017.

[8] J. Liker Dao Toyota, “14 principles of management of the world's leading company”. Trans. with English. - 9th ed. M. ALPINA PUBLISHER, 2014. 400 p.

[9] S. D. Shtovba, “Design of fuzzy systems using MATLAB." M. Hotline – Telecom, 2007. 288 p.