Main Approaches to the Analysis and Estimation of Risks of Information Security

Rakhmatullaev Doston

Master of Tashkent University of Information Technologies named after Muhammad al-Khorazmiy, Uzbekistan.

When constructing the system of ensuring information security developers are faced with the problem of determining the required level of availability, integrity and confidentiality of information resources and supporting infrastructure. To search for «borders» of the information system security certain standards and regulations in the field of information security can be used, but they are not always clearly defined. Certain methods of risk management are used to identify risks, rank them by severity, likelihood of occurrence, and to develop a method for the treatment of these risks.

The article describes the purpose of systems analysis and risk assessment, discusses the necessity and the reasons for the emergence of such systems, describes and compares the main approaches to the problem of risk management and describes and compares existing software tools that utilize these approaches.

Keywords: Audit of information security; information security risk; information security threat; information protection, risk management.

Introduction

Why is it necessary to investigate risks in the field of information security (IS) and what can this give when developing an information security system for an information system (IS)?

For any project that requires financial costs for its implementation, it is highly desirable to determine at an early stage what we will consider a sign of completion and how we will evaluate the results of the project. For tasks related to ensuring information security, this is more than relevant. After all, the costs of providing a high level of security may be unjustified. In fact, the question arises: what level of protection should the system in question have? To answer this question in the process of creating an information security system, two approaches can be used.

The first one focuses on the main standards in the field of information security (for example, [1]) or some other set of requirements. Then the criterion for achieving the goal in the field of safety is the fulfillment of a given set of requirements. The efficiency criterion is the minimum total cost of fulfilling the set functional requirements. However, the required level of security in these documents is not always strictly defined, so it is quite difficult to determine the effective level of IS security.

The second approach is related to risk assessment and management. Initially, it came from the principle of «reasonable sufficiency» applied to the field of information security. This principle is described by a set of statements:

- it is impossible to create an absolutely insurmountable defense;
- it is necessary to maintain a balance between the costs of protection and the resulting effect;
- the cost of means of protection should not exceed the cost of protected information;

• the offender's costs for unauthorized access to information must exceed the effect that he will receive by exercising such access.

An information security risk is a potential opportunity to incur losses due to a breach in the security of an information system (IS).

The risk analysis process is described in more detail in [2]. When analyzing risks, the IS is considered in its initial state, the amount of expected losses from information security incidents for a certain period is estimated. After that, an assessment is made of how the proposed security tools and measures affect risk mitigation, and how much they cost.

The "rudiments" of the idea of risk management arose back in the 70s, when the full overlap security model (or the Clements-Hoffman model) was developed. [3]).

Clements-Hoffman model

In its original form, the Clements-Hoffman model was very «idealized», but it was in the process of analyzing this model that the problem of the need to assess threats arose.

The model is built on the basis of the postulate that the security system should have at least one means to ensure security on each possible path of the intruder's influence on the IS.

To describe the information security system with full overlap, three sets are considered [3]:

- many threats $U = \{U_i\}$, $i = 1,m$;
- many objects of protection $O = \{O_j\}$, $j = 1,n$;
- many protection mechanisms $M = \{M_k\}$, $k = 1,r$.

The elements of the sets U and O are in a "threat-object" relationship between themselves, defined by a bipartite graph, which is shown in Figure 1. The arc <Ui, Oj> exists when Ui is a means of obtaining access to the object Oj.

On fig. 1 shows a bipartite graph «threat - object».

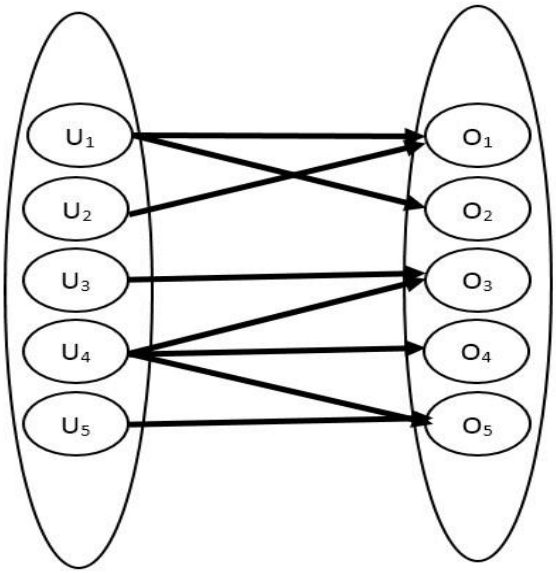

Figure 1.

It should be noted that the relationship between threats and objects does not have to be a one-to-one relationship - a threat can spread to any number of objects, and an object can be vulnerable to more than one threat.

The purpose of the defense is to close off each arc of the graph and erect an access barrier along the way. The general statement of the problem is formulated as follows: a set of information security tools M provides protection for a set of objects O from a set of threats U. Ideally, each tool mk should characterize some edge <Ui, Oj> from the indicated graph.

Applying a set of protections M transforms a bipartite graph into a tripartite one

(Fig. 2). On fig. 2 shows a three-part graph «threat - security tool - object».

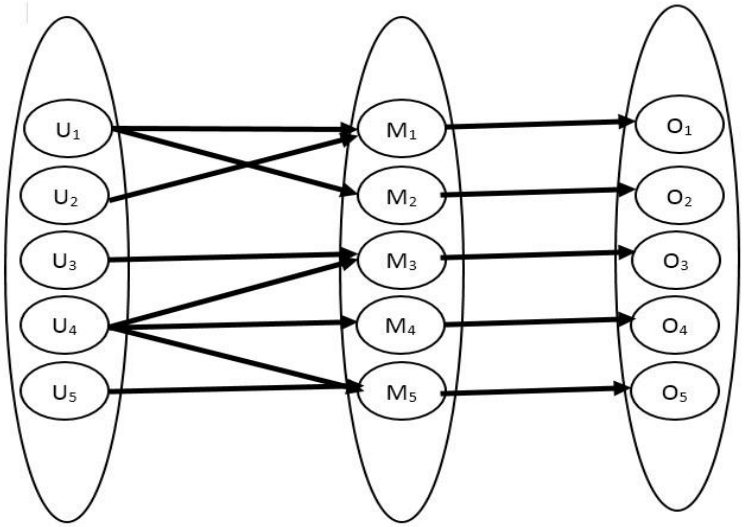

Figure 2.

In a secure system, all edges are represented as <Ui, Mk> and <Mk, Oj>. At the same time, the same protection tool can block more than one threat and protect more than one object.

The concept of «full coverage system» is introduced - this is a system in which there are means of protection for each possible penetration path.

The development of this model involves the introduction of two more elements [4]:

• V is a set of vulnerabilities determined by a subset of the Cartesian product U□O. The vulnerability of the protection system will be understood as the possibility of implementing a threat Ui against the object Oj;

• B is a set of barriers determined by the Cartesian product V□M. Barriers are ways of carrying out security threats blocked by means of protection.

We get a five-part graph. On fig. 3 shows a five-part graph «threat - security tool - barrier - vulnerability - object».

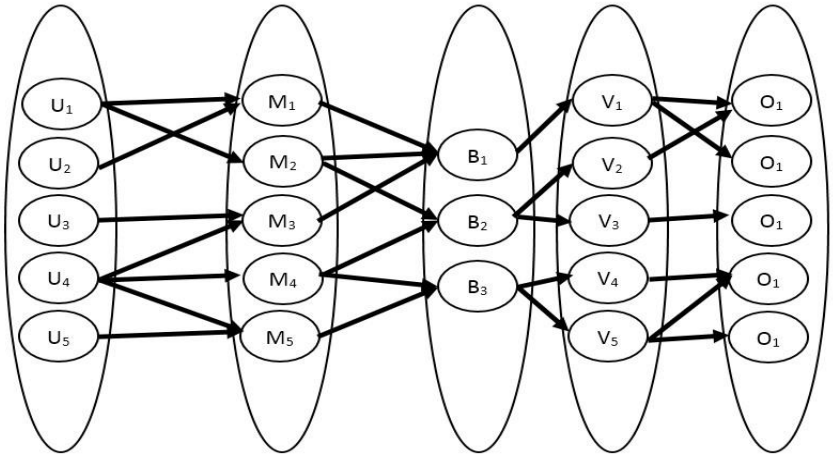

Figure 3

Now, if each arc of the graph is assigned a weight coefficient, then it is possible to quantify the degree of system protection.

Note that this model is «utopian» in nature. It does not take into account the cost of the implemented protection means, as well as the ratio of this cost to possible losses in the

implementation of a specific threat. Considering that we always have not only both material and time constraints when creating an information security system, it is not possible to build a system with full overlap.

Also, the search for all possible influences of an intruder on an object often cannot be performed. Indeed, in addition to the well-known methods of implementing the threat, new ones may arise in the future.

Thus, if it is impossible to provide protection against absolutely all threats, then the question arises of choosing those threats from which we will protect the system.

Finally, each barrier of protection in reality provides only some It is here that we are faced with the need to analyze the degree of protection of an object from a certain threat. Since the threat of the risk of a threat cannot be completely eliminated, certain methods of risk treatment (reduction, elimination, transfer or acceptance) are proposed.

Thus, when building an information security system, the problem of determining the degree of protection against existing security threats arises. To do this, we need to rank threats in a certain way depending on the degree of danger and develop measures to handle them.

Modern methods of risk management

In the process of solving the above problem, many risk management systems were created. The task of each of them is to assess the risks of IP by various parameters (possible damage, the likelihood of a threat, the severity of consequences, etc.) and to develop recommendations for risk management.

Despite the increased interest in risk management, the methods currently used are relatively ineffective, since this process is carried out independently by each division in many companies. Centralized control over their actions is often absent, which excludes the possibility of implementing a unified and holistic approach to risk management throughout the organization.

All known methods of risk assessment and analysis can be divided into [5]:

• methods that use risk assessment at a qualitative level (for example, on a scale of «high», «medium», «low»);

• quantitative methods (risk is estimated through a numerical value, for example, the amount of expected annual losses);

• methods using mixed assessments.

With a qualitative risk assessment, the consequences, probability and level of risk are determined according to expert scales; the assessment of consequences and probability can be combined; a comparative assessment of the level of risk in this case is carried out in accordance with qualitative criteria. The advantage of qualitative analysis is that it allows you to quickly and relatively «cheaply» (with minimal resource costs) determine the maximum possible number of factors and areas in which explicit or implicit manifestation of risks is possible. Using only a qualitative approach, we will analyze the causes of risks, the consequences of their implementation, however, the assessment scale used is subjective, and difficulties may also arise in comparing threats of the same category.

Quantitative analysis evaluates the practical significance and cost of the consequences, their probabilities, and gets the value of the risk level in certain units. A complete quantitative analysis may not always be possible. In this case, the ranking of risks by highly qualified specialists (experts) may be more effective. In the process of quantitative analysis, there is a comparison and a better prioritization and reinterpretation of risks. Using only a quantitative approach allows us to compare risks more accurately (numerically), but we do not take into account the causes of their occurrence, consequences.

Therefore, when analyzing information systems, given their complexity, it is desirable to use a mixed approach that uses both qualitative and quantitative assessment scales. This will provide the most comprehensive and integrated approach to solving the problem of risk management.

Risk management software products

Let's consider the main systems of risk analysis and assessment (for more information in [6-7]):

• CRAMM assessment (mixed approach)

This methodology does not take into account accompanying documentation, such as a description of business processes or reports on risk assessments conducted. With regard to the strategy of working with risks, CRAMM assumes the use of only methods to reduce them. The methodology lacks: the process of integrating management methods, monitoring the effectiveness of management methods used and methods of managing residual risks, the process of responding to incidents.

The disadvantages of CRAMM are the need to attract highly qualified specialists, the complexity and duration of the risk assessment process. In addition, it should be noted the high cost of the license. • VULTURE assessment (mixed approach)

The VULTURE methodology uses quantitative and qualitative methods of risk assessment, and also determines the conditions under which the latter can be accepted by the company, includes the calculation of the return on investment for the implementation of security measures. Unlike other risk analysis techniques, VULTURE offers all the ways to reduce risks (circumvention, reduction and acceptance). This methodology takes into account the accompanying documentation (description of business processes or reports on the conducted risk assessments of information security).

• RiskWatch assessment (quantitative approach)

The complexity of risk analysis using this method is relatively small. A significant advantage of RiskWatch is an intuitive interface and great flexibility of the method provided by te possibility of introducing new categories, descriptions, questions, etc

Disadvantages: risk analysis is carried out only at the software and technical level, administrative and organizational factors are not taken into account, very high cost [8-10]. • CORAS assessment (qualitative approach)

The disadvantage of CORAS is that it does not provide for the frequency of risk assessment and updating of their values, which indicates that the methodology is suitable for performing one-time assessments and is not suitable for regular use.

The positive side of CORAS is that the software product implementing this technique is distributed free of charge and does not require significant resources for installation and application.

• MSAT assessment (Qualitative approach)

Key indicators

Conclusion

The report reviewed and analyzed the process of risk analysis and assessment. The necessity and importance of using a risk assessment and analysis system when designing an information security system was emphasized. It is shown that ignoring this approach can lead to unreasonably high costs for building an information security system. The Clements-Hoffman model is presented, during the analysis of which the problem of risk management was raised.

The main risk management techniques are also described and analyzed. It was concluded that it is most effective to use an approach that combines both qualitative and quantitative risk assessment.

The analysis of several existing software products for risk management is carried out. Each of the products has its advantages and disadvantages, but the scope of their application depends on the enterprise itself. In some cases, the disadvantages of this product are not important for a particular company.

Literature

1. International standard ISO/IEC 27005:2008. Information technology – Methods of protection – Information security risk management.
2. Hoffman L.J. Modern methods of information protection // Trans. from English – M.: Soviet radio, 1980. – 264 p.
3. Averchenkov V.I., Rytov M.Yu., Gainulin T.R. Optimization of the choice of the composition of the means of engineering and technical protection of information based on the Clements-Hoffman model // Bulletin of the Bryansk State

Technical University, 2008. – No. 1. – Pp. 61-67.
4. National Standard of the Russian Federation GOST R ISO/IEC 31010:2009. Risk management. Methods of risk assessment.
5. Baranova S.Yu. Methods of analysis and assessment of information security risks, Bulletin
6. Witte Moscow State University. Series 3. Educational resources and technologies, 2015. – № 1(9). – Pp. 73-79.
7. Razumnikov S.V. Analysis of the possibility of using OCTAVE, RiskWatch, CRAMM methods to assess IT risks for cloud services // Modern problems of Science and Education, 2014. – No. 1. – pp. 247-248.
8. Petrenko S.A. Information risk management. Economically justified security // Petrenko S.A., Simonov S.V. – M.: IT Company; DMK Press, 2004. – 384 p. 9. Maksimenko V.N., Daricheva A.N. Methodological approaches to assessing the quality of contact center services // Economics and quality of communication systems, 2017. – № 1(3). – Pp. 79-88.
9. Maksimenko V.N., Yasyuk E.V. Comparative analysis of methodological approaches to information security risk assessment // in the collection: Mobile business: Prospects for the development and implementation of radio communication systems in Russia and abroad. 2017. – C. 15-16.