Akademik Tarih ve Düşünce Dergisi *Academic Journal of History and Idea*
ISSN: 2148-2292
11 (1) 2024

Araştırma Makalesi | Research Article
Geliş tarihi |Received:20.12.2023
Kabul tarihi |Accepted:21.01.2024
Yayın tarihi |Published:25.02.2024
https://doi.org/10.46868/atdd.2024.650

Elchin N. Taghiyev

https://orcid.org/0009-0008-7130-7313
Lecturer in Mingachevir State University, Phd student in Ganja State University, The theory and mehodology of education: teaching methodology of Informatics Ganja city, The Republic of Azerbaijan, elchin.taghiyev@mdu.edu.az

Atıf Künyesi | Citation Info

Taghiyev, Elchin N. (2024). Modeling the Process of Evaluation of Information Security Risks and its Methodology by the Application of Computer Systems. *Akademik Tarih ve Düşünce Dergisi, 11* (1), 93-100.

Modeling the Process of Evaluation of Information Security Risks and its Methodology by the Application of Computer Systems

Abstract

The main aim of the article is to study modeling the process of evaluation of information security risks by the application of computer systems. Thus, information security risk assessment and analysis of existing methods of information security risk assessment had been also studied in the article. The term "risk of information security" (IS) applies to the damage that can attack the information technology systems. IS risk is a wide range of potential threats, especially includes data violations, control measures, financial costs, reputation damage, etc. cover issues such as. IS risks include the failure of hardware and software, human errors, spams, viruses and harmful attacks, as well as natural disasters such as fires, cyclones or floods. Security risk assessment determines, assesses and implements key security controls in applications. It also focuses on prevention of software security defects and vulnerabilities. Information security risk is the potential probability of using vulnerabilities of an asset or group of assets as a specific threat to damage the organization.

Keywords: *Methodology, Pedagogy, İnformation Security, İnformation Security Risks, Threatening, Risk Assessment, Risk Management*

Bilgi Güvenliği Risklerinin Değerlendirilmesi Sürecinin ve Metodolojisinin Bilgisayar Sistemleri Uygulamasıyla Modellenmesi

Öz

Makalenin temel amacı, bilgisayar sistemlerinin uygulanmasıyla bilgi güvenliği risklerinin değerlendirilmesi sürecinin modellenmesini incelemektir. Bu nedenle, makalede bilgi güvenliği risk değerlendirmesi ve mevcut bilgi güvenliği risk değerlendirme yöntemlerinin analizi de incelenmiştir. "Bilgi güvenliği riski" (IS) terimi, bilgi teknolojisi sistemlerine saldırabilecek zararlar için geçerlidir. İG riski geniş bir yelpazedeki potansiyel tehditleri, özellikle veri ihlallerini, kontrol önlemlerini, finansal maliyetleri, itibar zedelenmesi vb. gibi konuları kapsamaktadır. IS riskleri, donanım ve yazılımların arızalanması, insan hataları, spamlar, virüsler ve zararlı saldırıların yanı sıra yangın, kasırga veya sel gibi doğal afetleri de içerir. Güvenlik risk değerlendirmesi, uygulamalardaki temel güvenlik kontrollerini belirler, değerlendirir ve uygular. Ayrıca yazılım güvenliği kusurlarının ve güvenlik açıklarının önlenmesine odaklanır. Bilgi güvenliği riski, bir varlığın veya varlık grubunun güvenlik açıklarının kuruma zarar vermek için belirli bir tehdit olarak kullanılma potansiyel olasılığıdır.
Anahtar Kelimeler*: Metodoloji, Pedagoji, Bilgi Güvenliği, Bilgi Güvenliği Riskleri, Tehdit, Risk Değerlendirmesi, Risk Yönetimi*

Introduction

Since the creation of the global information space, two centers of power have emerged that can really influence information processes. The first one is corporations that both implement technological processes and manage them, actually controlling the global information space. The second side is the state structures that own the information space, which in many cases act only as observers of the processes occurring due to their inability to influence information processes, or to confront this situation without reconciliation. The creators of global networks and the owners of key technologies want to keep things as they are, based on freedom of speech. The “other side” argues that from a humanitarian point of view, states are trying to manage this process through the application of legislation. At the same time, they strive to maintain a monopoly on information processes, forming international information law. The first party controls the advertising market, which is based on "free speech" and dodges taxes, and ultimately it turns out that the goal is commercial interests. The second “country” is the various “states”. Of course, states are interested in gaining a share of the advertising market, collecting taxes from the electronic market, protecting themselves from provocations, moral and ethical frameworks, and also fighting "various groups" and social "diseases" in active intervention in

information processes (Kazimi, 2018, s. 186). In any case, the reliable activity of the computer is ensuring that the security of the information covering the area is primarily. It is known that there are several approaches to the assessment of information security in the event of potential threats to information resources. The main stages of the creation of information protection systems are the analysis of topical threats and evaluating information security risks. The analysis of security threats provides for the identification of confidentiality, completeness or accessibility of information in the information system and the identification of unacceptable negative consequences (losses), events or processes.

1. Formulation of the problem

The role of systematic approaches to analyze and compares the quantity and quality of risks in the system by analyzing the criteria and determine their importance (Aliev, Djafarov, Babayev, Huseynov, 2005). During the analysis and risk assessment of information threats, the main definitive factor is the detection of those threats. In most cases, the violation of the computer system can be observed for both physical (disposal of the device), technical (user errors, harmful programs or cybercriminals) and natural (disasters, etc.). The most common information security risks in the field of activity include the following:

Phishing (phishing users are a breaking scheme who is deceived by downloading malicious messages);

- Malware;
- Ransomware (harmful software that prevents access to or reading access to a computer system, designed to require threatening);
- Data breach;
- Dangerous passwords;

The method of comperative analysis had been implemented during the research.

2.Concept and process of Information Security Risk Management

Risk, in a wider sense, is the probability of an event that entails certain losses (for example, physical injury, loss of property, damage to the organization, etc.). Information security risk is the potential probability of using vulnerabilities of an asset or group of assets as a specific threat to damage the organization. The main features of risk are inconsistency, alternativeness, and uncertainty. Classification of information risks is shown in Figure 1 and classified into five groups (Kuzminykh, 2021). Three additional terms are necessary to describe the risk assessment spectrum boundaries. An inconsistency in risk emerges when the subjective assessment does not adequately and reliably assess and describe the objectively existing risky actions. An alternativeness is the need to choose from two or more possible solutions or actions. If there is

no choice, then there are no risky situations and, consequently, risk. Uncertainty is the incompleteness or inaccuracy of information about the conditions of the decision. The existence of risk in itself is possible only when decisions are taken in absence of or with insufficient information about the implications of a decision. These features can lead to serious difficulties in the risk assessment process

The risk management covers the process of evaluating and managing information, which is first of all the information, then. The first stage of the process is to determine the potential risk of information. A few factor or data sources apply to the setting phase:

- Weaknesses are shortcames that are specific to the relationship between operators and techniques between objects, technologies, processes (including information risks, and techniques);
- Threats are people who can cause incidents on weaknesses, causing impacts and natural phenomena;
- Assets, that is information content covering the relevance and their storage servers, warehouses;
- The effects of incidents and disasters affecting assets and disasters that damage the interests of the organization and its business and often third parties;
- Events can change small, insignificant or significant scales;
- Tips, standards, etc. Cert, FBI, ISO / IEC, journalists, technology sellers, as well as information risk and security professionals (social networks) applies to relevant warnings and recommendations.

The Risk Assessment phase covers the review of all these information to determine the importance of various risks, which in turn determines priorities for the next stage. The entity's of risks to the threats are here, and this reflects the broader cultural factors and personal relations of specialists engaged in corporate strategies and policies, as well as risk management activities.

To prevent them from detrimental risks, it means that to alleviate, share and receive. This phase covers what and how to decide how to do (risk treatment decisions). The redirection of change is an open platform. The risks of information here are constantly changing in connection with various other factors outside the organization, as a result of the risk of information, partly risk treatment. In the lower part of the diagram, the organization is accepted that the organization should often meet foreign liabilities such as compliance and market pressures or expectations.

3.Determination of İnformation Security Risks in Computer Systems

The risk of information is a calculation based on the possibility of a permission of the unauthorized user, the probability that you transfer or have a negative impact on the confidentiality, integrity and existence. It is known that any technical system is almost inevitable for computer technology, and random failures and refusals (Aliev, 2004). Their emergence can be conditioned by both internal technological reasons (mechanical, climate, electromagnetic, biological, etc.). As a result of failures or refusal, the system stored and processed in the system may occur. To reduce security risks to minimize the adverse effects of the environment, the external factors must be taken into account in the process of developing the information security concept. In practice, it is obtained by the application of various technical measures such as use of special covers or the equipment of equipment (Kasumov, 2007). However, technological security measures are usually applied only for specialized computer systems. Considering that corporate computer systems are defended in constructively, they can be exposed to various other types of natural and artificial origin. It is important to follow their physical condition in storage and processing of data. Therefore, the development of information security risks assessment of information security risks in computer technologies used in enterprises is relevant.

4. Determination of İnformation Security Risk Assessment Methodology

Information security risk assessment is an important part of enterprises' management practices that helps to identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. Risk management refers to a process that consists of identification , management, and elimination or reduction of the likelihood of events that can negatively affect the resources of the information system to reduce security risks that potentially have the ability to affect the information system, subject to an acceptable cost of protection means that contain a risk analysis, analysis of the "cost-effectiveness" parameter, and selection, construction, and testing of the security subsystem, as well as the study of all aspects of security (Kuzminykh, 2021). As the object of research, the coordinating used in enterprises can be taken to individual computers or laptops. It is clear that the following components affect the integrity of information and apparatus in the computer system:

- Central Processor (CP)
- Temperatures of the body (motherboard) and hard disk;
- The growth rate of the corps.

It is known that the Central Processor (CP) temperature in computers in discrete mode varies between typically below 80-90 degrees Celsius, to avoid overheating and potential

damage. This indicator depends on production technology and depending on the manufacturer, the permitted heating range can be simply 100-110°C, and 110-130°C when the load. At the same time, in other cases, the temperature of the normal CP may be 50-80°C and the loading temperature will reach 70-90°C depending on the Kuller (cooling) system.

The temperature of the hard disk is a relatively unregy character that depends on a number of conditions. For example, the temperature can be 25-40°C degrees in winter, and in summer can rise to 50°C degrees. The main indicator that has to be formed here is the normal moisture of the system unit. In the 15-20% level, low humidity leads to the accumulation of static electricity in the air and eventually electrification of dust, pollution and current roads. Inadequate moisture (up to 30%) leads to the destruction of electronic plateau, drying and the insulation of the corps of the corps, and later results in their cracking. The moisture, which is more than 60%, causes corrosion and oxidation of contacts, which can cause a short circuit circuit. Settings viewed the affect of each other. Approbation of the result: The article had been researched in the Department of Informatics. The branch of the research is The theory and mehodology of education: teaching methodology of Informatics.

Results: The CP temperature may depend on the status of thermopast and the central processor's refrigerator ventilator. The ventilator installed on it in the temperature of the hard drive and the body. The frequency of ventilators depends on the temperature and is regulated by the motherboard. The moisture in the body depends on the condition of the room, and it is required to install a treasury corps for its assessment. The issue of comprehensive accounting of the agency of the parameters described requires specialized knowledge and euristic experience. Therefore, it is important to apply expert systems based on the development of reviews based on possible information risks in the computer system (Doljenko, 2009). Many insights related to security are high quality, in most cases, it is difficult to assess their quality based on quantitative size. In some cases, after the evaluation of the expert, it is carried out in the form of oral lingual statements related to numerical (mathematical) basis, because the expert's assessment of the expert may be subjective. This condition the need to apply the natural language of natural language, that is, the application of fuzzy logic apparatus from itself in similar security of information security.

5.Analysis of Existing Methods of Information Security Risk Assessment

In order to solve the problem of information security risk assessment, many software packages have been created according to the developed methods, which are now used by enterprises and auditors. There are over 30 methodologies and frameworks that can be used for

IT security risk assessment. A complete analysis of the entire risk analysis spectrum is beyond the scope of this work; in order to provide a substantial coverage based on the current usage trends, we focus on the subset that is most commonly used by enterprises, focusing on methodologies that include a budget decision. As a result, we do not consider frameworks designed for audit, IT governance, and certification, such as ISO/IEC 27001:2005, ISO/IEC 15408:2006 (Common Criteria for Information Technology Security Evaluation), COBIT (ISACA), and NIST SP-800 standard whose main purposes are audit, IT governance, and certification. This section highlights the most significant ones. The Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM) is one of the most common alternatives of risk control. Risk analysis using this method involves identifying and calculating risk levels based on estimates assigned to resources, threats, and resource vulnerabilities. Risk control is the identification and selection of countermeasures that can reduce risks to a level that the company can take. The study of the system using CRAMM is carried out in five stages:

1.Initiation, which produces a description of the boundaries of the information system, its main functions, categories of users, and personnel involved in the survey;

2.Definition and valuation of assets, to describe and analyze everything related to determining the value of system resources. At the end of this stage, it is determined whether the customer is satisfied with their existing practice or whether they need a full risk analysis. In the latter case, a model of information system will be built from
the position of the information security;

3.Threat and vulnerability assessment (optional stage, depending on whether the customer satisfies the basic level of information security), aiming to deliver a full risk analysis. Finally, the customer receives identified and assessed levels of threats and vulnerabilities for its system;

4.Risk analysis, to assess the risks either on the basis of assessments of threats and vulnerabilities in full risk analysis or by using simplified techniques for the basic level
of security;

5.Identification of countermeasures.

Following the above stages, the process then selects the criteria applicable to this information security and assesses the damage on a scale with values from 1 to 10. In the CRAMM descriptions, as an example, the rating scale is given according to the criterion “Financial losses associated with the restoration of resources” as follows:

• 2 points—less than USD 1000;

• 6 points—from USD 1000 to USD 10,000;

• 8 points—from USD 10,000 to USD 100,000;

• 10 points—over USD 100,000.

Conclusion

All the necessary input for the CRAMM methodology comes in the form of expert assessments and responses to surveys of employees of the organization on aspects of their use of various resources. These surveys are also formulated based on the data on the in-formation system of the organization entered by experts. This process of collecting data can be cumbersome and time-consuming, which represents one of the most significant drawbacks of this approach. From a processing perspective, the CRAMM software then generates a list of unambiguous questions for each resource group and each of the 36 threat types. The level of threats is rated, depending on the responses, as very high, high, medium, low, and very low. The level of vulnerability is assessed, depending on the answers, as high, medium, and low. Thus, CRAMM is an example of a calculation method in which the initial estimates are received at a qualitative level and then translated to a points-based quantitative assessment. One issue of CRAMM is that its implementation cannot be reused, as it cannot remember or reuse previous results as factors that affect risk parameters. In the scientific work, a methodology of assessing the condition of the computer (individual computer or laptop) is offered based on knowledge engineering technology and fuzzy logical extract mechanism.

References

Aliev, R. A., Djafarov, S.H., Babayev, M.Dj. Huseynov, B. G. (2005). *Principles And Projects of Building İntellectual Systems.* Nargiz.

Aliev, R. A., Aliev, R. R. (2004). *Soft Computing.* Chashioglu.

Kasumov, V. A. (2007). *Information security: Computer crime and cyber terrorism.* Science.

Doljenko, A .I. (2009). Model of risk analysis of consumer quality of projects of economic information systems. *Vestnik Severo-Kafkazskogo Gosudarstvennogo Tekhnicheskogo Universytety, 1* (18), 129-134.

Kazimi, P. F. (2018). *İnformasiya mühəndisliyi (Information engineering).* Mütercim.

Kuzminykh, I., Ghita, B., Sokolov, V., Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia,* 1, 602–617. https://doi.org/10.3390/ encyclopedia103005