DOI: https://doi.org/10.36719/2706-6185/37/21-24

Rovshan Humbataliyev
Azerbaijan State Maryne Academy
Doctor of Mathematical Sciences
rovshangumbataliev@rambler.ru
Elchin Taghiyev
Mingachevir State University
Ph. D. student
elchintagi@rambler.ru

MODELING THE PROCESS OF EVALUATION OF INFORMATION SECURITY RISKS BY THE APPLICATION OF COMPUTER MATHEMATICAL SYSTEMS

Abstract

Problem solving on the computer first of all involves formulating the problem statement, choosing a solution method, and developing a mathematical model of the solution. The sequential execution of the considered stages in an appropriate order, as a result, will create the basis for the machine solution of the issue. Therefore, there is a risk of information corruption. The term "risk of information security" (Information System) applies to the damage that can attack the information technology systems. Information System risk is a wide range of potential potential, including data violations, control measures, financial costs, reputation damage, etc. cover issues such as. Information System risk risks include the failure of hardware and software, human error, spam, 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.

Keywords: *information security, information security risks, threatening, risk assessment, risk management, methodology*

Rövşən Hümbətəliyev
Azərbaycan Dövlət Dəniz Akademiyası
riyaziyyat elmləri doktoru
rovshangumbataliev@rambler.ru
Elçin Tağıyev
Mingəçevir Dövlət Universiteti
doktorant
elchintagi@rambler.ru

Kompüter riyaziyyatı sistemlərinin tətbiqi ilə informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi prosesinin modelləşdirilməsi

Xülasə

Kompüterdə məsələ həlli ilk növbədə verilən məsələnin qoyuluşunun formalaşdırılmasını, həll üsulunun seçilməsini, həllin riyazi modelinin işlənib hazırlanmasını nəzərdə tutur. Baxılan mərhələlərin müvafiq qaydada ardıcıl olaraq icra edilməsi, nəticə etibarilə məsələnin maşın həllinə zəmin yaratmış olar. Ona görə də informasiya təhlükəsizliyi riski ortaya çıxır. "İnformasiya təhlükəsizliyi riski" (İnformasiya Texnologiyaları) termini informasiya texnologiyaları sistemlərinə hücum edə biləcək zərərlərə aiddir. İnformasiya sistemi riski potensialın geniş spektridir, o cümlədən məlumat pozuntuları, nəzarət tədbirləri, maliyyə xərcləri, nüfuzun zədələnməsi və sair kimi məsələləri əhatə edir. İnformasiya sistemi risklərinə aparat və proqram təminatının uğursuzluğu, insan səhvi, spam, viruslar və zərərli hücumlar, həmçinin yanğınlar, siklonlar və ya daşqınlar kimi təbii fəlakətlər daxildir. Təhlükəsizlik riskinin qiymətləndirilməsi tətbiqlərdə əsas

təhlükəsizlik nəzarətlərini müəyyən edir, qiymətləndirir və həyata keçirir. O, həmçinin proqram təminatının təhlükəsizliyi qüsurlarının və zəifliklərinin qarşısının alınmasına diqqət yetirir.

Açar sözlər: *informasiya təhlükəsizliyi, informasiya təhlükəsizliyi riskləri, təhdid, risklərin qiymətləndirilməsi, risklərin idarə edilməsi, metodologiya*

Introduction

In any case, the reliable activity of the computer is primarily 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.

The system of systematic approaches to analyze and compares the quantity and quality of risks in the system by analyzing the criteria to determine their importance (Aliyev et al., 2005). During the analysis and risk assessment of information threats, the main definitive factor is the detection of these 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.

1. Mehods

1.1. Information Security Risk Management 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 weaknesses 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, 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 (our social network) (our social network) (our social network) (our social network) (our social network) (our social network) (our social network) (our social network) (our social network) 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 risks to the risks 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 treating the risks, it means 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.

1.2. Determination of Information 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 (Aliyev, 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.

1.3. Determination of Information Security Risk Assessment Methodology

As the object of research, the coordinating coordinates 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 450 ℃ and 650 ℃. This indicator depends on production technology and depending on the manufacturer, the permitted heating range can be simply 30-350 ℃, and 70-750 ℃ when the load. At the same time, in other cases, the temperature of the normal CP may be 50-550 ℃ and the loading temperature will reach 80-850 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 40-45 degrees in winter, and in summer can rise to 50 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 affect each other.

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; 5). 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 (6; 7; 8). 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.

Conclusion

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

1. Aliyev, R. A., Djafarov, S. H., Babayev, M. Dj., Huseynov, B. G. (2005). Principles and projects of building intellectual systems (in Azerbaijani). Baku: Nargiz, 386 p.
2. Aliyev, R. A., Aliyev, R. R. (2004). Soft Komputing (in Azerbaijani). Baku: Chashioghlu, 640 p.
3. Kasumov, V. A. (2007). Information security: computer crime and cyber terrorism (in Azerbaijani). Baku: Science, 192 p.
4. 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), pp. 129-134.
5. Computers, models, computational experiment. Digest of articles. (1988). Moskva, p. 13.
6. www.mathcast.ru
7. www.math.ru
8. old.tusur.ru/export/sites/ru.tusur.new/ru/

Received: 13.05.2024 Accepted: 18.07.2024