THE CONCEPT OF INFORMATION SECURITY AND THE PROBLEMS OF PERFORMANCE INDICATORS

Kuldasheva Feruza Kurdoshevna
Teacher of Informatics at TSUE 1st Academic Lyceum
E-mail: feruzakuldasheva777@gmail.com

Abstract:
This article analyzes the concept of information security, its basic principles and the problems of assessing performance indicators. It also discusses the problems encountered in ensuring the security of information systems and ways to overcome them. Modern approaches and indicators for improving the effectiveness of information security are considered.
Keywords: Information security, performance indicators, information systems, security principles, threats, protective measures, data security, cybersecurity.

INTRODUCTION

Information security is one of the most pressing issues for organizations and government agencies today. As a result of the rapid development of digital technologies, threats to information systems are increasing. Therefore, ensuring information security and assessing its effectiveness are of great importance. Determining performance indicators and methods for measuring them play a key role in the formation of security strategies.

This study aims to analyze the concept of information security, identify criteria for assessing its effectiveness, and shed light on existing problems.

Methodology

The following methodological approaches were used in the study:

Theoretical analysis - scientific sources on information security and its effectiveness indicators were studied.

Comparative method - existing security systems and their effectiveness indicators were compared.

Expert assessment - analyses were conducted based on the opinions and experience of experts in the field.

Statistical analysis - existing data and indicators on information security were studied.

Based on these approaches, recommendations were developed to improve the effectiveness of information security.

The concept of information security and its basic principles

Information security is a system of measures aimed at protecting information resources from unauthorized access, modification, destruction or loss. It is based on the following basic principles:

Confidentiality - only authorized persons have access to information.

Integrity - ensuring that information is protected from damage or alteration.

Availability - the readiness of information and systems to be used when necessary.

Information security depends not only on technical, but also on legal, organizational and human factors and requires an integrated approach.

Indicators for assessing the effectiveness of information security

Various indicators are used to determine the effectiveness of information security. They are divided into the following main areas:

Technical indicators:

Level of system protection

Number of software vulnerabilities

Cyberattack failure rate

Organizational indicators:

Existence of security policies and procedures

Level of employee security awareness

Effectiveness of emergency response plans

Financial indicators:

Budget allocated to the security system and its effectiveness

Amount of material damage caused by cyberattacks

Current problems of information security

Today, the following problems are observed in ensuring information security:

Growth of cyberattacks - the number of hacker attacks and malicious programs is increasing.

Weak systems and software - outdated security systems remain vulnerable to cyberattacks.

Low level of employee awareness - errors in information security are often due to the human factor.

Lack of finance and resources – there is a lack of funds to implement security measures.

Legal and regulatory issues – weak or ineffective legislation against cybercrime.

Measures to improve information security effectiveness

The following measures should be taken to improve information security:

Implement strong authentication systems – use modern technologies such as two-factor authentication (2FA).
Software updates and monitoring – constant updating of systems and monitoring of cybersecurity.
Regular training of employees – organization of information security training and seminars.
Improving the legal framework – development and implementation of effective legislation against cybercrime.
Backups – regular backups of important data.
Implementation of an analysis and evaluation system – development and constant monitoring of an information security effectiveness assessment system.
These measures will help increase the level of information security and make it possible to effectively counter cybersecurity threats.
Conclusion
Information security is of great strategic importance in today's digital society, and ensuring its effectiveness is a priority for every organization and state institution. The study analyzed the basic concepts of information security, its performance indicators, and existing problems.
Technical, organizational, and financial indicators play a significant role in assessing the effectiveness of information security, and their systematic monitoring is necessary. An integrated approach is required to eliminate problems such as the increase in the number of cyberattacks, software vulnerabilities, and the human factor.
Based on the results of the study, the following recommendations were made to improve information security:
Introduction of modern security technologies
Improving the knowledge and skills of employees
Continuous updating of information systems and strengthening protective measures
Strengthening the legal framework and measures to combat cybercrime
Implementation of these measures will increase the level of information security and effectively counter threats to cybersecurity. It also creates the basis for improving organizations' strategic approaches to protecting information resources.
REFERENCES:
1. Bibliographic entry. Bibliographic description. General requirements and rules for compilation. - Moscow: Standartinform, 2003. - 38 p.
2. Stolbovoy V. A. Information security: Textbook. - 2nd ed., corrected. and add. - Moscow: Infra-M, 2019. - 312 p.

3. Chereshkin, A. V. Fundamentals of cybersecurity. - St. Petersburg: Piter, 2021. - 224 p.
4. Ivanov, P. A. Methods for assessing the effectiveness of information security // Information technologies. - 2020. - No. 3. - P. 15-23.
5. Smirnov, D. L., Petrov, K. V. Modern threats to cybersecurity and methods of their neutralization // Information protection. - 2021. - No. 5. - P. 48-55.
6. Information security, cybersecurity and privacy protection – Information security management systems – Requirements [Electronic resource]. – Access mode: https://www.iso.org, free (date of access: 03/18/2025).
7. NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations [Electronic resource]. – Access mode: https://csrc.nist.gov, free (date of access: 03/18/2025).