DOI https://doi.org/10.30525/978-9934-26-459-7-23

METHODS OF PROTECTING INFORMATION DATA

Roman Shpylovyi[1], Maiia Liuta[2], Marharuta Medolyz[2]
[1]ISMA University of Applied Science, Latvia
[2]Cherkasy State Business-College, Ukraine
**Corresponding author's e-mail: romshpil@gmail.com, maiialiuta@gmail.com, medolyz.mm@gmail.com*

Abstract

In the era of digital transformation, protecting information data is not only desirable but a critically important aspect for any organization or individual. Information security aims to protect the integrity, confidentiality, and availability of data. Although the number of threats is constantly increasing, more and more new viruses are appearing, the intensity and frequency of DDoS attacks is increasing, the developers of information protection tools are also not standing still. For each threat, new protective software is developed or the existing one is improved.

Key words: *Information Data Protection, Cybersecurity, Encryption, Authentication, Authorization, Network Security, Physical Security, Access Control, Security Policies, Incident Detection.*

Introduction

The key methods of information data protection are given.

1. Data Encryption.

Encryption is one of the most common methods of information data protection. This process involves converting data into an unreadable format that can only be understood by those who have the decryption key. Encryption is applied to both data at rest (e.g., on a hard drive) and data in transit (e.g., during transmission over a network).

2. Access Control.

Access control to data is a key element of information protection. It involves granting access to data only to authorized individuals. This can be implemented using various methods, such as password authentication, biometric authentication, card-based authentication, etc.

3. Data Backup and Recovery.

Regular data backup is an important security measure. This allows data to be restored in case of loss, damage, or deletion. Additionally, a data

recovery strategy should be developed that outlines how and when data will be recovered from a backup.

4. Antivirus Software.

Antivirus software helps protect the system from malicious software, such as viruses, Trojans, spyware, and others. This is done by scanning the system for malicious software and removing detected threats.

5. Updates and Patches.

Regular software updates and security patches are an important measure to protect information. This allows vulnerabilities to be eliminated that could be exploited by attackers to gain access to the system and data.

6. Employee Training.

Employee training on information security issues is an integral part of information data protection. Employees should be aware of security threats and ways to avoid them.

7. Use of Secure Passwords.

Creating and using secure passwords is a simple but effective way to protect data. A password should be complex, containing uppercase and lowercase letters, numbers, and special characters.

The purpose of information security is to protect the value of the system, to preserve and guarantee the accuracy and integrity of information, and to minimize destruction if the information is modified or destroyed. Information security requires consideration of all events during which information is created, modified, distributed, or accessed. Among the methods of information protection, the following can be distinguished:

Multi-Factor Authentication (MFA).

Multi-factor authentication is an authentication method that requires users to provide two or more verification factors to gain access to a resource, such as an application, online account, or a VPN. It adds an additional layer of security, making it harder for unauthorized users to gain access to sensitive data.

Intrusion Detection and Prevention Systems (IDPS):

Intrusion detection and prevention systems are security tools that monitor network traffic for suspicious activity and take action to block or prevent it. They can detect and respond to various types of attacks, such as denial of service (DoS) attacks, viruses, and other malicious activities.

Data Loss Prevention (DLP).

Data loss prevention is a strategy used to prevent sensitive data from being lost, stolen, or misused. It involves the use of technologies and processes to monitor and control the movement of data within and outside of an organization. DLP solutions can detect and prevent the unauthorized

transfer of sensitive data, such as credit card numbers, social security numbers, and other confidential information.

Virtual Private Networks (VPNs).

Virtual private networks provide secure, encrypted connections between devices and networks. They are commonly used to protect data in transit, especially when using public Wi-Fi networks. VPNs create a secure tunnel for data to travel through, protecting it from interception and eavesdropping.

Cloud Security.

Cloud security refers to the measures and technologies used to protect data, applications, and infrastructure in cloud computing environments. It includes a range of security controls, such as encryption, access control, and intrusion detection and prevention systems, that are designed to protect data in the cloud from unauthorized access, theft, and other security threats.

Regular Security Audits.

Regular security audits are an essential part of information data protection. They involve a systematic evaluation of an organization's information systems and security controls to identify vulnerabilities and ensure compliance with security policies and regulations. Security audits can help organizations identify and address security weaknesses before they are exploited by attackers.

Incident Response Plan.

An incident response plan is a set of procedures that an organization follows in the event of a security breach or other IT security incident. It outlines the steps that should be taken to contain the incident, assess the damage, and restore normal operations as quickly as possible. Having an incident response plan in place can help organizations respond effectively to security incidents and minimize the impact on their operations and reputation.

Conclusions

Protecting information data is a complex task that requires a comprehensive approach. Combining different data protection methods, such as encryption, access control, data backup and recovery, antivirus software, regular updates and patches, employee training, and the use of secure passwords, allows for the creation of an effective information data protection system.

Information data protection is a critical aspect of organizational security and requires a multi-layered approach. By combining various data protection methods, such as multi-factor authentication, intrusion detection and prevention systems, data loss prevention, virtual private networks, cloud

security, regular security audits, and incident response plans, organizations can create a robust and effective information data protection system.

References

1. Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 13 (1), 15–21.

2. Yevseiev S., Laptiev O., Korol O., Pohasii S., Milevskyi S., Khmelevsky R. (2021). Analysis of information security threat assessment of the objects of information activity. *International independent scientific journal*, 1(34), 33–39.

3. Golubnychiy D., Severinov O., Kolomiytsev O., Mysyura O., Tretyak V., Vlasov A. & Kruk B. (2021). Analysis of modern threats in information systems by components of threats: cyber security, information security and information security. *InterConf*, (45), 21–27.