ISSN: 2776-0960 Volume 2, Issue 11 Nov., 2021

SECURITY PARAMETERS IN THE PROTECTION OF INFORMATION SYSTEMS

Salimova Makhbuba
(Samarkand state university)

Annotation

This study provides theoretical information about the security of information systems. It provides a systematic analysis of the types of attacks on the network and organizations that provide information about their prevention, threats, and types of information security, the concept of threats to protected information, and its structure.

Keywords: Information systems, information security, security, threats.

Information

Currently, the development and improvement of information system security tools is relevant. All over the world, a number of works are being carried out to protect information systems. Based on this, we will list a number of public organizations that provide information about the types of network attacks and their elimination.

1. American Society for Industrial Security (ASIS) – an American organization for industrial security: offers the necessary security training and conducts the Certified Protection Professional certification. Information about its members and field departments website - www.securitymanagement.com

2. Computer Emergency Response Team Coordination Center (CERT / CC)- Computer Emergency Response Team Coordination Center: was founded by the Defense Advanced Research Projects Agency of the U.S. Department of Defense to study computer and network attacks, find ways to protect systems, and disseminate key information about attacks, and is currently located at the Carnegie Mellon University Software Development Institute. Website: www.cert.org.

3. Forum of Incident Response and Security Teams (FIRST) - Forum of Incident Response and Security Teams: an international organization for security, whose members are more than 100 educational institutions, administrations and commercial organizations. FIRST was created to help prevent incidents and respond quickly to them in local defense and international security. Website – www.first.org.

4. InfraGard: A private industrial consortium and a U.S. Federal Agency, led by the CIA, that exchanges information to protect the infrastructure of critical U.S. information systems. Source for more information about InfraGard: www.infragard.net

5. Information Security Forum (ISF) – Information Security Forum: Created by Coopers and Lybrand as the European Security Forum, the organization expanded through its international activities and became the ISF in 1992. The ISF focuses its activities on "practical research" through publication and placement at regional summits. You can learn more about this organization www.securityforum.org you can find out on the website.

6. The Information Systems Security Association (ISSA) is an information systems security association: It is also an international organization dedicated to training and research in the field of computer security. ISSA helps sponsor many certification programs, such as the Certified Information Systems Security Specialist (CISSP), the Certified Systems Security Practitioner (SSCP), and the Certified Information Systems Auditor (CISA). For information about the organization of the ISS, please visit this website: www.issa.org

7. National Security Institute (NSI) – National Security Institute: provides information on all types of security breach threats. The computer security part of this organization includes hazard announcements, research papers, information for supervisors, and information about regulatory documents and government security standards. Web address – nsi.org

8. SysAdmin, Audit, Network, Security (SANS) Institute – Institute of System Administrator, Audit, Network, and Security: offers information, training, research, and other resources for security professionals. Based on the SANS Institute Global Information Assurance Certification (GIAC) program, this organization offers a full training program in the United States and internationally. It provides online safety training along with paternity programs. SANS Internet Storm Center Institute (Internet Storm Center – isc.incidents.org), who founded. The Institute's website – www.sans.org

The threat of information security and its types. Objectives and conceptual framework for information security.

In general, the purpose of information protection can be expressed as follows:

- prevention of leakage, theft, distortion, falsification of information;
- prevention of threats to the security of the individual, society, and the state;

- prevention of illegal actions, such as deleting, modifying, damaging, copying, blocking information;
- prevention of other forms of illegal influence on information resources and information systems, ensuring the legal regime of documented information as an object of personal property;
- protection of the constitutional rights of citizens by maintaining the confidentiality and confidentiality of personal data contained in the information system;
- preservation of state secrets, ensuring the confidentiality of documented information in accordance with the law;
- ensuring the rights of subjects in information processes and in the design, development and application of information systems, technologies and means of their support.

The effectiveness of information protection is determined by its timeliness, activity, continuity and complexity. Comprehensive implementation of protective measures ensures the elimination of potentially dangerous channels of information leakage. It is known that only one open channel of information leakage dramatically reduces the effectiveness of the entire security system.

The concept of threats to protected information and its structure.

According to the general orientation, threats to information security are divided into:

- Threats to the development of the country's information, telecommunications and communications industry, to meet the needs of the domestic market, to bring its products to the world market, and to ensure the collection, storage and effective use of local information resources;

-Threats to the normal functioning of information and telecommunications systems implemented and created on the territory of the republic, the security of information resources. Therefore, the protection of information systems should be carried out taking into account the above information.

Conclusion

The study analyzed the security parameters in the protection of information systems. At the same time, organizations that provide information about the types and methods of repelling network attacks, threats to information security and their types, the concept and structure of threats to protected information were systematized.

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

References

1. Тутубалин П. И., Кирпичников А. П. Оценка криптографической стойкости алгоритмов асимметричного шифрования. Вестник технологического университета. Т.20, №10, с. 94-99, 2017.