International Journal of Academic Pedagogical Research (IJAPR)
ISSN: 2643-9123
Vol. 5 Issue 1, January - 2021, Pages: 70-73

Information Security Policy

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Information security refers to the protection of accidentally or intentionally affected information of a natural or artificial nature and the infrastructure that supports it. and can cause serious damage to information-supporting infrastructure.*

Keywords: Concept of information security, Information security policy, State system of information protection.

INTRODUCTION

The state system of information protection represents a set of agencies and executors, as well as objects of protection, which use information security techniques. This system is organized and operates in accordance with the legal, organizational and regulatory documents in the field of information security. At the same time, it is an integral part of the country's national security system and is aimed at protecting national security from internal and external threats in the field of information.

The concept of information security.

Information security refers to the protection of accidentally or intentionally affected information of a natural or artificial nature and the infrastructure that supports it. Such impacts affect information relationships, including information owners, information users and information. can cause serious damage to the infrastructure that supports protection.

METHODS

Information security policy

Measures to establish the Center for Development of Electronic Government and Information Security Centers under the State Committee for Communications, Information and Telecommunication Technologies of the Cabinet of Ministers of the Republic of Uzbekistan dated September 16, 2013 The centers were established and put into operation by the decision of the President of the Republic of Tajikistan.

The protection of information must ensure the prevention of damage caused by the voluntary loss of information (theft, tampering, falsification). Information security measures should be organized in accordance with applicable laws and regulations on information security and in the interests of information users. To ensure a high level of information protection requires the solution of complex scientific and technical problems and the improvement of security tools on a regular basis.

Today, there are three main principles that ensure information security: integrity of information, confidentiality of information, and access to information for all users with access rights; In addition, some areas of activity (law enforcement, defense and special structures, banking and financial institutions, information networks, public administration) have high requirements for the reliability of their information systems, depending on the importance and nature of the issues addressed in them. security requires special precautions.

The effectiveness of information security is determined by its timeliness, activity, continuity and complexity. Comprehensive protection measures eliminate dangerous channels through which information can be disseminated. However, a single channel of information that is left open can drastically reduce the effectiveness of the entire protection system.

There are three components that are interconnected in terms of information security in computer systems: information; hardware and software; attention is paid to service personnel and users.

The principles of information security can be divided into three groups: the use of information security in legal, organizational and technical intelligence protection, and the use of computer technology in information processing.

The practice of using information security systems shows that only complex information security systems can be effective.

In addition to the basic methods used by the user to protect information, the method of spiritual and educational protection of information plays a very important role. It is a person, an employee of an enterprise or organization, who is aware of confidential information, accumulates a lot of information in his memory, and in some cases can become a source of information leakage, and through his fault, others illegally access this information. will have. Educating the employee in the method of spiritual and enlightenment protection of information, carrying out special work with him aimed at the formation of certain qualities, views (patriotism, explaining the importance of information protection for him personally) and training in the rules and methods of information protection, the formation of practical skills in working with confidential media.

In crime prevention It is a complex system of licensing of organizations in the field of information security, including certification of information security tools and certification of information facilities on information security requirements, training, special communication systems, organization of research and development. The state system of information protection operates on the basis of the following laws and regulations:

- The Constitution of the Republic of Uzbekistan;

- Law on Protection of State Secrets;

- Law on Informatization;

- Law on Certification of Products and Services

- Law on Licensing of Certain Types of Activities

- Law on Standardization

- Law on Communications

- Law on Telecommunications

- Law on Guarantees and Freedom of Information

- Law on Principles and Guarantees of Freedom of Information

- Law on Electronic Document Management;

- Law on Electronic Digital Signature;

- Law on Electronic Commerce

- Decrees and resolutions of the President of the Republic of Uzbekistan;

- Resolutions of the Cabinet of Ministers of the Republic of Uzbekistan;

-Ministry, other institutions, agencies and other legal acts in the field of information security.

THANK YOU FOR YOUR ATTENTION !!!

RESULTS

In addition to the basic methods used by the user to protect information, the method of spiritual and educational protection of information plays a very important role. It is a person, an employee of an enterprise or organization, who is aware of confidential information, accumulates a lot of information in his memory, and in some cases can become a source of information leakage, and through his fault, others illegally access this information. will have. Educating the employee in the method of spiritual and enlightenment protection of information, carrying out special work with him aimed at the formation of certain qualities, views (patriotism, explaining the importance of information protection for him personally) and training in the rules and methods of information protection, the formation of practical skills in working with confidential media.

In crime prevention It is a complex system of licensing of organizations in the field of information security, including certification of information security tools and certification of information facilities on information security requirements, training, special

communication systems, organization of research and development. The state system of information protection operates on the basis of the following laws and regulations:

- The Constitution of the Republic of Uzbekistan;

- Law on Protection of State Secrets;

- Law on Informatization;

- Law on Certification of Products and Services

- Law on Licensing of Certain Types of Activities

- Law on Standardization

- Law on Communications

- Law on Telecommunications

- Law on Guarantees and Freedom of Information

- Law on Principles and Guarantees of Freedom of Information

- Law on Electronic Document Management;

- Law on Electronic Digital Signature;

- Law on Electronic Commerce

- Decrees and resolutions of the President of the Republic of Uzbekistan;

- Resolutions of the Cabinet of Ministers of the Republic of Uzbekistan;

-Ministry, other institutions, agencies and other legal acts in the field of information security.

DISCUSSION

The protection of information must ensure the prevention of damage caused by the voluntary loss of information (theft, tampering, falsification). Information security measures should be organized in accordance with applicable laws and regulations on information security and in the interests of information users. To ensure a high level of information protection requires the solution of complex scientific and technical problems and the improvement of security tools on a regular basis.

Today, there are three main principles that ensure information security: integrity of information, confidentiality of information, and access to information for all users with access rights; In addition, some areas of activity (law enforcement, defense and special structures, banking and financial institutions, information networks, public administration) have high requirements for the reliability of their information systems, depending on the importance and nature of the issues addressed in them. security requires special precautions.

CONCLUSION

Today, there are three main principles that ensure information security: integrity of information, confidentiality of information, and access to information for all users with access rights; In addition, some areas of activity (law enforcement, defense and special structures, banking and financial institutions, information networks, public administration) have high requirements for the reliability of their information systems, depending on the importance and nature of the issues addressed in them. security requires special precautions.

The effectiveness of information security is determined by its timeliness, activity, continuity and complexity. Comprehensive protection measures eliminate dangerous channels through which information can be disseminated. However, a single channel of information that is left open can drastically reduce the effectiveness of the entire protection system.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

6 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

7 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

8 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

9 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

10 See Vexov V.B. Computer prestupleniya: sposoby sovershеniya i raskrytiya. - M., 1996. –S.163.

11 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

12 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

13 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

14 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

15 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.