International Journal of Academic Pedagogical Research (IJAPR)
ISSN: 2643-9123
Vol. 5 Issue 1, January - 2021, Pages: 7-14

International and National Legal Base in the Field Of Information Security

Usmonov Makhsud

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

Abstract: *Legal provision of information security is a set of legislative acts, normative legal acts, rules, instructions, manuals that must be implemented in the information security system. The issue of legal support of information security is currently being actively studied, both in practice and in legislation.ISO / IEC 27001: 2005 - "Information technology. Security methods. Information security management systems. Requirements ". This International Standard consists of a model and requirements for the development, implementation, operation, monitoring, analysis, maintenance and improvement of an information security management system (IMS). The introduction of AIBT should remain a strategic decision of the organization. Security needs, objectives, processes used, and the size and structure of the organization should be taken into account in the development and implementation of the WTO. The AXBT and its ancillary systems are expected to change over time.*

Keywords: Legal, law, acts, standard, process approach, management system, risk assessment, security methods, risk management, own DSt, ISO / IEC, national standards, GOST 28147-89 .

INTRODUCTION

1. International standards in the field of information security

2. National standards in the field of information security

3. Regulatory documents in the field of information security

1. International standards in the field of information security

Legal support of information security is a set of legislative acts, normative-legal documents, rules, instructions, manuals, which must be implemented in the information security system. The issue of legal support of information security is currently being actively studied, both in practice and in law.

ISO / IEC 27001: 2005 - "Information technology. Security methods. Information security management systems. Requirements ". This International Standard consists of a model and requirements for the development, implementation, operation, monitoring, analysis, maintenance and improvement of an information security management system (IMS). The introduction of AIBT should remain a strategic decision of the organization. Security needs, objectives, processes used, and the size and structure of the organization should be taken into account in the development and implementation of the WTO. The AXBT and its ancillary systems are expected to change over time. Also, the scale of the AJBT expansion will depend on the needs of the organization, for example, a simple situation will require a simple solution for the AHBT. This standard can be used internally and externally to assess compliance.

METHODS

Process approach. This standard focuses on the application of a process approach to the development, implementation, operation, monitoring, analysis, maintenance, and improvement of the organization.

This standard simulates the planning - implementation - verification - action ["Rlan-Do-Check-Act" (PDCA)] that can be used in the development of each AXBT process.

This model demonstrates how the AHBT uses information security requirements and expected outcomes as input data, and obtains information that demonstrates that the declared requirements and expected outcomes are met as a result of the necessary actions and processes.

1-for example. Violations of information security may not be required to cause significant financial losses and / or any difficulties for the organization.

Example 2 For any serious conflict, such as a breach of an e-commerce site, the organization must have professionals with sufficient knowledge and experience to minimize the consequences of the breach.

Figure 19.1. Apply the PDCA model to AXBT processes.

Compatibility with other management systems. This standard is another management standard

ISO 9001: 2000 and ISO 14001: 2004 to improve compatibility and integration with

coordinated with standards. All in one properly designed management system

able to meet the requirements of these standards. Table 19.1 shows the ISO of this standard

Interrelationships with 9001: 2000 and ISO 14001: 2004 are shown.

This standard applies to the relevant requirements of other management systems that apply to the organization

allows you to customize or integrate with.

Information is an asset that has the same value as other important assets of the business and therefore must be properly protected. This is especially important in an ever-evolving practical work environment with interactions. At present, as a result of these interactions, information threats and vulnerabilities increase the number and variety of

The need for information security. Information and the processes that store it, information systems and network infrastructure are invaluable assets of a business. Identifying, providing, maintaining, and improving information security is critical to ensuring an organization is competitive, valuable, profitable, compliant with the law, and has a good business reputation.

Identify information security requirements. It is important for an organization to define its information security requirements based on three important factors:

- Threats to the organization's assets are identified by assessing the risks taken by the organization, taking into account the global business strategy and the goals of the organization, the vulnerability of the relevant assets and the likelihood of threats, as well as the possible consequences;

- other factors include the organization, its trading partners, contractors and service providers, the legal requirements to be met, the requirements of the legislation, regulatory and contractual requirements, as well as the socio-cultural environment of these parties;

Another factor is the special set of principles, goals and requirements developed by the organization to ensure its operation.

Information security risk assessment. Information security requirements are determined through regular risk assessments. The cost of information security management measures should be commensurate with the amount of damage that could be caused to the organization as a result of an information security breach.

Selection of information security management measures. Once information security requirements have been established and risks identified, information security management measures should be selected and implemented to ensure that risks are reduced to an acceptable level. These measures can be selected from this standard, from other sources, and measures can be developed to meet the specific needs of the organization in information security management. The choice of information security management measures depends on organizational decisions based on risk acceptance criteria, risk assessment options, and an overall approach to risk management in the organization. This choice should be coordinated with equivalent national and international legislation and norms.

A base point for the introduction of information security. Specific information security management measures can be adopted as guidelines for information security management and serve as a basis for its implementation. Such measures are based on the basic requirements of the legislation or can be adopted as a generally accepted practice in the field of information security.

From a legal point of view, the main measures to manage information security are:

- data protection and confidentiality of personal information;

- protection of organizational documents;

- The right to own intellectual property.

Information security management measures, which are considered to be a common practice in the field of information security, include:

- documentation of information security policy;

- distribution of information security responsibilities;

- training on information security rules;

- Proper processing of information in applications;

- technical vulnerability management strategy;

-management of the organization's continuity;

-management of information security conflicts and improvements.

The most important factors of success. Experience has shown that the following factors are crucial for the successful implementation of information security measures in an organization:

- compliance of information security objectives, policies and procedures with business objectives;

-compatibility of the approach to the introduction, promotion, monitoring and modernization of the security system with the corporate culture;

-real support and interest from management;

- clear understanding of safety requirements, risk assessment and risk management;

- Ensuring that managers and employees of the organization understand the need for effective marketing of information security, as well as the application of information security measures;

-provide information security policy guidelines, recommendations and relevant standards to all employees and subcontractors;

-conditions for financing information security management measures;

-ensure the necessary level of education and training;

- approval of the effective process of information security conflict management;

-olc a comprehensive and balanced system of indicators used to evaluate the effectiveness of information security management and suggestions from executors to improve it.

Develop organizational guidelines. This standard should be considered as a starting point for the development of guidelines for the specific needs of the organization. Not all guidelines and measures in this International Standard are applicable.

Additionally, additional measures not covered by this standard may be required. In this case, it may be helpful to keep references from multiple parties at the same time, which facilitates compliance checks by auditors and business partners.

UzDStISO / IEC 27005: 2013 - “Information technology. Security tips. Information Security Risk Management ”

This standard contains recommendations for managing information security risks in the organization.

This standard supports the general concepts set out in ISO / IEC 27001 and is designed to ensure that information security is based on the same risk management approach.

To fully understand this standard, it is necessary to know the concepts, models, processes and terminology described in Oz DSt ISO / IEC 27001 and Oz DSt ISO / IEC 27002.

This International Standard applies to all types of organizations (for example, commercial enterprises, government agencies, non-profit organizations) that plan to implement risk management that may undermine the organization's information security.

This standard uses references to the following standards:

Own DSt ISO / IEC 27001: 2009 Information Technology. Security methods. Information security management systems. Requirements.

Own DSt ISO / IEC 27002: 2008 Information Technology. Security methods. Practical rules of information security management

UzDStISO / IEC 27006: 2013 - “Information technology. Security tips. Audit of information security management systems and requirements for their certification bodies "

Its DSt ISO / IEC 17021 is a standard that sets criteria for bodies that audit and certify corporate governance systems. If these bodies are accredited as compliant with their DSt ISO / IEC 17021 in order to conduct certification and audit of information security management systems (IMS) in accordance with ISO / IEC 27001, then O 's DSt ISO / IEC 17021 requires guidance and additional requirements. They are presented in this standard.

The text of this standard repeats the structure of Oz DSt ISO / IEC 17021, the additional requirements specific to AXBT and the Guide to the application of Oz DSt ISO / IEC 17021 for certification of AXBT, “AX »Is indicated by the abbreviation.

The term "required" is used in this International Standard to indicate mandatory conditions that reflect the requirements of ISO / IEC 17021 and ISO / IEC 27001. The term "required" is used to describe the conditions under which a certification body is expected to accept, even if it is a guide to the application of these requirements.

ISO / IEC 15408-1-2005 - “Information technology. Security methods and tools. Criteria for assessing the safety of information technology "

ISO / IEC 15408-2005 International Standard ISO / IEC JTC 1 “Information Technology” Joint Technical Committee, SC 27 “IT Security Methods and Tools” Subcommittee. A text similar to ISO / IEC 15408-2005 has been published by the sponsors of the General Criteria project as version 2.3 (referred to as 2.3 UM) as “General Criteria for Assessing Information Security”.

The second edition of the standard repeals the first edition (ISO / IEC 15408: 1999), which had to be technically revised, and replaces it.

Similar to ISO / IEC 15408-2005, your DSt consists of the following sections under the general heading ISO / IEC 15408 “Information Technology - Security Methods and Tools - Information Technology Security Criteria”:

Part 1: Introduction and general model;

Part 2: Functional Requirements for Security;

Part 3: Security Trust Requirements.

Its DSt ISO / IEC 15408 allows comparison of the results of independent safety assessments. This is achieved by providing a common set of requirements for the security functions of IT products and systems and the confidence measures applied to them in security assessments.

Develop your own DSt ISO / IEC 15408 with security features for IT products and systems as well as in the procurement of commercial products and systems with such functionality useful as a guide. The evaluation of such an IT product or system is called an evaluation object (EO). Such BOs include, for example, operating systems, computer networks, distributed systems, and applications.

2. National standards in the field of information security

The standards presented in this section are based on modern requirements, based on the laws of the Republic of Uzbekistan "On electronic digital signature" and "On electronic document exchange".

These standards define the general algorithm for encrypting information and the rules of data encryption for computer networks, telecommunications, individual computing systems and computer information processing systems.

Oz DSt 1092: 2009 - “Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature ”

This standard defines an electronic digital signature algorithm (ERIA) for the formation and validation of an electronic digital signature (EDS) under a given message (electronic document) transmitted over unsecured public telecommunications channels.

The standard is intended for use in information processing systems for various purposes in the formation and validation of electronic digital signatures.

References to the following standards are used in this standard:

Oz DSt 1047: 2003 Information technology. Terms and definitions.

UzDSt 1109: 2006 Information technology. Cryptographic protection of information. Terms and definitions.

Own DSt 1105: 2009 - “Information technology. Cryptographic protection of information. Data Encryption Algorithm ”

This Data Encryption Algorithm (ISA) standard refers to a cryptographic algorithm designed to protect electronic data. MSHA is a symmetric block cipher that is used to encrypt information and convert it to source text. MShA can use a 256 or 512 bit cryptographic key to decrypt a 256-bit block of data and to decrypt the ciphertext into the original text.

The standard defines the rules of data encryption by installing a single algorithm for encrypting information in computer networks, computer systems and information processing systems on computers.

Data encryption algorithms are designed to be implemented in software, hardware or hardware-software cryptographic modules.

Organizations, enterprises and institutions can use this standard in the implementation of cryptographic protection of data stored and transmitted on computer networks, individual computing systems or computers.

References to the following standards are used in this standard:

UzDSt 1047: 2003 Information technology. Terms and definitions.

UzDSt 1109: 2006 Information technology. Cryptographic protection of information. Terms and definitions.

Own DSt 1106: 2009 - “Information technology. Cryptographic protection of information. Hashing function ”

This standard provides a hashing function for any sequence of binary characters used to perform electronic digital signature (hereinafter - EDS) procedures in the transmission, processing and storage of information in cryptographic methods of information processing and protection, including automated systems (hereinafter - EDS). - Defines the XF) algorithm and the calculation procedure.

References to the following standards are used in this standard:

GOST 28147-89 Information processing systems. Zashchita kriptograficheskaya. Algorithms kriptograficheskogo preobrazovaniya

Oz DSt 1047: 2003 Information technology. Terms and definitions

Own DSt 1109: 2006 Information Technology. Cryptographic protection of information. Terms and definitions

Own DSt 1204: 2009 - “Information technology. Cryptographic protection of information. Security requirements for cryptographic modules "

This standard specifies the unique security requirements for public and symmetric key cryptographic modules and is intended for the design, development, sale (delivery) and use of cryptographic information protection tools. The standard specifies the security requirements for computers, telecommunications networks, individual computing systems, or cryptographic modules that protect confidential information stored and transmitted on a computer.

References to the following standards are used in this standard:

Own DSt 1092: 2005 Information Technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signatures.

Own DSt 1105: 2006 Information Technology. Cryptographic protection of information. Data encryption algorithm.

Own DSt 1109: 2006 Information Technology yasi. Cryptographic protection of information. Terms and definitions.

3. Regulatory documents in the field of information security

RH 45-215: 2009 - Guidance document. Regulations on information security in the data transmission network. This document is implemented in place of N 100: 2002 "Regulations on ensuring information security in the national data transmission network" and regulates information security in the data transmission network (MUT). defines the main goals, tasks, functions and organizational and technical measures for maintenance.

RH 45-185: 2011-Guidance document. Procedure for developing information security programs of public authorities and administration. This document replaces RH 45-185: 2006 and sets out the procedure for developing information security programs for public authorities and administration.

The document sets out the standard requirements for the goals, objectives, structure and list of activities to be developed under information security programs.

RH 45-193: 2007 - Guidance document. Procedure for determining the level of information security of providers' servers and technical areas for hosting government websites. This document sets out a standard procedure for determining the level of information security of providers' servers and technical areas for hosting government websites.

The requirements of this document are mandatory for all businesses that provide hosting services for government websites.

TSt 45-010: 2010 - Network standard. Information security in the field of communication and information. Terms and definitions. This network standard was registered by the State Center for Standardization, Metrology and Certification under the Cabinet of Ministers of the Republic of Uzbekistan (Uzdavstandart) on August 6, 2002 under No. 112/066 TSt 45.010: 2002 “Otraslevoy standart. Informatsionnaya bezopasnost v sfere svyazi i informatizatsii. Terms and Definitions ”defines the basic terms and definitions of information security in the field of communications and information.

RESULTS

The second edition of the standard repeals the first edition (ISO / IEC 15408: 1999), which had to be technically revised, and replaces it.

Similar to ISO / IEC 15408-2005, your DSt consists of the following sections under the general heading ISO / IEC 15408 “Information Technology - Security Methods and Tools - Information Technology Security Criteria”:

Part 1: Introduction and general model;

Part 2: Functional Requirements for Security;

Part 3: Security Trust Requirements.

Its DSt ISO / IEC 15408 allows comparison of the results of independent safety assessments. This is achieved by providing a common set of requirements for the security functions of IT products and systems and the confidence measures applied to them in security assessments.

Develop your own DSt ISO / IEC 15408 with security features for IT products and systems as well as in the procurement of commercial products and systems with such functionality useful as a guide. The evaluation of such an IT product or system is called an evaluation object (EO). Such BOs include, for example, operating systems, computer networks, distributed systems, and applications.

2. National standards in the field of information security

The standards presented in this section are based on modern requirements, based on the laws of the Republic of Uzbekistan "On electronic digital signature" and "On electronic document exchange".

These standards define the general algorithm for encrypting information and the rules of data encryption for computer networks, telecommunications, individual computing systems and computer information processing systems.

Oz DSt 1092: 2009 - “Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature ”

This standard defines an electronic digital signature algorithm (ERIA) for the formation and validation of an electronic digital signature (EDS) under a given message (electronic document) transmitted over unsecured public telecommunications channels.

DISCUSSION

Information is an asset that has the same value as other important assets of the business and therefore must be properly protected. This is especially important in an ever-evolving practical work environment with interactions. At present, as a result of these interactions, information threats and vulnerabilities increase the number and variety of

The need for information security. Information and the processes that store it, information systems and network infrastructure are invaluable assets of a business. Identifying, providing, maintaining, and improving information security is critical to ensuring an organization is competitive, valuable, profitable, compliant with the law, and has a good business reputation.

Identify information security requirements. It is important for an organization to define its information security requirements based on three important factors:

- Threats to the organization's assets are identified by assessing the risks taken by the organization, taking into account the global business strategy and the goals of the organization, the vulnerability of the relevant assets and the likelihood of threats, as well as the possible consequences;

- other factors include the organization, its trading partners, contractors and service providers, the legal requirements to be met, the requirements of the legislation, regulatory and contractual requirements, as well as the socio-cultural environment of these parties;

Another factor is the special set of principles, goals and requirements developed by the organization to ensure its operation.

CONCLUSION

Selection of information security management measures. Once information security requirements have been established and risks identified, information security management measures should be selected and implemented to ensure that risks are reduced to an acceptable level. These measures can be selected from this standard, from other sources, and measures can be developed to meet the specific needs of the organization in information security management. The choice of information security management measures depends on organizational decisions based on risk acceptance criteria, risk assessment options, and an overall approach to risk management in the organization. This choice should be coordinated with equivalent national and international legislation and norms.

A base point for the introduction of information security. Specific information security management measures can be adopted as guidelines for information security management and serve as a basis for its implementation. Such measures are based on the basic requirements of the legislation or can be adopted as a generally accepted practice in the field of information security.

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

6 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.

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

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

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

10 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.

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

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

13 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 oxranyaемоy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

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