Chemical Technology, Control and Management

Volume 2020 | Issue 4 Article 11

8-29-2020

ANALYSIS OF INFORMATION SECURITY SYSTEM STANDARDS AND KEY ASPECTS OF SECURITY CONTROL

Abduhalil Abdujalilovich Ganiyev
Tashkent University of Information Technology named after Muhammad al-Khwarizmi Address: 108, Amir Temur street, Tashkent city, Republic of Uzbekistan E-mail: ganiyev_ab@mail.ru, Phone:+998-99-835-67-30, ganiyev_ab@mail.ru

Recommended Citation

Ganiyev, Abduhalil Abdujalilovich (2020) "ANALYSIS OF INFORMATION SECURITY SYSTEM STANDARDS AND KEY ASPECTS OF SECURITY CONTROL," *Chemical Technology, Control and Management*: Vol. 2020 : Iss. 4 , Article 11.
DOI: https://doi.org/10.34920/2020.4.71-74
Available at: https://uzjournals.edu.uz/ijctcm/vol2020/iss4/11

ISSN 1815-4840, E-ISSN 2181-1105
Himičeskaâ tehnologiâ. Kontrolʹ i upravlenie
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2020, №4 (94) pp.71-74. https://doi.org/10.34920/2020.4.71-74
International scientific and technical journal
journal homepage: https://uzjournals.edu.uz/ijctcm/
Since 2005

UDC 004.056

ANALYSIS OF INFORMATION SECURITY SYSTEM STANDARDS AND KEY ASPECTS OF SECURITY CONTROL

Ganiyev Abdukhalil Abdujalilovich

Tashkent University of Information Technology named after Muhammad al-Khwarizmi
Address: 108, Amir Temur street, Tashkent city, Republic of Uzbekistan
E-mail: ganiyev_ab@mail.ru, Phone:+998-99-835-67-30;

Abstract: *The standards of the information security management system (IMS) are considered and the main aspects of information security management are studied, in particular the international standard ISO/IEC 27001, the Process approach to the management of IS, the stages of development of the information security management system. The measures taken for the organization of information security management systems are defined. Organizational measures include the implementation of information security management systems in the organization.*

Keywords: *information system, information security tools, intelligent decision support tools, ISO/IEC 27001, information security management systems .*

Аннотация: *Ахборотни муҳофаза қилиш тизимининг стандартлари кўриб чиқилган ва ахборотни муҳофаза қилишни бошқаришнинг асосий жиҳатлари, хусусан, ISO/IEC 27001 халқаро стандарти, ахборотни ҳимоялашни бошқаришга жараёнли ёндашув, ахборотни муҳофаза қилиш тизимини ишлаб чиқиш босқичлари ўрганилган. Ахборотни ҳимоялашни бошқариш тизимларини ташкиллаштириш учун қилиниши керак бўлган чора-тадбирлар аниқланган. Ташкилотда ахборотни ҳимоялашни бошқариш тизимларини жорий этиш учун ташкилий чоралар келтирилган.*

Таянч сўзлар: *ахборот тизими, ахборотни муҳофаза қилиш воситалари, қарорларни қабул қилишни қўллаб-қувватловчи интеллектуал воситалар, ISO/IEC 27001, ахборотни муҳофаза қилиш менежменти тизими.*

Аннотация: *Рассмотрены стандарты системы менеджмента защиты информации (ЗИ) и изучены основные аспекты управления защитой информации, в частности Международный стандарт ИСО/МЭК 27001, Процессный подход к менеджменту ЗИ, этапы разработки системы менеджмента защиты информации. Определены меры, предпринимлемые для организации систем управления защитой информации. Организационные меры включают внедрение систем управления защитой информации в организации.*

Ключевые слова: *информационная система, средств защиты информации, интеллектуальных средств поддержки принятия решений, ИСО/МЭК 27001, системы менеджмента защиты информации.*

Introduction

Currently, the leadership of companies, government agencies and organizations has realized the importance of the problem of ensuring the protection of information.

However, the constant development of new methods and means of special software and hardware actions leads to the recent trend of constant growth in the number of cases of successful implementation of attacks [1].

The increasing complexity of modern information systems (IS) leads to the appearance in them of an increasing number of network devices and heterogeneous means of protection (SRH) of information, which generate a huge number of security events: tens or even hundreds of thousands of notifications per day [2], which the security administrator is physically impossible. One firewall (ITU) can generate more than 1 Gigabyte of data per day, a sensor anomaly detection system (SOA) - up to 50 thousand messages, of which up to 95% are false alarms [3]. In addition, it is almost impossible to

compare signals about security events from different systems; at the same time, responses to attacks must be taken immediately.

It is obvious that the technological process significantly outstrips the theoretical understanding of what is happening in the field of the creation and application of information technologies and the use of new communication opportunities. Consequently, there is a reason to make an assumption about the incomplete adequacy of the efforts being made to the existing tasks of information protection, not only in practical terms, but also in theoretical terms [4].

Main aspects of information security management

The main shortcomings of the systems of protection, information used everywhere are determined by the established rigid principles of building architecture [5] and the use of mainly defensive or offensive strategies of protection against known and most dangerous threats.

To solve the problem formulated above and the successful use of modern information technologies, it is necessary to efficiently and reliably manage not only networks, but also the information protection system, network security means [6]. Methods are required that make it possible to promptly control changes in the operating environment and prevent IS violations by managing network equipment and protection means, and a reasoned approach to increasing the effectiveness of IS measures is the development of intelligent decision support (IDS) for information security management.

The management of the IS has many aspects, presented in a structured form in Figure 1, and only with an integrated approach to solving this problem can a truly secure environment for the functioning of an enterprise's IS be created.

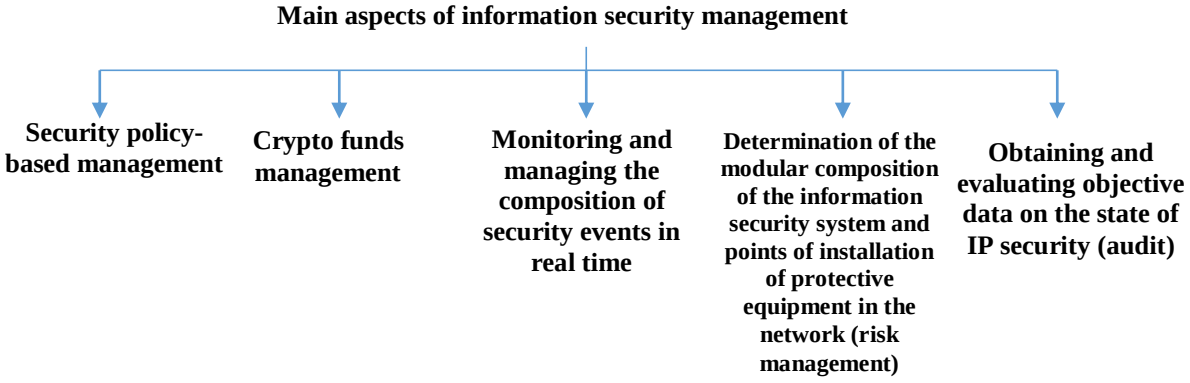

Figure 1. ***Main aspects of information security management.***

International Standard ISO/IEC 27001 [7] has been prepared to provide a model for the creation, implementation, operation, ongoing monitoring and analysis, maintenance and improvement of an information security management system (ISMS). The design and implementation of an organization's ISMS is influenced by its needs and objectives, security requirements, and the size and structure of the organization. An organization needs to identify and manage various activities in order to function effectively.

The process approach to IP management in this standard helps to emphasize the importance of the following points:

• establishing policies, objectives, processes and procedures related to managing risks and improving information security to deliver results consistent with the organization's objectives;

• implementation and operation of IP management policies, controls, processes and procedures;

• evaluating and, where applicable, measuring the performance of the processes in relation to the policy, objectives and practical experience in the field of RF management, their analysis;

• implementation of corrective and preventive actions based on the results of internal audit and analysis to achieve continuous improvement of the RF management.

This International Standard defines the requirements for the establishment, implementation, operation, ongoing monitoring, analysis, maintenance and improvement of an ISMS in the context of an organization's risks. The ISMS is designed to ensure that adequate security controls are selected.

ISMS includes: organizational structure, policy, planning activities, procedures, processes, resources.

ISMS is created in order to design an ISS, implement, operate, constantly monitor, analyze, improve information security.

To create an ISMS, an organization must do the following:

• define the boundaries of the ISMS;

• Establish principles of action for RFI, taking into account legal and regulatory requirements and protection objectives;

• establish criteria by which the significance of the risk will be assessed;

• define a risk assessment methodology that is appropriate for ISMS and meets regulatory requirements; the selected risk assessment methodology should ensure that the risk assessments produce comparable and reproducible results;

• identify risks (assets, threats and negative impacts that can lead to loss of confidentiality, integrity and availability of these assets, vulnerabilities);

• assess the significance of the risk (assess the likelihood of a security breach in the light of prevailing threats and vulnerabilities, assess the levels of risk, determine whether the risks are acceptable or require treatment);

• identify opportunities for risk treatment (possible actions include applying appropriate controls or accepting risks);

• select controls for risk treatment, taking into account the criteria for risk acceptance;

• obtain management approval for the implementation of the ISMS and prepare a statement of applicability (includes control objectives, controls, reasons for choosing them).

During the implementation and operation of the ISMS, the organization should perform the following:

• formulate a risk treatment plan, which would identify suitable management actions, resources, responsibilities, implement this plan, taking into account funding;

• implement controls in order to achieve control objectives;

• implement procedures and other controls that can enable rapid detection of an event in the information security system and response to incidents in the information security system.

• quickly identify ongoing and successful security breaches and incidents;

• detect events in the information security system and prevent incidents by using indicators;

• measure the effectiveness of controls to verify that requirements have been met;

• update the protection plans to take into account the data obtained during the ongoing monitoring and analysis activities;.

Conclusion

The ISMS documentation should include, among other documents, a description of the risk assessment methodology, a risk treatment plan, and documented procedures necessary for the organization to ensure effective planning.

The analysis of existing security management standards allows us to conclude that their goal is to form general concepts and models of security management; however, the standards do not develop specific approaches to safety management

References:

1. G.A.Popov, A.G.Popov, N.D.Shishkin, M.F.Rudenko, “The conceptual scheme of information security in the object protection model” *Вестник АГТУ.Сер.: Управления, вычислительная техника и информатика*, no. 4, pp. 45-53, 2017. DOI: 10.24143/2072-9502-2017-4-45-53
2. “Library of electronic resources. A priori suspicion” Access mode: http://www.safensoft.ru/security.phtml -P 366, free

3. “Library of electronic resources. Enterprise Security”, Access mode: http://arcsight.com/product_info_esm.htm, free.
4. S.Nesterov, *“Osnovy informatsionnoi bezopasnosti” [Fundamentals of information security]*, Saint-Petersburg, Lan' Publ, 2016. 324 p. (in Russian).
5. E.K.Baranova, A.V.Babash, *“Informatsionnaia bezopasnost' i zashchita informatsii” [Information security and information protection]*, Moscow, ITs RIOR, NITs INFRA-M, 2016. 322 p.
6. A.V.Galitskiy, S.D.Ryabko, V.F.Shangin, “Information security in the network - analysis of technologies and synthesis of solutions”, Moskva: DMK Press, 616 p. (Series "Administration and Protection").
7. GOST ISO / IEC 27001 [Electronic resource]. - Access mode: http://www.specon.ru/files/ISO27001.pdf, free.