MEST Journal
DOI 10.12709/mest.07.07.02.09

THE ORGANIZATIONAL PRINCIPLES OF INFORMATION PROTECTION MANAGEMENT SYSTEM REALIZATION

Valeryi Sereda
Department of the National Police of Ukraine in Lviv, and Department of Administrative and Legal Disciplines of the Lviv State University of Internal Affairs, Lviv, Ukraine

Zinaida Zhyvko
Department of Management of the Lviv State University of Internal Affairs, Lviv, Ukraine

Olga Balynska
Department of Theory and History of State and Law, Constitutional and International Law, Lviv State University of Internal Affairs, Lviv, Ukraine

Taras Rudyi
Department of Informatics of the Lviv State University of Internal Affairs, Lviv, Ukraine

JEL Category: **G32, H12, L86**

Abstract

In the modern world, information protection is a driving force at the state level. Therefore, it is necessary to effectively form the system of control of information protection following international standards. The objective of the paper is an explanation of the importance of aligning of the existing regulatory framework with the requirements of the international ISO/IEC standards for the development of information security policy and risk assessment in information protection. In the paper, there are discussed protection (information technology and management of the use of information security management system), and security (for information technology, security techniques, requirements for audit and certification bodies, information protection). The management of information flows between users, processes, and objects' needs to be carried out only by specially authorized users (administrators). The article clarifies that the existing regulatory framework should be substantially changed because it does not specify requirements for the development of information security policies and information protection (IP) risk assessment. Four basic security criteria are presented: accessibility, integrity, confidentiality, and observation. In conclusions, there is

Address of the corresponding author:
Zinaida Zhyvko
professor2007@ukr.net

proposed adoption of ISO/IES standards series 27000 to get an opportunity to legally participate in the state or private certification of technical systems for information protection (TZI) or develop their own qualitatively new security standards and policies.

Keywords: *information, regulatory framework, the legislation of Ukraine, management system, security system, international standard, risk, safety, protection, management of information.*

1 INTRODUCTION

Incorporation of legislation of Ukraine and the structure of standard and legal acts of Ukraine in the field of technical information security that are obligatory to performance, at the level of the legal doctrine, can be delivered as follows: Constitution of Ukraine; laws of Ukraine; decrees and orders of the President of Ukraine; resolutions and orders of Cabinet of Ministers of Ukraine; standard and legal acts of the Security Service of Ukraine, Public service of special connection and information protection (DSSZTZI) of Ukraine; international agreements of Ukraine concerning technical information protection, consent on obligatory performance of which is provided by the Supreme Soviet of Ukraine.

The regulatory and legal basis of the provision of IP in IS of NP subsections of Ukraine constitutes: Constitution of Ukraine; Resolution of the Supreme Soviet of Ukraine "On the concept of national security of Ukraine"; Laws of Ukraine "On information", "On scientific and technical information", "On the state secret", "On information protection of the information telecommunication systems", "On access to public information", "On protection of personal data", Resolution of Cabinet of Ministers of Ukraine "On approval of rules of information protection in informational, telecommunication and information and telecommunication systems".

A series of normative documents of the system of technical information protection is developed in Ukraine, the basis of which is ND TZI 2.5-004-99 "Criteria estimation of information protection of the computer systems from unauthorized access". This document is used to design and create complex systems of information protection (CSIP) of the state information resources including the IP system, in which information with limited access is processed.

However, any methodology used during CSIP design must be compatible with the main modern standards, such as ISO/IEC of a series 27000.

Therefore, organizational and legal principles of IP system of IS of subsections of National police of Ukraine must be formed according to recommendations of international standards and with the observance of provisions of the current legislation of Ukraine.

Such standards are:

- ISO/IEC 27001:2013 Information technologies. Protection methods. Information protection management systems;
- ISO/IEC 27002:2005 information technologies. Protection methods. The code of practice for information protection management;
- ISO/IEC 27003:2010 Information technologies. Protection methods. The management of usage of the system of management of information protection;
- ISO/IEC 27004:2009 Information technologies. Protection methods. Measurement;
- ISO/IEC 27005:2008 Information technologies. Safety methods. Risk management of information protection;
- ISO/IEC 27006:2007 Information technologies. Safety methods. Requirements to audit and certification bodies of information protection management systems (ISO/IEC 27001:2013), (ISO/IEC 27002:2013(en)), (ISO/IEC 27003:2017(en)), (ISO/IEC 27004:2016), (ISO/IEC 27005:2018), and (ISO/IEC 27006:2015).

2 ANALYSIS

In world practice, the development of technical systems of information protection (TZI) was parallel to the creation of standardization as a part of information protection management. The result of this was an approval of the international standard ISO/IEC 27001:2005, and later ISO/IEC 27001:2013 on the introduction of the information protection management system (IPMS). The standard allows organizing correctly the process of protection of information assets and risk management for these assets. For quality control of the process of management of information

protection, the Institute of certification was introduced. The certificate has an international status.

According to the requirements of the standard the developing process of IPMS includes such stages: planning – a stage of planning provides the correct task to a context and scale of IPMS, risks estimation and the corresponding plan of the processing of these risks; realization – the stage introduces ready decisions which were defined at a planning stage; the analysis of protection – an estimation stage of efficiency and reliability of functioning of the created IPMS, carrying out of IP audit, identification of shortcomings; reaction – a stage of performance of the correcting actions for improvement of IPMS functioning. The reaction requires primary investment, documentation activity, formalization of the risk management approach, the definition of analysis methods.

As the main objects of the IPMS functioning area, the following types of assets are considered:

- **informational assets**: information and data that are arbitrarily, stored, processed, transferred and announced (it is necessary to refer to this type the knowledge of workers, databases and the systems of biometric identification, documentation, methodical materials, descriptions of procedures, information on physical persons);
- **software**: applied software, the system software, the service software, and any other software, irrespective of a receiving form (purchase, own developing, or such that is freely extended) which is used by workers for work and in the process of interaction with other services;
- **physical assets**: workers, hardware of computer networks and network technologies, servers, workstations, firewalls, telecommunication equipment, communication equipment), accommodation, production equipment, technical means;
- **service assets:** information and communication services (corporate computer networks of a special purpose, Internet, E-mail, special communication channels), other technical services (heating, lighting, alarm systems and monitoring), all services connected with receiving, granting, usage, transfer and destruction of assets, all legal entities and individuals, organizations, institutions and enterprises (as well as their workers) to which certain services are transferred as IT outsourcing.

For each asset possible risks and ways of their minimization are defined, that is, the usage of risk-oriented approach is recommended.

For the processes of the System of Information Security Management (IPMS) the model PPCA are applied (plan - perform - check - act) which uses 5 principles of IP management realization: 1. Establishment of the centralized administration. 2. Authentication of the objects, subjects, and assets of IS. 3. Authorization of the objects, subjects, and assets of IS. 4. Risks analysis and operating influences formation. 5. Achievement of a necessary level of workers preparation.

An essential factor of effective implementation of these principles is the connecting cycle of activity which guarantees that IPMS is constantly directed to the current risks. It is important to timely estimate the existence of risks connected with the safety of IS.

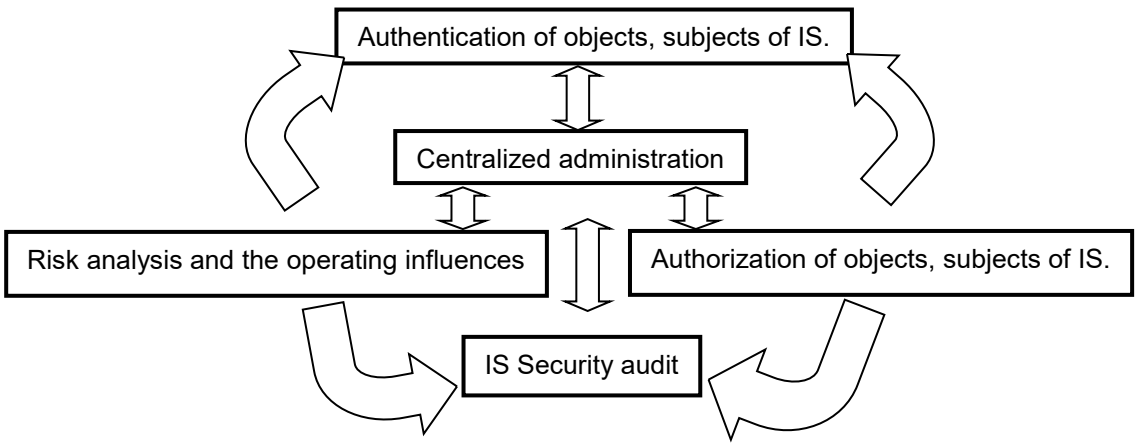

Fig. 1. The organizational principles of information protection management system realization

The efficiency of the control devices consists in estimation level due to different researches and the audit inspections. The obtained results provide an approach to the subsequent estimation of risks and define necessary changes in protection policies and control devices. All these actions are administered and coordinated in a centralized way, which is in the information systems of IPMS administrative management of access, is realized. The organizational principles of IPMS realization are given in fig. 1.

According to the authors, the estimation of the risk has to be carried out according to four main criteria of safety:

- **availability** – ensuring a continuous access to the information and accompanying assets of IS, services according to the rights conferred to users in a minimum necessary volume;
- **integrity** – protection of accuracy/correctness and completeness of assets and methods of an information processing;
- **confidentiality** – ensuring the availability to information assets only to officially authorized users in minimum necessary volume;
- **observation** – ensuring the possibility of definition – who, what and when has operated with or another information asset (ensuring the principle of not refusal of performed actions).

It means that the management of information streams between users, processes, objects, and subjects is carried out only by specially authorized users (administrators). Ordinary users cannot change the access rights of users to processes and passive objects and also perform any other functions of the management of IPMS means.

It should be noted that though all IPMS means in standards and normative documents are important, but the application of control facilities must observe the risks and possible threats for a concrete IS.

All procedures of providing IM must be addressed, that is, for each procedure, there has to be a certain list of users, performers and also the list of IS information assets which require their application.

Estimation of efficiency of the IPMS procedures, as a rule, is carried out according to the results of security audit and checks, the quality and frequency of which can significantly influence overall IS functioning.

Implementation of information strategy during the IPMS development requires necessary attention to the theory and practice of information audit which gives the chance to receive a complete and objective picture of a condition of the whole IS and its separate elements, to localize inherent problems with the purpose of creation of the effective and optimum development program of ensuring information protection.

In the conditions of introduction of technology of the systems with an open architecture which is distinguished by difficult interaction of IS of different nature (interoperability), the existence of the problems of transferring of application programs between different platforms (mobility) and other features, the question of the introduction of SISM gets more important.

For a long time, the security audit of IS has been considered as separate independent service which was followed by the creation and introduction of standards of audit activity in the sphere of information technologies. As a rule, these are closed standards.

Such approach does not comply with one of the main audit tasks – audit results must be objective, impartial and such which can be repeated and reproduced by any audit, at the best –by an external one which will use the same technique of audit.

Unlike closed standards of audit, there exist open standards of security audit of IS which outline organizational and legal structure of IP audit. Open standards connect IT and actions of auditors, unite and coordinate many criteria into one resource that allows at the modern level to introduce the information protection management system in IS, consider practically all features of IS (at program and hardware levels) of arbitrary scale and complexity.

It is impossible to ignore a new standard ISO/IEC 27035:2011 Information technologies. Safety methods. Management of incidents of information protection (ISO/IEC 27035:2016) which provides practical recommendations for identification, registration, and estimation of cases of violation of information protection of IS.

For the processing of IB events and incidents, it is necessary to organize the process of incidents response. The main objectives of incidents response process of IB are as follows: to provide response coordination to an incident; confirmation / denial of the fact of an incident emergence; to provide preservation and integrity of proofs of an incident emergence, creation of conditions for accumulation and storage of the exact information on occurred incidents; minimization of violations of an operating procedure and modification of data, renewal of IS working capacity in the shortest possible time under condition of its violation as a result of an incident; minimization of violation consequences of the confidentiality, integrity and availability of information in IS; protection of IS assets; creation of conditions for bringing a civil or a criminal case against malefactors; fast identification and/or prevention of similar incidents in the future.

It should also be noted that during the usage of information protection management system the incidents management process is one of the most important in supplying data for the analysis of functioning such systems, estimations of efficiency of the used actions, risks decrease, and planning of improvement of IS work.

Only the first version of ISO/IEC 27001:2005 received partially the status of state standard in Ukraine. The question of its practical application remains relevant. The standard that considers branch features is obligatory in the bank sphere – SOU of N of the NBU 65.1 SISM 1.0: 2010.

There exists a legal collision when international ISO/IEC standards of a series 27000 are not adopted in Ukraine, but “Estimation criteria of information safety of computer systems from unauthorized access" in 1999 has been decayed long ago (unlike current legislation IT and IP technologies have developed intensively), and it tends to the worst scenario point.

It is significant to find out the main causes of such a situation. Therefore, we have the case when a customer by own efforts or with the help of contractors develops the specification (S) on the Complex information security systems (KSZI), coordinates it with the State Service of Special Communications and Information Protection of Ukraine (DSSZTZI), and then, on the basis of TZ projects, realizes KSZI by the usage of organizational, hardware-software and engineering means and puts into trial operation. Further, based on the received application of DSSZTZI, he defines the company – licensee which acts as an organizer of state examination of KSZI.

The examination organizer owns a qualified expert’s staff, develops the program and a technique of expert tests, holds them and gives results of the work in the form of a project of an expert conclusion for consideration of advisory council concerning technical information security of DSSZTZI. In the case of a positive solution, KSZI receives the certificate in compliance with the requirements of the technical information safety system (TIS).

The existing system of KSZI design has some other shortcomings. Thus, for IS with different architecture, there are different requirements for IP provision that are based on different categories of access to information, there are standard functional profiles of security, that is some fixed sets of safety services. At the same time, the KSZI developer, while forming TZ, defines independently the protection objects. Experts from DSSZTZI during TZ coordination check specifications of services during TZ coordination, however, it is difficult to determine the level of adequacy of the requirements produced to operating conditions of the existing IS.

Considering the general principles of IP of IS, it is necessary to note that a complex IP of IS has in its basis the usage of organizational, program and hardware means of IP. Such means have to provide identification and authentication of users, access distribution to assets of IS, registration, and accounting of attempts of NSD (Rudyi, 2014).

3 CONCLUSIONS

Based on the carried-out analysis, authors consider that the existing standard and legal base has to be essentially added because it does not outline requirements to the policy development of information safety and estimation of risks in IS. For this purpose, it is necessary to adopt the ISO/IES standards of a series 27000 that will give the chance to legally take part in the state or private certification of the TZI systems or to develop own, qualitatively new standards of safety for the government law enforcement agencies.

According to the international ISO/IEC standards of series 27000, unlike normative documents of Ukraine, the protection object is the process of processing, access and integrity maintaining of information, but not KSZI.

WORKS CITED

ISO/IEC. (2013). *ISO/IEC 27001:2013.* Retrieved from ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO/IEC. (2013). *ISO/IEC 27002:2013(en).* Retrieved from ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

ISO/IEC. (2015). *ISO/IEC 27006:2015.* Retrieved from ISO: https://www.iso27001security.com/html/27006.html

ISO/IEC. (2016). *ISO/IEC 27004:2016.* Retrieved from ISO: https://www.iso.org/standard/64120.html

ISO/IEC. (2016). *ISO/IEC 27035:2016.* Retrieved from ISO: https://www.iso27001security.com/html/27035.html

ISO/IEC. (2017). *ISO/IEC 27003:2017(en).* Retrieved from ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en

ISO/IEC. (2018). *ISO/IEC 27005:2018.* Retrieved from ISO: https://www.iso27001security.com/html/27005.html

Rudyi, T. (2014). Polityka informatsiinoi bezpeky v informatsiinykh systemakh spetsialnoho pryznachennia. In O. Z. T.V. Rudyi, *Problemy zastosuvannia informatsiinykh tekhnolohii, spetsialnykh tekhnichnykh zasobiv u diialnosti OVS ta navchalnomu protsesi* (pp. 21-26). Lviv: LvDUVS.

Received for publishing: 15.04.2018
Revision received: 22.05.2019
Accepted for publication: 10.07.2019

How to cite this article?

Style – **APA** *Sixth Edition:*

Sereda, V., Zhyvko, Z., Balynska, O., & Rudyi, T. (2019, July 15). The Organizational Principles of Information Protection Management System Realization. (Z. Cekerevac, Ed.) *MEST Journal, 7*(2), 73-78. doi:10.12709/mest.07.07.02.09

Style – **Chicago** *Sixteenth Edition:*

Sereda, Valeryi, Zinaida Zhyvko, Olga Balynska, and Taras Rudyi. 2019. "The Organizational Principles of Information Protection Management System Realization." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 7 (2): 73-78. doi:10.12709/mest.07.07.02.09.

Style – **GOST** *Name Sort:*

Sereda Valeryi [et al.] The Organizational Principles of Information Protection Management System Realization [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, July 15, 2019. - 2 : Vol. 7. - pp. 73-78.

Style – **Harvard** *Anglia:*

Sereda, V., Zhyvko, Z., Balynska, O. & Rudyi, T., 2019. The Organizational Principles of Information Protection Management System Realization. *MEST Journal,* 15 July, 7(2), pp. 73-78.

Style – **ISO 690** *Numerical Reference:*

The Organizational Principles of Information Protection Management System Realization. **Sereda, Valeryi, et al.** [ed.] Zoran Cekerevac. 2, Belgrade – Toronto : MESTE, July 15, 2019, MEST Journal, Vol. 7, pp. 73-78.