Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 32 (2019) 278–285

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

The 12th International Conference Interdisciplinarity in Engineering

Information Safety Process Development According to ISO 27001 for an Industrial Enterprise

Nelli V. Syreyshchikova[a], Danil Yu. Pimenov[a,]*, Tadeusz Mikolajczyk[b], Liviu Moldovan

[a]*Department of Automated Mechanical Engineering, South Ural State University, 76, Lenin prosp., Chelyabinsk, Russia, 454080*
[b]*Department of Production Engineering, UTP University of Science and Technology, Al. prof. S. Kaliskiego 7, Bydgoszcz 85-796, Poland*
[c]*University of Medicine, Pharmacy, Sciences and Technology of Tirgu Mures, 38 Gherghe Marinescu street, 540139 Tirgu Mures, Romania*

Abstract

The development results of the information security process in accordance with the requirements of ISO 27001 for the conditions of an industrial enterprise are given. To implement the process, we used various information protection tools: software-based, organizational, mixed, etc. The process is described and visualized, the analytical models of process indicators and their quantitative criteria are developed. The methodology that regulates the procedure for the implementation, management and documentation of the information security process for an industrial enterprise was developed. Identification, analysis and assessment of process risks (identified ways of unauthorized receipt of information), developed a plan of preventive actions to minimize and eliminate risks, reflected in the methodology for the process. The results of the work performed have been approved and implemented at the enterprise and have significant practical significance not only for the enterprise, but also for the profile industry as a whole.

Keywords: process; tinformation security; enterprise; methodology, risks, implement.

* Corresponding author. Tel.: 7-351-267-9267; fax: +7-351-267-9273..
E-mail address: danil_u@rambler.ru

10.1016/j.promfg.2019.02.215

1. Introduction

The one who has information rules the world. Today, it seems, no one will challenge this assertion. And, above all, those who became the victims of information espionage. The first and most important thing that one should know about the protection of information is that virtually any, even very securely protected information can be the object of theft - everything depends on its potential value.

Nomenclature

P_t	Tension force
K	Coefficient of security of the information system
Ssy	The effectiveness of the information security system
U	The damage to the system of unprotected information security
R_p	The risks for a protected system
R_{up}	The risks for an unprotected system
S_i	The cost of the protected information
S_{oi}	The cost of the protected information object
S_{ssi}	The cost of the information security system
ΔR_i	The total information risk
ΔR_{oi}	The total risk of the information object
ΔR_{ssi}	The total risk of the information security system
$\Delta R_i + \Delta R_{oi} + \Delta R_{ssi}$	The reduction of risks for the information system
PR_{bi}	The probabilities of occurrence
U_i	The damages

Problems of information protection have a long history. Rock paintings and ancient manuscripts are nothing more than an attempt to preserve information about the realities of the objective world, and special measures for the preservation of information in secret were practiced in ancient times: the commander of Ancient Rome Caesar used for this purpose cryptographic transformation of texts. Russian cryptographic protection of information covers the historical period from the 9th up to the 20th century, the heyday falls on the 14th-18th centuries - the reign of Ivan the Terrible to the era of Peter I, who was the first of the Russian rulers to clearly understand the importance of cryptographic activity for ensuring the security of the state [1].

But today the issues of information protection in automated processing systems are being considered, and the period of consideration of the problem of information protection in the leading (from the point of view of informatization) countries (primarily the USA) is in the focus of attention of specialists and has been intensively developed for more than 30 years [2].

Today's Russia is accelerating the pace of the revolutionary development of the digital economy in accordance with Presidential Decree No. 203 of May 9, 2017 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030" [3]. Currently, the essential assets of any enterprise are the information supporting its processes, information systems and network infrastructure. Consequently, confidentiality, integrity and availability of information contribute significantly to ensuring competitiveness, liquidity, profitability, compliance with the law and business reputation of the enterprise. But enterprises, their information systems and networks are increasingly faced with various security threats, such as computer fraud, espionage, sabotage, vandalism, fires or floods. Such sources of damage as computer viruses, computer hacking and denial-of-service attacks become more common, more aggressive and increasingly sophisticated. Dependence on information systems and services means that organizations are becoming increasingly vulnerable to security threats [4].

2. Relevance of the topic

The theory of information protection is defined as a system of basic ideas relating to the protection of information in modern processing systems, providing a holistic view of the nature of the problem of protection, the laws of its

development and significant links with other branches of knowledge, formed and developing on the basis of practical experience tasks of protection and defining the basic guidelines in the direction of improving the practice of information protection [5].

The entire period of active work to protect information on approaches to the problem in question is conditionally divided into three periods: initial, developed and integrated. To the theoretical development of the initial period, characterized by the fact that the protection of information was mainly understood as the prevention of unauthorized receipt of it and for this purpose formal (functioning without human participation) funds, conditionally it is possible to refer the works [6-11]. Theoretical approaches considered in the works [12-16] can be conditionally attributed to the developed period characterized by intensive searches, development and implementation of methods, methods and means of protection. The theoretical development of the third complex period, the stage of the future, characterized by analytical and synthetic processing of the existing experience of theoretical research and the practical solution of problems of protection and the formation on this basis of a scientific and methodological basis for the protection of information, conditionally possible works [17-23].

The scientific importance of the issue of information security is defined long before the rapid development of information technology, as it does not require proofs and was considered in works of practical orientation such as the works [24-27] and others in the areas of information protection in computer corporate, local and global networks (problems, tasks, means of protection, cost of decisions, etc.).

Currently, virtually no enterprise can do without the use of information technology. Data processed in information systems can have high value for the company, because Information is an asset that, like other significant business assets, is important for the conduct of business of an enterprise, therefore, it is necessary that it be adequately protected. This is especially important in an increasingly interconnected business environment. As a result of this increasing interconnection, information is currently being exposed to an increasing number and growing variety of threats and weaknesses in the protection system. To date, threats and negative impact on information security are guaranteed with the use of the Internet, the transfer of information through information carriers, etc., so the heads of the enterprise have a problem of ensuring information security of information processes. In such cases, infringement of certain characteristics of security (confidentiality, integrity and accessibility) of critical information becomes unacceptable, as this can lead not only to serious damage, but also to call into question the continued existence of the organization [25].

In accordance with Section No. 9 "Ensuring Information Security" of the Digital Economy of the Russian Federation Program, 07/07/2017 № 1632-r at the present stage, the preservation of confidentiality of information received and transmitted is a vital aspect [28]. Information protection is the protection of information from a large variety of threats, carried out with the aim of ensuring business continuity, minimizing business risks and maximizing the return on investment and business opportunities. In this regard, there is a need to ensure the protection of information processed by the company.

3. Purpose and objectives of the research

Industrial Enterprise JSC "K" is no exception, and is currently facing problems that require the timely protection of information processes of the enterprise. The department of technology of automated engineering has carried out the research works (R&D) to design, develop and master the information security process in accordance with the requirements of ISO 27001 for the conditions of industrial enterprise JSC "K". To achieve the project goal, the following tasks were set:

- analysis of cases at the enterprise;
- comparison and selection of advanced domestic and foreign methods of information security;
- development of information security process;
- development of the methodology "Information security for the conditions of JSC "K" conducting the risk management of the process "Information Security ".

4. Basic provisions

To solve the first task of the research, the problems of the JSC "K" enterprise were diagnosed. As expected, the most pressing problem for JSC "K" is a violation of the information security of the enterprise and it can be divided into the following key areas:

- disclosure of information to third parties may occur because of incompetence of employees who do not comply with the rules for the protection of information, it can be transmitted through communication, publication, forwarding, loss, media, correspondence, conferences, personal meetings, etc.;
- unauthorized access to information, for example, the transfer of confidential information to persons who do not have the right to access it; conditions conducive to the seizure of information can be considered: bribery, poor performance of employees, low wages, lack of discipline, etc.;
- low qualification of specialists in information protection can create obstacles in creating the protection of information security of the enterprise;
- low level of implementation of the goals set for the creation of an information security system, and this situation is often encountered in enterprises, when the goals and objectives are lost at the performance level due to the lack of interest of the performer, due to bureaucracy;
- lack of understanding among employees of the importance of carrying out work to protect information; staff is not sufficiently informed about the aims and objectives of the enterprise and does not understand the importance of protecting confidential data;
- problems of a political nature associated with electronic intelligence, network wars, and in the interests of state secrets, it is necessary to protect information from such attacks.

The company JSC "K" has an established, implemented and certified quality management system for compliance with ISO 9001:2015, and according to the requirements of this standard (par. 7 "Means of support"), there is the following classification of resources: human resources, infrastructure, environment for the functioning of processes, documented information, etc. [29]. The binding of these resources is the information that is available in each of the classification directions. Large volume and efficient management with these information flows is a difficult task and is also a requirement of ISO 9001 (paragraph 7.5.3 "Management of documented information"). Information flow management should ensure compliance with the safety requirement in accordance with ISO/IEC 27001 [30].

To solve the second task of the research, the comparison and choice of information security methods were carried out, such as: cryptographic methods; logging and auditing; legal methods; internetwork screening; creation of backup copies of the system and documents, and other fragment of the results of which is presented in Table 1. The analysis of the merits and demerits of each method and the possibility of their application in the enterprise's conditions showed that for the reliable operation of enterprise information systems, it is recommended to apply a set of methods with the basic method of "logging and auditing".

The process of information security management for the conditions of the JSC "K" enterprise was identified and developed, it is built into the scheme of interaction of the QMS processes in the CDA cycle (plan, operate, verify, influence). The description of the process passport is given (see Table 2), the process is visualized by a sequence diagram (see Fig. 1); process evaluation indicators have been developed.

Table 1 Fragment of comparison of methods of information security

Method	Advantages	Disadvantages
Cryptographic method	Fast implementation. High degree of information security.	Cryptographic transformation of information takes a lot of time. Difficulties in using encrypted information. High security requirements. Reliability of protection depends on the type and method of encryption.
Logging and auditing	Identifies weaknesses in the protection of services, finds the culprit of the invasion, assesses the extent of the damage caused and the current security of the operation of the information system	Can reduce the performance of services
Firewall protection	Increasing the security of internal network objects by ignoring unauthorized requests from the external environment	Vulnerability when changing IP addresses
Creating backup copies of the system and documents	Possibility of emergency data recovery, protection against the loss of databases, corporate mail and other information.	Difficulty in managing backup copies, the human factor

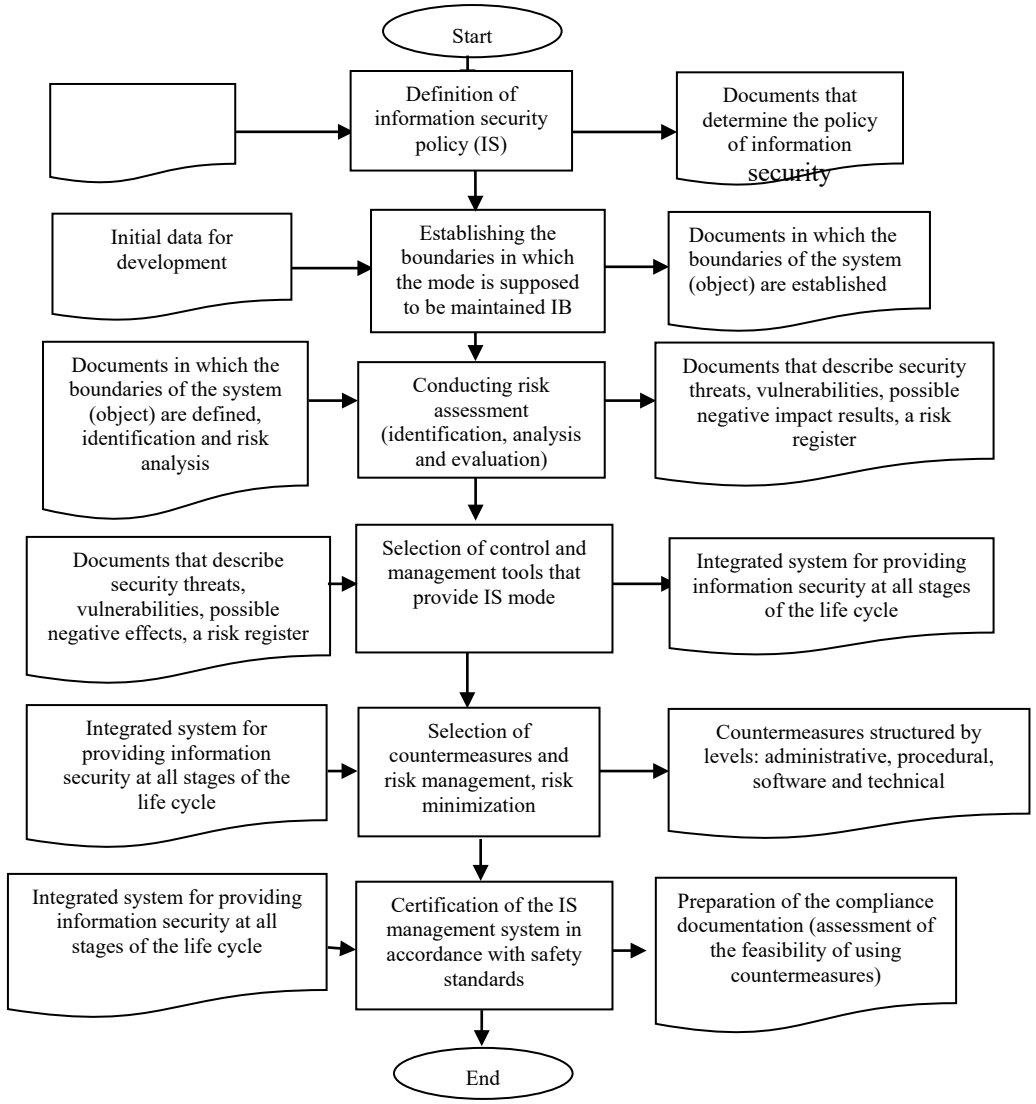

Fig. 1 Model of the process "Information Security" of the enterprise

Table 2 Passport of the process "Information Security Management"

1 Process	Information Security Management
2 Process code	OP 6.1-01-2018
3 Process purpose	Protection of information, monitoring of information flow and control of data transmission
4 Owner	Head of Information Management Department
5 Inputs	Information from external and internal sources (owners of the process, units, managers)
6 Providers	Internal and external consumers of information
7 Outputs	Information with a certain level of protection
8 Consumer	Divisions and leadership
9 Control action	GOST R ISO 9001-2015 Annual production plan; STO 7.5.3-01-2018, RK, KD, TD; ISO/IEC 27001
11 Resources	Infrastructure (equipment, office equipment, transport, software products, etc.). Staff (Information Security Specialists). Environment for the functioning of the process
12 Controlled parameters	Coefficient of security of the information system (K). The effectiveness of the information security system (Ssy). The damage to the system of unprotected information security (U)
13 Criteria of the effectiveness of the process	K no more than 5%, $S_{ssi} \le \Delta R_i + \Delta R_{oi} + \Delta R_{ssi}$, $\Delta R_{ssi} \le S_i + S_{oi}$
14 Methods of measurement	Statistical

Process evaluation indicators, their analytical models have been developed, criteria for the developed evaluation indicators have been established.

Coefficient of information system security (K_p) is determined through risks (1):

$$K_p = 1 - \frac{R_p}{R_{up}}, \tag{1}$$

where R_p is the risks for a protected system; R_{up} is the risks for an unprotected system.

The effectiveness of information security systems, for which the following conditions are met (2):

$$\begin{cases} S_{ssi} \le \Delta R_i + \Delta R_{oi} + \Delta R_{ssi}, \\ \Delta R_{ssi} \le S_i + S_{oi}, \end{cases} \tag{2}$$

where: S_i is the cost of the protected information; S_{oi} is the cost of the protected information object; S_{ssi} is the cost of the information security system; ΔR_i is the total information risk; ΔR_{oi} is the total risk of the information object; ΔR_{ssi} is the total risk of the information security system; $\Delta R_i + \Delta R_{oi} + \Delta R_{ssi}$ is the reduction of risks for the information system.

At JSC "K", as at every enterprise, there are a number of security threats *(i=0...n)*, which are characterized by the probabilities of occurrence PR_{bi}*;* and damages U_i . The task of protecting information is to eliminate every *i*-th threat.

The total damage to the unprotected system is determined by (3):

$$U = \sum_{i=1}^{n} P_{bi} \cdot U_i, \tag{3}$$

An information protection policy has been developed to ensure the direction of information protection management and support the protection of information in accordance with business requirements and applicable laws and regulations. Through the Information Security Policy, the management of the enterprise demonstrates support for the protection of information and the obligation to protect information.

A methodology for information security for the conditions of JSC "K" has been developed, which establishes the procedure for the development, implementation, management, functioning, documentation, monitoring, analysis, support and improvement of the enterprise information security process. The methodology contains measures to manage information security and its control for the enterprise and its units in accordance with the goals and objectives of ensuring information security established in the Policy.

The methodology articulates the enterprise's approach to managing information security. and the requirement for the contents of a program document in the field of information protection regarding the following:

- definition of the protection of information, its general purposes;
- wording of management intentions that support the goals and principles of information protection in accordance with the strategy;
- framework for setting objectives and management tools, including a framework for risk assessment and risk management;
- brief explanation of the policies, principles, standards and compliance requirements in the field of protection that are of particular importance to the enterprise, including:
    - compliance with requirements of law, norms and contracts;
    - requirements for education, training and awareness in the field of protection;
    - business continuity management;
    - consequences of violations of information protection policies;

- defining general and specific responsibilities for the management of information protection, including incident reports in the information security system. Specific means of protecting information for the purposes of the enterprise (technical, program, organizational and mixed) are defined.

The recommended set of measures to ensure the security of information of the enterprise includes such organizational measures to protect information, such as: restricting access to the premises in which the preparation and processing of information takes place; admission to processing and transfer of confidential information only to verified officials; storage of electronic media and registration logs in safes closed for access to unauthorized persons; the exclusion of viewing by outsiders of the content of processed materials through the display, printer, etc .; use of cryptographic codes for transmission of valuable information through communication channels; destruction of coloring tapes, paper and other materials containing fragments of valuable information.

In the recommended complex of measures to ensure the security of information of the enterprise, such special methods as cryptographic protection of information are included, namely, "electronic signature" with the transfer of confidential information through communication channels with the authentication of transmitted messages, storage of information (databases) on media in encrypted form.

In the recommended package of measures to ensure the security of information of the enterprise, technical means of physical type are provided, such as electronic-mechanical equipment for burglar alarm and surveillance, as well as locks on doors and grills on windows.

From the software of information security in the local network of the company, "logging and auditing" are selected. Logging provides collection and accumulation of information about events occurring in the information system, and the audit provides an analysis of the accumulated information, the purpose of which is to monitor the conformity of the process or network to the required safety rules, principles or standards and identifies all that can relate to security problems or all, which can lead to protection problems.

When solving the fifth task of research, the possible risks of the "Information Security" process and the reasons for their occurrence were analyzed and evaluated. The choice of risk assessment methods for the investigated object was carried out, such as: analysis of the "bow tie" and analysis of the types and consequences of failures. Assessment of: the likely damage to business as a result of information security breaches, taking into account the possible consequences of loss of confidentiality, integrity or accessibility of information and other assets; - the likelihood of such an infringement taking into account existing threats and vulnerabilities, as well as implemented measures to manage information security. Measures to prevent and reduce identified risks and preventive measures for potential risks of the developed process.

5. Practical significance

The results of the research are:

- development of the process of information security and the methods of its implementation;
- development and establishment of correspondence of goals, policies and procedures of information security to business objectives;
- coherence of the approach to the implementation of the security system with corporate culture;
- achievement of visible support and interest on the part of management;
- staff of the enterprise have a clear understanding of security requirements;
- mastering the developed methodology for the implementation of ongoing risk assessment and risk management;
- ensuring understanding of the need to apply information security measures to management and employees of the organization;
- development of measurable indicators used to assess the effectiveness of information security management and proposals for its improvement, received from performers.

6. Conclusion

The purpose of the research - designing, developing and mastering the information security process in accordance with the requirements of ISO 27001 for the conditions of the industrial enterprise JSC "K" - is achieved, the tasks are solved.

The main results of the research are:

- ensuring the availability of data for authorized users - the ability to quickly obtain information services;
- guaranteeing the integrity of information - its relevance and security against unauthorized alteration or destruction;
- ensuring the confidentiality of company information.

Acknowledgments

The research was carried out within the South-Ural State University Project 5-100 from 2016 to 2020 aimed to increase the competitiveness of leading Russian universities among the world research and educational centers. The work was supported by Act 211 Government of the Russian Federation, contract № 02.A03.21.0011.

References

[1] S.E. Korotchenko, Development of information security in Russia at the present stage. Kuban State University. (2016) 10 p.
[2] E.B. Belov, Fundamentals of Information Security. Moscow: Hot line: Telecom. (2006) 544 p.
[3] Decree of the President of the Russian Federation of May 9, 2017 No. 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030".
[4] I.A. Vishnyakov, V.R. Radaev, General theory of risks. 2 nd ed., Pererab. and additional. Moscow.: Publishing corporation "Logos". (2008) 200 p.
[5] V.I. Nesterov, Fundamentals of Information Security. Study Guide. Moscow: Publishing Center "Saturn" (2014) 368 p
[6] V.V. Erokhin, G.A. Kulikova, N.V. Mudrova, E.M. Shadoba, V.A. Romanov, N.V. Podobai, Controlling access to the information and software in a commercial bank, Int. J. Appl. Bus. Econ. Res. 15(12) (2017) 159-170.
[7] V.I. Averchenkov, Audit of information security, a textbook for higher education. 2 nd ed., A stereotype. Moscow: Flint. (2011) 269 p. - ISBN 978-5-9765-1256-6.
[8] O.V. Laponina, Fundamentals of Network Security. M .: Prophinform. (2009) 296 p.
[9] B. Schinier, Applied Cryptography. John Wiley & Sons. (1996) 784 p.
[10] S.M. Bellovin, W.R. Cheswick, Network Firewalls, IEEE Communications Magazine 32(9) (1994) 50-57. http://dx.doi.org/10.1109/35.312843
[11] V.Yu. Statuev, V.A. Tinkoff, Information security of distributed information systems. Information society. 1 issue, (2008) 71 p.
[12] E. Ries, The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses. New York: Crown Business, (2011) 336 p.
[13] E.I. Abalmazov, Methods and engineering-technical means of countering information threats. Moscow: Groteck. (1997) 248p.
[14] R.F. Abdeev, Philosophy of Information Civilization. Moscow: VLADOS. (1994) 336p.
[15] A.B. Agapov, Fundamentals of public administration in the field of information in the Russian Federation. Moscow: Jurist. (1997) 344p.
[16] D. Aikov, Computer crimes: a guide to combat computer crime. Moscow: Mir. (1999) 351p.
[17] V.I. Andrianov, V.A. Borodin, A.V. Sokolov, "Spy things" and devices for the protection of objects and information: help, manual. St. Petersburg: Lan. (1996) 272p.
[18] L.V. Babash, G.P. Shankin, History of cryptography. Part I. Moscow: Helios ARV. (2002) 256p.
[19] A.P. Alferov, AP, Zubov, A.Yu., Kuzmin, AS, A.V. Cheremushkin, Fundamentals of cryptography. Moscow: Yurlitinform. (2012) 296 p.
[20] V.B. Baiburin, M.B. Brovkova et al., Introduction to the protection of information: a textbook. Moscow: FORUM: INFRA-M. (2004) 128p.
[21] B.M. Baranov, G.V. Valkov, M.A. Eremeev et al., Protection of information in systems and communications: a textbook. St. Petersburg: VIKKA named after A.F. Mozhaisky. (1994) 113p.
[22] B.C. Barsukov, V.V. Marushchenko, V.A. Shigin, Integral security: information guide. Moscow: RAO "Gazprom". (1994) 170 p.
[23] I.L. Bachilo, B. Tporornina, Information law: a textbook / Ed. acad. RAS. SPb.: Legal Center Press. (2001) 352 p.
[24] D.I. Blumenau, Information and information service. L .: Science. (1989) 192 p.
[25] J.I. Brillouin, Science and Information Theory. Moscow: Fizmatgiz. (1960) 214 p.
[26] N.B. Vanchakov, A.N. Grigoryev, Practical basis of information protection. Technical methods and means. Kaliningrad. (2000) 265 p.
[27] I.V. Vasilevsky, Ways and means of preventing leakage of information through technical channels. Moscow: Nitc Nelk. (1998) 200 p.
[28] The program "Digital Economy of the Russian Federation", approved. № 1632-r of 07/28/2017.
[29] GOST ISO 9001 - 2015. Quality management system. Requirements. Moscow: IPK Publishing House of Standards. (2015) 32 p.
[30] GOST R ISO / IEC 27001-2006. Methods and means of ensuring security. Information security management systems. Requirements. Moscow: IPK Publishing House of Standards. (2006) 27 p.