Modeling the information security management system (ISMS) of a medical organization

O.M. Safonova[1,*] and *N.V.* Kotelnikov[1]

[1]Irkutsk National Research Technical University, ul. Lermontova, d. 83, 664074, Irkutsk, Russia

Abstract. The implementation of information security systems is one of the main components, without which the existence of any modern medical institution is impossible. This question is actual for the healthcare industry. This is confirmed by the presence of large-scale measures that are being implemented as part of the Russian Federation's healthcare modernization program. But the result of informatization is not always achieved easily and successfully. This process includes the equipment of the technical support of the organization and the fragmentary implementation of information systems to the full informatization of medical institutions with the introduction of full-featured medical information systems. Informatization of healthcare organizations makes it possible to systematize a large amount of information. In turn, this requires the implementation of personal data protection systems, storage, archiving and access to this data. The introduction of these systems into the healthcare industry of the Russian Federation has recently entered a new stage. It has complex tasks to integrate new technologies that provide information security to medicine. So, the most pressing problem of the medical industry is information protection, that is, the creation of an ISMS (information security management system).

1 Introduction

Modern ISMS practices are based on the international standard ISO/IEC 27001. Compliance with the standard allows medical institutions to bring together information security management processes, namely: development of a security policy, as well as organization of information security; organization of management of internal assets and resources that form the basis of key business processes; protecting personnel and reducing internal threats; physical and environmental safety; communication and equipment management; access management and control; development and maintenance of hardware and software systems [1].

Consider a systematic approach to building an ISMS. This method involves the analysis of several components:

- legislative, regulatory and scientific base;
- structure and tasks of the IT security department;

[*] Corresponding author: olyastefanovskaya@mail.ru

- measures and methods of information security, as well as organizational, regime and technical components;

- development and application of information security software.

The ultimate goal of solving the problem of information security of a medical institution is the need to build an Information Security Management System (ISMS). This article describes the application of ISO/IEC 27001, " Information technology — Security techniques — Information security management systems — Requirements". It was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) based on the British standard BS 7799. This standard defines the requirements for an information security management system and defines it as "maintaining the confidentiality, integrity and availability of information." [2].

Looking at the standard, we can say that the ISMS represents a model for creating, implementing, operating, monitoring, analyzing, maintaining and improving the protection of information assets in order to achieve business goals. This model is based on risk assessment and on the acceptance of the organization's risk levels, which is designed to effectively consider and manage risk. [3]. Further, the authors highlighted the basic principles of ISMS implementation, which describe the functions of the standard:

- understanding by the management of a medical organization of the need to introduce an information security management system;
- availability of responsible persons (involvement of special services) for the information security of the institution;
- assessment of all kinds of risks, as well as analysis of acceptable risks;
- active and immediate warning of information security incidents;
- providing an integrated approach to information security management;
- continuous reassessment and modification of the information security system (ISO/IEC 27001).

A mandatory and initial stage of building an ISMS should be the general provisions of the Information Security Policy of a medical organization, where technical, organizational and other requirements will be described, as well as information security means are found and described. The basis of this standard is the methodology known as the "PDCA cycle" (Plan - Do - Check - Act). In general, the ISMS model is presented in the standard, but the development of its elements must be analyzed for a specific healthcare facility, taking into account its specific properties.

Today, a very popular term is "big data". The development of this software is necessary due to the enormous amount of information flowing into the healthcare sector, which cannot be managed without the use of IT technologies. The formation of a data analysis system makes it possible to analyze the entire volume of incoming information and build a real model for managing information flows. At the moment, this is possible thanks to the Compulsory Health Insurance Fund. It receives an array of data from territorial authorities, including data from the register of insured people, ICD-10 codes and ciphers, compulsory medical insurance classifiers and the nomenclature of medical services.

It is advisable to load information from the state register of medicines and the state register of medical devices, as well as federal and sectoral forms of statistical observation to the analytical block of the software product. [4]. In our opinion, this will allow us to group the received data in any combination (depending on the task). Let's give an example. So, in order to track the quality of execution of the order of the Ministry of Health of Russia No. 520 n "On the approval of the criteria for assessing the quality of medical care" by medical institutions, it is necessary to form the required lists of a group of patients, for example, patients who need anesthetic therapy. In turn, the program will start forming the list.

The created Federal State Information System for Monitoring the Movement of Medicines also has great priorities. The program tracks the movement of medicines from the manufacturer to the end consumer using labeling (code) and package identification. This will ensure effective quality control of medicines in use. Among other things, the program is able to actively fight counterfeiting, control the inventory of medicines in medical institutions.

Based on the order of the Ministry of Health of Russia dated November 30, 2015 No. 866, since January 1, 2017, an IT system has been in operation to control medicines, which are included in the seven high-cost nosologies. And since January 1, 2018, the program includes medicines from the VED list (Vital and Essential Medicines). Also, the Ministry of Health of Russia has created an information and analytical system (IAS) for monitoring and controlling the procurement of medicines to meet state and municipal needs. The purpose of its creation was the need to improve the processes of organizing the provision of citizens with medicines. This can be achieved by increasing the efficiency of spending budget funds, competition and lower medicines prices for state and municipal needs. The implementation of the listed tasks made it possible to switch to a unified approach in the formation of the initial contract price for the purchase of medicines and increased the efficiency of procurement of medicines.

Further, the authors of the article propose to consider several IT programs that can increase the level of ISMS of a medical institution with any organizational and information structure.

NetCheck software is used to centrally oversee, configure, and update security mechanisms for Microsoft products on the corporate network. In other words, the program is designed to timely update all IT programs.

Another source of ISMS danger is the use of removable media (flash cards and disks). This is the reason why the USB ports of the computers of most employees should be blocked, and if the ports are open, it is necessary to install a special DeviceLock product to prevent information leaks.

It is necessary to conduct regular analysis of event logs using ArcSight Logger to detect facts of unauthorized access to information in modern medicine. According to IT specialists, the advantage of this complex is the ability to store large amounts of information for a long time.

Mandatory, as for any field of activity, is the installation of anti-virus programs on a PC, the timely installation of which will block external threats to the database.

To ensure confidentiality and control the integrity of information, it is recommended to use cryptographic protection during information exchange of data throw the unsecured communication channels (sending information containing personal data) by using the CryptoPro tool. This allows you to control the access of subjects to encryption operations and cryptographic keys and implements cryptographic algorithms developed and recommended by the FSB of Russia [6].

2 Materials and methods

As described above, the construction of an ISMS is based on the PDCA (Deming Cycle) model in accordance with the requirements of ISO/IEC 27001 [8]:

- Plan (planning) - stage of creating an ISMS, analyzing risks and choosing measures to eliminate them;
- Do (action) - implementation phase;
- Check (check) - the stage of assessing the effectiveness of an ISMS implementation by internal auditors;
- Act (improvements) – phase of creation and implementation of corrective actions.

Highlight the following main steps in creating an ISMS:

- making a decision by the director of the company to create an ISMS and informing staff;
- preparation for ISMS creation;
- analysis of all kinds of risks;
- ISMS policy development;
- introduction of ISMS into operation;
- preparation for certification.

Next, let's look at the steps in more detail.

1. Making a decision by the director of the company to create an ISMS and informing the staff. The decision to create an ISMS should be made by the top management of the organization (director, board of directors, etc.). Thus, the company's management gives its support to the beginning of the creation of an ISMS. Also, the head of the company must notify the company staff about the implementation of this process.

2. Preparation for the creation of an ISMS. The first thing to do at this stage is the need to create a working group that is responsible for the implementation of the ISMS. It should include:

- top management of the company;
- representatives of departments covered by the ISMS;
- specialists of departments that ensure the information security of the organization, necessarily competent in IT technologies.

Employees who are part of the working group should understand the universal components of quality management systems, know the requirements of the applicable standard, and should also be trained in the implementation and operation of an ISMS.

Among other things, the working group may also include hired consultants.

The second step is regulatory and methodological support. The working group must have all the necessary regulatory and methodological base for the successful creation of an ISMS that meets the requirements of the standard.

The following are the ISMS standards that should be used [1]:

- ISO/IEC 27000 - dictionary and definitions.
- ISO/IEC 27001.
- ISO/IEC 27003. ISMS Implementation guide.
- ISO/IEC 27004. Information security metrics.
- ISO/IEC 27005:2018 - Information Technology. Security methods. Information security risk management.

The next step is the need to select the area of the company that will be covered by an ISMS. To do this, you need to take into account the following factors:

- type of company activity;
- information to be secured;
- business processes that provide for the processing of information. Business processes are the implementation of any program that can automate the work of an organization. As an example, we will give the introduction of an electronic document management system, which is a multifunctional software and hardware complex for automating the management of an organization in conditions of distributed use of information by different specialists. This business process covers the processing of a wide variety of documentation: orders, protocols and extracts from the protocols, contracts, additional agreements and acts, orders for training and secondment; technical and regulatory documentation; personnel, tender, accounting documents, audio and video content, graphic files, etc.
- departments and employees of the organization who are involved in these processes;
- software and hardware tools, IT technologies of the company that ensure the functioning of these processes;

• territorial sites of the company, within which the collection, processing and transfer of all information takes place.

The result of this step is the activity area for which the ISMS is created. This area must be agreed with the company management.

The fourth step is the need to find all the inconsistencies It is necessary to analyze organizational measures in the field of planning, implementation, audit and modernization of measures to ensure information security, as well as software and hardware tools and mechanisms for protecting information. It is good practice at this stage to pre-audit the certification body to identify problems. The result of such work should be a list of non-conformities to the standard, as well as a work plan for the implementation of an ISMS.

3. Analysis of all kinds of risks. The most important task solved in the process of creating an ISMS is the analysis of information security risks.

The analysis process is accompanied by [2]:

• identification of all assets in a given area of activity. Assets are everything that has value for the organization, its successful development and functioning. One of the stages of risk analysis is the identification of all objects (asset classification) that need protection. Some assets are clearly classified. But some assets (for example, people using information systems) require special identification, in which the chances of a breach of the information security regime are zero.

The following asset identification can be used:

- Hardware: processors, modules, keyboards, terminals, workstations, personal computers, printers, disc drives.
- Software: source code, object modules, utilities, diagnostic programs, operating systems, communication programs.
- Data: processed, directly accessible, archived, stored in the form of a backup copy, logs, databases, data transmitted over communication lines.
- People: users, service personnel.
- Documentation: software, hardware, system, administrative procedures, security.

• determining the value of identified assets;

• identification of threats and vulnerabilities of identified assets;

• risk assessment for possible cases of successful implementation of information security threats in relation to identified assets;

• selection of risk acceptance criteria;

• preparation of a risk treatment plan.

The fulfillment of these conditions is carried out in accordance with the developed procedure for risk analysis, which reflects the methodology and identifies organizational aspects for each of these conditions.

Risk analysis is the basis of an ISMS. It is necessary to select a risk analysis method that can always be used with minimal changes. There are 2 ways to solve this problem. The first path is the need to use existing risk assessment tools. The second way is the need to develop your own solution that best suits the organization's activities. The second way is the most preferable, because most of the existing companies that implement one or another risk analysis methodology do not meet the requirements of the standard. The authors of the article highlighted the typical disadvantages of existing risk analysis methods, these are:

• a typical set of IT threats, which is largely impossible to change;

• acceptance as assets (assets are understood as information input/output data; information records; resources: people, infrastructure, equipment, company software) only of software, hardware and information resources, without considering human resources, services or other resources;

• the overall complexity of the technique and understanding of its sustainable and repetitive use.

In the process of risk analysis for each of the assets or a group of assets, possible threats and vulnerabilities are identified, the probability of realization of each of the threats is assessed and, taking into account the amount of possible damage to the asset, the amount of risk is determined, reflecting the criticality of a particular threat [3]. It is important to note that in accordance with the requirements of the standard, the criteria for accepting risks and acceptable levels of risk must be identified. These criteria must be based on the achievement of the company's strategic, organizational and management goals. The management of the organization uses these criteria to decide on measures to counter the identified risks. If the identified risk does not exceed the established level, it is acceptable, and further measures for its treatment are not carried out. [2]. If the identified risk has exceeded the acceptable level of criticality, the company management must make one of the following urgent decisions:

- taking the risk;
- avoidance of the risk;
- transfer of the risk to another area (its insurance).

4. ISMS policy development. The development of the regulatory framework, which is so important for the functioning of the ISMS, can be carried out simultaneously with the implementation of the activities of the risk treatment plan. At this stage, the documents are developed that are specified in the standard. Typically, this stage includes the following procedures:

- ISMS scope;
- ISMS policy;
- information security mechanisms (anti-virus protection policy; policy for providing access to information resources; policy for using cryptographic protection means)
- ISMS procedures, namely,[4] -
- document management;
- internal audits;
- corrective action;
- preventive actions;
- incident management. An incident is a single event of an unpredictable nature that can affect the business processes of an organization, compromise and violate the level of information security protection. Management of this process is based on identifying the threat, notifying all employees of the company about the incident, registering the incident (for analyzing the incident as a process, in order to gain certain experience to prevent subsequent threats), eliminating the causes and consequences, investigating the incident, in which all available information is sent to IT services, security and support services [9].
- assessment of the effectiveness of ISMS management mechanisms. An example of incident management is the «SearchInform CIB» program, which responds urgently to violations of security policies and provides the IT specialist with a large evidence base.

We have developed procedures that cover the following key ISMS processes:

- risk management;
- system performance management;
- personnel management;
- document management and information security management;
- revision and modernization of the system.

Based on the above, it should be noted that as a result of this process, not only the documentary base of the ISMS is created, but also there is a real distribution of responsibilities for ensuring information security among the personnel of the organization.

5. Implementation of the ISMS into operation. The date the ISMS is put into operation is the date when the management of the organization approves the ISMS applicability

statement. This document is public and declares the objectives and means chosen by the organization for risk management. [5]:

The Regulation developed by us contains:

- controls selected during the risk treatment phase;
- management and control tools existing in the company;
- tools to ensure compliance with legal requirements;
- tools to ensure the fulfillment of corporate obligations.

The commissioning of the ISMS into operation involves all the developed methods and tools that implement the selected goals and controls (Fig. 1).

6. Preparation for the certification process. At this stage, the company is advised to perform a preliminary audit. The preliminary audit is carried out by the same certification body, which is supposed to pass certification in general. After a preliminary audit, the certification body draws up a report, it notes all the advantages of the created ISMS, as well as all inconsistencies and recommendations for their elimination (in this case, the company's ISMS must work for at least 6 months). The result of the last stage is the ISMS of the company, which is ready to go through the certification process.

Having considered all the main stages (as well as the requirements for them) of creating an ISMS, we can say that this process is very complicated. But the efforts that will be involved in the creation of the company's ISMS will allow this company to reach a new level of functioning, as well as increase its competitive advantages.

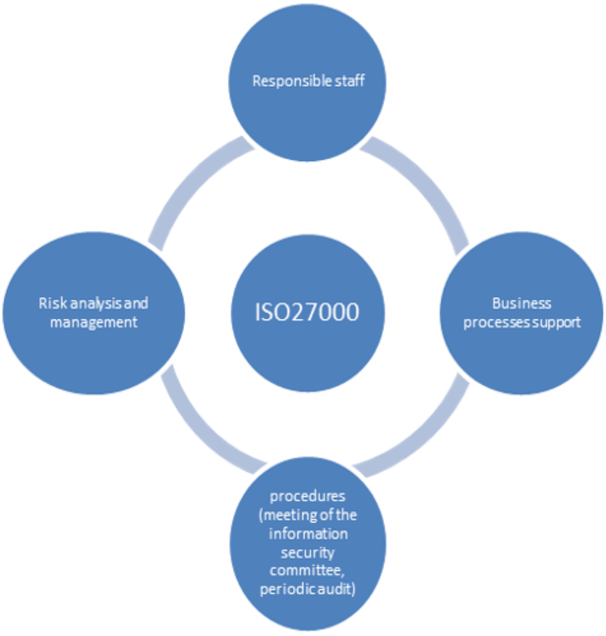
Responsible staff
Risk analysis and management
ISO27000
Business processes support
procedures (meeting of the information security committee, periodic audit)

Fig. 1. Basic ISMS mechanisms.

3 Results

Based on the above, the authors found that the creation of an information security management system is a very complex and lengthy process. The creation of such a system is accompanied by risks that need to be able to manage and apply an appropriate approach to eliminate these risks. The created and certified ISMS gives a medical organization a number of advantages, namely:

• increasing competitive advantages;

• growth of the organization's rating, transition to the international level;

• demonstration to partners and clients of the company of a high level of reliability due to high information security;

• reducing the risks associated with possible damage to the company's assets;

• increasing the transparency of the information security management process in the organization.

The listed advantages are obtained due to the certificate of conformity to the standards discussed in the article. The most time-consuming step on the path to certification is the creation of an ISMS itself.

4 Discussion

Summing up, it should be noted that the priority areas of the medical industry are:

- standardization of the structure of activities of medical institutions;
- introducing a risk-oriented approach to the healthcare organization;
- informatization of the healthcare sector based on modern information technologies and software;
- creation of a unified ISMS;
- development and implementation of national standards (ISO 27001 series) for quality and safety of healthcare activities.

An important result from the implementation of an ISMS is the optimization of information security costs, reduction of risks associated with possible damage to the company's assets. Implementation of an ISMS will also allow ensuring compliance of the level of information security with legislative, industry, contractual, internal corporate requirements and goals of medical institutions.

Also, the result of the implementation of an ISMS will be a significant reduction in the number of incidents and the response time to an incident (for example, a virus attack).

References

1. 2018 *ISO 31000, Risk management – Principles and guidelines, International Organization for Standardization*
2. 2018 *ISO 45001:2018 Occupational health and safety management systems – Requirements with guidance for use, International Organization for Standardization*
3. 2018 *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management*
4. 2015 *ISO 14001:2015* - *Environmental management systems – A practical guide for SMEs, International Organization for Standardization*
5. 2013 *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization*
6. 2015 *ISO 9001:2015 Quality management systems — Requirements, International Organization for Standardization*
7. Livshitz I I, Lontsikh P A, Kunakov E P, Semenov V V, Kibirev Y V 2019 *International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)* DOI: 10.1109/ITQMIS.2019.8928361
8. Livshitz I I, Lontsikh P A, Lontsiklr N P, Karascv S, Golovina E *2019 International Conference "Quality Management, Transport and Information Security, Information*

Technologies" (IT&QM&IS) DOI: 10.1109/ITQMIS.2019.8928349

9. Eliseev S V, Livshitz I I, Lontsikh P A, Karasev S N 2019 *International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)* DOI: 10.1109/ITQMIS.2019.8928376
10. Eliseev S V, Livshitz I I, Lontsikh P A, Stefanovskaya O M 2019 *International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)* DOI: 10.1109/ITQMIS.2019.8928403
11. Livshitz I I, Lontsikh P A, Stefanovskay O M, Golovina E Y, Kibirev Y V 2019 *International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)* DOI: 10.1109/ITQMIS.2019.8928308
12. Stefanovskaya O M, Lontsykh P A, Konyukhov V Yu, Kibirev Yu V 2019 *International Scientific Conference «Information Society: Health, Economics and Law»* http://dx.doi.org/10.34648/SIDPO.2019.34.76.040
13. Vladimirtsev A V, Golovina E Y, Kayi V, Lontsikh N P, Stefanovskaya O M 2019 *International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)* DOI: 10.1109/ITQMIS.2019.8928371
14. Livshitz I I, Lontsikh P A, Kunakov E P, Lontsikh N P, Tatarnikova L I 2019 *International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)* DOI: 10.1109/ITQMIS.2019.8928452
15. Lontsikh P A, Moskvitina V A, Golovina E Yu, Kibirev Yu V 2019 *Scientific journal "University News. Investments. Construction. The property"* **9.1(28)** 10 http://journals.istu.edu/izvestia_invest/journals/2019/28/articles/01?view=0
16. DOI: http://dx.doi.org/10.21285/2227-2917-2019-1-10-25