UDC 004.223.2

# BASIC ASPECTS OF SAFETY IN MEDICAL INFORMATION SYSTEMS

*YAUHENI MIANITSKI, DMITRY PASTUKHOV*
Polotsk State University, Belarus

*The article presents the main aspects of architectural features in the provision of security and the protection of confidential data in medical information systems. The algorithm of the technology of distribution of access rights in medical information is considered.*

Introduction. With the increase in the volume of concentrated information in the medical field, there is a need for the formation of standardized and uniform storage systems for this information. This question helps to solve the development of specialized medical information systems.

The medical information system is different from other software products, especially in that it stores and processes personal and confidential information. In this regard, they are subject to increased requirements for reliability and limitations of access to information, legal responsibility, technical measures to protect data. Any user who accesses the medical information system bears full (moral, administrative and criminal) responsibility for the confidentiality of information that he makes, uses or transfers to other users.

Methods of information protection in medical information systems. At the moment there is a question of information security in medical information systems from two points of view:

1. Protection of the rights of the individual from the dissemination of confidential information;
2. Protection of interests of the state and departments. Possibility of information leak, abuse, violation of ethics.

Based on these requirements, the following tools should be used to ensure the protection of information and programs of medical information systems: [1]:

1. Legal;
2. Organizational and administrative;
3. Technical (hardware-software).

Legal means prevent unauthorized use of information and are a deterrent to potential violators.

These include the rights and obligations for obtaining, processing and restricting the dissemination of information, which are prescribed in the legislative framework of the state, which is subject to actions to work with the medical information system.

To ensure the safety information, this legislative base should be subject to both medical information systems and all participants taking part in the work with it.

Organizational and administrative means regulate the functioning of medical information systems, the use of its resources, personnel activities, as well as the interaction of users with the system and users with system administrators.

Based on this, the health information systems should have a hierarchy of roles, each of which is related to different positions of medical workers, their areas of activity, and the role of the patient. Each of these roles must have a number of unique rights to interact with the system. This distinction serves to admit to that part of the information that corresponds to the competence of the user. This feature is implemented through technical means of protection, and is regulated by legal means.

Technical means perform the following protection functions: creating obstacles to possible ways of penetration and access of potential infringers to the medical information system, identification and authorization of users, delineation of access rights to resources, registration of events, cryptographic protection of information [2].

The software and hardware measures of the health information security system should provide means for allocating access rights, ensuring that the user can only access the information and programs that are necessary to perform the functional duties. These funds traditionally use the following concepts:

1. 1. User Authorization (a technology that confirms that the real user and the person whose name is being accessed is the same person)
2. Access groups (logical grouping of users into one group for which the system grants the same rights)
3. Access rights (differences in the ability to work with a medical information system, for example - reading information, reading and changing data, deleting documents or even modifying code)
4. Access control list (a table that groups access groups and their associated rights levels for a particular system object).

**Algorithm for the distribution of access rights.** The algorithm of the operation of the technology of the distribution of access rights in the medical information system is as follows:

- During the start of the system, user authorization is performed. For authorization, a login-password link is often used, where the login identifies the user, and the password is a means of verifying the identity. In this case, the password must be presented in an encrypted form, when stored in the system. The most commonly used algorithms are AES, DES, Blowfish and others. In addition, when working on the network, it is necessary to provide password transfer via secure protocols, such as SSL - an information transfer protocol that uses asymmetric cryptography to authenticate exchange keys, symmetric encryption to preserve confidentiality, message authentication codes for message integrity. [3]
- At the moment of the first access to the server after the authorization, a session with the server is created. During the initialization of the session, the system determines which groups the user belongs to and uniquely associates the user with these groups. All further actions in the system, including opening the database, displaying its design elements or other program elements, are carried out only based on the current list of access groups.
- If the client requests the system objects sequentially on the server side, it checks for the presence or absence of the necessary access rights to the object. If none of the user groups is included in the object, the server does not provide the client with information about the presence and properties of the object. Given the highest priority of the security system, unauthorized access to such an object (server, database, presentation, program, document or single field) becomes theoretically and practically impossible.
- At the same time, the system at the kernel level includes the functions of logging of unauthorized access and software processing of exceptions in the system code that simultaneously allow the administrator to see all suspicious requests from the security point of view and, on the other hand, provide the required level of stability and performance of applications of the system.

In addition to the distribution of access rights, the software and hardware security measures of medical information systems should provide for encryption of various textual information as well as multimedia. Various multimedia data must be stored in binary form in the database, taking into account the encryption algorithms, and presented to the user as decrypted data in the interface. Figure 1 shows a variant of the encrypted image stored in the database as a type of binary type Blob, suitable for encryption.

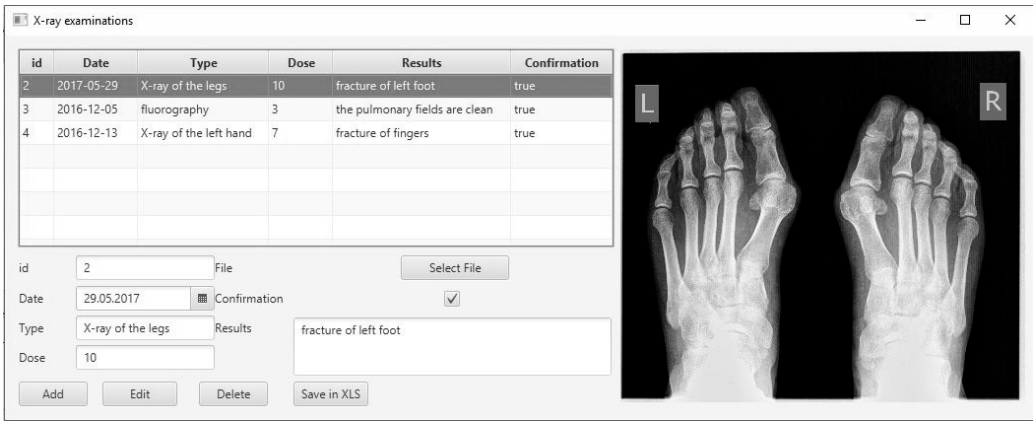


Fig. 1. An example of an interface with an image of the Blob type encrypted by the AES algorithm.

**Conclusion**. The described technical, regulatory and other means of ensuring security to date allow medical information systems to provide the entire necessary set of measures to protect information and programs, which is a prerequisite for the suitability of such systems for their operation.

REFERENCES

1. Моисеенко, Е.В. Информационные технологии в экономике. Методы и средства защиты информации / Е.В. Моисеенко, Е.Г. Лаврушина ; под ред. Л.З. Анипко. – С. 25–30.
2. Информационная безопасность и её составляющие [Электронный ресурс]. – Режим доступа: http://vtit.kuzstu.ru/books/shelf/book4/doc/chapter_4.html. – Дата доступа: 26.12.2017.
3. SSL протокол [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/SSL. – Дата доступа: 26.12.2017.