https://orcid.org/0000-0002-9374-2833
https://orcid.org/0000-0002-8047-7647

UDC 004.772

H.T. SAMOYLENKO[*], Yu.Yu. YURCHENKO[*]

KEY ASPECTS OF DESIGNING INFORMATION INFRASTRUCTURE FOR A MEDICAL ENTERPRISE

[*]State University of Trade and Economics, Kyiv, Ukraine

Анотація. *Забезпечення необхідної інформації для діяльності будь-якого медичного закладу є складним та трудомістким процесом, націленим на вирішення професійних, організаційних та соціальних завдань. Ефективне інформаційне забезпечення в галузі охорони здоров'я має велике значення для якості надання медичних послуг на всіх етапах та рівнях, починаючи від первинної медико-санітарної допомоги до онлайн консультацій. У статті розглядаються ключові аспекти проєктування, включаючи вибір необхідних технологій, розробку архітектури системи та її інтеграцію з існуючими медичними процесами. Розглядається процес аналізу потреб медичного підприємства щодо обміну та обробки інформації. Визначаються ключові вимоги та функціональні можливості медичної інформаційної системи. Обґрунтовано важливість ефективного інформаційного забезпечення в медичних закладах для поліпшення якості надання медичних послуг. Акцентується увага на важливості захисту конфіденційної медичної інформації. Розглядаються заходи безпеки, такі як шифрування даних, контроль доступу та системи резервного копіювання. Також розглядаються практичні аспекти впровадження медичної інформаційної системи, включаючи аналіз вимог, захист даних та навчання персоналу. Розглядаються важливість розробки і впровадження систем контролю доступу, що дозволяють обмежувати права доступу до медичних даних тільки вповноваженого персоналу. На підставі аналізу предметної області та початкових вимог замовника сформульовані функціональні й нефункціональні вимоги до створюваної ІС, здійснено моделювання поведінки системи шляхом побудови діаграми UML та побудову діаграми класів із документацією їх специфікацій. Особлива увага приділена розробці додаткової функції маркування критичного синдрому пацієнта.*
Ключові слова: *інформаційна інфраструктура, інформаційна система, проєктування інформаційної інфраструктури, безпека.*

Abstract. *The provision of necessary information for the operations of any medical institution is a complex and labor-intensive process aimed at addressing professional, organizational, and social challenges. Effective information support in the healthcare sector is crucial for the quality of medical services at all stages and levels, ranging from primary healthcare to online consultations. This article explores the key aspects of designing an information infrastructure, including the selection of necessary technologies, system architecture development, and integration with existing medical processes. The paper delves into the process of analyzing the information exchange and processing needs of a medical enterprise. Key requirements and functional capabilities of a medical information system are identified. The importance of efficient information support in medical facilities to enhance the quality of healthcare services is justified, with particular emphasis on the protection of confidential medical information. Security measures such as data encryption, access control, and backup systems are considered. Additionally, practical aspects of implementing a medical information system, including requirement analysis, data protection, and staff training, are examined. The significance of developing and implementing access control systems to restrict access to medical data only to authorized personnel is highlighted. Based on the analysis of the domain and initial customer requirements, functional and non-functional requirements for the proposed information system are formulated, and system behavior is modeled through the construction of UML diagrams and class diagrams with accompanying specifications. Special attention is given to the development of an additional feature for labeling critical patient syndromes.*
Keywords: *information infrastructure, information system, designing information infrastructure, security.*

DOI: 10.34121/1028-9763-2023-3-59-64

1. Introduction

Designing an information infrastructure of an enterprise is highly relevant in the business environment. In the modern world, data volumes are rapidly increasing, and businesses need to effectively manage, store, and process this data. An efficient information infrastructure allows enterprises to achieve the necessary scalability, performance, and security for working with large data volumes. The adoption of microservices architecture and distributed computing is becoming increasingly common. This requires the creation of an infrastructure that enables effective communication, load balancing, monitoring, and management of these distributed systems. Since data security is of utmost importance, the enterprise's information infrastructure should incorporate effective security measures, including network protection, encryption, authentication, and access control, to prevent unauthorized access and damage [1]. An efficient information infrastructure should be capable of scaling to provide the required resources and performance according to the growing needs of the enterprise. Designing an effective information infrastructure allows enterprises to optimize costs related to equipment, software, and system management. This can be achieved through the use of cloud services, virtualization, automation, and other efficient approaches. All these factors confirm the relevance of designing the information infrastructure of an enterprise, which helps businesses maintain competitiveness, work effectively with data, ensure security and scalability, and optimize IT expenses.

The aim of the article is to investigate the peculiarities of designing information infrastructure for a medical enterprise.

2. Results of the research

The information infrastructure of medical institutions encompasses a comprehensive system of technologies, software, and networking resources used for storage, retrieval, processing, and transmission of medical information [2, 3]. The key aspects to know about the information infrastructure of medical institutions include:

• Needs analysis: a thorough analysis of the enterprise’s needs, including data volume, data types, security level, accessibility, performance requirements, scalability, and other factors. This will help to understand the necessary components and technologies for building the infrastructure.

• System architecture: the development of the infrastructure architecture, including network topology, servers, data storage, security tools, monitoring, and backup. It’s important to consider scalability, availability, and system reliability.

• Cloud services: the utilization of cloud services such as Amazon Web Services, Microsoft Azure, or Google Cloud Platform. They can provide the flexibility, scalability, and availability needed for expanding your infrastructure.

• Security: it encompasses network protection, data access, backup, encryption, and authentication. It’s also crucial to devise a security strategy and utilize reliable technologies to safeguard enterprise information.

• Monitoring and management: designing monitoring, logging, and management mechanisms to track system performance, detect issues, and ensure effective administration.

• Scaling strategy: developing infrastructure scaling mechanisms to address growing enterprise needs, utilizing horizontal and vertical scaling to ensure productivity and availability.

• Automation: using automated tools and processes for deployment, configuration, and management of the infrastructure. This will help to reduce time and risks during the implementation and maintenance of the system.

It is advisable to further examine each component of information infrastructures of medical institutions:

• Electronic medical documentation (EMD). EMD includes systems for collecting, storing, and processing electronic patient information. This can include patient records, medical history, laboratory test results, images, prescriptions, and other medical information. EMD systems provide access to this data for physicians and medical staff, enabling efficient diagnosis, treatment, and patient monitoring.

• Laboratory information system. It is used for processing and managing laboratory data. It involves collecting laboratory test results, data storage, report generation, and sharing access to this information between the laboratory and physicians. The laboratory information system helps to automate laboratory processes and provides quick access to results.

• Picture archiving and communication system (PACS). PACS is a system for storing, processing, and transmitting medical images obtained from radiological examinations such as X-rays, tomographic images, ultrasound scans, etc. It allows physicians to view, analyze, and exchange images in electronic format. PACS greatly facilitates access to radiological images and contributes to fast diagnosis and treatment.

• Patient management system. This system assists in patient registration and managing associated processes. It includes functions for patient registration, appointment scheduling, medication management, reminders, and other aspects related to patient flow management. The patient management system helps to ensure organized and efficient patient reception and treatment.

• Network infrastructure. The network infrastructure includes all network components such as routers, switches, servers, wireless access points, etc. It enables communication and data exchange between different systems and devices within the medical institution. The network infrastructure needs to be reliable and scalable and ensure data transmission security.

• Security measures. Data security is a critical aspect of the medical institution's information infrastructure. This includes data encryption, access controls for systems and confidential information, authentication and authorization mechanisms, intrusion monitoring and detection, and other security measures. The goal of these measures is to protect important medical information from unauthorized access, damage, or loss.

Each of these components has its own peculiarities and implementation requirements [3, 4]. The information infrastructure of medical institutions is a complex system that integrates various components to facilitate efficient operations and data exchange in the medical environment.

3. Materials and methods

The information infrastructure of medical enterprises includes a complex of technologies, systems, and processes used for the collection, processing, storage, and transmission of information in the medical environment. These infrastructures aim to improve the efficiency, security, and quality of healthcare services. Ensuring the confidentiality of medical information is an extremely important aspect of the information infrastructure of medical enterprises. They must adhere to appropriate standards and regulations to protect patients' personal data. The confidentiality of medical information refers to the protection of personal and private medical information of patients. This means that any information obtained or created during a medical examination, treatment, or patient care must be processed and stored with the utmost confidentiality.

The key principles of confidentiality and protection of medical information include:

1. Patient consent. Patients should provide their consent for the collection, processing, and transmission of their medical information. This consent can be expressed in writing, orally, or through electronic means of communication.

2. Access restriction. Medical information should only be accessible to authorized individuals directly involved in patient healthcare. These may include doctors, nurses, medical administrators, etc. Access to medical information should be limited and controlled through password establishment, access levels, and other security measures.

3. Protection against unauthorized access. Medical information should be protected against unauthorized access such as hacking attacks or data theft. Various security measures such as data encryption, firewalls, antivirus programs, and other protection technologies are used for this purpose.

4. Protection against data loss. Medical information should be stored in a secure location and protected against accidental or intentional loss. This may involve data backup, the use of data recovery systems, and other data preservation strategies.

5. Compliance with rules and regulations. Medical enterprises must comply with relevant rules, regulations, and normative requirements regarding the confidentiality of medical information.

Protection against unauthorized access to medical information is a critical aspect of data confidentiality and security. Some tools and strategies used to protect against unauthorized access include:

• User authentication. This process verifies the user's identity before granting access to medical information. Authentication may involve the use of unique identifiers (logins) and passwords, biometric methods (fingerprint, facial recognition), or the use of electronic keys.

• Authorization and role management. After successful authentication, the system establishes the user's level of access based on their role or privileges. Administrators of the medical information system determine which data and functionalities each user can access based on their role (doctor, nurse, administrator, etc.). This allows limiting access to confidential information to only necessary individuals.

• Data encryption. It is used to protect medical information from unauthorized access during transmission or storage. Encryption transforms data into an unreadable form using cryptographic algorithms. Only a person or system with the appropriate decryption key can access the understandable information.

• Physical protection. It involves restricting physical access to server rooms or premises where computers with medical information are located. This may include the use of controlled access, video surveillance cameras, alarm systems, and other physical security measures.

• Monitoring and auditing. Medical enterprises can use monitoring and auditing systems that track users' actions within the system. This helps to detect suspicious or unauthorized activities and monitor changes in access to and use of medical information.

• Training. Increasing user awareness of security rules and the confidentiality of medical information is an important aspect of protection. Users should be trained to use passwords correctly, not disclose their data to unauthorized individuals, and avoid suspicious links or virus attachments.

4. Designing

When designing an information infrastructure of a medical enterprise, a crucial stage is the development and implementation of a medical information system (MIS). It is a set of informational, organizational, programmatic, and technical tools intended for the automation of medical processes and/or organization. There are various classification options for MIS. One of the most characteristic classifications is as follows:

– technological information medical systems (TIMS);
– medical service information banks (MIMS);
– statistical IMS;
– research IMS;
– educational IMS.

This classification was based on four formative factors: the object of description, the addressed social problem, the user, and the level of information aggregation in source documents. Technological information medical systems provide informational support for doctor-patient rela-

tions [3, 5]. Medical information systems are classified based on a hierarchical principle that corresponds to the healthcare structure as a field, including:

– basic ones (clinical);

– facilities (clinics, hospitals, dispensaries, etc.);

– territorial ones (specialized medical services and regional authorities);

– national ones (national institutions and authorities).

The advantages of using medical information systems in hospitals depend on the type of MIS and its successful implementation in a particular institution. When a suitable medical information system is chosen, its implementation can lead to positive changes in the organization of the institution's work, such as simplifying access to necessary information, eliminating the need for redundant data entry, using document templates, facilitating resource searches, and providing access to reference information. At the same time, during the implementation of an information system in a healthcare institution, the staff needs to make efforts, including entering information into the system using available templates and forms, consistently maintaining electronic medical documentation, and following the workflow with a particular information system. The advantages that the healthcare institution's management will gain from using the medical information system depend on the tasks they set when selecting and implementing a specific system. Typically, these advantages can be summarized as follows:

– transparency of patient service systems;

– transparency of financial activities and material resources;

– extensive reporting capabilities, including real-time reporting.

Patients of healthcare institutions also benefit from using the medical information system. These benefits depend on the capabilities of the system itself and the functions that the institution allows patients to access. As a result of investigating all aspects of the developed information system, the following use case diagram has been created, which describes the functionality of the software module (Fig. 1).

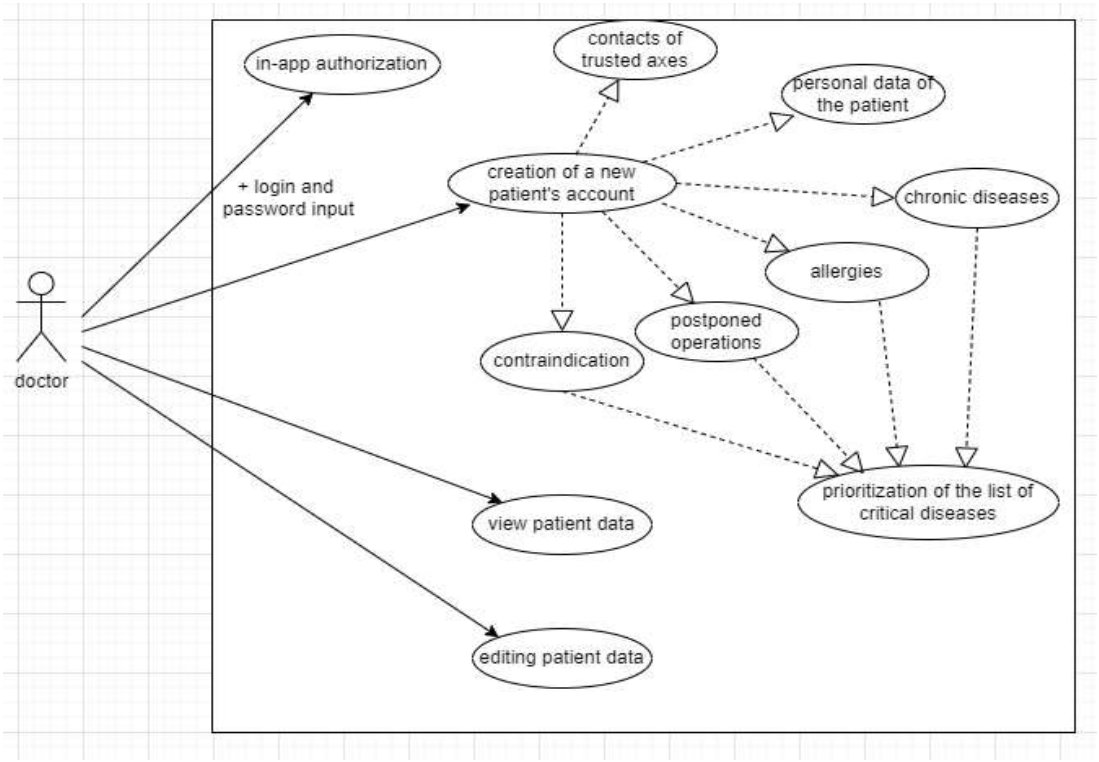

Figure 1 – Use case diagram for the Patient Management Software Module

5. Conclusions

The article examines the peculiarities of designing the information infrastructure of a medical enterprise and implementing a medical information system. One of the key aspects of the research involved the examination of technological information medical systems that provide informational support for the interaction between doctors and patients. The use of medical information systems in hospitals and healthcare facilities has the potential to improve the quality of healthcare services. The appropriate selection of a medical information system and its successful implementation will contribute to optimizing work processes, ensuring financial transparency, facilitating resource discovery, and providing access to necessary information. Involving staff in data entry using the system and adhering to work algorithms will promote the effective utilization of the system.

REFERENCES

1. Гайворонський М.В. Безпека інформаційно-комунікаційних систем: навч. посіб. К.: Видавнича група BHV, 2014. 608 с.
2. Денісова О.О. Автоматизоване проектування інформаційних систем: навч. посіб. К.: КНЕУ, 2011. 412 с.
3. Reid S.J., Naidu C., Kantor G., Seebregts C.J. Do electronic patient information systems improve efficiency and quality of care? An evaluation of utilisation of the Discovery HealthID application. *South African Medical Journal.* 2020. Vol. 110 (3). P. 210–216.
4. Hallinan D., Bernier A., Cambon-Thomsen A., Crawley F.P., Dimitrova D., Medeiros C.B., Nilsonne G., Parker S., Pickering B., Rennes S. International transfers of personal data for health research following Schrems II: a problem in need of a solution. *European Journal of Human Genetics.* 2021. Vol. 29 (10). P. 1502–1509.
5. Plakhotnij S.A., Klyuchko O.M., Krotinova M.V. Information support for automatic industrial environment monitoring systems. *Electronics and Control Systems.* 2016. Vol. 1, N 47. P. 29–34.

Стаття надійшла до редакції 30.06.2023