UDC 004.56.5

DOI: 10.18372/2073-4751.81.20127

[1]**Gasimov V.A.**,
orcid.org/0000-0003-3192-4225,
e-mail: vaqasimov@bei.edu.az,
[2]**Mammadzada N.F.**,
orcid.org/0000-0001-5349-9616,
e-mail: mammadzada.nargizw@gmail.com,
[1]**Mammadov J.I.**,
orcid.org/0000-0003-3939-4708,
e-mail: camammadov@beu.edu.az,
[1]**Aliyeva K.J.**,
orcid.org/0000-0003-3924-7951,
e-mail: kaliyeva@beu.edu.az

THE PROBLEM OF INFORMATION PROTECTION IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS OF MEDICAL ORGANIZATIONS

[1]**Baku Engineering University**
[2]**Azerbaijan Technical University**

Introduction

The creation and operation of electronic document management systems (EDMS) in medical institutions arises from the requirements of the modern era. Thus, on the one hand, personal and medical information entered into EDMS in medical organizations, especially psychological and sexual health status, genetic data, etc. are information of serious sensitivity for patients, and protecting their confidentiality is of great importance. The seizure of this information by outsiders can cause moral damage to the patient and negatively affect his psychological state.

On the other hand, the organization of the collection, reliable storage, confidentiality, completeness and accessibility of information about medical activities of patients, laboratory tests, results of USM, MRI, etc. examinations, treatment procedures, etc. in the database, and the prevention of unauthorized use, modification and dissemination is of great importance for medical organizations. Thus, unauthorized interference with medical data, alteration of medical documents, including diagnoses and test results, can hinder the proper treatment of the patient, monitoring of his health, preparation of reports, resolution of insurance issues, investigation and investigation of problems and disputes that may arise between the patient and the doctor or medical organization, and the correct assessment of responsibilities in forensic medical documents [1-2].

In general, the registration and storage of medical documents in the EDMS in medical organizations should provide solutions to the following important issues [1]:

- legal security of medical documents;
- protection of the confidentiality of patients' personal and medical information, prevention of unauthorized disclosure, modification, deletion, loss of documents;
- monitoring and evaluation of patients' diagnosis and analysis data, treatment process;
- determination of the responsibilities of medical personnel and medical organizations;
- ensuring the efficient conduct of various statistical reports;
- accessibility of documents to all authorized users;
- timely detection of possible errors in documents.

Keeping personal and medical information confidential increases patients' trust in the medical organization, including treatment, and allows them to easily share all information about their health with medical personnel. It is known that medical personnel have professional obligations to protect the confidentiality of patient information, which strengthens the doctor-patient relationship and increases confidence that the patient's personal information is in safe hands. At the same time, patients have the right to demand that their medical information be kept confidential and that this information be accessible only to the relevant medical personnel.

To ensure the security of medical documents, including the protection of patients' personal and medical data, it is necessary to comprehensively consider the aspects specified in regulatory legal acts. The main criteria for organizing the protection of an electronic document include the following aspects related to threats to its confidentiality, integrity and availability [3]:

- Confidentiality – only authorized persons can access the document;
- Authorization – determines what permissions other persons have in the process of working with the document;
- Accountability – what procedures are allowed to be performed with the document;
- Integrity – determines the authenticity of the document and the registration of changes to it;
- Authenticity – confirms the authenticity of the document, its identity with the original;
- Non-repudiation – ensures that the author of the document cannot refuse it.

From the above, it can be concluded that there is a need to take serious security measures to ensure the confidentiality, completeness and availability of medical documents, including personal and medical information of patients, in EDMS of medical organizations. The article is devoted to the study of this topical issue.

International experience in the field of legislation on the protection of medical documents

It should be noted that in most countries there are strict legislative acts regulating the protection of personal data, and the protection of the confidentiality of medical data is also ensured within the framework of regulatory legal documents intended for personal data. Although these guiding documents have different names in different countries, they essentially serve the same purpose – to resolve the problem of protecting personal data, including medical data, through legislation.

The Health Insurance Portability and Accountability Act (HIPAA), passed by the US Congress on August 21, 1996, is specifically designed to regulate the protection of patients' medical information. Medical personnel are required to comply with the requirements of these regulatory legal documents, violations of which create serious legal liability.

This document combines the following main provisions [4]:

- Ensuring the confidentiality of patient information;
- Protection of electronic documents;
- Immediate detection and notification of violations of the rules;
- Determination of liability and application of a penalty system in case of violation of the rules;
- Compliance of the organization's partners with the requirements of the HIPAA act.

The GDPR (General Data Protection Regulation), which sets out the regulation on the protection of personal data in the European Union countries, has been in force since May 25, 2016. This document generally provides the following provisions:

- Personal data must be processed and stored in accordance with the law;
- Personal data may be obtained only for specified purposes and may not be used for other purposes;
- Only parts of personal data that are necessary may be collected and stored;
- Personal data must be accurate, not falsified or distorted;
- Personal data must be protected with a high level of security measures.

GDPR provides for ensuring a high level of data protection within the framework of the law, as well as determining liability and applying penalties in case of violation of these rules.

In countries such as Turkey and Azerbaijan, the protection of medical data is similarly carried out within the framework of regulatory legal documents ensuring the confidentiality of personal data. Thus, in Azerbaijan, on May 11, 2011, the Law of the Republic of Azerbaijan "On Personal Data" was adopted, and on September 6, 2010, the "Requirements for the Protection of Personal Data" were approved.

Distributed structured EDMS for medical organizations

In practice, structural units (outpatient and inpatient examination and treatment clinics, laboratories, etc.) included in medical organizations, as well as branches, can be located and operate at geographically distant distances from each other. This also affects the structure of the databases of the EDMS operating in that medical organization. At the same time, it should be noted that branches of medical organizations may differ from each other in terms of functionality, for example, one branch of a medical organization may specialize in a certain field and may work with documents in different formats (with images, graphics, videos, etc.). Diagnostic equipment or laboratory analysis equipment in that branch may not be available in other branches. This also creates the need to create and exchange different medical documents prepared in each of the branches. In this regard, the structures of the databases used in separate structural units of a medical organization should be harmonized and their mutual functionality should be ensured, or a single database should be created and all structural units should operate with that database. It is clear that it can be efficient for each branch and structural unit to have its own separate server and database. Thus, when a patient applies to the same branch or structural unit again, it can be faster and more secure to obtain previous medical information from the local database rather than from the central database. However, such an approach requires additional costs (for the server and other equipment, software, IT specialists, security measures), and difficulties may arise in exchanging information between other branches and structural units.

In the second approach, which has a central server and database, branches and structural units, in addition to storing all medical documents in their own databases, also transfer them to the database located on the central server. In this case, the EDMS of a medical organization has a distributed structure. Such a structure includes a central server and database that stores all information, as well as local databases of each branch or structural unit.

Based on the principles considered, the functional scheme of a distributed database for storing medical information in a medical organization and its subordinate branches is depicted in Fig. 1.

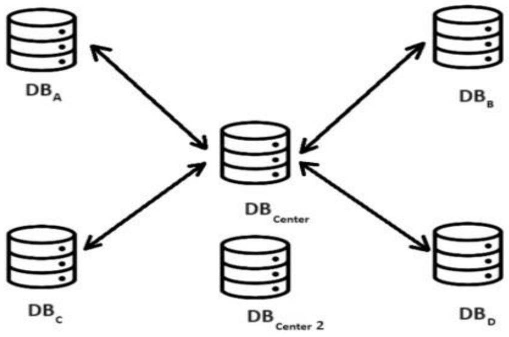

Fig. 1. Distributed structured database of medical organizations

In the figure, DBA, DBB, etc. are databases belonging to branches or structural units, DBCenter is the central database, and DBCenter 2 is a backup copy of the central database.

In general, data in distributed databases can be geographically or functionally distributed. A distributed database system is a network of databases in which data is stored at multiple geographical and functionally different physical or logical locations. Depending on the type of query entered into the database system, the query is directed to all databases or to specific databases for response. Database distribution allows for timely execution of queries across large amounts of data, successful error recovery, and more reliable security by placing them in different physical databases.

Access control model in EDMS of medical organizations

Access control is of particular importance for data protection in EDMS of medical organizations. By implementing proper access control, it is possible to guarantee that only authorized persons can access certain resources or perform appropriate authorized operations within the system. Failure to implement access control mechanisms at the required level can pose a serious threat to ensuring the confidentiality, integrity and accessibility of medical data (documents) [5].

In the absence of access control, unauthorized persons may access medical data without authorization, which can lead to threats such as leakage of that data, unauthorized access, unauthorized modification, corruption, deletion, etc. Prevention of unauthorized access leads to a reduction in potential cybersecurity risks. Thus, strong control measures such as strict identification and two-factor authentication during system access, and encryption of passwords significantly prevent unauthorized access attempts.

In addition, managing the authority of the personnel working with this information is also of great importance in ensuring the security of patients' personal and medical information. In the distributed structured EDMS of the network of medical organizations, the authority of the personnel working with medical information to work with documents can be generally divided into the following levels:

- System or network administrator can perform writing and reading processes on all types of documents, and can sign them.
- Doctor has the authority to write, read, and sign on all documents he has compiled and can view all patient documents available in the system.
- Laboratory assistants can read all documents related to their activities and sign all documents they have created.
- Operators can read and write all types of registration and referral type documents.

The above is schematically shown in Fig. 2.

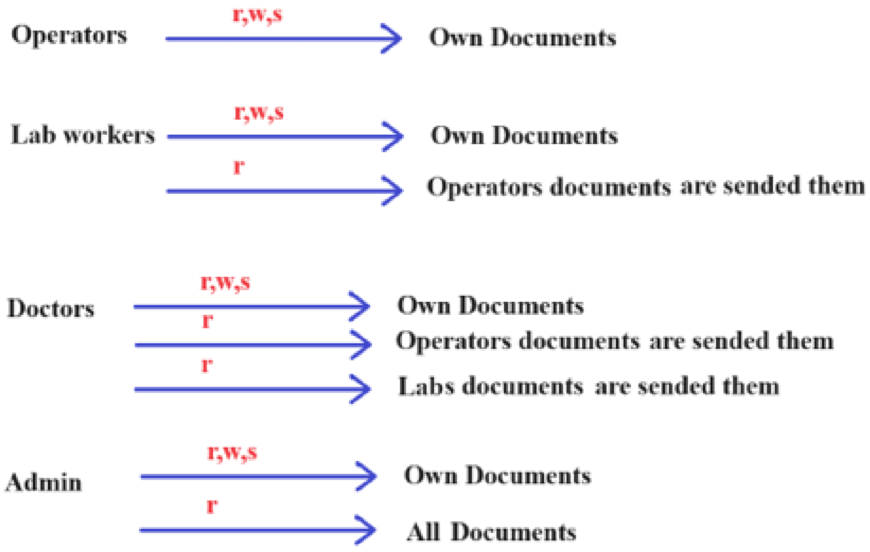

Fig. 2. Personnel authority for working with medical documents
(r – reading, w – writing, s – signing and sending)

The organization of access permissions to medical documents is based on the Role-Based Access Control (RBAC) model [6]. This model has certain advantages compared to other models. These include ease of management, prevention of leaks, restriction of unauthorized access, reduction of the risk of unauthorized modification and deletion of data, scalability, and ease of information exchange between users with roles.

It should be noted that when managing access to resources for medical documents, in many cases, it becomes necessary to dynamically organize the permissions of assigned roles. Thus, when doctors, laboratory technicians or other employees using the system are given permissions outside the assigned role or when some of the powers in the roles are prohibited, it becomes necessary to organize dynamic permissions. For example, the provision of additional powers to personnel newly appointed to a position or on probation in a certain position, or the dynamic change of roles in the event of a reduction in some of the powers initially granted, allows for more convenient management in the data security system.

In these cases, the compilation of tables of roles and permissions allows for dynamism. Thus, in addition to the roles assigned to the user in connection with the current position, in exceptional cases, he can be given separate permissions. It is clear that each permission in itself gives access to certain resources, which is organized by matching that permission with the ID of the resource. In this case, the authorization process uses tokens to match the ID assigned to the user with the IDs of individual resources and determines whether the user has permission to that resource. In order to ensure dynamism of access to documents (resources), in addition to assigning roles to users, it is advisable to define separate “user-permission” relationships for granting external permissions or prohibiting permissions in existing roles (Fig. 3).

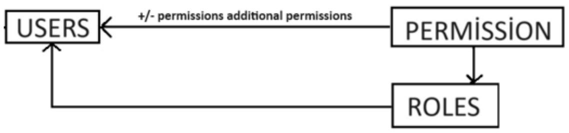

Fig. 3. Dynamic role-based permissions organization

Another positive aspect of the dynamic role switching in the RBAC model is that dynamic role switching allows users to access the appropriate resources only at the right time, thereby increasing the level of security and preventing users from acquiring excessively long-term privileges. On the other hand, according to this model, access to sensitive patient data can be allowed only at certain time intervals, which has a positive effect on preventing data leakage.

Another positive aspect of the RBAC model is that it provides more flexible management. Thus, quick adaptation to emergencies or other changing work modes is an important feature for medical organizations. In such situations, medical personnel can be given temporary roles and can be taken back after the work is completed.

The dynamics of changing roles ensure more efficient use of resources. Thanks to changing roles according to needs, medical personnel only use the resources appropriate to their tasks, thereby preventing the use of unnecessary resources.

Protection of medical data during exchange in the EDMS of a medical organization

As mentioned, corporate computer networks operate in medical organizations, the exchange of medical documents and information about patients is carried out through an EDMS. In this case, all documents and information of the EDMS are stored on a central server. The server is strictly physically protected and direct interference with it is excluded. It is considered possible to interfere with the information circulating and processed in the system at the level of individual nodes and during the transmission process.

Experience shows that, like other critical infrastructures, medical organizations are regularly subjected to cyberattacks. Some of such attacks are targeted at information during the exchange of information between nodes of the enterprise network, and malicious actors attempt to seize personal and medical information of patients through methods such as “Sniffing”, “Man-in-the-Middle”, “Spoofing”, “Phishing and DNS Spoofing”, etc. In this regard, the main focus in such systems is on the problems of identification, authentication, confidentiality, completeness and availability.

To prevent the mentioned attacks and ensure information security, the application of necessary protection methods, including reliable authorization, identification and authentication systems, encryption algorithms, key exchange protocols, can give effective results. For this purpose, along with standard methods, it is proposed to use special methods and algorithms, software and hardware tools developed by the authors. The advantage of the proposed methods and tools is that, on the one hand, they are less known than standard methods and tools, so the probability of their vulnerabilities being discovered is low, and on the other hand, their implementation is many times cheaper.

Authentication and authorization of users in the EDMS

In order to increase the level of protection of patients' medical data, it is important to solve the authentication and authorization issues in the proposed system. Authentication is the first stage of the process of ensuring the security of applications of users of the EDMS of a medical organization (persons registered in the system) and determines the procedure for their entry into the system and confirmation of their identity. Authorization, on the other hand, includes determining the access rights of users to the system resources within the framework of the established authorities and whether they are granted permissions.

Authentication and identification processes are performed in the following sequence. First, the system administrator assigns a name (ID) and an initial password (Password) to the user. During the first login to the system, the user is required to change this password. Thus, the confidentiality of the password is ensured.

We will compare the following two existing approaches to session management and authentication [10]:

- Cookie or Session-based approach;
- JSON Web Token (JWT)-based approach.

Cookie-based authentication involves storing relevant authentication information in the browser via cookies when users log in to a site. During login, the user is given a token. The user must present this token to the server each time with his request. In order to perform the request, the server compares the token sent with the request with the corresponding data in the database, confirms that the request was indeed sent by that user, and returns a positive response to the server (Fig. 4).

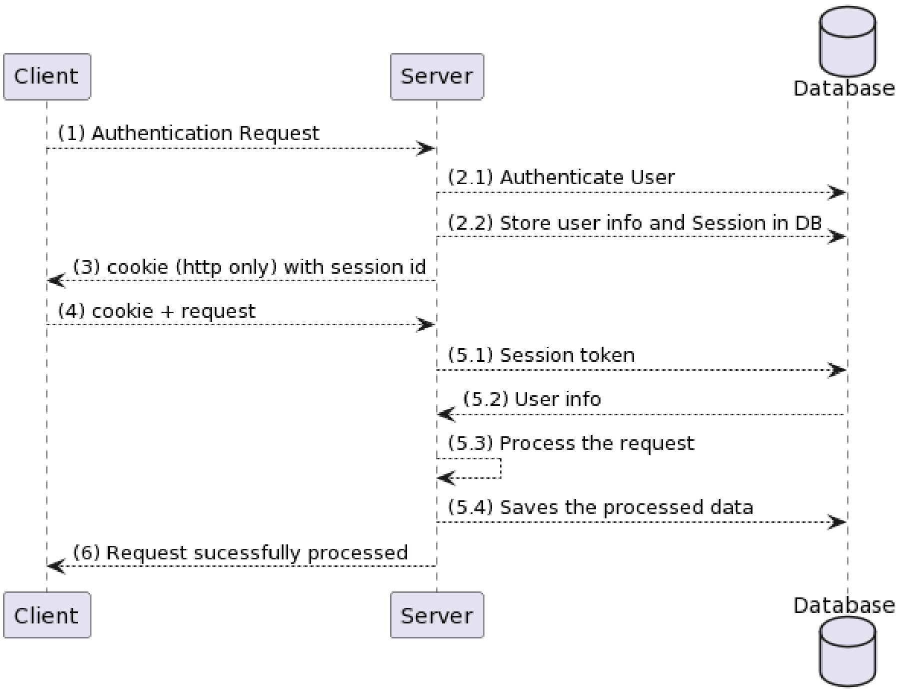
Client
Server
Database
(1) Authentication Request
(2.1) Authenticate User
(2.2) Store user info and Session in DB
(3) cookie (http only) with session id
(4) cookie + request
(5.1) Session token
(5.2) User info
(5.3) Process the request
(5.4) Saves the processed data
(6) Request sucessfully processed
Client
Server
Database

Fig. 4. Cookie-based user authentication [10]

In the JWT-based approach, database access is not required for each request. Here, the user information is stored in the signature created for the session. To protect the user's information, the token part is signed and verified using a secret key known only to the server. As a rule, the use of JWT tokens is considered appropriate to reduce the load on the database and ensure faster processing of requests. When a request is sent using a token during the authorization process, it is checked whether the user has access to the requested resource by comparing it with the permissions assigned to him (Fig. 5).

Ensuring confidentiality of information

In distributed structured information systems, it is considered advisable to transmit data through secure tunnels to prevent interception during exchange. It is assumed that all documents created by users and entered into the system are stored in their original form on the server. Each time a new session is started during document exchange, and the data is encrypted using the secret key created for that session and transmitted to the other party.

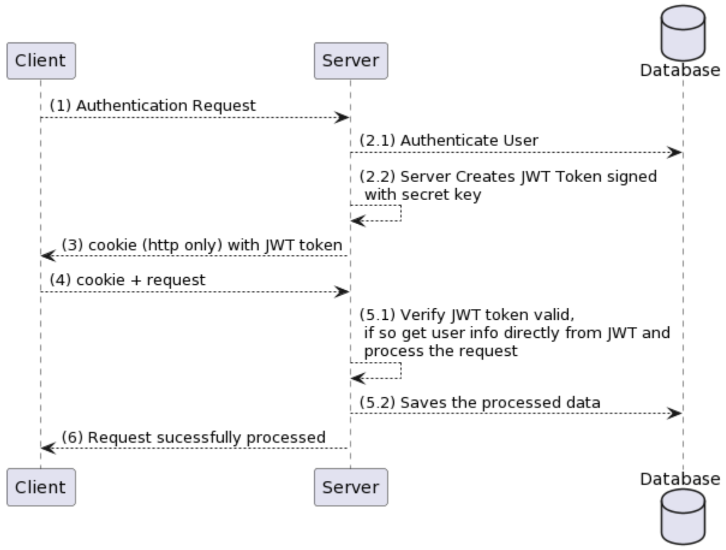
Client
Server
Database
(1) Authentication Request
(2.1) Authenticate User
(2.2) Server Creates JWT Token signed with secret key
(3) cookie (http only) with JWT token
(4) cookie + request
(5.1) Verify JWT token valid, if so get user info directly from JWT and process the request
(5.2) Saves the processed data
(6) Request sucessfully processed
Client
Server
Database

Fig. 5. JSON-based user authentication [10]

The algorithm for creating a secure tunnel and transmitting information through this tunnel in the EDMS is as follows:

1. A secret session is created when an electronic document compiled by each user using the network is placed in the system, as well as when a document in one node is transferred to another node;
2. Secret keys intended for use during each secret session are created using a special key exchange protocol and transmitted to the parties [7]. This key is intended for one-time use. A new key is generated during a new session;
3. Based on the type and format of the file to be exchanged, the appropriate one from the available encryption methods is selected. For text-formatted documents, a chaotic encryption method based on the movement of molecules [8] is used, and for image-formatted documents, a labyrinth generation-based encryption method [9] is used. The sender encrypts the document with a secret key obtained through the appropriate protocol and transmits it to the other party via the network;
4. After receiving the encrypted document, the recipient performs the decryption operation using the secret session key and restores the original document;
5. End.

If a new document needs to be transferred, another session is created and the above steps are repeated.

The procedure for creating a secret key for a session is illustrated in Fig. 6, and the procedure for transferring documents via a secret tunnel within a session is illustrated in Fig. 7.

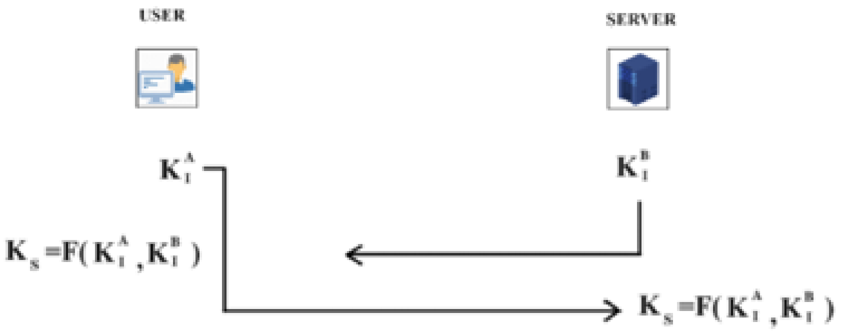

Fig. 6. Generating a secret key for a session

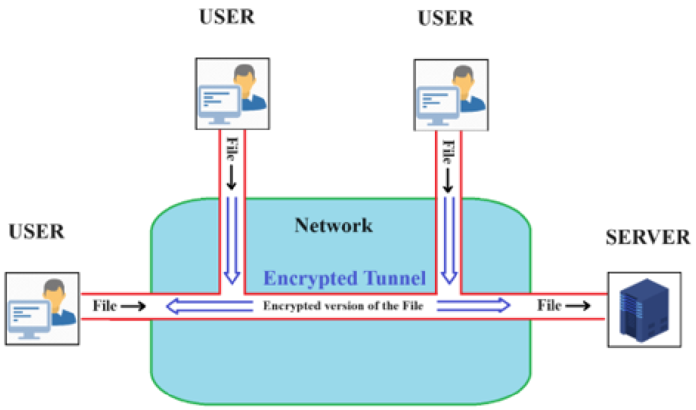

Fig. 7. The process of transferring documents via a secret tunnel within a session

It should be noted that when accessing documents within the system, the exchange process is executed after determining whether the user has permission to that document.

Conclusion

In order to organize electronic document management in medical organizations and protect patient data, it was proposed to create a unified EDMS, to create appropriate methods and tools to ensure reliable protection of medical documents and data, and to apply them systematically. Thus, it was considered appropriate to implement the EDMS in medical organizations as a distributed structured database and to store all data in a central (server) database along with local databases. To organize the access of various authorized users in terms of the functional duties of the medical organization to the EDMS, a dynamic role-based access control model was developed, and a reliable authorization procedure was envisaged. To ensure the confidentiality of data in the network exchange process, it was proposed to use secure tunnels, key exchange protocols and appropriate encryption methods.

References

1. Uchishik H. Fehim Health Law. 4th ed. (renewed). Istanbul : Ötüken Publishing Inc., 2017. 504 p.

2. Saeed S., Lino J. Electronic Health Records: The Significance of Cybersecurity. 2024. URL: https://www.researchgate.net/publication/377926125_Electronic_Health_Records_The_Significance_of_Cybersecurity.

3. Gasimov V. Fundamentals of information security. Baku, 2009. 340 p.

4. Olawunmi I. Safeguarding health data in a digital era: a comparative study of the GDPR and HIPAA. 2023. 19 p. URL: https://www.researchgate.net/publication/370934056_SAFEGUARDING_HEALTH_DATA_IN_A_DIGITAL_ERA_A_COMPARATIVE_STUDY_OF_THE_GDPR_AND_HIPAA.

5. Georgieva M. Access Control Models. *Cybernetics and Information Technologies*. 2021. Vol. 21. P. 77–104. DOI: 10.2478/cait-2021-0044.

6. Mudarri T., Abdo S., Al-Rabeei S. Securıty fundamentals: access control

models. Interdisciplinarity in theory and practice. *International journal of interdisciplinarity in theory and practice*. 2015. No. 7. P. 259–262.

7. Gasimov V., Mammadzada N., Mammadov J. New Key Exchange Protocol Based on Matrix Algebras. *2023 5th International Conference on Problems of Cybernetics and Informatics (PCI)* : proceedings, Baku, Azerbaijan, 28–30 August 2023 / IEEE. 2023. P. 1–3. DOI: 10.1109/PCI60110.2023.10326004.

8. Gasimov V., Mammadov J., Mammadzada N. Stream encryption method based on the chaotic brownıan motion model of molecules. *4th International Conference on Innovative Data Communication Technologies and Application (ICIDCA 2022)* : proceedings, Coimbatore, India, 3–4 November 2022 / Procedia Computer Science. 2022. Vol. 215. P. 577–588. DOI: 10.1016/j.procs.2022.12.060.

9. Gasimov V. et al. Maze based image encryption method constructed by random number generation. *Eurasian Journal of Mathematical and Computer Applications*. 2024. Vol. 12, iss. 3. P. 35–50.

10. Shriganesh H. Effective Ways to Authenticate Users: JWT vs Sessions, which one to choose? Web Development. URL: https://blogs.halodoc.io/user-authentication-jwt-vs-session/.

Gasimov V.A., Mammadzada N.F., Mammadov J.I., Aliyeva K.J.

THE PROBLEM OF INFORMATION PROTECTION IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS OF MEDICAL ORGANIZATIONS

The article is devoted to the study and processing of methods for creating electronic document management systems of medical organizations, increasing the level of protection of documents and information stored and processed in this system. For this purpose, International and local experience in the field of legislation on the protection of documents containing personal and medical information of patients in medical organizations was commented in the article, the issue of creating a distributed structured electronic document management system for medical organizations was considered, various protection methods were used to ensure the confidentiality of personal and medical information of patients, it was proposed to use the authentication procedure and secure encryption methods.

***Keywords**: electronic document management systems; confidentiality; authorization; authentication; distributed databases; access control model.*

Касумов В.А., Маммадзаде Н.Ф., Маммадов Дж.І., Алиева К.Дж.

ПРОБЛЕМА ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ МЕДИЧНИХ ОРГАНІЗАЦІЙ

Стаття присвячена вивченню та обробці методів створення систем електронного документообігу медичних організацій, підвищенню рівня захисту документів та інформації, що зберігаються і обробляються в цій системі. З цією метою в статті був прокоментований міжнародний і місцевий досвід в області законодавства про захист документів, що містять особисту і медичну інформацію пацієнтів в медичних організаціях, розглянуто питання створення розподіленої структурованої системи електронного документообігу для медичних організацій, використані різні методи захисту для забезпечення конфіденційності для обробки особистої та медичної інформації пацієнтів було запропоновано використовувати процедуру аутентифікації і безпечні методи шифрування.

***Ключові слова**: системи електронного документообігу; конфіденційність; авторизація; аутентифікація; розподілені бази даних; модель управління доступом.*