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

UDC 004.772

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

# FEATURES OF MATHEMATICAL RATIONALE FOR A COMPLEX DATA SECURITY SYSTEM OF A MEDICAL ENTERPRISE

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

***Анотація.*** *Стаття присвячена аналізу проблем захисту даних, зокрема, персональних даних, у медичних установах різних форм власності. Обґрунтовано необхідність впровадження комплексних систем захисту даних. Моделлю, що розглянуто як базу для розвитку комплексної системи захисту даних у підприємстві, є модель Бела-ЛаПадула. Модель Бела-ЛаПадула представляє систему керування доступом до інформації, що ґрунтується на ієрархічній структурі доступу до даних. Використання жорсткого ієрархічного підходу при побудові інформаційної інфраструктури підприємства на цій моделі, з урахуванням різних рівнів конфіденційності інформації, може не враховувати можливість втручання з боку інсайдерів на вищих рівнях. У статті проаналізовано основні положення цієї моделі, включаючи присвоєння спеціальних рівнів безпеки всім учасникам процесу обробки даних та документам, що містять захищені дані. У статті детально розглядаються основні аспекти моделі, включаючи призначення спеціальних рівнів безпеки для всіх учасників процесу обробки даних та для документів із захищеною інформацією. Для забезпечення безпеки та регулювання доступу, на основі адаптованої моделі, для кожного користувача запропоновано індивідуальні рівні доступу, що відповідатимуть обов'язкам та рівню конфіденційності. Після впровадження комплексної системи захисту конфіденційних даних та надання всім учасникам процесу обробки захищених даних та документів спеціальних рівнів безпеки виникла можливість чіткого розмежування прав власності на інформацію різної цінності. Це сприяє подальшому розширенню кола співробітників, які мають доступ до цієї інформації, скороченню часу доступу до неї та формуванню інформаційно-аналітичних звітів щодо роботи системи контролю доступу. Використання ієрархічної моделі доступу Бела-ЛаПадула дозволяє досягти ефективного контролю над доступом до інформаційної системи та забезпечити загальну безпеку підприємства.*

***Ключові слова:*** *захист даних, моделі безпеки, рівні доступу.*

***Abstract.*** *The article is dedicated to the analysis of data protection issues, particularly personal data, in medical institutions of various ownership forms. The necessity of implementing comprehensive data security systems is justified by the Bell-LaPadula model, which is considered a foundation for the development of a complex data security system within the enterprise. The Bell-LaPadula model represents an access control system based on a hierarchical data access structure. However, using a rigid hierarchical approach when building an information infrastructure of an enterprise based on this model, taking into account different levels of information confidentiality, might not account for the possibility of insider intervention at higher levels. The article analyzes the key aspects of this model, including assigning special security levels to all participants in data processing and to documents containing the protected data. To ensure security and access regulation based on an adapted model, individual access levels that correspond to each user's responsibilities and confidentiality level are proposed for them. After implementing a comprehensive system for protecting confidential data and assigning special security levels to all participants in the processing of protected data and documents, a clear differentiation of ownership rights to information of different values emerged. This facilitates further expansion of the circle of employees with access to this information, reduces access time, and forms informational and analytical reports on access control system performance. The use of the hierarchical Bell-LaPadula access model allows for effective control over access to the information system and ensures overall enterprise security.*

***Keywords:*** *data protection, security models, access levels.*

DOI: 10.34121/1028-9763-2023-4-51-57

## 1. Introduction

Data protection issues, including personal data, are quite relevant in any enterprise. Medical institutions of various ownership types are no exception and require the implementation of comprehensive data protection systems. The use of models, such as simplified descriptions of important components of the system, allows for simplifying the solution to the task of creating a security system that is adequate to real threats. As the basis for the development of a comprehensive data protection system in the enterprise, the Bell-LaPadula model was chosen, as its key provisions include assigning special security levels to all participants in the data processing process and the documents containing the protected data.

*The aim of the article is* to investigate the implementation of the Bell-LaPadula model for data security in medical institutions, considering their specific characteristics and confidentiality levels.

## 2. Results of the research

The Bell-LaPadula model represents an information access control system based on a hierarchical organization of data access. However, the use of a rigid hierarchical approach when creating an enterprise's information infrastructure based on it, taking into account different levels of information confidentiality, may not account for insider intervention at higher levels. Therefore, in real conditions, it is often necessary to introduce classification restrictions for information access schemes. The Bell-LaPadula model belongs to the formal model of mandatory access control. The classical model is based on the rules of secure document flow [1]. According to this model, each object and subject (user) in the system are assigned their own access level. All access levels in the system are clearly defined and ordered by increasing secrecy according to the following rules:

- A user can only read objects with an access level no higher than their own.
- A user can modify only those objects whose access level is not lower than their own.

However, one of the peculiarities of this model is the exchange of information between users of the same level, as they may perform different functions in the organization, and what is allowed for user A may be prohibited for user B.

The relevance of adapting the hierarchical Bell-LaPadula access model arises with the aim of applying it in information systems with an adapted level of information confidentiality and increased resistance to external attacks. The process of implementing the model in a medical enterprise will involve adapting the existing model of information flow distribution in the existing information and communication system of the enterprise, while simultaneously maintaining the hierarchical access model and directory service. The key provisions of the Bell-LaPadula model include assigning special security levels to all participants in the data processing process and the documents containing the protected data. The application of the hierarchical Bell-LaPadula access model was directed towards the following steps:

- Taking into account the level of confidentiality: during the adaptation of the model to the new information system, additional access levels were established according to the specifics of the medical enterprise and different types of confidential information.
- Increasing resistance to attacks: the adapted model includes taking security measures to prevent threats (increased user authentication, action auditing, and access monitoring).
- Preserving the hierarchical structure: the hierarchical model is quite effective for access control, and this characteristic of the structure was maintained during implementation.

The process of adapting the Bell-LaPadula model was carried out considering all the peculiarities and requirements of the medical enterprise to ensure an optimal level of protection for confidential information and the prevention of potential internal threats [1, 2].

## 3. Materials and methods

According to the law on personal data protection and the internal policy of the medical enterprise, the following categories of data are considered restricted access information:

1. Accounting documentation.
2. Human resources department documentation.
3. Medical information system server.
4. Personal (confidential) patient information of the medical enterprise (personal data, treatment and medical records, financial transactions).
5. Normative and legal acts of the medical enterprise.
6. Computer and software infrastructure of the medical enterprise.
7. Information about ongoing and implemented projects at the medical enterprise.
8. Expansion plans of the medical activities of the enterprise.
9. Investment plans, procurement, sales, and their technical and economic justification.
10. Information about clients, contractors, suppliers, and business partners of the medical enterprise.
11. Information related to the content of contracts, agreements, and other organizational obligations.
12. Information about security procedures, access control (access control system), alarm systems, and the structure of internal communication within the medical enterprise.

Currently, there exist a considerable number of methods for formalizing the process of assessing the value of information [3, 4]. However, subjective judgments still significantly influence this process. In modern research, information value is understood as a quantitative measure that determines its usefulness for the information owner, and the functional relationship between information value and its parameters is expressed as follows:

$$VOI = \frac{\sum_{i=1}^{n} a_i}{n}, \tag{1}$$

where $n$ is the number of information indicators affecting its value and $a_i$ is the coefficient characterizing the quantitative influence of the $i$-th information indicator on its value [4].

The calculation of the information value is based on methodologies and approaches from systems analysis, providing a framework for determining relevant coefficients within the range [0…1].

For the assessment of the information value within the institution, a mathematical model has been employed, allowing for the determination of a numerical value by calculating the average sum of corresponding coefficients. Each of these coefficients is computed using a ranking method. The significance of each information indicator is determined either from official documents regulating the information security organization or through an expert group. Contemporary approaches to information value determination often overlook indicators that characterize the degree of importance and ownership rights concerning the information.

Indeed, the level of access restriction serves as a criterion by which the impact of information access limitation and time on the final information value can be evaluated. This indicator takes into account how the access restriction label affects information «aging» – the process of losing credibility due to changes and the emergence of new data. In order to establish effective rules for the access distribution of confidential information, its classification into various categories according to its value level is necessary. To examine the influence of different value categories of confidential information in medical institutions, the use of access restriction levels to information (designated as $r_i$) has been proposed, encompassing confidential information, while considering the time of its further aging [4, 5]. Through the application of a ranking method, the coefficient of the impact of the level of information access restriction on its value, denoted as $\beta_1$, was obtained. Subsequently, the normalization of this coefficient was carried out using the following formula:

$$\beta_1 = \frac{r_i}{\sum_{i=1}^{n} r_i}, \tag{2}$$

where $n$ is the number of levels of access to information and $r_i$ is the coefficient that reflects the importance of the $i$-th level of access to information.

To determine the coefficient of the impact of the final aging time of information on its value for a specific level of access to information, denoted as $\beta_2$, the following expression was used:

$$\beta_2 = \frac{t_i}{\sum_{i=1}^{n} t_i}, \tag{3}$$

where $n$ is the number of levels of access to information and $t_i$ is the final aging time of information for the $i$-th level of access.

The coefficient that reflects the impact of the «Access Restriction Level» indicator on information value, denoted as a1, consists of two equivalent components – $\beta_1$ and $\beta_2$, and its value is calculated as the arithmetic mean of these two coefficients. The term «critical» refers to information the loss or unauthorized access to which would cause significant damage to the institution or result in a complete halt of its operations. The significance of information and its importance level is suggested to be determined by a panel of experts from the institution, with the quantitative value obtained through normalizing importance levels using the following expression:

$$a_2 = \frac{im_j}{\sum_{j=1}^{k} im_j}, \tag{4}$$

where $k$ is the number of levels of access to information and $im_j$ is the $j$-th level of information importance.

The level of ownership rights concerning the information circulating within the institution and subject to protection is determined by a panel of experts from the institution, while the quantitative value is obtained by normalizing the levels of ownership rights to the information using the following expression:

$$a_3 = \frac{o_i}{\sum_{i=1}^{m} o_i}, \tag{5}$$

where $m$ is the number of levels of information access types and $o_i$ is the $i$-th level of information access type [4, 5].

After the implementation of a comprehensive information security system with access level segregation and directory service, changes occurred in the indicators of information importance levels and ownership rights to information. The results of these updates are provided in Table 1 and Table 2.

Table 1 – Information importance levels (after access restrictions implementation)

| Information by importance level | *im j* | $a_2$ |
|---|---|---|
| Vitally essential | 5 | 0.333 |
| Very important | 4 | 0.267 |
| Important | 3 | 0.200 |
| Useful | 2 | 0.133 |
| Insignificant | 1 | 0.067 |

Table 2 – Information ownership rights levels (after access restrictions implementation)

| Information by ownership rights type | *o j* | $\alpha_3$ |
|---|---|---|
| Collective (institution) | 3 | 0.5 |
| Collective (department within institution) | 2 | 0.3 |
| Personal | 1 | 0.2 |

## 4. Designing

After implementing a comprehensive data protection system and granting all participants involved in data processing access to documents of various security levels, a clear differentiation of ownership rights to information of different values has been achieved. The results of the information value assessment and indicators reflecting changes in access restriction levels are presented in Table 3 and Table 4.

Table 3 – Information value calculations (initial data)

| *Information Names* | $a_i$ | $a_2$ | $a_3$ | *VOI* |
|---|---|---|---|---|
| Accounting documentation | 0.183 | 0.400 | 0.200 | 0.78 |
| Human resources department documentation | 0.289 | 0.300 | 0.200 | 0.79 |
| Medical information system server | 0.478 | 0.400 | 0.200 | 1.08 |
| Personal (confidential) information about patients of the medical enterprise (personal data, treatment and medical records, financial transactions) | 0.183 | 0.400 | 0.500 | 1.08 |
| Regulatory acts of the medical enterprise | 0.289 | 0.300 | 0.200 | 0.79 |
| Computer and software resources of the medical enterprise | 0.183 | 0.300 | 0,200 | 0.68 |
| Information about projects developed and implemented at the medical enterprise | 0.183 | 0.300 | 0.200 | 0.68 |
| Expansion plans of the medical enterprise | 0.478 | 0.400 | 0.167 | 1.04 |
| Investment plans, procurement, sales, and their technical and economic justification | 0.478 | 0.400 | 0.167 | 1.04 |
| Information about clients, contractors, suppliers, and business partners of the medical enterprise | 0.289 | 0.200 | 0.200 | 0.69 |
| Information regarding the content of agreements, contracts, agreements, and other organizational commitments | 0.289 | 0.200 | 0.200 | 0.69 |

Continuation of table 3

| | | | | |
|---|---|---|---|---|
| Information about security measures, access control (access control system), alarm system, and internal communication structure at the medical enterprise | 0.183 | 0.300 | 0.200 | 0.68 |

Table 4 – Information value calculations (after access restrictions implementation)

| *Information Name* | $a_i$ | $a_2$ | $a_3$ | *VOI* |
|---|---|---|---|---|
| Accounting documentation | 0.157 | 0.333 | 0.333 | 0.82 |
| Human resources department documentation | 0.113 | 0.267 | 0.333 | 0.71 |
| Server infrastructure of the medical center (medical information system server, file servers, terminal servers, backup servers, access management servers) | 0.391 | 0.333 | 0.333 | 1.06 |
| Personal (confidential) information about patients of the medical enterprise (personal data, treatment and medical records, financial transactions) | 0.072 | 0.267 | 0.500 | 0.84 |
| Regulatory acts of the medical enterprise | 0.113 | 0.200 | 0.333 | 0.65 |
| Computer and software resources of the medical enterprise | 0.072 | 0.267 | 0.333 | 0.67 |
| Information about projects under development and implementation at the medical enterprise | 0.072 | 0.267 | 0.333 | 0.67 |
| Expansion plans of the medical enterprise | 0.243 | 0.267 | 0.167 | 0.68 |
| Investment plans, procurements, sales, and their technical and economic justification | 0.243 | 0.333 | 0.167 | 0.74 |
| Information about clients, contractors, suppliers, and business partners of the medical enterprise | 0.113 | 0.133 | 0.333 | 0.58 |
| Information about the content of agreements, contracts, arrangements, and other organizational commitments | 0.113 | 0.133 | 0.333 | 0.58 |
| Information about security procedures, access control (access control system), alarm system, and internal communication structure within the medical enterprise | 0.072 | 0.267 | 0.333 | 0.67 |
| Informational and analytical reports on the operation of the access control and video surveillance system of the medical enterprise | 0.113 | 0.267 | 0.333 | 0.71 |
| Medical and statistical reports on the operation of the medical enterprise | 0.024 | 0.133 | 0.333 | 0.49 |

The comparative analysis of Table 3 and Table 4 reveals that following the implementation of a comprehensive data protection system and the assignment of special security levels to all participants involved in the processing of protected data and documents, a clear distinction in ownership rights to information of varying values has been achieved. Consequently, this allows for an expansion of the group of employees utilizing the information, a reduction in access time, and the generation of information-analytical reports regarding the performance of the access control system.

## 5. Conclusions

The value of information increases based on several factors: the level of access restriction to the information, the information importance level, and the level of ownership rights to the information. Restricted access heightens interest and designates the information as important and valuable. Information that holds key significance for decision-making or goal achievement becomes more valuable to an organization or an individual. To ensure security and access control based on the adapted model, different access levels will exist for each user according to their responsibilities and confidentiality. In general, the use of the hierarchical Bell-LaPadula access model allows for effective access control to the information system and ensures enterprise security.

## 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. 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.

4. Бойченко О.С., Костерев Д.С., Маковський І.Ю., Грищук О.М. Математична модель розрахунку цінності інформації установи. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. 2022. Вип. 22. С. 30–40.

5. Мороз Б., Молотков О., Ульяновська Ю. Методи визначення цінності інформації для організації її захисту. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2001. Вип. 2. С. 46–53.

6. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Вид-во НА СБ України, 2020. 256 с.

*Стаття надійшла до редакції 17.09.2023*