The Development of the Information Technology Architecture for the Anonymisation of Stakeholders Personal Data of Digitalized Education based on Formulated Criteria and Requirements

Iuliia Khlevna, Isus Raichuk and Oleksandr Timinskyi

Taras Shevchenko National University of Kyiv, 60 Volodymyrska Street, Kyiv, 01033, Ukraine

Abstract

The article shows that currently, the question of protecting the personal data of stakeholders in the digitalized educational sphere is important. The object of the research is the protection processes of personalized data of stakeholders in the digitalized educational sphere. The solved issue is a formalization of parameters and criteria when forming requirements for the information system and the development of a concept for the architecture of information technology based on which requirements for such kind of technology are justified. The assessment of the degree of positive effect from the functioning of the information system depending on the selected criteria is offered. Based on the completed formalization the requirements to the architecture for information solution of anonymization of personal data in the digitalization of education is defined; also, the requirements to the components of architecture solution of information technology are formed. The architecture of information technology on anonymization of personal data in the educational sphere is developed. The characteristics of such a system are represented and they are evaluated as well. Well-developed requirements and architecture are going to become the basis for the information technology of anonymization of personal data of stakeholders of digitized education. The prospects for further research are outlined.

Keywords [1]

Digitalization, educational space, anonymization, architecture of information technology, information system requirements, assessment of information system.

1. Introduction

In the era of great and fast development of digital technologies, virtualization and the growing dependence from online resources the question of personal data protection become relevant as never before. It mostly refers to the field of education, where digitalization is becoming necessary to ensure access to knowledge at any time and from any place. However, along with this opportunity the threat of violating the confidentiality of personal information of digital education stakeholders is rising. The growing amount of data collected in educational institutions and platforms requires ensuring the appropriate level of confidentiality and protection of personal information of students, teachers, administration and other participants in the educational process.

Anonymization is a necessary tool that allows you to save valuable data for the analysis and improvement of educational processes, while ensuring the anonymity and privacy of the persons whose data is processed. In this regard, the development and application of information technologies in the educational environment is a key aspect of the anonymization of personal data. At the same time, it is worth to take into account that the main element in the formation of any information technology is the formation of requirements for it. An urgent scientific task based on the above rises, which consists of the development of the concept of the architecture of information technology, based on which the requirements for such technology will be substantiated.

Information Technology and Implementation (IT&I-2023), November 20-21, 2023, Kyiv, Ukraine
EMAIL: yuliia.khlevna@knu.ua (Iuliia Khlevna); neversaydie.jr@gmail.com (Isus Raichuk); o.timinskyi@knu.ua (Oleksandr Timinskyi)
ORCID: 0000-0002-1874-1961 (Iuliia Khlevna); 0000-0002-0968-4811 (Isus Raichuk); 0000-0001-8265-6932 (Oleksandr Timinskyi)

2. Literature review

The accumulation of data, their processing, and the formation of decisions based on them is a modern requirement, including in the educational sphere [1, 2]. The issue that scientists and practitioners are addressing is the preservation of data confidentiality. In the digitized educational space, the integration of data, and their aggregation from various sources for various educational and scientific purposes is becoming increasingly widespread [3]. The responsibility for preserving the confidentiality of the personal data of the stakeholders of the educational process remains open. It can be argued that this is a task of legislation [4], but the question of how to protect this data is a question of the institution that carries out educational activities.

The organizational processes of saving personal data in the digital space are reflected in [5-7]. The disadvantage is that the formation of models, methods, and principles of confidentiality preservation only with the use of organizational methods is not effective in the digital space. The continuation of the research, in particular, the combination of anonymization operations, privacy models, and presentation of some anonymization tools is presented in the article [8]. The disadvantage of the work is that the work offers tools with ready-made solutions for data protection, with the involvement of third-party platforms, which do not take into account the peculiarities of the activities of educational institutions. Also, the use of external platforms that offer their own data protection is presented in the work [9]. However, this protection may be outside the educational environment, which may conflict with the requirements of the educational space. In works [10, 11] a solution was proposed using information technology tools. The shortcoming of the works is that they do not single out the requirements for information technologies of anonymization, and do not present an assessment of the functioning of the information system of digitized education. The issue of anonymization of information extraction and automatic display of confidential documents is presented in the work [12]. The disadvantage is that the information system can process a limited type of data. Recently, the use of artificial intelligence tools for saving conference information has become particularly widespread [13-15]. The disadvantage of this method for implementation in the educational field is that data is required for training systems, and artificial intelligence requires access to information transmitters, storage, etc. It is appropriate for educational institutions to develop information technology in which the main focus will be on the source of data in the middle of the educational environment.

Therefore, the analysis of the resources has shown that the research aimed at solving issues related to the formalization of the anonymization of personal data of stakeholders in the digitalized educational sphere and the formation of the concept of requirements for the information technology of the anonymization of personal data and the formation of its technological solutions is promising.

3. Purpose and objectives of the research

The purpose of the research is to develop an information technology architecture for the anonymization of personal data of stakeholders in the digitized educational sphere based on the formalization of parameters, needs and requirements for the information system which will make it possible to develop protection of confidentiality, integrity and availability of data in the conditions of digitization of the educational sphere with the use of information technologies.

To achieve this goal, the following tasks must be solved:

- to propose indicators and criteria reflecting the degree of positive effect from the functioning of the information system of anonymization of personal information in the digitized educational sphere;
- to form requirements for the architecture of the information solution for personal information anonymization in the digitized educational sphere;
- to develop the architecture of the information system of personal data anonymization.

4. Indicators and criteria reflecting the degree of positive effect from the information system functioning of personal information anonymization

The growing volume of data accumulated in the digital Eco space of education is a prerequisite for the formalization of indicators of personal data anonymization in relation to its stakeholders. A classification of indicators and criteria for anonymization of stakeholder's personal data in the digitized educational sphere is proposed (Table 1). The main condition of the classification is the validity of the indicators and criteria of anonymization of personal information in the digitized

educational sphere, which reflect the degree of positive effect from the functioning of the information system.

Table 1

Formalization of indicators and criteria that reflect the degree of positive effect from the information system functioning of personal information anonymization in the digitized educational sphere

The validity of the need for effective anonymization in the conditions of digitized education	Classification index	Criteria	Indi-cati-on
With the increasing use of digital platforms and tools in education, students, teachers, parents and other stakeholders are disclosing a significant amount of personal information. Anonymization allows you to protect this data from unscrupulous persons and avoid possible misuse of this information	Ensuring the privacy of stakeholders (PS)	Reducing the risk of stakeholder data leakage	P_r
		Keeping data useful	P_c
		Data access control	P_a
		Context preservation	P_k
		System performance	P_o
		Reliability of the anonymization method	P_{re}
		Scalability	P_s
		Flexibility	P_f
		Protection against discrimination of educational process stakeholders	P_d
		Economy of anonymization	P_e
Legislation on the protection of personal data (for example, GDPR [16]) sets strict requirements for the processing of personal information. Anonymization allows educational institutions to meet these requirements without burdening the analysis and use of data to improve processes	Compliance with legislative regulations (S)		S
Anonymization of personal data allows for analysis and research without risking the disclosure of identifying information. This promotes a healthy balance between collecting valuable data to improve the educational process and preserving user privacy	Balanced analytics of anonymization of personal data of stakeholders in the digitized educational sphere (A)	Validity of processing	A_p
		Analysis and tracking of changes	A_c
		Work with different types of data	A_t
		Deanonymization of data within the local information network of the educational institution	A_d
		Integration of anonymized system	A_i
		The validity of the accumulation, processing and transmission of information	A_{dm}
	Increasing the confidence of stakeholders regarding the protection of their personal data	Distribution of anonymized data only with authorized external consumers of personal information	A_a

The carried-out formalization, according to the presented parameters and criteria, became the basis for determining proposals for the development of requirements for the technology of anonymization of personal data of stakeholders of digital education. In particular, on the basis of the formalization carried out, the requirements for the architecture of the information solution for the anonymization of personal information in the digitized educational sphere were formed:

1. Full anonymization – the system must ensure that no personally identifiable information can be recovered from anonymized data. This ensures that information remains confidential and private.

2. Preservation of the usefulness of data - during anonymization, it is important to preserve the value of data for further analysis and research. Data must remain sufficiently representative and useful to provide holistic insight without the risk of identity disclosure.

3. Specialized anonymization algorithms – the use of appropriate anonymization algorithms is key to ensuring a high level of privacy. These algorithms may include data substitution, encryption, and masking techniques.

4. Access control – the system must have a thorough access control mechanism that allows restricting access to anonymized data only to authorized users with the appropriate authority.

5. Data encryption – to prevent possible unauthorized access to anonymized data, it is important to use strong encryption at the level of data storage and transmission.

6. Preservation of context – the system must preserve some level of context to ensure the validity and usefulness of the data. This helps to correctly interpret and analyze anonymized data.

7. Monitoring and auditing – it is important to conduct constant monitoring and auditing of the anonymization system in order to identify possible privacy violations and eliminate them in a timely manner.

8. Ease of integration with the existing ecosystem – the personal data anonymization system should be developed taking into account the ease of its integration into the existing information and technological infrastructure of the educational institution. This allows you to reduce efforts and risks when implementing a new system, while keeping the work of other components of the ecosystem unchanged. Ease of installation and use facilitates faster and more efficient implementation of personal data anonymization, ensuring a smooth transition to a new level of data protection in a digitized educational environment.

9. In addition, the information system of personal data anonymization should possess such properties as: scalability, flexibility, speed of processing, combination of anonymization methods.

The degree of the positive effect of the functioning of the information system of anonymization of personal data in the digitized educational space is proposed to be evaluated by:

$$\begin{Bmatrix} P_r \Rightarrow min, \;\; P_c \Rightarrow max, P_a \Rightarrow max, P_k \Rightarrow max, P_o \Rightarrow max, \\ P_r \Rightarrow max, P_s \Rightarrow max, P_f \Rightarrow max, P_d \Rightarrow max, P_e \Rightarrow min, \\ S \;\; \Rightarrow max, \\ A_p \Rightarrow max, A_c \Rightarrow max, A_t \Rightarrow max, A_d \Rightarrow max, \\ A_i \Rightarrow max, A_{dm} \Rightarrow max, A_a \Rightarrow max. \end{Bmatrix} \quad (1)$$

If there is no information technology in the educational environment that meets the specified requirements, anonymization can be estimated with some integrated value a-, and with the use of information technology that meets the established requirements - value a+, and at the same time, the anonymization value is much higher than before the use of the information system, which meets the stated requirements (a+>>a-), then we can say that the developed information system is effective. Anonymization is justified. We believe that meeting these requirements will help create an effective personal data anonymization system that ensures a high level of confidentiality and privacy protection for participants in the digitalized educational sphere.

5. Development of the information system architecture of personal data anonymization

The modular architecture of the personal data anonymization information system, which meets the established requirements, is presented in fig. 1. The main components of the proposed information system are: the information management system of the educational institution, the interconnection of

various information systems of the educational institution (integration layer), the system of anonymization of personal data of stakeholders of the digitized educational sphere.

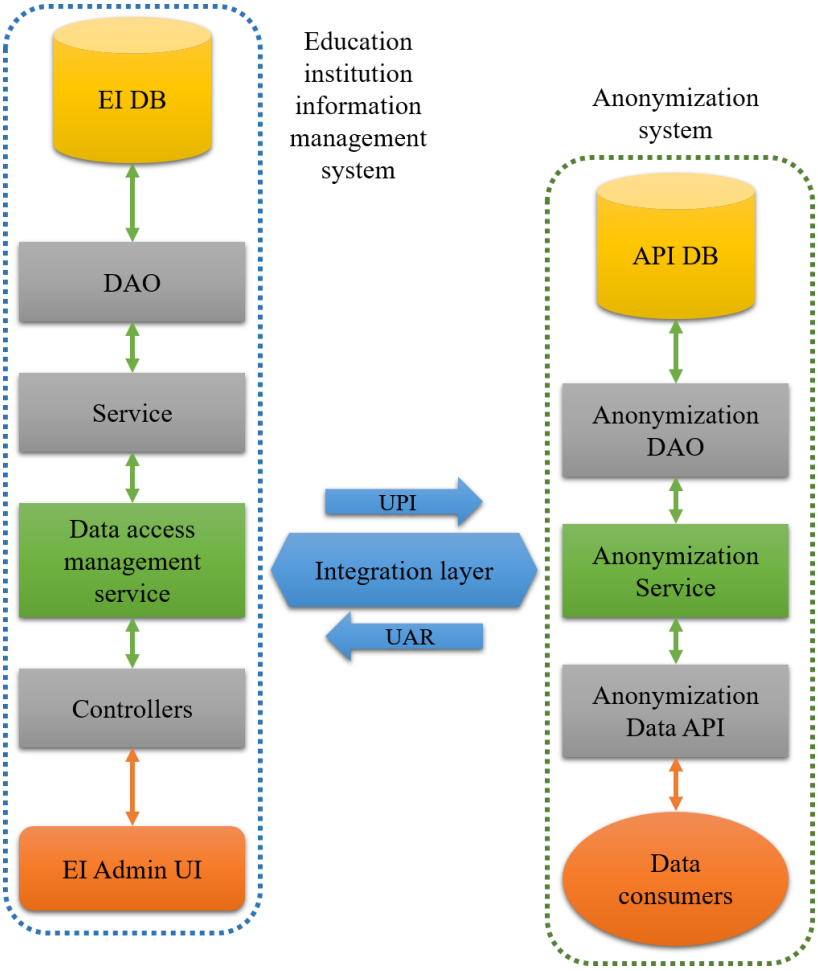

Figure 1: Architecture of information technology of personal data anonymization

1. Educational institution information management system (Education institution information management system) - the existing centralized digital system for managing all information of the educational institution with which the future integration of the personal data anonymization system will take place. The following structure of this block is proposed:

- The database of the educational institution (EI DB) is a digital repository of all the information necessary for the full functioning of the educational institution.
- The data access layer (DAO) is a specific implementation of the mechanism for providing read and write operations to the database.
- The business logic layer (Service) is a management layer that provides all the necessary functions for manipulating the data structure of an educational institution.
- Data access management service of the educational institution is one of the most important elements of the system, a layer that provides authorized access to the data of the educational institution.
- The controller layer (Controllers) is a layer that provides and declares ways of obtaining and manipulating information.
- The admin panel of the educational institution (EI Admin UI) is a tool for managing the digital information of the educational institution by appropriately trained personnel.

2. Integration layer – a layer that ensures internal communication of various information systems of an educational institution. In the context of integration with the personal data anonymization system, this layer ensures the distribution of personal data to the anonymization system, respectively,

for their further anonymization by this system. The flow of new data (reports, assessments, etc.) obtained from external sources will go in the opposite direction.

3. Information system of anonymization of personal data of stakeholders of the digitized educational sphere (Anonymization system) - a system whose purpose is to integrate into the existing digital data management tools of the educational institution is to ensure a high level of protection of personal data of stakeholders of the educational process. The architectural components of the personal information anonymization system are as follows:

- The database of the anonymization system (API DB) is a repository for saving generated anonymous data and all metadata necessary for their internal identification and processing.
- The layer of access to the database of the anonymization system (Anonymization DAO) is a layer that provides access to the information of the database of the anonymization system and provides tools for working with it.
- The business logic layer of the anonymization system (Anonymization Service) is a layer in which real data is processed, their anonymous substitute copies are generated, identifiers are de-anonymized, and other business logic is related to the anonymization and de-anonymization of personal information.
- Anonymization Data API – an interface that provides an authorized exchange of information between an educational institution and external educational platforms used by stakeholders of the educational ecosystem to ensure the effectiveness of the educational process.

The main characteristics of the information technology of personal data anonymization have been determined, from the point of view of ease of use and efficiency of performance of the functions assigned to the system. Such indicators are often decisive when integrating new functional units into the existing information technology. The characteristics of the proposed architecture of the anonymization system are:

1) Scalability (Ps) such an architecture is able to effectively scale with respect to the growing amount of data accumulated in the educational process. After all, the use of a separate layer of access to the database allows, by modifying only it, to switch to different models of data storage, such as distributed databases. This will ensure reliable operation of the system even with an increase in the volume of information.

2) Flexibility (Pf): such an architecture can be adapted to different types of data that are processed in an educational context. After all, the data types of the anonymized database essentially repeat the already existing data types (tables) in the database of the educational institution.

3) Various methods of anonymization (Adm) having the logic of anonymization in a separate layer (Anonymization Service) modification of the only particle will allow to support various methods of anonymization, including substitution, general encryption, hashing and others. This allows you to choose the best approach for a specific type of data and specific privacy requirements.

4) Integration with existing systems (Ai): such a modular, separate architecture of the anonymization system can be compatible with various existing information systems and platforms of the educational institution. After all, it does not require changes to the existing digital data management system of the educational institution, but is a separate addition. That is, it is enough to simply configure the integration layer of messaging between the existing data management system and the anonymization system of users' personal information. This approach ensures convenient and smooth implementation of the future data anonymization system.

5) Processing Speed (Po): This approach (separate system) is efficient in terms of data processing speed. After all, the system is able to provide timely anonymization with minimal impact on the productivity of the entire digital management system of the educational institution.

These are characteristics that together create a simple, reliable and effective architecture of the system of anonymization of personal data of stakeholders in the digitized educational sphere, ensuring reliable protection of the confidentiality and privacy of participants in the educational process and reflecting the extent of the positive effect of the functioning of the information system in the digitized educational space.

When forming the architectural vision of the information system for the anonymization of personal data of stakeholders in the digitized educational sphere, the next step was the formation of

requirements for the components of the architectural solution of the information technology of personal data anonymization. The following requirements are proposed for:

- *Databases of the anonymization system:*

1. The database must use strong encryption for data storage and transmission.
2. Regular data backup helps ensure recovery of information in case of possible data loss.
3. Ability to track and store different versions of anonymized data, which allows analysis and tracking of changes.
4. Different types of data and ways of processing them to meet the different needs of the educational field.
5. Large volumes of data in the educational field require high speed of processing and queries to the database.
6. The ability to audit user actions in the database helps identify and respond to potential security threats.

- *Layer of access to the database of the anonymization system:*

1. The layer should include measures to protect against SQL injection attacks, which can be used by attackers to gain access to the database.
2. The implementation of the toolkit should be based on current information technologies to ensure the maximum level of speed and data protection.
3. A mandatory requirement is the possibility of asynchronous transactional work with the database.
4. Speed of data return is a key goal.

- *The business logic layer of the anonymization system:*

1. The service layer should be ready for integration with existing systems of educational institutions, ensuring convenient and joint work with data.
2. The service layer should provide the ability to process user requests for anonymized data and ensure their integrity.
3. The system should be able to manage the anonymization process, including the choice of methods, parameters and saving mappings for possible data recovery (provided that this does not violate confidentiality).
4. The service layer should ensure the implementation of various data anonymization methods, such as substitution, encryption, hashing, and others.

- *Data access interface by external consumers:*

1. The data access interface (DIA) must use authentication mechanisms to verify the identity of external consumers and authorization systems to control their level of access to anonymized data.
2. The interaction between external consumers and the system should take place using secure data transfer protocols, such as HTTPS, to ensure data privacy and security.
3. The API must have clear and understandable documentation that explains functionality, request and response parameters, and interaction rules.
4. The API must provide the ability to restrict access to certain types of data or certain operations in accordance with user access rights.
5. To provide additional security, it is possible to implement authentication using API keys or tokens.
6. The API must provide stability and unbroken interoperability for external consumers, ensuring that changes to the API do not break existing functionality.
7. The access interface should include protection measures against possible attacks, such as brute force attacks, injections, and others.
8. Ability to use mechanisms for limiting the number of requests from one consumer to prevent system overload.
9. The API should be able to track and log the activity of external consumers for analysis and monitoring.

It was determined that the anonymized data base of the system and the data access interface deserve special attention. Researching the API layer is not very cost-effective, because there are many standards for building APIs of various systems (such as REST, SOAP, etc.), as well as authorization standards (OAuth, OpenID, etc.). Speaking of DBMS implementations, there is also something to

choose from here, but considering the importance of this block, it is worth developing the database structure of the information technology of personal data anonymization in accordance with the established requirements.

6. Scheme of the information technology database of personal data anonymization

A fragment of the generalized scheme of the relational database is presented in fig. 2.

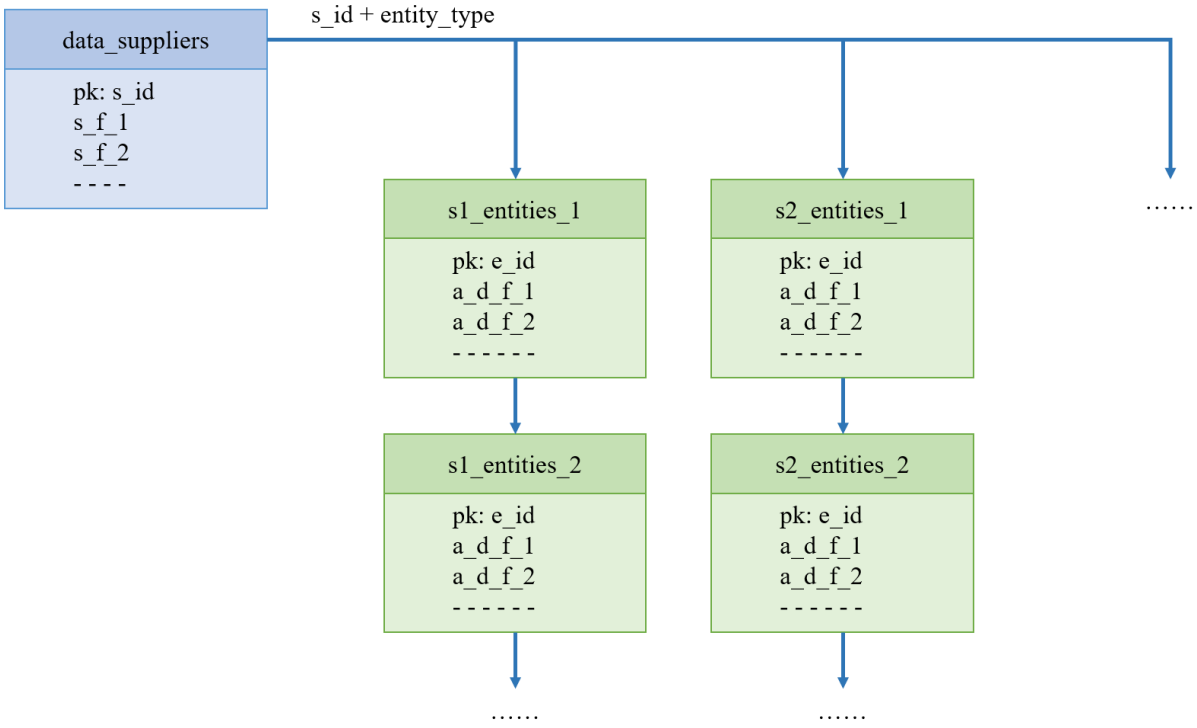

Figure 2: Database scheme of the personal information anonymization system

Basically, this scheme consists of two parts. Table-register of consumers of personal information (data_suppliers) - a list of existing consumers of personal data of the educational edition with their unique identifier (s_sd). The set of fields of such a table depends on the necessary information of the educational institution about a certain data consumer.

$$SF = \sum_{i=1}^{n} F = sf_1 + sf_2 + \cdots + sf_n \qquad (2)$$

Where SF – a set of fields of the table of consumers of personal information, F and sf – a certain field of such a table, n is the number of all fields of the table. A set of tables for each type of data for each consumer (s_id + entity_type) is a set of tables (AT) for storing anonymized instances of each type of data of an educational institution for each consumer of such data separately.

$$\sum_{i=1}^{n} E = E_1 + E_2 + \cdots + E_n \qquad \sum_{i=1}^{m} S = S_1 + S_2 + \cdots + S_m \qquad AT = \sum_{i=1}^{n} E * \sum_{i=1}^{m} S \qquad (3)$$

Where E is a certain type of data stored by the educational institution, n is the number of such types; S is a specific user of educational institution data, m is the number of such users. AT is the final set of tables. The set of fields of such tables will contain all the same fields that contain real tables of each type, as well as an additional identifier (e_id). That is, the list of fields of such a table can be expressed as follows:

$$\sum_{i=1}^{n} EF = EF_1 + EF_2 + \cdots + EF_n \qquad ESF = \sum_{i=1}^{n} EF + e_{id} \qquad (4)$$

Where EF is a set of database table fields of a certain type stored by an educational institution, n is the number of such fields in the educational institution's table; ESF - a set of table fields of the anonymization service database of a certain type of data stored by the educational institution; e_id is a field for storing the identifier of a certain table. As a result, we get the following features of such an anonymous database table scheme. First of all, the more the integrated educational institution with the greater number of consumers of anonymous data, the greater the number of tables we will have in the database scheme. Secondly, the more different types of personal data the educational institution stores, the more tables of anonymous versions of them the scheme of the anonymous data base will have. Therefore, we've got such a conclusion:

$$P_s \Rightarrow max \tag{5}$$

That is, it is possible to increase the number of tables in the scheme of the anonymous data base of the educational institution. But for modern DBMS, thousands or even hundreds of thousands of tables do not cause any problems.

$$P_o \Rightarrow max, A_c \Rightarrow max, A_t \Rightarrow max, A_{dm} \Rightarrow max. \tag{6}$$

We have a separate set of tables for each consumer, that is, a separate table for each type of data. Hence, parallel work with data for each individual type of data of each individual consumer does not in any way affect the consistency of data of other users, as well as the speed of processing requests of other data consumers. Which, as stated earlier, is a key requirement for the system of anonymization of personal information of stakeholders of a digitized educational institution.

7. Conclusions

The article has formalized indicators and criteria that reflect the degree of positive effect from the functioning of the information system of anonymization of personal information of stakeholders in the digitized educational sphere. The indicators are: ensuring the privacy of stakeholders, compliance with legal regulations, balanced analytics of anonymization of personal data of stakeholders in the digitalized educational sphere, and increasing the trust of stakeholders regarding the protection of their personal data. Criteria are given for each indicator. An assessment of the degree of positive effect of the functioning of the information system is proposed, depending on the selected criteria. The carried-out formalization became the basis for determining the requirements for the architectural component of the anonymization of the personal data of stakeholders.

The requirements for the architecture of the information solution for the anonymization of personal information in the digitized educational sphere have been determined, and the requirements for the components of the information technology architectural solution have also been formed. It was established that the database of anonymized data of the system deserves special attention when forming requirements. The architecture of the information technology solution for the anonymization of personal data in the field of education has been developed. The main features of the obtained solution are described. The database scheme in the environment of the information technology architecture of anonymization of personal information of stakeholders of the digitized educational sphere has been developed and described in detail. An algorithm for its formation is also proposed, taking into account the specifics of the educational institution's data scheme.

Further research in this direction is planned to be focused on the detailed selection of technologies and standards for the implementation of the system of anonymization of personal information of stakeholders of a digitized educational institution based on the developed architecture. As well as further implementation of the anonymization system itself and its integration into the educational institution.

8. References

[1] Khadija Ahaidous, Mohamed Tabaa, Hanaa Hachimi, Towards IoT-Big Data architecture for future education, Procedia Computer Science, Volume 220, 2023, Pages 348-355, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.03.045.

[2] Lu Zheng, Cong Wang, Xue Chen, Yihang Song, Zihan Meng, Ru Zhang, Evolutionary machine learning builds smart education big data platform: Data-driven higher education, Applied Soft Computing, Volume 136, 2023, 110114, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2023.110114.
[3] Xinxiao Yang, Xincan Zhu, Dianbing Chen, Discourses regarding education governance in the digital age at K-12 level: Possibilities, risks, and strategies, Teaching and Teacher Education Volume 132, 2023, 104261, ISSN 0742-051X, https://doi.org/10.1016/j.tate.2023.104261.
[4] Hiroshi Ueda, Hiroaki Ogata, Tsuneo Yamada, Developing Policies for the Use of Education and Learning Data in Japan, Procedia Computer Science, Volume 192, 2021, Pages 5015-5022, https://doi.org/10.1016/j.procs.2021.09.279.
[5] Ewa Mazur-Wierzbicka, E-communication and CSR - a new look at organizations' relations with stakeholders in the time of digitalization, Procedia Computer Science, Volume 192, 2021, Pages 4619-4628, https://doi.org/10.1016/j.procs.2021.09.240.
[6] Isus Raichuk, Iuliia Khlevna, Oleksandr Timinskyi, Oleksandr Voitenko. Cognitive model of digitalization of business processes of a project-oriented it company. CEUR Workshop Proceedings, 2022. https://ceur-ws.org/Vol-3382/Paper12.pdf.
[7] Huang, R.H., Liu, D.J., Zhu, L.X., Chen, H.Y., Yang, J.F., Tlili, A., Fang, H.G., Wang, S.F. (2020). Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents. Beijing: Smart Learning Institute of Beijing Normal University.
[8] Zuo Z, Watson M, Budgen D, Hall R, Kennelly C, Al Moubayed N. Data Anonymization for Pervasive Health Care: Systematic Literature Mapping Study. JMIR Med Inform. 2021 Oct 15;9(10):e29871. doi: 10.2196/29871. PMID: 34652278; PMCID: PMC8556642.
[9] Tatomyr Iryna. Cyber security of universities as a way to counter phishing scams. Economic discourse. 2020. Issue 1. p. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7.
[10] Anju Kalluvelil Janardhanan, Kavitha Rajamohan, K.S. Manu, Sangeetha Rangasamy, Chapter 2 - Digital education for a resilient new normal using artificial intelligence—applications, challenges, and way forward, Editor(s): Upasana Gitanjali Singh, Chenicheri Sid Nair, Susana Gonçalves, In Chandos Information Professional Series, Digital Teaching, Learning and Assessment, Chandos Publishing, 2023, Pages 21-44, https://doi.org/10.1016/B978-0-323-95500-3.00001-8.
[11] Zongda Wu, Shaolong Xuan, Jian Xie, Chongze Lin, Chenglang Lu, How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective, Computers in Biology and Medicine, Volume 147, 2022, 105726, ISSN 0010-4825, https://doi.org/10.1016/j.compbiomed.2022.105726.
[12] Rodrigo Juez-Hernandez, Lara Quijano-Sánchez, Federico Liberatore, Jesús Gómez, AGORA: An intelligent system for the anonymization, information extraction and automatic mapping of sensitive documents, Applied Soft Computing, Volume 145, 2023, 110540, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2023.110540.
[13] Luca Belli, Nicolo Zingales, Data protection and artificial intelligence inequalities and regulations in Latin America, Computer Law & Security Review, Volume 47, 2022, 105761, https://doi.org/10.1016/j.clsr.2022.105761.
[14] Khlevna I., Koval B. Fraud detection technology in payment systems. // IT&I 2020 – Information Technology and Interactions. Proceedings of the 7th International Conference "Information Technology and Interactions" (IT&I-2020). Workshops Proceedings. Kyiv, Ukraine, December 02-03, 2020. CEUR Workshop Proceedings, – P. 85 – 95.
[15] Lu Zheng, Cong Wang, Xue Chen, Yihang Song, Zihan Meng, Ru Zhang, Evolutionary machine learning builds smart education big data platform: Data-driven higher education, Applied Soft Computing, Volume 136, 2023, 110114, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2023.110114.
[16] General Data Protection Regulation (GDPR), Official Journal of the European Union, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679