Ministry of Education of the Republic of Belarus

Educational institution

Belarusian State University of Informatics and Radioelectronics

UDC 621.391;621.383.92

Zhu Shuoyu

# Development of a Scheme for Depersonalization of Personal Data Based on the DES Standard

Master degree thesis

Specialty 1-98 80 01 Information Security

_____

**Supervisor:**

Тимофеев, А.М

**Associate Professor**

_____

**Minsk2026**

# INTRODUCTION

The rapid development of information technologies and the widespread implementation of automated data processing systems have led to an exponential growth in the volume of personal data circulating within the information systems of organizations of various ownership forms. Concurrently, there is a steady trend toward tightening legislative requirements in the field of personal data protection, both at the international level and within national legal frameworks. In the Republic of Belarus, the fundamental regulatory legal act in this area is the Law of the Republic of Belarus No. 99-Z of May 7, 2021, "On Personal Data Protection", as well as a number of subordinate acts and presidential decrees aimed at improving mechanisms for personal data protection.

One of the key tools for ensuring the information security of personal data during their processing in information systems is depersonalization (anonymization) – a process as a result of which it becomes impossible, without the use of additional information, to determine the affiliation of personal data to a specific subject. Depersonalization of personal data significantly reduces the risks of unauthorized access and leakage of confidential information and also expands the possibilities for the legitimate use of depersonalized data for statistical research, analytical processing, and software testing without threatening the violation of the rights of personal data subjects.

Existing depersonalization methods, such as the identifier introduction method, the method of changing composition or semantics, the decomposition method, and the shuffling method, possess varying degrees of effectiveness and security. However, most of them either do not provide an adequate level of cryptographic protection, require significant computational resources for implementation, or do not fully preserve such important properties of depersonalized data as completeness and representativeness. In this regard, an urgent scientific and technical task is the development of new approaches to the depersonalization of personal data, based on the application of proven cryptographic algorithms and ensuring an acceptable balance between the level of security and computational efficiency.

The relevance of the research topic is determined by the necessity to develop effective and secure methods for depersonalizing personal data that comply with the requirements of the legislation of the Republic of Belarus in the field of information protection and take into account modern information security threats. The Data Encryption Standard (DES), despite its age and known limitations regarding key length, continues to be one of the most studied and widely used block ciphers, possessing high performance and the capability for efficient software and

hardware implementation. Modifying the DES algorithm for personal data depersonalization tasks and developing, on its basis, a structural scheme that ensures the required level of security constitutes a relevant scientific and applied task.

The aim of the master's thesis is to develop a structural scheme for the depersonalization of personal data based on the DES standard, ensuring the required level of information security while preserving the completeness and representativeness of the depersonalized data.

To achieve the stated aim, the following tasks must be solved:

1. Conduct an analysis of the current state of the problem of personal data depersonalization, including a review of the regulatory framework and existing depersonalization methods.
2. Investigate the architecture and operating principles of the DES standard and assess its applicability for solving personal data depersonalization tasks.
3. Develop a structural scheme for the depersonalization of personal data based on a modified DES algorithm.
4. Describe the functioning principles of the developed scheme, including procedures for depersonalization and re-identification of personal data.
5. Develop a software implementation of the proposed scheme and conduct its testing.
6. Perform an information security assessment of the developed scheme and its compliance with the requirements of the legislation of the Republic of Belarus.

The object of research is methods and means of depersonalization of personal data in information systems.

The subject of research is a structural scheme for the depersonalization of personal data based on the DES standard.

The scientific novelty of the work lies in the development of a modified algorithm for the depersonalization of personal data based on the DES standard, which differs from existing solutions by the combined application of cryptographic transformations and the decomposition method, thereby ensuring an increased level of information security while maintaining computational efficiency and the completeness of depersonalized data.

The practical significance of the work consists in the creation of a software package that implements the developed scheme for depersonalizing personal data, which can be integrated into the information systems of organizations that process personal data and require ensuring their protection in accordance with the legislation of the Republic of Belarus.

Approbation of the work results . The main provisions and results

of the master's thesis were presented and discussed at the following scientific conferences:

1. XXI International Scientific and Practical Conference "Management of Information Resources", Minsk, March 28, 2025.

2. XXX Scientific and Practical Conference "Complex Information Protection", Lida, May 14-16, 2025.

# MAIN PART

Chapter 1 This chapter introduces the definition and relevant Belarusian laws of personal data depersonalization. It analyzes five common depersonalization methods and compares their performance. It also reviews mainstream cryptographic algorithms, focusing on the principles, strengths and weaknesses of the DES cipher. Finally, the research goals are put forward: to build a DES-based depersonalization solution balancing security, efficiency and data completeness.

Chapter 2 A conceptual system model is designed following security and compliance rules. The standard DES algorithm is modified with CTR mode, format-preserving encryption and attribute-based key derivation. Combined with the decomposition method, a complete operational process for data depersonalization is proposed. This chapter also illustrates the algorithms for depersonalization and authorized re-identification, plus supporting security control measures.

Chapter 3 The scheme is implemented with Python and related libraries in a modular structure. Multiple tests are conducted on datasets of different sizes. Results prove the system works correctly with stable performance (around 460 records per second) and strong resistance to common statistical attacks. Compared with traditional methods, this solution provides much higher security at a reasonable cost.

Chapter 4 This part defines potential security threats and four types of attackers, and evaluates corresponding risks. Cryptographic analysis shows the modified DES scheme can resist brute-force and typical cryptanalytic attacks effectively. In addition, the developed system fully complies with Belarusian personal data protection regulations and is suitable for practical application.

# CONCLUSION

In the course of completing this master's thesis, a relevant scientific and applied task was solved – the development of a structural scheme for the depersonalization of personal data based on the DES standard, ensuring the required level of information security while preserving the completeness and representativeness of the depersonalized data.

The following main results were obtained in the work:

1. An analysis of the current state of the problem of personal data depersonalization was conducted. The analysis showed that existing depersonalization methods either do not provide an adequate level of cryptographic protection or are characterized by high computational complexity. The regulatory framework of the Republic of Belarus in the field of personal data protection was reviewed, and the key requirements for depersonalization procedures were identified.

2. The architecture and operating principles of the DES standard were investigated, and an assessment of its applicability for solving personal data depersonalization tasks was performed. It was established that DES, despite its limitations in key length, possesses a number of advantages (high performance, simplicity of implementation, extensive study) that make its use promising for depersonalization tasks, provided that it is combined with additional protection mechanisms.

3. A structural scheme for the depersonalization of personal data based on a modified DES algorithm was developed. The scheme includes the following main stages: preliminary data preparation, generation of key information, cryptographic transformation of attributes using CTR mode and Format-Preserving Encryption, formation of link tables, and storage of depersonalized data. The combined application of cryptographic methods and the decomposition method ensures a high level of information security.

4. The functioning of the developed scheme in the modes of depersonalization and re-identification of personal data was described. Algorithms for the main procedures were presented, and requirements for ensuring the security of the re-identification process were formulated.

5. A software implementation of the proposed scheme was developed using the Python programming language and the PyCryptodome library. Functional and performance testing of the implementation was conducted, confirming the correctness of the algorithms and acceptable performance (up to 460 records per second).

6. An information security assessment of the developed scheme was performed. The analysis showed that the scheme is resistant to known types of cryptanalytic attacks, including brute-force, linear, and differential cryptanalysis. The scheme complies with the requirements of the legislation of the Republic of Belarus in the field of personal data protection.

The scientific novelty of the work lies in the development of a modified algorithm for the depersonalization of personal data based on the DES standard, which differs from existing solutions by the combined application of cryptographic transformations (CTR mode, Format-Preserving Encryption) and the decomposition method, as well as the use of attribute-specific key derivation. This approach allows for an increased level of information security while maintaining computational efficiency and the completeness of depersonalized data.

The practical significance of the work consists in the creation of a software package that implements the developed depersonalization scheme, which can be integrated into the information systems of organizations processing personal data and requiring their protection in accordance with the legislation of the Republic of Belarus.

Recommendations for further development of the topic:

1. Investigation of the possibility of replacing the DES algorithm with more modern block ciphers (AES, GOST 28147-89) while preserving the overall architecture of the developed scheme.
2. Development of a distributed version of the system using blockchain technologies for the secure storage of link tables.
3. Integration of the developed scheme with existing data masking and tokenization systems.
4. Conducting a more detailed study of the resistance of the Format-Preserving Encryption implementation to various types of attacks.
5. Extending the functionality of the system with support for streaming data processing in real time.

The obtained results allow for the conclusion that the set goal of the work has been achieved, and the stated tasks have been fully solved. The developed structural scheme for the depersonalization of personal data based on the DES standard is an effective and practically applicable solution that ensures the required level of information security and can be recommended for use in information systems of organizations of the Republic of Belarus.

# LIST OF THE AUTHOR'S PUBLICATIONS

1-A. Timofeyev A.M., Voskova K.R., Zhu Shuoyu. Ensuring Information Security of Personal Data during Processing in Information Systems // Proceedings of the 30th Scientific and Practical Conference on Comprehensive Information Protection, Lida, 14–16 May 2025 / Standing Committee of the Union State of Belarus and Russia, Apparatus of the Security Council of the Russian Federation, Parliamentary Assembly of the Union of Belarus and Russia. Minsk: Kolorgrad, 2025. pp. 241–245.

2-A. Timofeyev A.M., Voskova K.R., Zhu Shuoyu. Personal Data Depersonalization Based on the Decomposition Method // Proceedings of the 21st International Scientific and Practical Conference on Information Resources Management, Minsk, 28 March 2025 / Academy of Public Administration under the aegis of the President of the Republic of Belarus; Editorial Board: V.G. Shvaiko et al. Minsk: Academy of Public Administration under the aegis of the President of the Republic of Belarus, 2025. pp. 307–308.