In summary, a discrete communication channel can be used to study independently by the technical engineers in the field of telecommunications technology using virtual simulation modeling. As it is not always possible for engineers to assemble and use telecommunications equipment at home, and this program analyzes the performance of discrete channels at home, the probabilistic characteristics of a discrete channel are standard elements and blocks of the Simulink section of MATLAB. allows you to do it independently. This process can save engineers real-time mode and increase and strengthen their work efficiency skills by 60-70%. In turn, the formation of remote monitoring of the work process of the object helps to bring the modern communication system to a new stage of development.

References

1. Z. Ghassemlooy, W. Popoola, S. Rajbhandari. Optical Wireless Communications: System and Channel Modelling with MATLAB - CRC Press; 1st Edition (August 8, 2012) Page No – 333.
2. Gultyaev A. Vizualnoe modelirovanie v srede Matlab. SPb.: Piter, 2000. Page No – 432 (In. Russian).
3. M. Guizani, A. Rayes Network Modeling and Simulation. - John Wiley & Sons Ltd, 2010-p-226.
4. T.O. Rakhimov, U.K. Matyokubov, and MR Yangiboyeva. Immediate modeling of matlab-simevents transmitting communication work process // Acta of Turin Polytechnic University in Tashkent, 9(1):4 2019. pp. 76–79.
5. Davronbekov D.A., Matyokubov U.K. The role of network components in improving the reliability and survivability of mobile communication networks // Acta of Turin Polytechnic University in Tashkent, 10(3):10, 2020.
6. Davronbekov D.A., Matyokubov U.K., Abdullaeva M.I. Evaluation of reliability indicators of mobile communication system bases // Acta of Turin Polytechnic University in Tashkent, 10(3):10, 2020. pp. 22-27.
7. Matyokubov U.K., Davronbekov D.A. Approaches to the organization of disaster resistant mobile network architecture in Uzbekistan // Acta of Turin Polytechnic University in Tashkent, 10(2):10, 2020. pp. 34-42.
8. Rakhimov T.O. Matlab-simevents are modeling a camergus servicing system for moving it information // Acta of Turin Polytechnic University in Tashkent, 1/2019 pp. 71-75.

THE ANALYSIS OF METHODS OF DATA DEPERSONALISATION IN INFORMATION SYSTEMS

Ganiev Abduhalil Abdujalilovich[1], Azizova Zarina Ildarovna[2]

[1]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
a.ganiev@tuit.uz
[2]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
z.i.azizova@mail.ru

Abstract. *This article deals with methods of ensuring the protection of personal data through the use of the process of anonymisation, as well as with the definition of the process of data anonymisation as a strategy for preserving basic information from the full set of personal data and mitigating possible risks that need to be taken into account in the use of data anonymisation methods.*

Keywords: *personal data, anonymisation process, ID introduction method, method of changing composition or semantic, mixing methods, depersonalisation of personal data, degree of depersonalization*

1. Introduction

A huge amount of open data processed and created by devices, sensors and networks, as well as new types of data in an environment of increasing public interests and the need to reuse this data at a time when the cost of storage is low can only benefi society, individuals and organisational structures significantly if the rights of everyone to personal data and privacy are guaranteed.

It is assumed that the depersonalisation of personal data should provide not only protection against unauthorised use, but also the possibility of processing it. Thus, data after depersonalisation must have such properties of completeness, i.e. the proper preservation of the available information about specific users or user groups, which was available before the data change; structured, i.e. the preservation of the structure links between the depersonalised data of a specific user or user group, corresponding to the links which were available before depersonalisation; relevance, i.e. the possibility to process requests and to receive answers to requests concerning personal data in the same way.

Anonimisation can be a good strategy to preserve the usefulness of data and reduce the risks of data compromise. In cases where the data set is anonymised and the identification of individual subjects is not possible, the data protection law loses its force. An analysis of scientific publications on this topic has shown that creating a truly anonymous data set from a huge set of personal data, taking into account the preservation of only important and required information, is a rather complex task.

Detection of personal data is used to reduce the attacker's attempts to use public information to detriment of an individual. As this method of protection does not require the use of means of protection, it also significantly reduces costs. According to the Law of the Republic of Uzbekistan "About personal data" [1], depersonalisation does not allow determining whether personal data belongs to an individual without applying additional information, i.e. the most important property of depersonalised data is the possibility of depersonalisation and the absence of such possibility is recognised only a private case.

Privacy is the right of a person to determine which personal information about himself/herself may be communicated to others. In the terms of data publishing, privacy is the right of a person or an entity to be secure from unauthorized disclosure of sensitive information. Sensitive information could be contained in an electronic repository, or can be derived as aggregate or complex information from data stored in an electronic repository.

Privacy preserving data mining has been proposed as a paradigm of exercising data mining while protecting the privacy of individuals. To protect the privacy of the respondents to which the data refer, released records are usually ensure by removing all explicit identifiers such as names, personal identification numbers, addresses, and phone numbers. Although apparently anonymous, the de-identified data may contain other data that often combine uniquely and can be linked to publicly available information to re-identify individuals.

Thus, in Uzbekistan, for the process of depersonalisation the same relevance for the direct and reverse task has been established.

2. The main part

The basis for the analysis of the state of the problem is the study of available scientific publications on depersonalisation of personal data in Uzbekistan, and not only. All areas of research can be conventionally divided into four groups of methods of depersonalisation applied. Table 1 shows that the presented identification and decomposition methods based on the separation of identifying information from impersonal data. Therefore, a common challenge for them is to ensure that the separated parts are linked during the work session. The identification part is not available to the intruder during storage, but may be available during other processing sessions (input, output). It should be noted that in terms of implementation algorithms of these two methods are fundamentally very close.

The methods of composition/semantics change and mixing are based on concealing the location of identifying information in an impersonal data set. A common challenge for such methods is ensuring that the algorithm secured during the session. At the same time, the identifying secured during the session. Identifying part is publicly available, so there is a danger of the algorithm being calculated by an intruder in any work mode.

A common, although less critical, disadvantage for all methods is the selection of a group of identifying attributes. The reason of this problem is the lack of a method for quantifying effectiveness of depersonalisation methods. In terms of costs, the problem is the need to modify the database structure and the application software to implement the depersonalisation method. Required modification may be technically impossible and economically unprofitable if the software development outsourced to an external organisation.

The anonymisation process is the result of processing personal data in order to irreversible prevent identification of the subject. As noted in Jeff Sedayao's research paper, the potential value of anonymisation lies in its application as a strategy for the use of open data both by individuals and by society, as a whole with the potential to reduce actual risks of certain subjects. Anonymisation can be the result of processing personal data with the aim of irreversibly preventing the identification of the

data subject, and at the same time, the possibility of using several methods of anonymisation not excluded, because there is no prescriptive standard in the legislation to which adherence would be a prerequisite [2].

Table 1.

Characteristics of methods of depersonalising personal data

Name of the method	Working principle	Element of secrecy	Weaknesses
Introduction of identifiers	The group of identifying attributes replaced by an abstract identifier, the group is kept in a separate table	Cross-reference table	The necessity to select the composition of the identification group; generation of an identifier; linking the table with impersonal data
Changing composition or semantics	Change in the number, position and size of fields (structure) or changes in the value of identifying attributes	Modification algorithm	The need to select the composition of the identification group; generation of the modification algorithm; providing the confidentiality of the algorithm
Decomposition	Splitting the database into several parts. storing communication information in a separate table	Relationship table	The necessity to select the composition of parts; generation of the modification algorithm; providing communication between parts
Shuffle	Moving a group of identifying attributes to records of others entities	Movement algorithm	The need to select composition of the identification group; generation of the algorithm for moving records; providing the secrecy of the moving algorithm

A key requirement for depersonalisation methods is the reversibility feature, namely the possibility of depersonalisation. Thus, the research work [3] confirms the possibility of dividing one personal database into several in order to reduce the requirements for processing part of the information, using the possibility of depersonalisation of each specific record when performing the functions of an operator. The authors note that this approach does not solve the problems, since the data are processed in full by the same operator. If this reduces the processing requirements, the probability of an attack at the time of depersonalising personal data increases, which in turn is a significant disadvantage for such systems.

The uniqueness of a surname under certain conditions is sufficient information to identify a subject and using an impersonal database with a simple shuffle method, a large amount of this type of information can be obtained. For example, if the mixed database contains information about the salary or position of the user, there is a high probability of determining to whom the knocked out information from the general range of numbers belongs.

Alternatively, by knowing the name and having it in the database, additional information can also be determined from this data. In some cases, the goal is to completely eliminate the reversibility of the information. Only one of the four data considered in the article answers this task, namely the method of changing the composition/semantics, which involves depersonalising personal data by replacing it with the results of statistical processing, summarising or deleting part of the data.

The anonymisation process has a risk factor that must be taken into account in assessing the validity of any anonymisation method, including the use of data that is subject to the anonymisation

process through the anonymisation method. It is important to assess the probability of the risk and the level of severity of the risk.

An effective solution to the anonymisation process does not allow all parties to identify the subject in a data set, to link two entries in a data set (or between two separate data sets) and to display any information in that data set. The removal of the direct identification elements will therefore not be sufficient to guarantee that the subject cannot be identified. It will often be necessary to take additional measures to prevent identification [4], depending on the context and purpose of their further processing for which anonymous data is intended.

3. Conclusion

Unfortunately, the lack of uniformly accepted method for quantifying the effectiveness of depersonalisation methods makes it impossible to compare the results of depersonalisation of data carried out using different methods.

Instead, it is possible to apply method of calculating the effectiveness of data depersonalisation using indicators of probability of identification and the degree of depersonalisation for methods of introducing identifiers [5], changing composition or semantics [6] and shuffle [7]. Figure 1 shows the identification probability values for different attributes, calculated using the method [5] for the method of introducing identifiers before and after modernisation. A level of identification probability equal to 0.01 is critical for identification. Sensitive attribute – PersonalName (identification probability equal to 1, excluded during the upgrade), insensitive attribute – UserID (identification probability equal to 0.0027, required identifier), insensitive attribute – UserBirthday (identification probability equal to 0.0014, excluded during the upgrade, because a pair of attributes UserID+UserBirthday is sensitive: identification probability equal to 0.75)

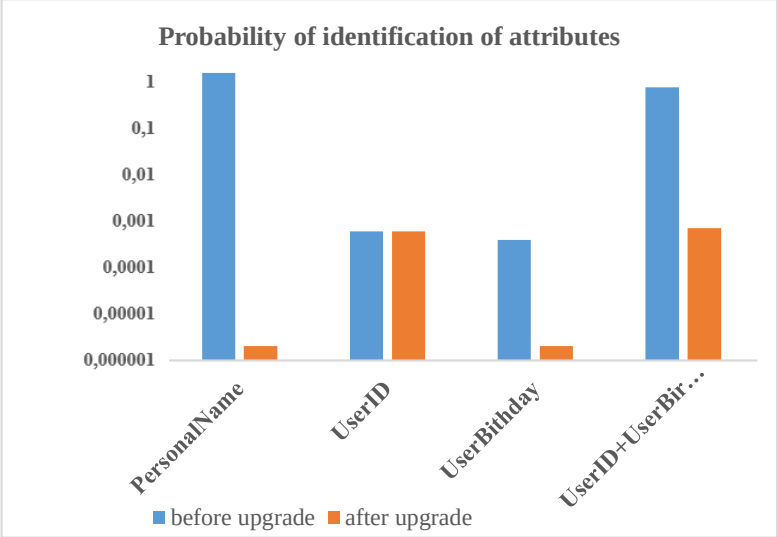

Fig.1. ***Changes of probability of identification in the implementation of the method of identifiers.***

The process of anonymisation, as a strategy to reduce privacy risks, is accompanied by of the following nature: *identification*, which corresponds to the ability to isolate some or all of the records that identify a person in data set; *ability to connect*, i.e. the ability to link at least two records relating to the same data subject or group of data subjects (either in the same database or in two different databases); and *logical conclusion*, which represents a possibility with a significant degree of certainty.

The degree of depersonalisation is an integral characteristic for the totally of attributes of individuals. Before the upgrade, its value was zero due to the presence of sensitive attributes in the database. After modernisation, the depersonalisation rate reached 0.997. Compared to the critical level of 0.997, this value can considered as a better. Thus, the application of depersonalisation (with the

obligatory possibility of depersonalisation) can provide effective protection of personal data. The most important is the dependence of depersonalisation effectiveness on the method of depersonalisation.

Despite the absence of a methodological basis for assessing the effectiveness of depersonalisation, it can be stated quite confidently that the most effective method from the point of view of providing the security of personal data is the introduction of identifiers. It is difficult to make reliable assessment of the economic efficiency of implementations, because the goal of achieving economic efficiency was not pursued in all cases. In order to introduce various methods of depersonalisation of personal data more widely, it is planned to improve the method of assessing the effectiveness of depersonalisation in the direction that makes it possible to form the relevant regulatory framework.

References

1. The Law of the Republic of Uzbekistan dated 2 July 2019 No.545 “About Personal Data” [Electonic Recource]: https://lex.uz/docs/4396428.
2. Jeff Sedayao, Rahul Bhardwaj, Nakul Gorade, Making Big Data, Privacy and Anonymisation work together in the Enterprise. Computer Science // IEEE International Congress on Big Data, 27 June 2014.
3. Trifonova U.V., Zharinov R.F., Opportunities of depersonalization personal data in systems using relational databases, TUSUR reports No. 2 (32), June 2014
4. Information Commissioner’s office, “Anonymization: managing data protection risks, code of practice”, 2012.
5. Mishchenko E.Y., Quantitative analysis of the procedure for depersonalising personal data. Method of identifiers introduction // SUSU Bulletin. Ser.: Computer technologies, management, radio electronics. – Chelyabinsk: SUSU Publishing Center, 2015. – T. 15, №3, p.18-25.
6. D.Sanchez, S.Martinez, J.Domingo-Ferrer, Supplementary materials for “How to avoid reidentification with proper anonymisation”, 2015.
7. Mishchenko E.Y., Quantitative analysis of the procedure for depersonalising personal data. Method of composition or semantic change / Vestnik Ural District. Security in information sphere. – Chelyabinsk: SUSU Publishing Center, 2016, №1(19), p.30-38.

AN INTELLECTUAL METHOD TO OPTIMALLY CONTROL THE PROCESS OF MICROWAVE DRYING OF THERMOLABILE PRODUCTS

A.Artikov[1], Z.Masharipova[2], F.Rakhmatov[3]

[1,2]Tashkent Chemical-Technological Institute, Tashkent, Uzbekistan
[3]Gulistan State University, Sirdaryo, Uzbekistan
fmhayat9393@mail.ru

Abstract. *The article enlightens the issue of an intellectual method for optimal control of high-quality drying of thermolabile products in a microwave installation.*

Mathematical and computer models were compiled by multi-stage system thinking and analysis, and their adequacy was established with a probability of 0.95. The optimal control mode allows you to maintain the temperature of the material in the specified limit and produce a high-quality dried product. A system of microprocessor-based discrete automatic control of a microwave dryer is proposed to enable the heater to be switched on at various specified ranges with a decreasing frequency of material temperature changes, where the length of discrete heating oscillations at the end of the process is ten times less than the initial one.

Keywords. *Thermolabile, microwave, cost-effectiveness of the process, mass transfer, venture.*

1. Introduction.

Drying is the heat and mass transfer process of removing liquid from solid, liquid substances or their mixtures by evaporation. Most often, the liquid to be removed is moisture or volatile solvents. The direct choice of the drying method and methods depends on the physical condition of the raw material, its chemical composition, the required properties of the final product and the cost-effectiveness of the process [2,3,11-15]. Microwave technologies are widely used in the production of many food products.