Ensuring the information security of personal data when submitting electronic appeals to the public authorities

E N Polyakova, OI Filonova, K G Prokofyev, S A Sutyagin

Kurgan State University, ul. Sovetskaya, 63, building 4, Kurgan, 640020, Russia

Abstract. The article is devoted to the actual problem of information security of personal data, circulating on the internet portals of State government body and municipal government. Scientific development of technical aspects of the mechanism of electronic application of the public to the authority organs agrees with priority policy of creation of information society and electronic government, and personal data security is one of the tasks of integrated support of the state information security and this determines the relevance of the article topic. Basing on the analysis of legislation, content-analysis of portal centres of provision of state and municipal services, by carrying out experiments the problems have been found out and the proposals on technical information security of personal data while applying to the government body electronically have been developed.

As a result of the content-analysis of regional portals of Multifunctional centres of provision of state and municipal services, it has been revealed that in most regional portals of Multifunctional centres personal data are sent in open, unencrypted form, which threatens their security. To study the possibility of interception of people personal data two experiments have been fulfilled. As a consequence of the experiment all the sent people’s personal data have been got. On the basis of the received information the model of threats has been developed for information systems of personal data of Multifunctional centre, for this system values of initial system security, probability of threats realization have been defined, assessment of the possibility of threat realization and danger has been done. The solution to the problem of probable data loss while filling in electronic application can be obligatory usage of data encryption protocol HTTPS on the internet portals of public authority, this protocol is intended to provide the three most important security aspects: encryption, authentication (of users), integrity. To get authentication of users Multifunctional centres will have to give people their own digital signature, with the help of which applicant’s personal data will be certified; data should be signed with the help of the privacy key of a Multifunctional centre.

The results of the study are a software package aimed at secure data transfer, the layout of the site of a Multifunctional centre, recommended as a standard, proposals how to improve the legislation in the sphere of personal data security – will help to solve the problems of the society and state.

Key words: information technologies, state services, information security, personal data, electronic applications, prevention of data loss, security threat, brittleness.
1. Introduction

The protection of confidential information, including personal data of citizens, is relevant in almost any country in the world.

Scientists from the UK Killian W. and Funkat D. point out the importance of ensuring the confidentiality of data using information technologies [1]. According to Weitzner D., despite the fact that technical innovations in cryptography and network security ensure the confidentiality of personal data in information systems, most Internet users are still concerned about their privacy rights and correctly believe that they are much more vulnerable today than previous generation [2].

Chinese scientists Liu Zhihang, Yuan Quan, Liu Lu focus on the problem of ensuring the confidentiality of personal information and resources of Internet users [3]. Scientists from Eastern European countries Voykovic G. and Milenkovic M. point out that from May 25, 2018 a new general Data Protection Statement is being applied, which regulates personal data protection issues in a more modern way than was provided by previous resolutions [4]. Trabelsi Slim offers a platform based on a privacy policy language in which each user can control their personal information by imposing access restrictions and control of use [5]. One group of Chinese scientists, dealing with the problem of security of personal data of users in cloud services, proposes to ensure a high degree of confidentiality through electronic signatures and hierarchical attribute encryption [6]. Another group of scientists from China offers a secure and reliable model for user authentication and data encryption on a personal computer platform [7]. Hungarian researchers analyze the security problems of personal data in the implementation of the Hungarian digital national development program [8].

The problems, methods and means of protecting this information are similar, but each country has its own characteristics.

In Indonesia, with the help of information technology, social security is being developed as part of government services through the E-Balance application [9]. Indonesian researchers are researching personal data protection tools based on confidentiality using content analysis [10]. Confidential data in the field of health care, terms of access and access of third parties are the focus of attention of Portuguese researchers [11]. American scientists are studying the problem of protecting personal data in a university model [12]. Information technology specialists from South Africa offer a context-oriented application aimed at improving the overall security of the content of a mobile device [13]. Nigerian scientists also talk about the need to protect personal data [14].

The introduction of digital technologies in the sphere of citizens' appeals to government bodies has undoubted advantages. These include: saving time when submitting appeals and when searching for data necessary for answering and rendering state or municipal services; reduction of economic costs for the delivery of documents; reducing the risks associated with the loss of information; the possibility of using technical means of protection to ensure data integrity and confidentiality of information.

The system of electronic applications to the public authorities should be developed for the formation of the information society and electronic government, ensuring information security of personal data by means of electronic communications. The procedure of sending the application to the public government body and the requirement of time to answer them is regulated in Russia.

Nowadays at the time of development of information technologies electronic workflow takes a leading position, as it has a number of advantages in comparison with paper workflow: saving time of the search of the necessary data, decrease of the risk of information loss, decrease in expenses on deliverance of paper-based documents, opportunity to use cryptographic protection, allowing to increase data confidentiality and integrity.

Today to apply the necessary documents to the state government body or municipal government with the aim of their consideration, it’s enough to fill in and send the paperwork from your home computer. Functioning of the system of citizens’ applications, transferred through information systems of common use to the public government body, not only contributes to the protection of rights and legal interests of citizens but also lets the government fulfil systematic monitoring the state of the whole social sphere [15, p.248].

But in the technical support there are gaps, which threaten information security of personal data (later on PDn) of the citizens.
In particular, under threat there are personal data of citizens. Federal law №152-FL “About personal data”, personal data are defined as any data, relating to a certain natural person (the subject of personal data).

The problem of protecting citizens and protecting personal data is attracting the attention of scientists - information security technicians.

I.S. Kozin and S.V. Bezateyev developed an analysis of key measures aimed at ensuring the security of personal data during their processing in information systems, and a method for determining the danger of threats was proposed [16]. O.N. Bogulskaya, M.M. Kucherov, E.A. Cresan proposed a model of restricting access to information based on confidentiality [17]. A.S. Shaburov and A.A. Mironov identified areas of activity to improve the system for the protection of personal data in open information systems [18]. I.I. Barankova, V.V. Mikhailova, G.I. Lukyanov as one of the possible and most effective ways to protect information is considering the introduction of a system to protect against leakage of confidential data [19].

As a result of the carried-out content-analysis of regional portals of Multifunctional centres of provision of governmental and municipal services some drawbacks have been detected in the sphere of personal data security of the citizens, using the service of applying electronically.

The aim of the study is the detection of problems and development of proposals on technical provision of personal data information security, transferred on the internet portals of the state government body or municipal government.

The following tasks were set: - to analyze the problems related to this subject area; - consider the mechanism of electronic appeals and identification of threats to the security of PD; - develop proposals on the order of work to ensure the safety of PD when submitting electronic applications; - develop a software package for the safe transfer of personal data when submitting electronic applications to public authorities.

Problem statement is determined by the importance of scientific elaboration of the mechanism of personal data security while applying electronically to the government body within priority state policy, aimed at the development of information society and electronic government, at interaction of civil society and the state.

The results of the study are a software package aimed at secure data transfer, the layout of the site of a Multifunctional centre, recommended as a standard, proposals how to improve the legislation in the sphere of personal data security – will help to solve the problems of the society and state.

2. Types of direction of citizens’ applications

In the Russian Federation there are requirements for government service portals and regional portals for state and municipal services, for organizing services in electronic form and the need to provide opportunities for applicants to request inquiries and other documents using the information and communication infrastructure. In this regard, it is implied that it is possible to fill in an electronic application from the portal of public services and regional sites of multifunctional centers.

It seems reasonable to consider the above-mentioned Internet resources on the availability of the stated functions.

2.1. SPGS (the Single Portal of Governmental Services)

In 2009, the Unified Portal of State and Municipal Services (https://www.gosuslugi.ru) was created - the federal state information system that provides a wide range of services.

The portal provides with different services depending on the type of the applicant (natural or legal person), the chosen region, the character of the application. For example, application for the replacement of the passport, for the appointment to the doctor, etc.

As a result of a visual consideration of the site contents the form of the electronic application to the state government body has not been found, as a consequence the request to the technical support of the portal has been sent. The following answer has been got: “The service of direction of the application to some department on Single portal of governmental services is not provided, on the fact of service request some departments let to send a message to the representative within the framework of the provision of the service”.

3
It seems that in this case the practice fails to meet the requirements of electronic government tasks. In particular, on Single portal of governmental and municipal services (later on SPGS) there is no possibility to send an application, proposal or complaint to some particular department. The solution of this problem may be the addition of such a service by creation a separate Internet-page, having a form to apply and the place to fill in personal data.

2.2. Regional portals of Multifunctional centres of provision of governmental and municipal services

Multifunctional centers operate in accordance with Russian legislation. The tasks set for multifunctional centres are the following: significant decrease of time and simplification of the process of provision of services due to the realization of the principle of “one window”; decrease in the list of the documents necessary for the provision of the services; decrease in corruption risks while providing the service; improvement of quality of applicants’ service; organisation of effective interdepartmental interaction among institutions while providing the service.

In the mechanism of applying, transferring and answering electronic requests (User – MFC – State body) PD are protected only at intermediate stage – relations of MFC and state body are protected by the system of interdepartmental electronic interaction, but at the stage of applying and sending the answer to the applicant there is a threat of identity fraud [20, p.32].

As a result of a conducted content-analysis of regional portals of certain constituent entities of the Russian Federation, it has been found out that requirement, connected with giving the opportunity to form applications on the sites of multifunctional centres, is complied only within a small number of information structures, which decreases the level of convenience of service provision to applicants. Moreover, it has come to light that not all the sites ensure a necessary security of personal data of RF citizens, using this service. Let’s consider this opportunity more closely on the example of the site of MFC of Kurgan region (https://www.mfc45.ru).

To send an application the user has to choose the appropriate tab on the menu on the main page and go on to fill in the form. At this stage one has to agree with the condition of transfer, which is as follows: “I confirm my agreement to the storage of information in the electronic form of application (as well as personal data) through the open communication channels of the Internet”. If one disagrees, the action will not be fulfilled. After filling in all the offered form fields (full name, address, telephone, e-mail) the formation of application is over by pressing “Send”. The data is sent simultaneously to the server and to the mail of organisational analytical department. After the study of the contents, the request is formed to the indicated body. Governmental or municipal body considers the application and answers it strictly within the time bound by legislation by sending the answer to e-mail or the address where the applicant lives.

The study of the results of the content-analysis allows making a conclusion that of the regional portals, which provide the fore-mentioned opportunity, most don’t ensure security of personal data while transferring applications. The data are sent in open, unencrypted form, which threatens the security of citizens’ personal data.

The necessity to take measures to protect PD has arisen with the development of such technical possibilities as copying, data distribution; the level of information technologies has reached such a level that self-protection of information rights is not an effective way against breaches of privacy any more.

On the basis of the received information the model of threats has been developed for information systems of personal data (later on ISPD) of Multifunctional centre. For this system values of initial system security, probability of threats realization have been defined, assessment of the possibility of threat realization and danger has been done; as well a list of actual threats of information security of ISPD has been stated.

Classification of the threat as actual has been carried out in accordance with Methodology of definition of actual threats of personal data security while data processing in the personal data information systems, adopted by Federal service on technical and export control of the Russian Federation (later on FSTEC of Russia) dated 14 February 2008.

3. The problems of transfer of personal data and methods of their solution
3.1. Problems of transfer of personal data in the open way

Protection of personal data is now determined by international standards, which serve as a legal guide in the development of Russian legislation and law enforcement practice. There are fears that the introduction of electronic systems for personal data does not fully meet the requirements of the inviolability and safety of a person's personal life. In 2015, the Federal Law “On Personal Data” introduced a provision on the localization of personal data of Russian citizens, which has additional advantages in terms of protecting personal data.

In accordance with the provisions of the Federal Law No. 149-ФЗ “On Information, Information Technologies and Information Security”, any confidential information as well as personal data must be protected. The first priority should be a qualitative assessment of the protection of personal data in information systems. It follows that each regional multifunctional center should provide users with a secure connection of the https type, which, as the study showed, is provided in a few cases.

Security of data transfer among participants of interdepartmental electronic interaction, i.e. multifunctional centre and governmental bodies, is guaranteed by Single system of interdepartmental electronic interaction (later on SMEV). SMEV is a federal governmental information system, which is intended to provide information interaction among information systems of SMEV participants with the aim of provision of governmental and municipal services in the electronic from.

To study the possibility of interception of people personal data two experiments have been fulfilled.

In the course of experiment №1 there was a hacker attack in the conditions of having direct access to the local net of the attacked host.

After filling in all the necessary form fields, the application was successfully sent, which was confirmed on the screen. The attack was made with the help of a specially designed device, which captured traffic, got and transferred by attacked host, and software complex Wireshark, aimed at examining the contents of the packages, entering the network interface. With the help of the complex Wireshark, it was possible to trace data packages, sent from the attacked host to the host with the indicated IP-address and to save the package with POST-request (request to save data on the web-server). Having saved it in a separate file, it was possible to look through all the data, which the user has filled into the form for electronic application. So, as a result of this experiment, all the personal data of the applicant, which have been given in the form of the electronic application on the site of the studied multifunctional centre, have been got.

In the course of experiment №2, the situation was modelled, when there was an access only to the device of Internet-provider interconnection inside the house, i.e. to the connection box. To check information retrieval from implementation medium of transfer Ethernet, 4-pair cable UTP of category 5e was used. Special patch-cord with connector 8p8c at one end and with clips at the other end was plugged into one of the connectors on the patch-panel in the switchboard. Having joined contact clips to bare spots, the connector was switched to the device, with the help of which there was an attack, software was run and coming to network map traffic (Wireshark). As in the first experiment all the form fields were filled in and there was information retrieval while transferring data packages to the server of multifunctional centre. In the course of the experiment all the transferred personal data of the user were got.

It was found out that some sites which provide the service of electronic application, for example sites of municipal authorities are in the same way vulnerable.
So, there is a possibility of data loss of citizens while forming electronic application, but at the same time regional multifunctional centres and governmental bodies, as a rule, don’t inform citizens of such a threat.

3.2. The use of the protocol HTTPS

To ensure the information security of personal data transmitted on the Internet portals of public authorities, it is necessary to use the Protocol of data encryption HTTPS (HyperText Transfer Protocol Secure – secure hypertext transfer Protocol), which is an extension to the standard HTTP, transmitting data in clear form. Information in HTTPS is transmitted through encrypted transport mechanisms of SSL (Secure Sockets Layer – secure sockets layer) or TLS (Transport Layer Security – transport layer security) – its improved version.

The Protocol adheres to three fundamental aspects of security:
– encryption;
– authentication;
– integrity.

Encryption is provided by the use of public key cryptography, in which each party has both private and public keys that are mathematically related. For encryption, a public, accessible to all key is used, for obtaining the same source code, it is necessary to use a private, secret, key.

User authentication is performed by authenticating certificate files that are signed by the Identity Center and that bind the public key to the specified organization. Thus, when making an Internet connection, you can be sure that on the other side of the communication channel there is a trusted user, not an attacker who “listens” to traffic in order to intercept sensitive data (logins, passwords, Bank account numbers, etc.).

The integrity of the transmitted information is guaranteed by the first two properties.

In Internet browsers, the application on the website HTTPS-connection is displayed as a lock image in the address bar, the inscription “Protected” or the name of the organization that owns the Internet resource, on a green background. The cost of this protection measure varies depending on the number of sites on the specified IP address, the purpose of the Protocol and the external display option. On average, it will cost from 1500 to 25,000 rubles a year.

3.3. Authentication of an applicant while transferring personal data

Personal data are defined as any data, relating directly or indirectly to a certain or defined natural person (the subject of personal data).

So, to the personal data include: 1) surname, name, patronymic (the last – if there is); 2) date and place of birth; 3) residential address; 4) marital status; 5) education; 6) profession; 7) income, etc.

As the above-mentioned list does not identify the citizen at a full extent, other information can be added to personal data as well.

To validate authenticity of transferred personal data, it is necessary to apply to them electronic digital signature.

Electronic signature is seen as information in the electronic form, which is added to other information in the electronic form (signed information) or connected with this information in another way or which is used to identify the person, signing information. The provisions of Federal Law “About electronic signature” create conditions to use electronic digital signature in electronic documents, while performing which it is considered equivalent to a handwritten one and attaches electronic digital document juridical importance.
Unreliability of personal data in the application may appear in two cases:
1) a citizen gives incorrect data by mistake;
2) a citizen gives incorrect data on purpose.
Intentional substitution may be used with the aim of falsifying of user’s information, for example for personal gain.
To avoid such situations, the personality of the sender must be authenticated. This is possible while sending an application in a form of a text document verified by an electronic digital signature. But not many people have electronic signature as most citizens either didn’t have any necessity to get it or they were not informed of the advantages of its use or they had no desire or ability to pay for a qualified electronic signature.
Possible solution of this problem is in need of multifunctional centres to give citizens their own electronic digital signature with the help of which they will verify personal data of the applicant. The data should be signed by a privacy key of MFC. To check the signature and for confidence of the person in the authenticity of two keys, together with the message certificate X.509 is passed, which will connect two key to a multifunctional centre, so one can verify which multifunctional centre of what region has sent the message. The centre of certification signs each certificate with the help of its digital signature, verifying the authenticity of two keys by this. To ensure secure work of this technology the net of multifunctional centres must have a single centre of certification, which will give two key and privacy key to multifunctional centres.
On the territory of Russia Single portal of governmental services functions, where the problem of authentication of a personality of a user is solved with the help of creation of personal area, containing personal data of a user, connection with which is secure (HTTPS-connection). In this regard one of the possible solutions of the problem is reasonable connection of Portal of Governmental services and sites of multifunctional centres on the shared platform.

3.4. Absence of unique structure of MFC
The next problem is the absence of the unique structure of multifunctional centres.
As a result of conducted content-analysis of the Internet portals of multifunctional centres of all regions of Russia, it has been found out that this organisation has not a unique structure and consequently there are significant differences in the quantity of the services provided on the sites of multifunctional centres in different constituent entities of the Russian Federation. The analysis has shown that of about 100 sites only 23 follow the provisions of the legislation and provide services in the electronic form. At the same time information security of personal data is ensured by still fewer of them.
May be for the solution of the problem it is necessary to perform a reorganisation of all regional multifunctional centres, making unique structure, controlled by the government. It is necessary to reform existing regional sites of multifunctional centres in the form of Single portal in the same way, which allows applying unique format (brand-book), and solve the problem of authentication of users and provide secure Internet-connection as well.

4. Software complex of secure transfer of electronic application of citizens
Effective use of public funds to improve the protection of information containing personal data of citizens is an urgent task.
To solve the problem of providing information security of personal data of citizens, while sending electronic applications to public authorities, software complex of secure transfer of electronic application of citizens was developed – client-server application, providing secure transfer of data from a user’s device to the server with a further conservation of them in the data base. The application provides secure transfer of personal data, sent by the user while using the service of sending an electronic application to public authorities. Client’s part of the application is responsible for encryption of transferred data, and server part – for reception and de-encryption. Client’s part is in the form of desktop application for operating system (later on OS) Windows, as well as in the form of application for OS Android.
Client part of the application asks for the login and password of the user. In case of successful authentication the application is connected to the server, and the user gets an opportunity to form text of the application. After the user confirms that the application form is ready, the application checks that data have been entered correctly, encrypts the information and sends to the server part. If the server is not available, the user gets the following message. The connection is closed. On getting the application, the server de-encrypts it and shows on the screen, informing of the fact.

Operating environment-1. The application is installed on a computer running Windows 7 and older.
Operating environment-2. The mobile application is installed on a smartphone running Android OS at least version 2.2.

Requirement to security – 1. All network transactions, including identifiable personal information, should be encrypted.
Requirement to security – 2. Users are obligatorily registrated to enter the system for performing all the operations.
Requirement to security – 3. Customers must register to enter the system according to the policy of limited access to computer systems.

5. Summary and conclusion
According to the Doctrine of information security of the Russian Federation, adopted 5 December 2016, security of personal data is one of the most important tasks of complex providing of information security of the state. So compliance with the requirements of use of specialised ways of security is an obligatory condition for effective and secure functioning of governmental information systems.
We have been set a task to develop technical and legal proposals improving the level of personal data information security, transferring on the internet-portals of public authorities. In the course of the solution of this question the analysis of normative legal acts has been fulfilled; the mechanism of sending electronic application has been considered and the threats to the security of personal data have been revealed; proposals on measures for providing security of personal data, while sending electronic applications, have been developed and the result of the study is a developed software complex of secure transfer of personal data, while sending electronic applications into public authorities, this complex will be tested in the automated information system of MFC of one of the regions of Russia with the connection to the data base of the applicants.
On Single portal of governmental and municipal services there is no opportunity to send an application specific department. It seems reasonable make the addition of the extra-service by creation a separate Internet-page, having a form to apply and the place to fill in personal data.
Most portals of multifunctional centres do not provide information security of personal data of citizens while sending applications – data are sent in open, unencrypted form. Meanwhile, regional multifunctional centres and governmental bodies, as a rule, don’t inform citizens of the possibility of the threat of personal data loss while forming electronic application. Here arises ethical and political problem: if citizens are actively forewarned of personal data loss, won’t it stop realization of the political course of development of information society and electronic government.
Scientific development of the mechanism of electronic applications of citizens into public authorities of the Russian Federation corresponds to the priority governmental policy of development of information society and electronic government, to the course of interaction of civil society and government, which determines the relevance of the article topic.

6. References
[1] Kilian W., Funkat D. 2000 Structuring legal knowledge on data protection: the EU- data protection research project DAPRO IEEE Conf. Proceedings 11th International Workshop on Database and Expert Systems Applications pp. 1061-1065
[2] Daniel J. Weitzner 2007 Personal Privacy without Computational Obscurity: Rethinking Privacy Protection Strategies for Open Information Networks IEEE Conf. Twenty-Third Annual Computer Security Applications Conference pp. 173-175
[3] Liu Zhihan, Yuan Quan, Liu Lu 2016 Decentralized mobile SNS architecture and its personal information management mechanism IEEE China Communications 13(2) pp. 189-199
[4] Vojković Goran, Milenković Melita 2018 GDPR in access control and time and attendance systems using biometric data IEEE Conf. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics pp. 1138-1142

[5] Trabelsi Slim, Sendor Jakub, Reinicke Stefanie 2011 Privacy Policy Engine IEEE International Symposium on Policies for Distributed Systems and Networks pp. 184 - 185

[6] Fan Kai, Tian Qiong, Huang Nana and Wang Yue 2016 Privacy protection based access control scheme in cloud-based services IEEE/CIC International Conference on Communications in China pp. 1-5

[7] Mingdi Xu, He Jian, Zhang Bo and Zhang Huanguo 2007 A New Data Protecting Scheme Based on TPM IEEE Conf. Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing pp. 943-947

[8] Zoltan Nyikes, Zoltan Rajnai 2015 Big data, as part of the critical infrastructure IEEE Conf. 13th International Symposium on Intelligent Systems and Informatics pp. 217-222

[9] Gunawan Wang, Novi Fitriani and Ahmad Nurul Fajar 2017 Behavioral analysis of use personal service e-balance Indonesian social security IOP Conf. Series: Materials Science and Engineering 237

[10] Rosmaini E., Kusumasari T F, Lubis M., Lubis Insights A R 2018 Insights to develop privacy policy for organization in Indonesia IOP Conf. Series: Journal of Physics: Conf. Series 978

[11] Isabel Maria, Lopes Pedro Oliveira 2018 Implementation of the general data protection regulation: A survey in health clinics IEEE Conf. 13th Iberian Conference on Information Systems and Technologies pp. 1-6

[12] Earp J.B., Payton F.C. 2001 Data protection in the university setting: employee perceptions of student privacy IEEE Conf. Proceedings of the 34th Annual Hawaii International Conference on System Sciences pp. 6

[13] Marsh Stephen, Wang Yao, Noël Sylvie and Robart Lewis 2013 Device Comfort for mobile health information accessibility IEEE Conf. Eleventh Annual Conference on Privacy, Security and Trust pp. 377 - 380

[14] Abdulrauf L.A., Fombad C.M. 2016 Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms Liverpool Law Review pp. 105-134

[15] Morukova A A and S V Kalinina 2017 Ensuring information security when citizens send applications to public authorities in electronic form Actual problems of administrative and administrative procedural law (Saint-Petersburg, Petersburg University of the Ministry of Internal Affairs of the Russian Federation) pp 245-249

[16] Bezateev S V, Kozin I S 2017 The method for determining the danger of personal data threats when they are processed in the information systems Proceedings of Saint Petersburg Electrotechnical University (Saint-Petersburg, Saint Petersburg Electrotechnical University “LETI” named after V.I. Ulyanov (Lenin)) pp 19-26

[17] Bogulskaia O N Kucherov M M and Kresan E A 2012 Protection of personal data in information systems Reports of Tomsk State University of Control Systems and Radioelectronics 1 (25) part 2 pp. 47-51

[18] Shaburov A S and Mironova A A 2015 About increasing the efficiency of protection of personal data in open information systems Perm National Research Polytechnic University 16 pp 106-117

[19] Barankova I I, Mikhailova V V and Lukyanov G I 2018 Development of the WordSearch system for protecting confidential information from leakage UrFR Newsletter. Information Security (Chelyabinsk, O O O “South Ural Legal Newsletter”) 1 (27) pp. 14–18

[20] Vasilyeva A A, Sutyagin S A, Polyakova E N and Moskvin V V 2016 The problems of information security of citizens’ personal data when submitting electronic applications to the state departments UrFR Newsletter. Information Security (Chelyabinsk, O O O “South Ural Legal Newsletter”) 4 (22) pp. 31-34