CLASSIFICATION OF PERSONAL DATA SECURITY THREATS IN INFORMATION SYSTEMS

DOI: 10.36724/2072-8735-2020-14-1-56-60

Vladimir A. Dokuchaev,
MTUCI, Moscow, Russia, ***v.dok@tlsf.ru***

Victoria V. Maklachkova,
MTUCI, Moscow, Russia, ***v.maklachkova@tlsf.ru***

Vyacheslav Yu. Statev,
JSC "RZD", Moscow, Russia, ***svu@rnt.ru***

Keywords: *Personal Data, Information, Security, Threats, Risks, Information Systems, Classification.*

The purpose of this work is to analyze and classify threats that arise when working with personal data in information systems. In the field of information technology in any country, one of the national interests is to ensure and protect the constitutional rights and freedoms of man and citizen in so far as it relates to the receipt and use of information, as well as confidentiality when using information technologies. In this regard, special attention is currently being paid to the organization of processing and ensuring the security of personal data in information systems, including during their cross-border transfer. In the European Union, this activity is regulated by the General Data Protection Regulation (GDPR), which was put into effect on May 25, 2018. Personal data are in a high-risk area, especially in organizations that operate with large amounts of personal data, such as passport data, solvency data, employers, contact details, phone numbers, addresses, email, and other information that represents interest for potential computer attacks. The solution to the problem of ensuring the security of personal data is impossible without identifying and classifying potential threats to personal data in information systems. The proposed classification can serve as the basis for a threat model of a specific information system designed to process personal data.

Information about authors:
Vladimir A. Dokuchaev, *DSc (Tech), Professor, Head of the Department "Multimedia Communication Networks and Services" MTUCI, Moscow, Russia*
Victoria V. Maklachkova, *Senior Lecturer of the Department "Multimedia Communication Networks and Services" MTUCI, Moscow, Russia*
Vyacheslav Yu. Statev, *PhD, Head of the Department, JSC "RZD", Moscow, Russia*

Для цитирования:
Докучаев В.А., Маклачкова В.В., Статьев В.Ю. Классификация угроз безопасности персональных данных в информационных системах // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. №1. С. 56-60.

For citation:
Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. (2020) Classification of personal data security threats in information systems. *T-Comm*, vol. 14, no.1, pp. 56-60. (*in Russian*)

Introduction

With the development of information technology, attention and interest in the problem of privacy and the further development of the Institute of Personal Data began to significantly increase.

In the Russian Federation, one of the national interests in the information sphere is "ensuring and protecting the constitutional rights and freedoms of man and citizen in so far as it concerns the receipt and use of information, privacy in the use of information technology ...".

From this follows the attention that is currently being paid at enterprises to the organization of processing and ensuring the security of personal data, including when they are processed in information systems.

With the entry into force in May 2018 of the Global Data Protection Regulation (GDPR), personal data operators have faced new threats related to the cross-border transfer of personal data.

Personal data refers to any data that in one way or another relates to an identifiable or identifiable person. An identifiable person is a natural person that can be established directly or indirectly by reference to a certain identification number, as well as by one or more factors specific to its physiological, physical, mental, economic, cultural or social affiliation.

The subjects of personal data in the organization are employees, retirees, candidates for filling vacant posts and others. The purposes of processing personal data may be: providing services to a client of the organization, processing data in accordance with labor legislation, etc. Personal data are divided into categories such as: publicly available, special, as well as other personal data that do not fall under the first two categories.

Former or current employees of an organization at present time commit many violations of the confidentiality of personal data. This is due to the presence in companies of information systems for processing personal data, access to which are available to employees who are able to transfer confidential information to third parties. The existence of such a vulnerability in the company can significantly facilitate the ability of an attacker to obtain personal data, while making a computer attack more effective.

There are a number of mandatory measures that enterprises must take in order to “correctly” store and process personal data in the information system. The functioning of the entire business model of the activity of the personal data operator and the cost of risks associated with the processing of personal data depend on how competently the business processes for organizing automated processing of personal data are implemented.

According to company “InfoWatch” analysis, in 2018 the share of personal data leaks amounted to 80.2% of all confidential information leaks. Type of data compromised by retiring employees shown at Table 1.

Table 1

	Personal Data, %	State Secret, %	Trade Secret, %	Other, %
2017 year	47.2	2.8	36.1	13.9
2018 year	35.3	3.9	58.8	2.0

Source: company InfoWhatch

To create a model for protecting personal data, it is necessary to identify and classify potential threats to personal data in information systems.

Classification of Personal Data Threats

There are two classes of threats to personal data in information systems:

- threats that cannot be correlated with attacks;
- threats that can be correlated with attacks.

There are threats incompatible with attacks that can not only lead to the loss, distortion or compromise of the subject’s personal data, but also create conditions for their use by various violators for their own purposes.

These threats include:

- threats not related to human activities: natural disasters and natural phenomena (earthquakes, floods, hurricanes, etc.);
- threats of a socio-political nature: strikes, sabotage, local conflicts, accompanied by an attack on an object that hosts information system resources, etc .;
- erroneous actions and (or) violation of requirements by personnel and users of the information system of the corresponding operational, organizational, technical or other documentation;
- threats of anthropogenic nature, for example: accidents, various malfunctions, interference and interference, leading to violations and malfunctions in the hardware components of the information system.

Protection against threats that cannot be correlated with attacks is regulated by instructions developed and approved by the authorized services of the personal data operator, taking into account the specific conditions for the functioning of the information system, as well as the current regulatory framework.

Protection against threats that can be correlated with attacks should be provided with the help of protective measures and means used by the information system and designed mainly to counter attacks.

The composition and content of security threats to personal data is determined by the combination of conditions and factors creating the danger of unauthorized, including accidental, access to personal data.

The totality of such conditions and factors is formed taking into account the characteristics of the information system, the properties of the distribution medium of informative signals containing protected information, and the capabilities of the sources of threats.

The following characteristics of an information system can cause threats for personal data:

- structure, category and amount of personal data processed in the information system;
- availability of information system connections to public communication networks and (or) the Internet;
- security subsystem characteristics and personal data processing modes;
- modes of differentiation of access rights of users of the information system;
- location and conditions of placement of technical equipment of the information system.

The main elements of the information system in which personal data is processed are:

- personal data contained in databases, as a combination of information and its sources used in the information system;
- information technology, as a set of methods and methods of using computer technology in the processing of personal data;
- software and hardware that process personal data;
- information security tools;
- additional hardware and systems.

The properties of the information distribution medium containing the protected information are characterized by the type of physical environment in which personal data is distributed, and are determined when assessing the possibility of implementing a security threat channel for personal data.

The security threat to personal data is realized as a result of the formation of channels for the implementation of a security threat to personal data between the threat source and the personal data carrier, creates the necessary conditions for violating the security of personal data.

The main elements of the channel for implementing a security risk to personal data are:

- source of threat - a subject, material object or physical phenomenon that creates a threat to the security of personal data, for example, a violator of the security of personal data, the capabilities of which with respect to the system are determined in the model of the violator;
- an environment for the distribution of personal data or influences in which a physical field, signal, data or program may be distributed and affect the protected characteristics of personal data. These characteristics include: confidentiality, integrity, accessibility;
- personal data carrier - an individual or material object, including a physical field, in which personal data are reflected in the form of symbols, images, signals, technical solutions and processes, quantitative characteristics of physical quantities.

Other security characteristics of personal data that are important to the operator, such as data authenticity, are also possible.

Personal data carriers may contain information presented in the following forms: acoustic (speech) information; textual and visual information; processed (circulating in the information system) information.

A classification of threats to the security of personal data is proposed according to the following criteria:

- by types of possible sources of security risk to personal data, caused by deliberate or unintended actions of users of the information system: with or without access to it. It should be noted that the sources of threats in relation to the information system can be both external and internal;
- by type of unauthorized actions carried out with personal data:

➢ threats leading to a violation of the confidentiality of personal data (copying or unauthorized distribution), the implementation of which does not directly affect the content of the information;

➢ threats leading to unauthorized, including accidental, influence on the content of information, as a result of which personal data is changed or destroyed;

➢ threats leading to unauthorized, including accidental, impact on the software and hardware elements of the information system, as a result of which personal data is blocked;

- by methods of implementing a security risk to personal data:

➢ threats implemented in information systems when they are connected to public communication networks;

➢ threats implemented in information systems when they are connected to international information exchange networks;

➢ threats implemented in information systems that do not have connections to public communication networks and the Internet.

- by type of channels for implementing a security risk to personal data:

➢ threats implemented through channels arising from the use of technical means to intercept information processed in the information system (technical channels for information leakage);

➢ threats realized due to unauthorized access to personal data in the information system using standard software or specially developed or applied software.

The implementation of any of the listed threats and (or) their combination can lead to the following consequences for the subjects of personal data:

- significant negative consequences;
- negative consequences;
- minor negative consequences.

Consider typical security threats for personal data in information system.

Threats of information leakage through technical channels:

- threats of leakage of acoustic (speech) information - in the presence of voice input functions or functions for reproducing personal data by acoustic means of an information system;
- threats to leakage of specific information - by viewing information using optical (optoelectronic) means from display screens;
- threats of information leakage due to the presence of electromagnetic radiation, mainly monitors and system units of personal computers and servers from the information system.

Threats of unauthorized access to personal data in the information system:

➢ threats of access (penetration) into the operating environment of computers or servers of the information system using standard software:

- realized direct access threats:

– during and after loading the operating system;

– due to the installation of hardware bookmarks and the introduction of malware.

- remote access threats:

- analysis of the transmitted and received network traffic;
- network scanning and password identification;
- substitution of a trusted network object with or without a virtual connection;

– the imposition of a false route and the introduction of a false network object;

– denial of service:

✓ partial and complete exhaustion of resources;

✓ violation of logical connectivity between data or objects;

✓ the use of errors in programs that implement network exchange protocols.

– remote launch of applications:

✓ distribution of files containing unauthorized executable code;

✓ remote launch of the application by overflowing the server application buffer or using the remote control capabilities of the system provided by hidden software and hardware bookmarks.

– introduction of malware;

➢ threats to create abnormal operating modes of software and hardware due to deliberate changes in service data, characteristics of the processed information, distortions (modifications) of the data itself, etc .;

➢ combined threats, which are a combination of the above threats.

Organizations that directly work with personal data are required to take all appropriate measures to prevent the above threats. Therefore, it is important that all departments provide security for employees with access to confidential data. The following rules must be followed.

1. Departments must protect their information systems with appropriate technology. They must be sure that this technology is working in an appropriate condition, sufficient to counter emerging threats.

2. Departments need to identify cases of unauthorized access (internal or external). It is also necessary to identify the addition, deletion and editing of data. To identify this kind of action, audit logs should be used, in which information about the similar state of the information system will be recorded. Information systems containing personal data in which they do not record information about the available viewing or reading conditions need to be investigated and immediately corrected. Departments must take into account external influences on the performance of this system. If this functionality cannot be enabled, and there is a risk of unauthorized access to personal data, then a decision should be made on changing the architecture or functionality of the information system for processing personal data.

3. Access to files that contain personal data should be constantly monitored. Organization staff should be informed of this. To maintain this observation, it may be necessary to create additional information systems.

Conclusion

This list of threats underlies the threat model of a specific information system for processing personal data and having connections to public communication networks and (or) the Internet.

References

1. Dokuchaev V.A., Gorban E.V., Maklachkova V.V. (2019). The system of indicators for risk assessment in high-loaded infocommunication systems. *IEEE. Conference proceedings "2019 Systems of Signals Generating and Processing in the Field of on Board Communications"*.

2. Dokuchaev V.A., Gorban E. V., Maklachkova V.V. (2018). Architecture of the Regional Transport Navigation and Information Systems". *IEEE. Conference proceedings "2018 System of Signals Generating and Processing in the Field of on Board Communications"*.

3. Vladimirova K.S., Dokuchaev V.A., Maklachkova V.V. (2018). Classification of personal data subject to automated processing". *XVI International Scientific and Practical Conference "Actual problems and prospects economic development"*. Simferopol-Gurzuf, October 19-21, 2018.

4. Dokuchaev V.A., Maklachkova V.V. (2017). Risk analysis for personal data processing in the enterprise information system". *XVI International Scientific and Practical Conference "Actual problems and prospects economic development"*. Simferopol-Gurzuf, October 19-21, 2017.

5. Dokuchaev V.A., Mitenkov S.S., Statev V.Y. (2017). Audit and risk management in corporate information and communication systems". *XVI International scientific and practical conference "Actual problems and prospects economic development"* (Simferopol-Gurzuf, October 19-21, 2017), pp. 37-38.

6. ISO 31000:2018. Risk management – Guidelines.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Докучаев Владимир Анатольевич, *МТУСИ, Москва, Россия,* ***v.dok@tlsf.ru***
Маклачкова Виктория Валентиновна, *МТУСИ, Москва, Россия,* ***v.maklachkova@tlsf.ru***
Статьев Вячеслав Юрьевич, *ОАО "РЖД", Москва, Россия,* ***svu@rnt.ru***

Аннотация
Целью данной работы является анализ и классификация угроз, возникающих при работе с персональными данных в информационных системах. В сфере информационных технологий в любой стране одним из национальных интересов является обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий. В связи с этим в настоящее время уделяется особое внимание вопросам организации обработки и обеспечения безопасности персональных данных в информационных системах, в том числе, при их трансграничной передаче. В Европейском союзе данная деятельность регламентируется Общим регламентом по защите данных (General Data Protection Regulation, GDPR), вступившим в силу 25 мая 2018 г. Персональные данные находятся в зоне повышенного риска, особенно в организациях, которые работают с большими объемами персональных данных, таких как паспортные данные, данные о платежеспособности, работодатели, контактные данные, номера телефонов, адреса, электронная почта и другая информация, представляющая интерес для потенциальных компьютерных атак. Решение задачи обеспечения безопасности персональных данных невозможно без определения и классификации потенциальных угроз персональным данным в информационных системах. Предлагаемая классификация может быть положена в основу модели угроз конкретной информационной системы, предназначенной для обработки персональных данных.

Ключевые слова: *персональные данные, информация, безопасность, угрозы, риски, информационные системы, классификация.*

Литература

1. *Dokuchaev V.A., Gorban E.V., Maklachkova V.V.* The system of indicators for risk assessment in high-loaded infocommunication systems // IEEE. Conference proceedings "2019 Systems of Signals Generating and Processing in the Field of on Board Communications", 2019.
2. *Dokuchaev V.A., Gorban E.V., Maklachkova V.V.* Architecture of the Regional Transport Navigation and Information Systems // IEEE. Conference proceedings "2018 System of Signals Generating and Processing in the Field of on Board Communications", 2018.
3. *Владимирова К.С., Докучаев В.А., Маклачкова В.В.* Классификация персональных данных, подлежащих автоматизированной обработке. Труды XVI Международной научно-практической конференции "Актуальные проблемы и перспективы развития экономики". (Симферополь-Гурзуф, 19-21 октября 2018).
4. *Докучаев В.А., Маклачкова В.В.* Анализ рисков при работе с персональными данными в информационной системе предприятия. Труды XVI Международной научно-практической конференции "Актуальные проблемы и перспективы развития экономики". (Симферополь-Гурзуф, 19-21 октября 2017),
5. *Докучаев В.А., Мытенков С.С., Статьев В.Ю.* Аудит и управление рисками в корпоративных инфокоммуникационных системах. Труды XVI Международной научно-практической конференции "Актуальные проблемы и перспективы развития экономики". (Симферополь-Гурзуф, 19-21 октября 2017). С. 37-38.
6. *Владимирова К.С., Докучаев В.А., Маклачкова В.В.* Классификация персональных данных, подлежащих автоматизированной обработке. Труды XVI Международной научно-практической конференции "Актуальные проблемы и перспективы развития экономики". (Симферополь-Гурзуф, 19-21 октября 2018).
7. ISO 31000:2018. Risk management – Guidelines.

Информация об авторах:
Докучаев Владимир Анатольевич, *д.т.н., профессор, зав. кафедрой МСиУС МТУСИ, Москва, Россия*
МаклачковаВикторияВалентиновна, *старший преподаватель МТУСИ, Москва, Россия*
Статьев Вячеслав Юрьевич, *к.т.н., с.н.с., начальник отдела ОАО "РЖД", Москва, Россия*