https://doi.org/10.36719/2663-4619/111/212-215

Rahim Rahimli
Khazar University
https://orcid.org/0009-0005-2061-6093
UOT 005:004
rehim4028@gmail.com

Protection of Information in Personal Data Information Systems

Abstract

The processing of personal data, which is mandatory for any institution or organization, requires the implementation of personal data information systems and, of course, their protection. Existing methods and techniques for protecting information are overwhelmingly focused on protecting the resources of corporate information systems. This fully applies to the processing of personal data, the protection of which is provided for by current legislation.

Keywords: *information security, protection of information, personal data, information system for processing personal data, protection of personal data, threats to personal data*

Rəhim Rəhimli
Xəzər Universiteti
https://orcid.org/0009-0005-2061-6093
UOT 005:004
rehim4028@gmail.com

Fərdi məlumatların informasiya sistemlərində informasiyanın mühafizəsi

Xülasə

İstənilən qurum və ya təşkilat üçün məcburi olan fərdi məlumatların emalı fərdi məlumatların informasiya sistemlərinin tətbiqini və təbii ki, onların mühafizəsini tələb edir. Məlumatın qorunması üçün mövcud üsul və üsullar böyük əksəriyyəti korporativ informasiya sistemlərinin resurslarının qorunmasına yönəldilmişdir. Bu, mühafizəsi mövcud qanunvericiliklə nəzərdə tutulmuş şəxsi məlumatların emalına tamamilə aiddir.

Açar sözlər: *informasiya təhlükəsizliyi, məlumatın mühafizəsi, fərdi məlumatlar, fərdi məlumatların emalı üçün məlumat sistemi, fərdi məlumatların mühafizəsi, fərdi məlumatlara təhlükə*

Introduction

Information technologies are widely used in data processing, as well as in their exchange between different users. Such processes cover not only a separate organization or its structures, which act as internal users, but also external users. Under such conditions, taking into account the increasingly widespread use of information technologies, problems arise in protecting information resources, including data processing and data transfer.

Therefore, information security issues are given considerable attention.

Information resource security covers a number of issues related to organizational measures, protection from external threats, and protection from leakage of confidential information. It should be noted that most information security systems are aimed at protecting against external threats and leakage of confidential information. Such systems use various methods of protection, in particular, information filtering with content analysis to prevent unwanted disclosure of confidential information by publishing files, sending letters, transferring files over the network, etc. However, as shown by the results of studies by various centers working in the field of information security, a significant number of incidents related to violation of information security are caused by internal threats. The source of such threats are legal users of information systems (Bazovaya model' ugroz bezopasnosti

personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh, 2008).

Research

The problem of protecting information resources is especially important from the point of view of protecting personal data. Such protection involves minimizing losses that arise when threats to the security of personal data are realized with the ensuing consequences – physical, material and financial harm to the subject of personal data. Therefore, recently, many countries around the world have been paying considerable attention to the issues of protecting personal data (Informatsionnaya bezopasnost' biznesa, 2014).

First of all, this concerns the issues of developing systems for protecting such data. Technical methods occupy an important place in them, which should include software, hardware or hardware and software tools that perform information protection functions. They should be built taking into account the concepts of personal data protection, in accordance with their structure, models of threats to the security of personal data, methods of processing, analysis and management of data, and the structure of databases. In other words, the problem of protecting personal data involves the implementation of a set of organizational and technical measures that form the structure of the personal data protection system, which is implemented within the framework of the (Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh, 2014).

Information security threats are the second most relevant among the main business threats such as: economic instability, industrial espionage, intellectual property theft, damage to reputation, etc.

It has been established that issues of internal security of information systems, in particular the issue of uncontrolled dissemination of data, are currently relevant (NIST Special Publication 800-53: Security and Privacy Controls. U.S. National Institute of Standards and Technology's guidelines for securing information systems, 2020).

This is due to the steadily growing number of recorded cases of information leaks in all countries of the world. Compared to 2023, when the main source of threats were current employees, in 2020 threats more often came from former employees of companies. At the same time, among all sources of threats, the largest increase (58 %) compared to the previous year was noted in incidents related to former service providers. In 2015, the number of information security incidents identified by study participants was 2.5 times higher than the same indicator in the previous year. The number of cases of intellectual property theft (Measures to protect data in the state information systems, 2014).

Among the threats to information security, two groups of threats are distinguished: internal and external. External threats include threats that arise and are managed outside of information systems (IS). From the point of view of protecting information and information resources, preference is given to external threats, i.e. the fight against external threats. Almost all enterprises use software and hardware protection tools that are designed to combat external threats and counter them quite effectively. For example, antivirus and antispam systems, access control systems and firewalls, IDS/IPS systems, etc. (Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh, 2008; Verizon 2023 Data Breach Investigations Report, 2023).

When classifying an information system, a number of initial data are taken into account: the category of information (data) processed in the information system, the volume of information processed, the security characteristics of the information or information resources specified by the operator, the structure of the required information system, the presence of connections of the information system to public communication networks or international information exchange networks, the necessary information processing modes, the location of the technical means of the information system, etc (Federal'nyy zakon RF ot, 2006).

There are also other software and hardware means of protecting information from leakage that cannot be directly attributed to those listed above. For example, means of blocking external storage media. Such systems cannot recognize information by categories, do not distinguish restricted information from general information, and are an implementation of individual functions of the specified information protection systems. Today, only information leak detection and prevention

systems, the so-called DLP systems, which are the most widespread, are used to prevent information leakage beyond the protected space of the information system in real time based on data filtering or external attributes that accompany the process of data movement (Chernyshova & Ovchinnikov, 2015).

The key function of D LP systems is the automatic detection of restricted data in information flows using special algorithms. The efficiency of their work primarily depends on the quality of detection of the information specified for search in the general data flow. Therefore, it is the methods and algorithms of information analysis that are key in the operation of such systems. Various methods, technologies and algorithms are used. These include methods of processing text documents in order to obtain meaningful information about the structure of the data being studied (ISO/IEC 27001: Information Security Management. International standard for managing information security, 2013, revised in 2022).

Initial data for determining current threats are formed on the basis of a list of sources of such threats, vulnerable links of the information system, a list of technical channels of information leakage. Threats to information security are determined based on the results of an assessment of the capabilities (potential, equipment and motivation) of external and internal violators, an analysis of possible vulnerabilities of the information system, possible ways of implementing threats to information security and the consequences of violating the properties of information security (confidentiality, integrity, availability) (General Data Protection Regulation (GDPR) Overview, 2016).

This fully applies to the protection of PDn, which have certain features, i.e. the concept of PDn may concern not a block of information, but individual definitions. For data of this type, it is important to form a conceptual approach with the definition of measures that must be implemented when forming a PDn protection system (Data Protection and Privacy in the Digital Age. Research paper discussing global trends in personal data protection, 2021).

Taking into account the possible types of threats to the security of PD and the requirements for their processing, it is necessary to implement an information system within the CIS that will be aimed at processing PD. In order to establish the required level of PD security, the development and implementation of such systems requires the use of the following information security measures (ENISA Threat Landscape Report, 2023):

- identification and authentication of access subjects and access objects;
- access control of access subjects to access objects;
- software environment restrictions;
- protection of machine storage media;
- registration of security events;
- anti-virus protection;
- detection (prevention) of intrusions;
- control (analysis) of information security;
- ensuring the integrity of the information system and information;
- ensuring the availability of information;
- protection of the virtualization environment;
- protection of technical means;
- protection of the information system, its means and communication and data transmission systems.

Conclusion

The use of the above security measures minimizes the threats associated with unauthorized access to PD resources, and partially the threats associated with the unauthorized dissemination of data.

References

1. Chernyshova, G. Yu., & Ovchinnikov, A. N. (2015). Primeneniye metodov intellektual'nogo analiza dannykh dlya klasterizatsii tekstovykh dokumentov [Application of methods of

intellectual data analysis for clustering textual documents]. *Informatsionnaya bezopasnost' regionov*, 4(21), 5-12.
2. Data Protection and Privacy in the Digital Age. (2021). *Research paper discussing global trends in personal data protection*. https://www.sciencedirect.com/science/article/pii/S0267364921000933
3. European Union. (2016). *General Data Protection Regulation (GDPR) Overview*. https://gdpr-info.eu/
4. European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape Report*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape
5. Federal Service for Technical and Export Control of the Russian Federation. (2008). *Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh (vypiska)*. FSTEK Rossii. [Sample model of personal data security threats during processing of personal data in information systems. Approved by the Federal Service for Technical and Export Control, Russia].
6. Federal Service for Technical and Export Control of the Russian Federation. (2008). *Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh*. FSTEK Rossii.
7. Federal Service for Technical and Export Control of the Russian Federation. (2014, February 11). *Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh*. Methodological document. Approved by FSTEK Rossii.
8. Federal Service for Technical and Export Control of the Russian Federation. (2014, February 11). *Measures to protect data in the state information systems*. Guidelines. Approved by the Federal Service for Technical and Export Control, Russia.
9. International Organization for Standardization. (2022). *ISO/IEC 27001: Information Security Management*. International standard for managing information security. Retrieved from https://www.iso.org/isoiec-27001-information-security.html
10. Kaspersky Lab. (2014). *Informatsionnaya bezopasnost' biznesa. Rezul'taty issledovaniya* [Information security of business: Research results]. https://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf
11. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53: Security and Privacy Controls*. U.S. National Institute of Standards and Technology's guidelines for securing information systems. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
12. Russian Federation. (2006, July 27). *Federal'nyy zakon RF ot 27 iyulya 2006 g. № 152-FZ "O personal'nykh dannykh"* [Federal Law of the Russian Federation from July 27, 2006, No. 152-FZ "On personal data"].
13. Verizon. (2023). *Verizon 2023 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

Received: 27.09.2024
Revised: 19.11.2024
Accepted: 05.01.2024
Published: 22.02.2025