Risk Management in Personal Data Processing Within University-Corporate Partnership Interactions

Kruglov D.V[1], Lyashenko V.E.[2*]

[1]*Professor of the Department of Economics and Management of Socio-Economic Systems, Saint-Petersburg University of Management Technologies and Economics*
[2]*Saint-Petersburg University of Management Technologies and Economics*

* Corresponding author
doi: https://doi.org/10.21467/proceedings.7.6.41

Abstract: The exchange of personal data between universities and their corporate partners has become an integral component of educational, research, and business processes. However, such data exchange is associated with risks that may result in losses, necessitating effective risk management strategies. This paper examines current issues related to personal data processing within universities and their interactions with corporate partners. Using NetworkX and Matplotlib, a model illustrating the interaction of personal data processing entities both within the university and in cooperation with business partners has been developed. The study highlights that an increase in the number of participants involved in personal data flows leads to heightened risks in data storage, processing, and transmission. Through an analysis of security threats and academic research, the most common risks in this domain have been identified. The paper concludes that effective risk management in personal data processing is a critical function ensuring the secure and efficient development of business processes between universities and corporate partners. A comprehensive risk management approach will mitigate threats and establish a reliable ecosystem for secure data exchange.

Keywords: personal data, data exchange, risk management

In the contemporary context of the progressive development of the digital society, the processing and exchange of personal data between individuals and institutions have become an integral part of their interactions. Personal data is collected, processed, and stored on a large scale, covering all spheres, including public and municipal administration systems, telecommunications, transportation, healthcare, education, and more. The exchange of personal data between universities and their corporate partners is increasingly becoming an essential component of educational, research, and business processes. In their interactions with partner companies, universities not only process the personal data of students, faculty, and staff but also exchange information related to academic performance, internships, scientific research, and professional activities. However, such data exchange entails risks that may result not only in financial and material losses but also in reputational damage. Consequently, effective management is required to ensure security and uphold the rights of data subjects.

The processing and protection of personal data are governed by regulatory and legal acts that define and regulate the procedures for data processing, storage, and transfer, as well as measures to ensure data security. Key regulatory legal acts include:

1. The Constitution of the Russian Federation, which guarantees citizens the right to privacy and the protection of their personal data.

Proceedings DOI: 10.21467/proceedings.7.6; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-989164-9-5

2. Federal Law No. 152-FZ of July 27, 2006 on Personal Data [1] establishes the fundamental rules for processing personal data, liability measures for violations, and methods of protection. This law also defines personal data (PD), which refers to any information that directly or indirectly relates to a specific individual (data subject). Such data may include a person's name, residential address, date of birth, email address, and other information that allows for personal identification.
3. Order of Resources and Technology No. 18 of February 24, 2021 on Approval of Requirements for the Content of Consent to the Processing of Personal Data Permitted by the Data Subject for Distribution [2], and Decree of the Government of the Russian Federation No. 1119 of November 1, 2012 [3] establish requirements for the content and protection of personal data during processing in information systems. These documents regulate measures to ensure the security of such systems.
4. Order of the Federal Service for Technical and Export Control of Russia (FSTEC) No. 21 of February 18, 2013 [4] regulates organizational and technical measures to ensure the security of personal data when using information systems.

International legislation in the field of personal data processing, including the interaction between universities and employers, is regulated by several key regulations. The most famous of them are GDPR (General Data Protection Regulation) in the European Union and FERPA (Family Educational Rights and Privacy Act) in the United States. These laws establish the rules for processing, storing and transferring personal data, including students and graduates. We pay attention to table 1.

Table 1. GDPR and FERPA in the field of personal data processing

Key aspects	GDPR (EU)	FERPA (USA)
The scope of application.	All organizations processing the data of EU citizens.	Educational institutions receiving federal financing.
Agreement	A clear consent for data processing is required.	Consent is required to disclose educational records.
Rights of subjects	The right to access, correction, deletion and restriction of processing.	The right to access and correct educational records.
Data transmission	Data can be transmitted only if there are legal grounds.	Data can be transmitted only with the consent of the student or as part of exceptions.

For several years, numerous academic studies have been dedicated to investigating the criteria for classifying information as personal data, the legal aspects of its protection, potential risks, and measures for their mitigation. For instance, A.N. Batlynova [5], R.F. Nugaeva [6], A.V. Minbaleev [7], and V.A. Pikov [8] analyze personal data from a legal perspective. Meanwhile, A.S. Isaev [9], T.T. Gazizov [10], V.I. Averchenkov, M.Y. Rytov, V.A. Shkaberin, and O.M. Golembiovskaya [11] complement their research with risk and threat assessments related to personal data processing and

transmission. Furthermore, the works of E.V. Burykova [12], D.A. Skvortsova [13], A.V. Filimonov [14], and S.G. Yanbaeva [15] focus on data protection measures and risk mitigation strategies, particularly in the context of higher education institutions. Having analyzed various scholarly approaches, it is important to note that many of these studies remain highly debated. The issues surrounding the collection, processing, storage, and transfer of personal data within universities are subject to diverse viewpoints. However, most authors do not address the problematic aspects of university-corporate interactions concerning the exchange or transfer of personal data and the associated risks.

Universities, in compliance with legal requirements in this domain, develop internal policies for personal data protection. These policies take into account regulatory documents that govern internal processes related to data processing, storage, and transfer. In modern universities, personal data is processed at every stage of interaction with applicants, students, faculty, staff, and alumni. Ensuring effective protection of such data requires a comprehensive approach, encompassing compliance with legal requirements, structuring internal processes, and appointing responsible personnel. Universities adapt these requirements to the specific nature of the educational process. This includes safeguarding the personal data of applicants during the admission process (document processing, entrance exam results), managing and storing data of students and employees (academic records, medical certificates, financial documents), and protecting alumni information (archival records, employer interactions). As a result, universities contain both data controllers and processors who are in constant interaction.

Using the NetworkX library for graph construction and Matplotlib for visualization, we present a model of personal data interaction subjects within a university in Figure 1.

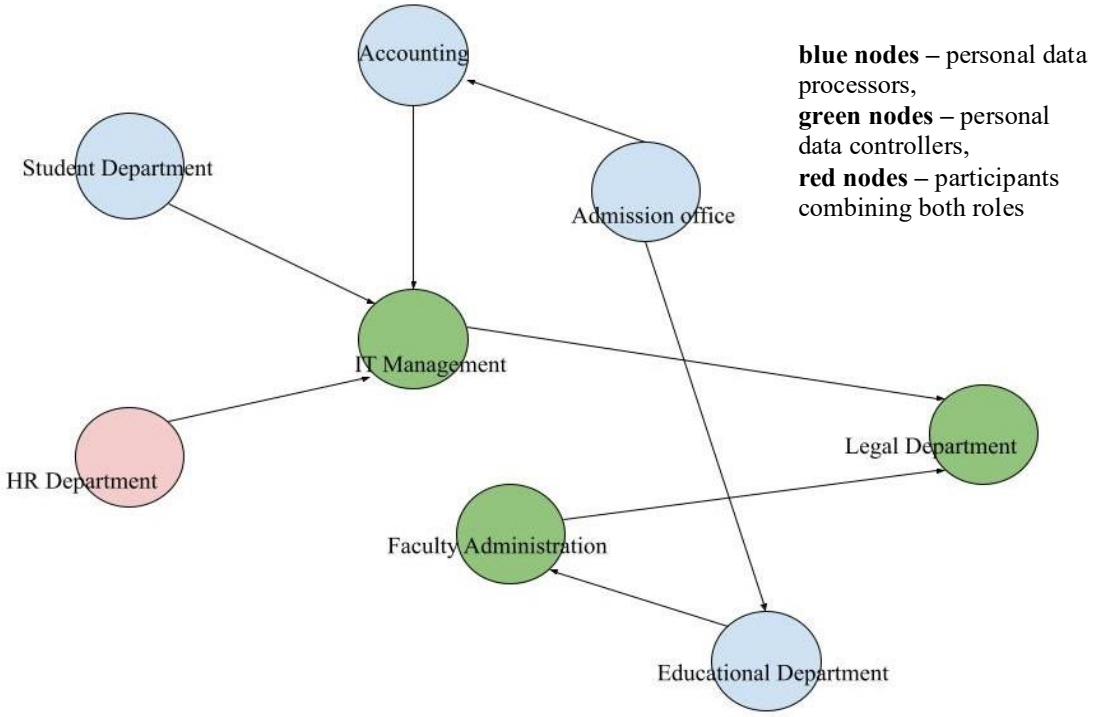

Fig.1. Network Graph of Personal Data Processing Entities within a University

The diagram illustrates the interaction between personal data processors and personal data controllers within a university. Blue nodes represent university entities acting as personal data processors, green nodes denote personal data controllers, while red nodes indicate areas of interaction where entities perform both roles. The connections depict the flow of data and the mechanisms of control.

Personal data processors are university staff and departments responsible for handling personal data as part of their official duties at various stages of the educational and administrative processes. In a higher education institution, these roles are fulfilled by: t*he Admissions Office*, which collects and processes applicants' data (passport details, educational background, and contact information); *faculty academic departments*, which record student enrollment, academic performance, and attendance; *the HR Department*, which manages personnel records related to scientific and administrative activities; *the Accounting Office*, which handles financial operations involving personal data. Personal data controllers are structural units that oversee the storage, security, and governance of personal data. They define the objectives and methods of data processing and bear responsibility for ensuring compliance and protection. This category includes: *the IT Management Department*, responsible for digital data security; *the Legal Department*, ensuring regulatory compliance; *Faculty Administration* and *the HR Department*, coordinating data governance. Within the university, data exchange occurs between these units. For example, the admissions office transfers enrollment records to academic departments and accounting for further processing.

It is important to note that this model does not account for external interactions between the university and third parties, which is a significant factor in assessing the risks associated with data processing and transmission. Therefore, we propose an expanded model incorporating external participants such as corporate partners, alumni associations, military enlistment offices, and applicants themselves. The revised diagram (Figure 2) introduces additional yellow nodes representing external data sources, while the blue and green nodes continue to indicate internal processors and controllers. Gray nodes represent external data recipients, including business partners and alumni organizations. This model visualizes the entire data lifecycle within a university, from initial collection to transmission to external stakeholders.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

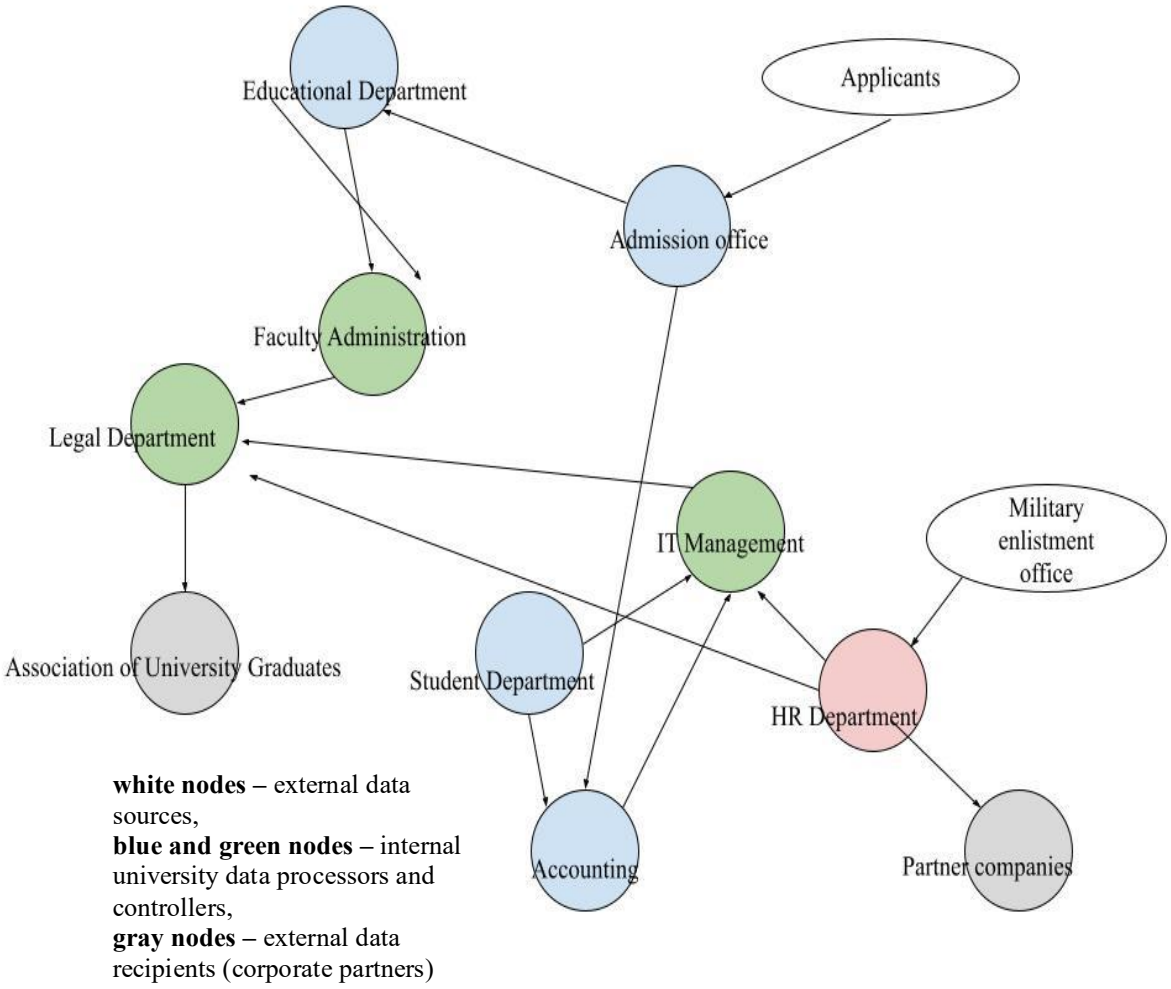

Fig.2. Personal Data Flow from University Admission to Transmission to External Corporate Partners (compiled by the author)

The interaction between university departments responsible for processing and storing personal data, as well as their exchange with external corporate partners, involves the following key stages and activities:

— Admissions Office (Data Entry): collection of primary applicant information, including passport details, educational background, and contact information.

— Faculties and Academic Departments: processing of student data throughout the learning process, including academic performance, attendance, and course-related records.

— Security and Access Control: storing of data necessary for managing university access permissions, such as student ID cards and entry records.

— Student Services Office (Document Processing Department): handling student requests for certificates, official statements, and supporting documents.

— Alumni Relations Office, Career Development Center, or HR Department (Data Exit): storing and processing alumni data to maintain graduate databases and facilitate post-graduation interactions.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

The distribution and processing of personal data within the university and during interactions with corporate partners should be regulated by internal normative legal acts (NLAs). These acts must define the procedures for data collection, storage, transfer, and protection, ensuring clear accountability for each university department. Furthermore, these regulations should govern external interactions with corporations, ensuring strict compliance with legal requirements and contractual obligations between all parties involved. The increase in the number of participants involved in personal data flows inherently leads to heightened risks associated with data storage, processing, and transmission. By analyzing real-life cases of security threats and existing academic research [9, 10, 11], we identify the most common risks in this domain:

1. Data breaches due to unauthorized access or dissemination of personal information (e.g., SQL injection attacks).
2. Unauthorized transmission of data to third parties without the consent of data subjects, including the disclosure of confidential information to unauthorized users.
3. Non-compliance with legal regulations, such as violations of Federal Law No. 152-FZ of July 27, 2006 on Personal Data.
4. Human errors by university staff or corporate partners, which may result in data leaks.
5. Vulnerabilities in information systems due to insufficient IT infrastructure protection, allowing unauthorized remote access to database management systems (DBMS) or physical access to DBMS servers. We pay attention to table 2.

Table 2. Indicators for risk assessment

Indicator	Description	How to measure
Number of cases of data transfer without contract	The number of facts of informal data transmission	Polls, internal audit
The presence of encryption when transmitting data	Whether encryption is use	Poll IT Departure, those. documentation
Number of cases of company access to data without consent	Facts of access of companies without the consent of the data subject	Audit, survey
The level of informing of personnel	Do employees know about PD protection policy	Polls, testing
Top fixed leakage incidents	Over the past year	Security reports analysis

And so the result may be look at Table 3

Table 3. Collection and analysis of data assessment of personal data processing risks

№	Indicator	Cases (units) recorded	Permissible level (by law)	Risk (yes/no)
1	Data transfer without contract	5	0	yes
2	Data transfer without consent	2	0	yes
3	Lack of encryption	1	0	yes
4	The presence of trained employees	60%	100%	yes
5	Fixed leaks	1	0	yes

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Based on the data, we can conclude that the organization identified violations in the field of personal data protection during the interaction of the university and partners, as violations have been identified in all 5 positions. We determined that within two positions, risks can be minimal.

Following an analysis of these risks and their impact within universities, we propose risk mitigation strategies, summarized in Table 3.

Table 4. Risk Management Measures and Their Characteristics in Universities and External Partnerships (compiled by the author)

Measure Type	Management Action
Legal Measures	Signing confidentiality and data protection agreements with corporate partners. Defining rights and responsibilities of all parties involved in data processing. Obtaining explicit consent from data subjects for data processing and transfer.
Organizational Measures	Appointing responsible personnel for personal data processing and protection. Conducting regular training for university staff on information security. Performing audits of organizational and IT security measures.
Technical Measures	Implementing modern encryption methods for secure data transmission and storage. Restricting data access based on role-based access control (RBAC). Deploying risk monitoring systems to detect and mitigate security threats.
Incident Management	Identifying and assessing potential security threats. Evaluating the likelihood and impact of each risk. Establishing rapid response protocols for security incidents. Documenting and analyzing security incidents to prevent recurrence.

It is important to emphasize that the proposed measures must be implemented systematically by integrating them into the digital environment that facilitates interactions between universities and corporate partners. This responsibility can be assigned to audit and risk management committees, which oversee risk mitigation strategies. Establishing such committees will significantly enhance personal data protection efficiency. Figure 3 illustrates a schematic representation of the risk management process for handling personal data when universities interact with corporate partners.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

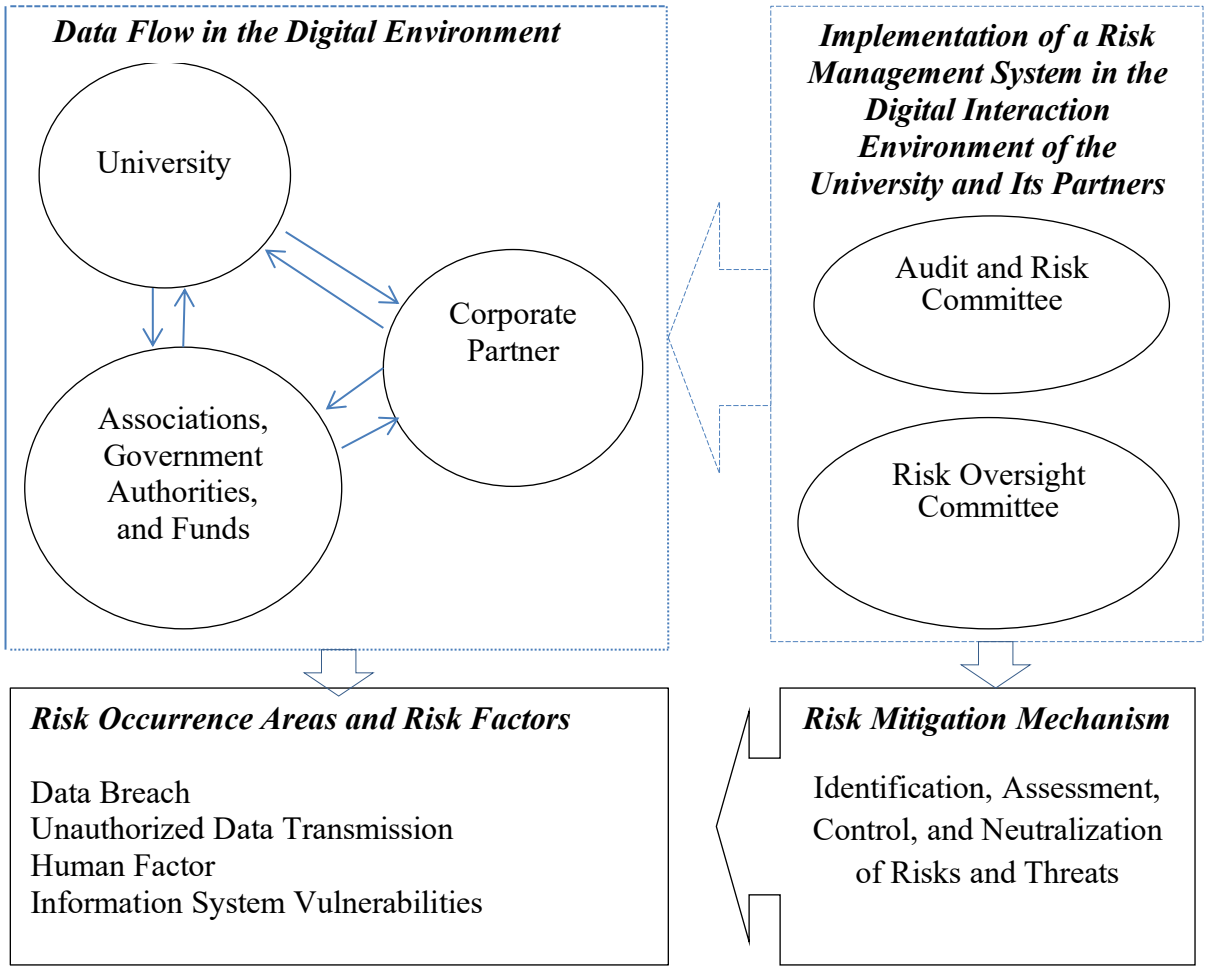

Fig.3. Risk Management in Personal Data Collection, Processing, and Exchange Between Universities and Corporate Partners (compiled by the author)

In the modern digital society, personal data protection has become critically important, particularly in light of the growing digitalization across all fields and their interconnectedness. Organizational security measures play a fundamental role in ensuring data protection. Accurately identifying potential threats allows for the selection of effective safeguards, thereby minimizing data breach risks and preventing unauthorized access. Effective risk management in personal data processing when universities collaborate with corporate partners is a strategic necessity. It ensures both secure and efficient business process development among stakeholders. A comprehensive risk management approach, incorporating legal, organizational, and technical measures, will mitigate threats and foster the development of a reliable and secure data exchange ecosystem.

References

[1] Federal Law No. 152-FZ of July 27, 2006 on Personal Data // Collected Legislation of the Russian Federation, http://pravo.gov.ru, last accessed 2025/01/31.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

[2] Decree of the Government of the Russian Federation No. 1119 of November 1, 2012 on Approval of Requirements for the Protection of Personal Data during Their Processing in Information Systems of Personal Data, https://base.garant.ru/70252506/?ysclid=m6kh4497mv58560587, last accessed 2025/01/31.

[3] Order of Resources and Technology No. 18 of February 24, 2021 on Approval of Requirements for the Content of Consent to the Processing of Personal Data Permitted by the Data Subject for Distribution, http://pravo.gov.ru, last accessed 2025/01/31.

[4] Order of the Federal Service for Technical and Export Control of Russia (FSTEC) No. 21 of February 18, 2013 on Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data during Their Processing in Personal Data Information Systems, https://fstec.ru/, last accessed 2025/01/31.

[5] Batlynova, A.N. Personal Data. Administrative Law. No. 4. P. 25. (2020).

[6] Nugaeva, R.F., Pavlov S.Yu. Personal Data as an Object of Administrative Legal Regulation. International Journal of Humanities and Natural Sciences. No. 12-1(75). P. 217-220. (2022).

[7] Minbaleev, A.V. Problems of Legal Support for Cybersecurity in the Dissemination of Personal Data on the Internet under the Updated Legislation. Bulletin of the Ural Federal District. Information Security. No. 2(40). P. 65-71 (2020).

[8] Pikov, V.A., Vergasova A.E. Implementation Method of the Requirements of Federal Law No. 152-FZ of July 27, 2006 on Personal Data in the Russian Segment of the Information and Telecommunication Network “Internet”. Bulletin of the Russian New University. Series: Complex Systems: Models, Analysis, and Management. No. 4. P. 139-154. (2018).

[9] Isaev, A.S. Automation of the Threat Model Formation Process for the Security of Personal Data during Their Processing in Personal Data Information Systems Based on the Theory of Expert System Development. Scientific and Technical Bulletin of the Volga Region. No. 2. P. 133-135 (2014).

[10] Gazizov, T.T., Mytnik A.A., Butakov A.N. A Typical Threat Model for the Security of Personal Data in Information Systems for Automating the Educational Process. Reports of Tomsk State University of Control Systems and Radioelectronics. No. 2(32). P. 47-50 (2014).

[11] Averchenkov V.I. , Rytov M.Yu., Shkaberyn V.A., Golembiovskaya O.M. Automation of Personal Data Protection in a University. Proceedings of the International Association of Slavic Universities. No. 1. P. 126-134 (2011).

[12] Burykova, E.V. Personal Data Protection System in a Higher Education Institution. Intelligence. Innovation. Investment. No. 7. P. 69-74 (2017).

[13] Skvortsova, D.A., Vikhman V.V. Development of a Comprehensive Methodology for the Protection of Personal Data Processed in a University. News of Science and Education. Vol. 6. No. 6. P. 13-15 (2017).

[14] Filimonov, A.V. Development of Requirements for a Personal Data Protection System. Information and Computing Technologies and Their Applications: Proceedings of the XXIV International Scientific and Technical Conference, Penza, August 27–28th. P. 123-125 (2020).

[15] Yanbaev, S.G., Larinbaeva. Measures and Restrictions on Access to Information and Personal Data in the Russian Federation. International Journal of Humanities and Natural Sciences. No. 2-3(89). P. 181-185. (2024).