DOI: 10.17747/2618-947X-2026-1-73-83
УДК 332

Enterprise Information Security Strategy: Monitoring and Management

T.A. Rudakova[1, 2]
O.Yu. Rudakova[2]
[1] Altai State Technical University named after I.I. Polzunov (Barnaul, Russia)
[2] Altai State University (Barnaul, Russia)

Abstract

The security of an economic entity's information and the infrastructure that supports it remains one of the key challenges at the current stage of economic relations. Unauthorized access to information, accidental or malicious impacts on information, and third-party intrusion into the operation of the supporting infrastructure threaten to reduce economic benefits and cause damage to economic entities, both legal entities and individuals. Under these conditions, one of the tasks of an organization's economic security service is to prevent threats and mitigate risks related to unauthorized access to sensitive and financial information about the enterprise and to employees' personal data. The objective of the study is to develop methodological recommendations for organizing the process of managing enterprise information security risks. In the course of the study, the authors obtained the following scientific results: the elements of information security (information protection, access restriction, encryption, security system, two-factor authentication, information transfer, document forgery, verification of the vulnerability of the information source, and information authenticity) were examined comparatively, considering both their current state and their historical development; information on participants involved in information theft and methods of unauthorized access was systematized; factors limiting compliance with personal data protection principles were analyzed; and information security risks were systematized in the context of object-vulnerability-threat. The practical significance of the research results lies in the possibility of integrating them into an organization's management system and developing an internal control system to minimize threats and mitigate the risks of unauthorized access to sensitive and financial information and employees' personal data.

Keywords: personal data, sensitive and financial information, risks of unauthorized access

For citation:

Rudakova T.A., Rudakova O.Yu. (2026). Enterprise Information Security Strategy: Monitoring and Management. *Strategic Decisions and Risk Management*, 17(1): 73-83. DOI: 10.17747/2618-947X-2026-1-73-83. (In Russ.)

企业信息安全保障战略：监测与管理

T.A. Rudakova[1, 2]
O.Yu. Rudakova[2]
[1] 波尔祖诺夫阿尔泰国立技术大学（巴尔瑙尔，俄罗斯）
[2] 阿尔泰国立大学（巴尔瑙尔，俄罗斯）

摘要

经济主体信息及其保障该信息运行的基础设施的安全性，仍然是当前经济关系发展阶段面临的挑战之一。对信息的未授权访问、对信息的偶然或恶意影响，以及第三方侵入相关支撑基础设施的运行，都会导致经济利益受损，并对经济主体—无论是法人还是自然人—造成损害。在这种背景下，组织经济安全部门的任务之一，就是防范威胁并控制企业敏感信息、财务信息以及员工个人数据遭受未授权访问的风险。本文旨在提出关于企业信息安全风险管理流程组织的方法建议。研究过程中，作者取得了以下成果：从比较视角考察了信息安全各项要素—包括信息保护、信息访问限制、加密、安全系统、双因素认证、信息传输、文件伪造、信息来源脆弱性检验以及信息真实性—的现状及其历史演变；系统梳理了信息窃取及未授权访问信息的方式；分析了制约个人数据保护原则落实的因素，并在"对象—脆弱性—威胁"框架下系统归纳了信息安全风险。研究结果的实践意义在于，可将其整合到组织管理体系和内部控制体系建设中，以最大限度减少针对敏感信息、财务信息和员工个人数据的未授权访问威胁，并控制相关风险。

关键词： 个人数据，敏感信息与财务信息，未授权访问风险

引用格式：

Rudakova T.A., Rudakova O.Yu. (2026)。企业信息安全保障战略：监测与管理。战略决策与风险管理, 17(1): 73–83. DOI: 10.17747/2618-947X-2026-1-73-83. （俄文）

Introduction

The global digital transformation of the economy is accelerating the development of information technologies and the integration of innovative solutions across economic sectors and public administration. For active participants, this creates competitive advantages, reduces costs, improves service quality, enhances production efficiency, and increases economic returns in the short term, with similar benefits expected in the future. At the same time, these positive developments are accompanied by negative effects, most notably the growing information vulnerability of economic entities.

Within the economy, information serves both as an object of exchange and as a source of data about business entities. Under current conditions, the task of those generating information is not only to ensure its accuracy but also to protect it from unauthorized interference. This includes safeguarding both the data itself and the infrastructure that supports it—what is commonly referred to as information security. Most researchers and practitioners dealing with the assessment of data security and supporting infrastructure agree that unauthorized access to business data remains a persistent risk. The ability to predict and prevent such incidents depends on multiple factors, while effective management of these risks helps minimize potential damage. In August 2025, the Russian analytical platform TAdviser conducted a survey among experts and business representatives. According to the results, "two out of three Russian companies (67%) can be breached within less than a day, and in more than 60% of cases, an incident capable of disrupting business operations can be successfully executed."[1]. These findings suggest that the level of cybersecurity claimed by businesses is substantially lower than the level of protection actually required, while risks and threats continue to be underestimated. At the same time, the time required to compromise a target system continues to shrink. Developers of innovative information security solutions attribute this situation to several factors.

First, management often prioritizes tasks such as timely reporting to investors and government institutions, conducting audits, obtaining positive audit opinions on financial statements, ensuring management efficiency, and maintaining business continuity.

As a result, information protection and control over unauthorized access tend to receive less attention. The rapid pace of technological development and the increasing use of advanced IT solutions in illicit activities make information systems more vulnerable. Moreover, the convenience of modern technologies often reduces their resilience. This creates an illusion of manageable risk at the management level. However, experts highlight persistent weaknesses in information security, including issues related to identification and authentication, as well as privilege management—such as excessive access rights in Active Directory, service accounts without multi-factor authentication, outdated or reused passwords, and persistent VPN access for contractors. Additional vulnerabilities include legacy Windows environments, unmanaged updates, and weak network segmentation, where the compromise of a single user device can lead to the failure of critical systems[2].

Information security, along with the challenges and factors limiting the legal protection of data, including personal data, has been widely studied in both domestic and international research. For example, the impact of big data technologies and related tools on personal data protection was analyzed in [Savelyev, 2015]. Information security and payment card industry standards were examined in [Borhalenko, 2015]. A bibliometric analysis of phishing attacks and WhatsApp[3] crelated threats using VOSviewer was presented in [Sujiwana et al., 2024]. International legal regulation of the digital environment was discussed in [Yastrebova, 2025]. Cybercrime and its regulation in countries of the Global South were analyzed in [Tsyplakova, 2025]. The role of intelligent systems in decision-making within the legal framework was explored in [Selivanova, Konopiy, 2025]. The use of explainable artificial intelligence for detecting attacks on corporate networks was proposed in [Yaz, Süzen, 2023]. The importance of human and social factors in monitoring information security risks was emphasized in [Van Deursen et al., 2013]. A quantitative model for assessing information security risks was proposed in [Jouini, 2015]. The role of financial and non-financial information in cybersecurity was analyzed in [Cristea, 2020]. Finally, [Lee, 2011] proposed a model for optimizing returns on investments in customer information security.

1. Unauthorized Access to Information

In Russian dictionaries, the term "to authorize" is defined as "to grant permission." Accordingly, information obtained without the consent of its owner may be considered stolen. Unauthorized access to information in the context of digital transformation represents a serious threat affecting both individuals and organizations, regardless of their size, ownership structure, or industry. This issue has attracted the attention of researchers since the early days of computing. The actors involved in in-

[1] https://clck.ru/3Pt26q/.
[2] Ibid.
[3] Owned by Meta, an organization recognized as extremist and banned in the Russian Federation.

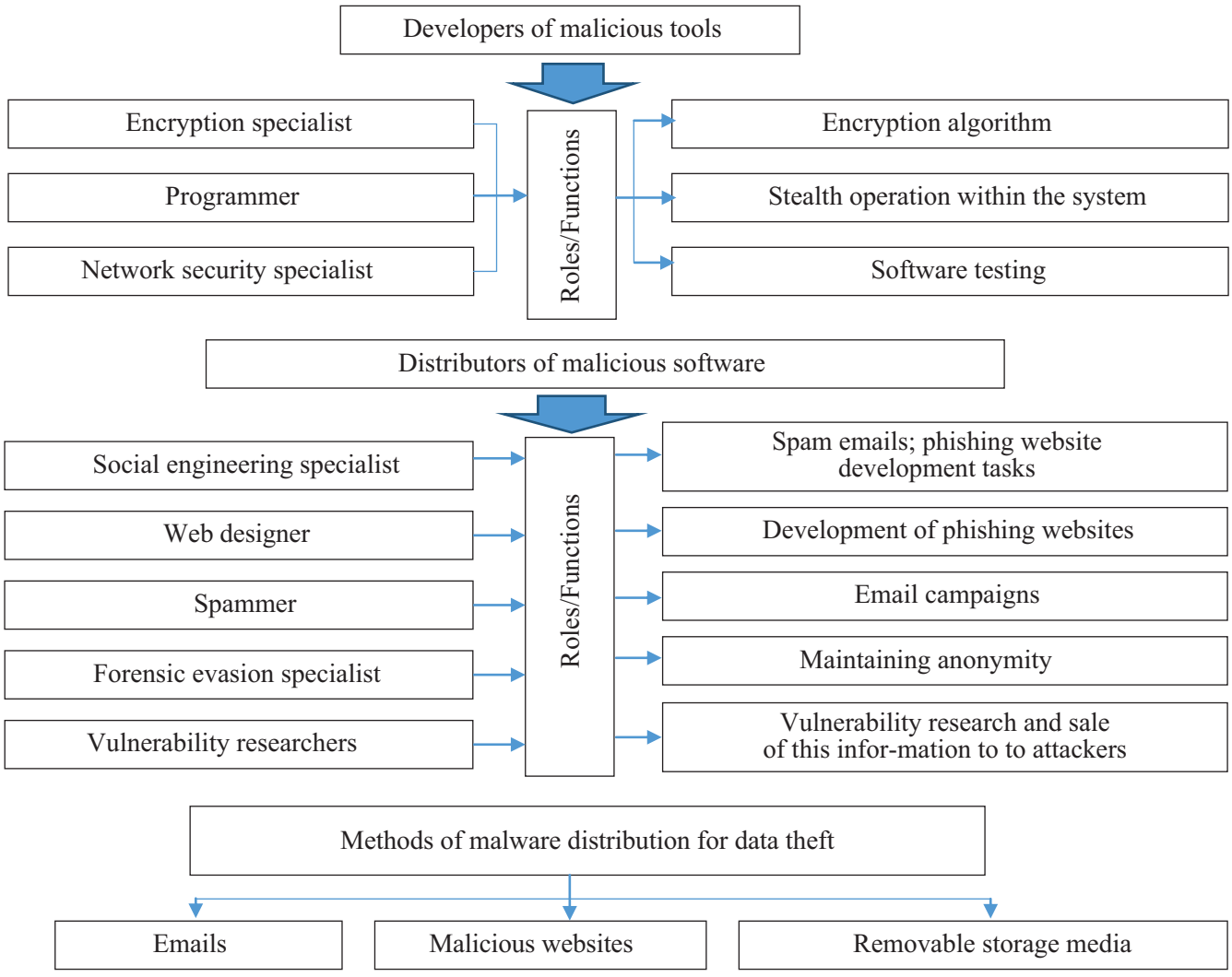
formation theft and the methods used to obtain data are presented in Figure 1.

The process of information theft typically involves the creators of malicious tools, distributors of malware, target objects, and access channels to data storage systems. These tools may be developed by a single specialist or a team possessing expertise in encryption algorithms, stealth techniques, and software testing. The distribution of malicious software is carried out by social engineering specialists, web designers, spammers, and experts responsible for maintaining anonymity and identifying software vulnerabilities.

2. Technological Innovation and the Risks of Information Leakage

The main channels through which information may be accessed include email in the absence of spam filtering and antivirus protection, malicious websites visited by users, applications downloaded to devices, and removable storage media that may be infected with malware. In all such cases, the primary source of vulnerability is the user of the device, whether a personal computer, tablet, or mobile phone.

In 2025, a ransomware strain capable of embedding itself in processor microcode was reported. At a confer-



Source: compiled by the authors.

Fig. 1. Actors Involved in Information Theft and Methods of Unauthorized Access

ence, K. Baik, Senior Director of Threat Analytics at Rapid7, described this threat and noted that he had developed a proof-of-concept malware sample capable of modifying the microcode of AMD Zen processors, which are used in a wide range of devices, including desktop computers, laptops, servers, and embedded systems. Because such malware remains invisible to conventional security tools, it represents a particularly serious threat. In Baik's view, cybersecurity professionals have become overly focused on advanced technologies, including artificial intelligence, while neglecting basic cybersecurity practices and longstanding security weaknesses[4].

The range of technological innovations in information acquisition, storage, and transmission has recently expanded to include tools based on generative artificial intelligence, of which there are now more than two thousand. These tools are used across a wide variety of fields. Their adoption is rapid and continues to gain momentum, while platforms built around them are developing at high speed. This points both to their broad practical use and to their substantial potential to transform socioeconomic processes.

According to the Big Data Association in cooperation with the consulting company B1 and TAdviser, the big data market showed strong growth in 2024 compared with 2023. Nearly all segments—services, application software, and infrastructure—grew by 26% to 33% (Table 1).

Within the services segment, the highest growth rate is seen in analytics and DaaS (Data as a Service) (Table 2).

The highest growth rate in the software segment—139.9%, or RUB 13 billion—is observed in analytical software (AI platforms) (Table 3).

Table 1
Big Data and Artificial Intelligence Market in Russia

Indicator	Market Size (RUB bln)		Growth	
	2023	2024	Absolute (RUB bln)	Relative (%)
Services	179	239	60	133.51
Application Software	95	127	32	133.68
Infrastructure	53	67	14	126.41
Total	327	433	106	132.41

Source: compiled by the authors based on TAdviser: https://www.tadviser.ru/a/910779.

Table 2
Services Segments of the Big Data and Artificial Intelligence Market in Russia

Indicator	Market Size (RUB bln)		Growth	
	2023	2024	Absolute (RUB bln)	Relative (%)
IT consulting, business consulting, data labeling, and model training support	85	105	20	123.5
Analytics and DaaS				
Advertising data products	44	67	23	152.2
Non-advertising data product	50	67	17	134

Source: compiled by the authors based on TAdviser: https://www.tadviser.ru/a/910779.

Table 3
Software in the Big Data and Artificial Intelligence Market in Russia

Indicator	Market Size (RUB bln)		Growth	
	2023	2024	Absolute (RUB bln)	Relative (%)
Application Software	29	39	10	134.48
Digital infrastructure	22	29	7	131.81
AI platforms	33	46	13	139.39
BI, EPM, and IBP analytics, geoinformation systems, search software, and software for intelligent content processing	11	13	2	118.18

Source: compiled by the authors based on TAdviser: https://www.tadviser.ru/a/910779.

[4] https://cnews.ru/link/a640902.

The use of generative artificial intelligence tools by employees to perform professional tasks creates a risk that personal, payment-related, and sensitive information may be transmitted through uploaded files and prompt content. This should not be regarded as unauthorized access to personal data or corporate information; rather, it reflects a lack of corporate culture and unprofessional employee conduct resulting from ineffective internal control and risk management systems.

This creates a need for business organizations to develop internal policies governing the use of generative artificial intelligence tools. Otherwise, personal data leaks may result in financial losses, including a fine of RUB 15 million for a first incident and up to 3% of a company's turnover in the event of a repeated breach where the responsible party cannot be identified.

The capabilities of modern innovative technical solutions are largely determined by the volume of information stored in digital devices, as socioeconomic processes have increasingly moved into the online environment. The amount of data is growing exponentially, and conventional tools are no longer capable of handling it effectively. This is where generative artificial intelligence, and tools built on it, become relevant: they can generate any information contained in the underlying data sets, though not always with the consent of individuals, in the case of personal data, or of legal entities, in the case of sensitive and financial information. This is inherent in big data analytics technologies, which comprise tools and methods designed to process and structure continuously expanding and rapidly changing data flows and thus provide the foundation for the use of generative artificial intelligence tools [Savelyev, 2015].

Today, information plays a central role in both business activity and public administration. It has rightly come to be treated as a commodity—often referred to as "the new oil" [Arthur, 2013]—and is now regarded as one of the factors of production. The quality and volume of this asset allow those who possess it, provided they have the necessary technical capabilities, to occupy a key position in the value chain, increase productivity, reduce costs, and thereby contribute to the growth of industries that support data analysis, including both technology and related services.

3. Information Security: A Historical Perspective

The need to protect information in storage and transmission from unauthorized interference and misuse has long required information creators not only to ensure the authenticity of documents but also to restrict unauthorized access to them. This is evidenced by studies of early cryptographic practices, which show that concerns about information security have existed for centuries (Table 4).

Firewalls—systems that monitor and filter network traffic to prevent unauthorized access to a device or computer network—have replaced the wax, parchment, and threat of execution once used in the fourteenth century to ensure the secure delivery of information from sender to recipient. Today, one of the main means of transmitting and exchanging large volumes of data remains email, whereas historically this function was performed by messengers. In the past, unauthorized access to information was constrained through homophonic encryption of messages written on parchment, which increased their unpredictability, or entropy. Encryption, or encoding, remains a means of protecting information today. Historically, the design of a cipher was the responsibility of its creator. In diplomatic correspondence, homophonic ciphers were widely used: letters were replaced with symbols, and the same letter could be represented by different symbols. At the same time, the limited literacy of the person carrying or encoding the message often prevented them from understanding its content. Information was also protected against loss and interception by sending duplicate messengers and dividing the key to the protected information among them [Larin, 2010].

Today, access to information is restricted through differentiated access rights, individual passwords, two-factor authentication when logging into an account, and biometric systems. In earlier periods, these functions were performed by wax seals and the sender's handwriting. In modern conditions, information transmitted through telecommunication channels is protected by software tools such as antivirus programs. In the past, double envelopes were used, with one containing non-essential information and the other the message intended for the recipient. Letters were often duplicated to increase the chances of successful delivery, and secret markings were used to make intercepted messages more difficult to exploit. The authenticity of information was confirmed by a wax seal attached to the letter; such seals were possessed by persons of rank, including bishops, dukes, and kings. The modern analogue of this mechanism is the electronic signature, which may be protected in different ways depending on the owner and the significance of the document being certified.

Nevertheless, regardless of the tools available at a given stage of social and economic development, information forgery has always existed. This was done by altering the text of a letter written on parchment or paper, either by modifying it directly or by inserting additional text after it had been signed.

Modern society faces supply chain attacks, in which cybercriminals exploit vulnerabilities in software or hardware supply chains to gain access to the systems of a target organization. In such cases, information becomes accessible and may be used for extortion or blackmail. One current way of combating cybercrime is vulnerability identification through bug bounty programs, that is, open initiatives aimed at discovering vulnerabilities in software products. This may be compared with reports of forged coats of arms and seals in earlier periods: if such reports proved false, the informant could be severely punished for providing inaccurate information in a denunciation.

4. Information Security Standards and Personal Data Protection

Establishing an information security system is one of management's priority tasks. The regulation of this area is based on applicable national and international standards. In Russia, the basic rules governing standardization and the application of national standards were established by Federal Law *On Technical Regulation*[5] and State Standard GOST R 1.0-2004 *Standardization in the Russian Federation. Basic Provisions*. National information security standards were developed with reference to international experience and standardization practices. The currently applicable standard GOST R ISO/IEC 27005-2010 *Information Technology. Security Techniques. Information Security Risk Management* refers to international standards only where no equivalent national standard exists. Since national standards are regularly updated, the correct application of GOST R ISO/IEC 27005-2010 requires continuous monitoring of changes in the relevant national documents.

Personal data protection requirements are established both by international law and by national regulations. It should be noted that the international community began addressing the problem of unauthorized access to personal data much earlier than Russia did. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was adopted by the Council of Europe in Strasbourg in 1981, becoming the starting

Table 4
Information Security Elements: Modern Practices and Historical Analogues

Concept	Modern Practice	Historical Analogue
Information protection	Antivirus software	Double envelopes containing non-essential and important information, duplicate letters, secret markings, and steganography on parchment
Restriction of access to information	Access control through individual passwords	Division of decryption keys among messengers
Encryption	Encoding information to prevent unauthorized access	Homophonic encryption designed to make message content less predictable
Security system	Firewalls, which monitor and filter network traffic to prevent unauthorized access to a computer network or device	Wax, parchment, and the threat of execution for messengers
Two-factor authentication	Two different factors used to verify identity when logging into an account or system; biometrics	Wax seals used to secure letters; handwriting
Information transmission	Mail and email	Messengers
Information tampering / falsification	Supply chain attacks, in which attackers exploit vulnerabilities in software or hardware supply chains to gain access to a target organization's systems	Tampering with written documents by altering the text after signature
Vulnerability assessment	Bug bounty programs for identifying vulnerabilities in software products	Reports of forgeries of coats of arms and seals
Information authenticity	Electronic signature	Wax and sealing-wax seals

Source: compiled by the authors.

[5] https://www.consultant.ru/document/cons_doc_LAW_40241/.

point for the adoption of national laws and a series of EU directives across Europe.

The Russian legal framework was supplemented by Federal Law No. 152-FZ of 2006 *On Personal Data*[6], which entered into force in 2007 following Russia's ratification of the Council of Europe Convention in 2005.

This suggests that the legal framework contains a substantial body of provisions governing personal data protection. At the same time, doubts remain as to whether these requirements are consistently observed by all participants in information exchange, both at the stage of data collection and processing and at the stage of data transfer and generation. Individuals voluntarily disclose personal data not only to employers and state institutions, which assume responsibility for protecting such information, but also through messengers, online platforms, and internet resources. As a result, personal data become part of big data sets and may be used to generate new information by combining them with other data unrelated to either the original purpose of disclosure or the stated purposes of personal data processing (Table 5).

Failure to comply with the principle that personal data must be processed only for the purposes for which they were collected may result from a number of factors. These include the employer's technical capacity to handle employees' personal data and store copies of HR documents; the qualifications of personnel who have access to such data; employees' digital literacy; the use of generative artificial intelligence tools in the performance of professional tasks involving personal data; failure by employees to observe digital hygiene practices; and the absence of any guarantee that the economic entity providing storage space for personal data on its platform will remain in operation until the end of the contract term, whether because of voluntary closure or compulsory insolvency proceedings.

An increasing number of organizations are using cloud technologies in workforce management. Once a contract has been concluded, responsibility for the security of HR documents shifts to the cloud service provider, which creates certain information security risks for the client organization. This is because the cloud provider owns the relevant infrastructure. Although storing data in a public cloud offers clear advantages, it does not relieve the organization of its obligation to comply with information security and personal data protection requirements. On the contrary, it requires organizational and technical measures that ensure long-term document retention and continued accessibility. Not all cloud-based HR document management solutions are capable of preserving the legal validity of documents, including electronic signatures, and not all can ensure long-term storage. Therefore, the client organization must be able to export such documents and place them on its own server.

Table 5
Personal Data Protection Principles with Barriers to Their Compliance

Principle	Barriers to Compliance
Voluntary consent of the individual, provided that the operator discloses the purpose of processing	The large volume of information provided by the operator on the purposes of processing, which is difficult to review when accessing the resource The complexity of the way this information is presented by the personal data operator, which may require legal knowledge on the part of the individual
Personal data must not be combined with other sources to generate new information	The logic of big data analytics, which is based on data reuse The accumulation of personal information voluntarily left on websites, online platforms, messengers, and other digital resources
Personal data must be processed in accordance with the operator's stated purposes for collection	Technical limitations Staff qualifications Staff digital literacy Failure of the operator's employees to follow digital hygiene practices The need to ensure business continuity on the part of the economic entity leasing out cloud storage space Phishing

Source: compiled by the authors.

[6] https://www.consultant.ru/document/cons_doc_LAW_61801/.

An analysis of regulatory documents and academic sources leads to the rather discouraging conclusion that unauthorized access to personal and sensitive information remains a pressing issue for all participants in socioeconomic relations and market activity under current conditions and is unlikely to lose its significance in the near future. This is due to the transformative processes taking place in both the economy and society under the influence of digitalization, the migration of information into cloud environments, the adoption of new technological advances in the era of big data, and the development of generative artificial intelligence tools. Digitalization is a long-term process, and each new stage of technological development will bring new challenges, generate new problems, and create new tasks for its participants.

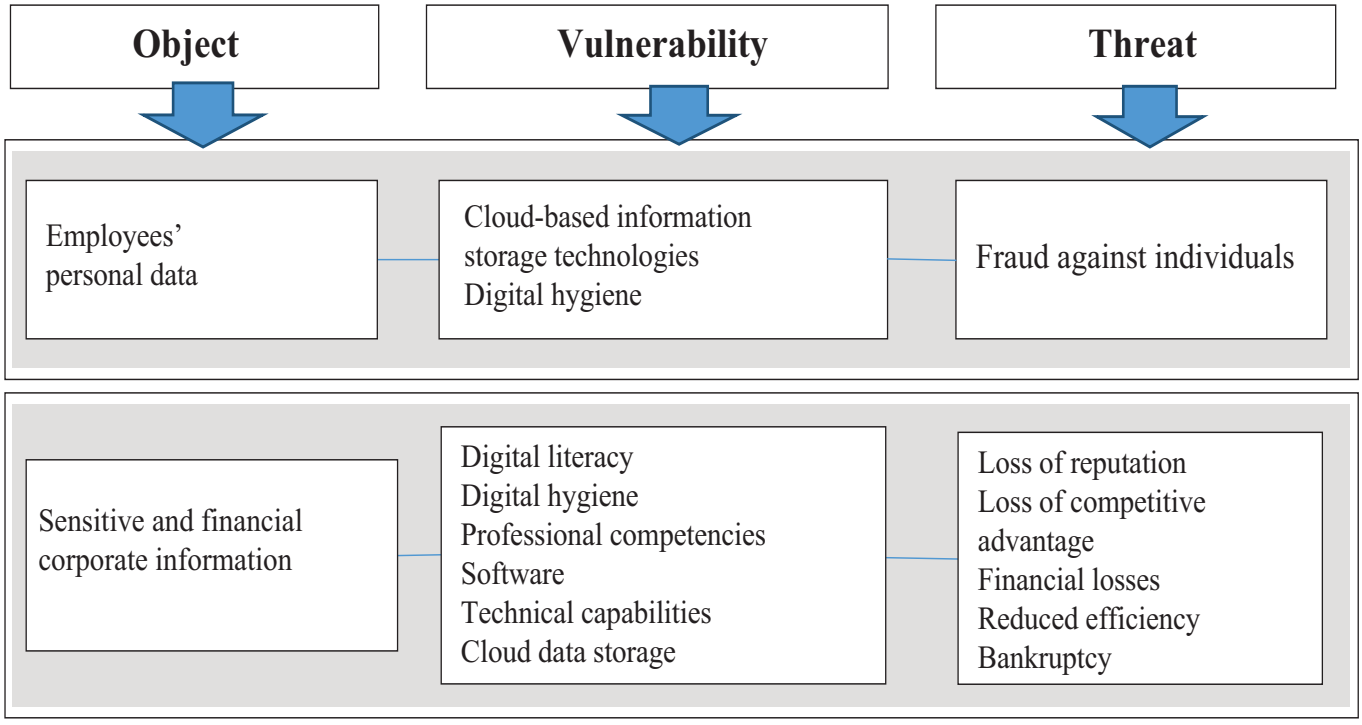
At the present stage of socioeconomic development, unauthorized access to information, its underlying causes, and ways of preventing it should be regarded as fundamental challenges. Participants in socioeconomic relations must be prepared to address them. Above all, this concerns the competencies required of everyone involved in information exchange. Leaders of organizations and public institutions need competencies not only in management but also in building information security systems at both the corporate and personal levels. This, in turn, requires continuous monitoring of developments in information security technologies and of measures aimed at restricting unauthorized access to employees' personal data. Individuals, with due regard to age-related characteristics and other limitations, should also be taught the basic rules of digital hygiene. Since information is now a commercially valuable asset, management must ensure that this value is protected in both a direct and a broader sense by identifying the relevant priorities and tasks.

5. Monitoring and Management of Information Security Risks in an Enterprise

From an information security perspective, risk management should begin by identifying the asset at risk, assessing the vulnerabilities of the relevant tool or resource, and determining the potential threats and adverse consequences associated with those vulnerabilities (Figure 2).

The second stage in organizing the management process should focus on specifying the relevant objects, describing their vulnerabilities, and identifying potential threats and the consequences of their realization for the organization (Table 6).

The allocation of responsibilities for monitoring and overseeing information security assets across an organization's divisions, or responsibility centers, and among individual managers may depend on a number of factors, including the size of the business, its financial resources,



Source: compiled by the authors based on [Lapina et al., 2024].

Fig. 2. Components of Information Security Risk

Table 6
Information Risk Management Framework

Object	Vulnerability	Threat	Risks
Human resource management			
Personnel with the required competencies	Insufficient qualifications in information technology	Poor digital hygiene; accidental or deliberate disclosure of information to third parties	Reputational; financial
Information risk management			
Software	Origin (foreign or domestic)	Lack of a software license or difficulties in obtaining or renewing one	Information loss; data recovery costs; financial losses caused by business interruption during migration to alternative software (revenue loss, profit loss, fines, penalties)
Technical infrastructure capacity	Insufficient capacity to store large volumes of information	Contractual limits on mandatory long-term storage of large volumes of information in cloud repositories	Loss of access to information that must be retained long term (including HR records)
Electronic documents	Unauthorized access; limited retention periods	Loss of legal validity of electronic signatures when HR and other documents are stored in the cloud on leased services	Loss of access to information intended for long-term retention
Personal, sensitive, and financial information	Insufficient protection against unauthorized access	Theft, falsification, blackmail	Reputational, financial

Source: compiled by the authors.

the specifics of its organizational structure, staffing, and related considerations.

Both historical experience and current business needs suggest that information security, as a component of an economic entity's broader economic security, will remain one of the most urgent tasks in the short term. This is driven by the rapid growth in the volume of information, the migration of key business and social processes to the internet, and the increasing role of information as a valuable asset in both commercial activity and public administration. Information technologies have made it possible for many processes and social interactions to move online, thereby enabling intrusion into individuals' private lives and reshaping the boundaries of personal space. A number of regulations have been developed to govern the handling of corporate and personal information and to prevent unauthorized access, distortion, and fraudulent use. However, these measures are no longer sufficient in view of the rapid development of information technologies and the emergence of innovative technical solutions that make it possible to exploit internet-based information with a digital footprint. To organize effective efforts aimed at minimizing threats and containing potential information risks, an economic entity needs more than legal expertise alone.

Within the management system, the following measures should be prioritized:

1. Objects requiring close attention within the organization's risk management system should be identified, together with their vulnerabilities, potential threats, and the likely consequences of those threats.

2. Powers and responsibilities for monitoring and analyzing events involving the organization's information and employees' personal data should be clearly allocated among divisions and personnel in order to prevent unauthorized access to sensitive and financial information and to personal data.

3. Employees should be regularly informed about current methods of unauthorized access to private and corporate information and should continuously develop the competencies needed to counter such threats. Failure to observe digital hygiene practices increases the likelihood of financial risks not only for the organization but also

for the individual and may also result in administrative liability under Article 13.11 of the Code of Administrative Offenses of the Russian Federation.

The development and continuous improvement of employees' competencies in handling sensitive information and personal data should become an integral part of the organization's human resource management system. This will help ensure that the economic entity operates within the legal framework governing personal data protection, minimize violations of employees' personal boundaries, and reduce risks of various kinds, including financial ones.

References

Borhalenko V.A. (2015). Verification of the pci DSS 3.1 Standard for Compliance with the Requirements of the Legislation of the Russian Federation. *Cyberspace Issues*, 5(13): 11-15. (In Russ.)

Lapina M.A., Medvedeva A.S., Lapin V.G., Boikov N.S., Ledyan D.I. (2024). Information Security Risk Analysis of Economic Information Systems. *Audience*, 2(42). https://.cyberleninka.ru/article/n/analiz-riskov-informatsionnoy-bezopasnosti-ekonomicheskih-informatsionnyh-sistem. (In Russ.)

Larin D.A. (2010). Information Protection in Ancient Russia. *History and Archives*, 12(55): 13-35. (In Russ.)

Savelyev A.I. (2015). Problems of the Application of Legislation on Personal Data in the Era of Big Data. Law. *HSE Journal*, 1: 43-66. (In Russ.)

Selivanova E.S., Konopiy A.S. (2025). Legally Significant Features of Artificial Intelligence and Their Impact on the Legal Status of Decisions Made by Intelligent Systems. *Law and Management. XXI Century*, 21(3): 49-61 (In Russ.)

Tsyplakova A.D. (2025). Countering Cybercrime in Selected Countries of the Global South: Current State, Problems and Prospects. *Law and Management. XXI Century*, 21(3): 62-75. (In Russ.)

Yastrebova A.Yu. (2025). The Concept and Protection of Personal Data in the Context of the International Legal Regulation of the Digital Space. *Law and Management. XXI Century*, 21(2): 15-25. (In Russ.)

Arthur C. (2013). Tech Giants May Be Huge, but Nothing Matches Big Data. *Guardian*, August 23. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data/

Cristea L.M. (2020). Current Security Threats in the National and International Context. *Journal of Accounting and Management Information Systems*, 19(2): 351-378.

Jouini M.A. (2015). Multidimensional Approach towards a Quantitative Assessment of Security Threats. *Procedia Computer Science*, 52: 507-514.

Lee Y.J. (2011). Profit-Maximizing Firm Investments in Customer Information Security. *Decision Support Systems*, 51(4): 904-920.

Sujiwana R.K., Ridho A.F.A., Aryanti D.C., Rakhmawati N.A. (2024). Analisis Bibliometrik Mengenai Serangan Phishing dan Whatsapp menggunakan Vosviewer. *Jurnal Esensi Sistem Informasi dan Sistem Komputer*, 8(1): 101-105.

Van Deursen N., Buchanan W.J., Duff A. (2013). Monitoring Information Security Risks within Health Care. *Computers & Security*, 37: 31-45.

Yaz Ö., Süzen A.A. (2023). Kurumsal Ağlara Yapılan Saldırılarda Açıklanabilir Yapay Zekânın Yeri. *International Conference on Applied Engineering and Natural Sciences*, 1(1): 528-534.

About the Authors

Tatyana A. Rudakova
Cand. Sci. (Econ.), Associate Professor, Department of Economics, Altai State Technical University named after I.I. Polzunov (Barnaul, Russia); Associate Professor, Department of Economic Security, Accounting, Analysis and Audit, Altai State University (Barnaul, Russia). ORCID: 0000-0002-8735-7058.
Research interests: digital finance, economic security, risk management, accounting and analytical aspects of bankruptcy, reliability of accounting and reporting information, risks of the real sector of the economy.
aleks_rudakova@mail.ru

Oksana Yu. Rudakova
Cand. Sci. (Econ.), Associate Professor, Head of the Department of Management, Business Organization and Innovation, Altai State University (Barnaul, Russia). ORCID: 0000-0001-9714-2483.
Research interests: anti-crisis management, change and development management, economic security, management consulting, innovation.
rud-oksana@yandex.ru

作者简介

Tatyana A. Rudakova
经济学博士，副教授，伊·伊·波尔祖诺夫阿尔泰国立技术大学经济学系（巴尔瑙尔，俄罗斯）；副教授，阿尔泰国立大学经济安全、会计、分析与审计系（巴尔瑙尔，俄罗斯）。ORCID: 0000-0002-8735-7058。
研究方向：数字金融、经济安全、风险管理、破产的会计与分析问题、会计报告信息的真实性、实体经济部门风险。
aleks_rudakova@mail.ru

Oksana Yu. Rudakova
经济学博士，副教授，阿尔泰国立大学管理、商业组织与创新系主任（巴尔瑙尔，俄罗斯）。ORCID: 0000-0001-9714-2483。
研究方向：危机管理、变革与发展管理、经济安全、管理咨询、创新。
rud-oksana@yandex.ru

The article was submitted on 10.02.2026; revised on 26.02.2026 and accepted for publication on 28.02.2026. The authors read and approved the final version of the manuscript.
文章于 10.02.2026 提交给编辑。文章于 26.02.2026 已审稿。之后于 28.02.2026 接受发表。作者已经阅读并批准了手稿的最终版本。