

# Informal Methods and Means of Information Protection in Enterprise Information Security

Mikhail Skorev<sup>a</sup>, Irina Kirishchieva<sup>b</sup> and Anna Zhigunova<sup>c</sup>

Rostov State Transport University, Rostovskogo Strelkovogo Polka Narodnogo Opolcheniya Sq. 2, Rostov-on-Don, Russia


**Keywords:** Informal Methods and Tools, Information Security, Information Protection, Information Policy, Confidential Information, Company Personnel, Personal Data.


**Abstract:** The period of active development of information technologies contributes to the emergence of new ways of information theft, which implies the need to protect information. On the one hand, information security methods combine legal, organizational, and technical methods. On the other hand, information security methods and tools can be divided into two areas: hardware and software security (formal) and information security through communication channels (informal). When providing information security by informal methods and means, the organization must comply with the laws related to information security and have its own internal regulations, which will contain internal rules and measures. Regulatory and legal methods involve the implementation of measures to establish the procedure for working with information, tools and determining responsibility for violations of the information security of the enterprise. The legal framework for information security is provided by means at the state level. The regulatory framework for ensuring the information security of the enterprise should be made up of local regulations. In the field of organizational and administrative means of information security, the information policy should be called. The moral and ethical means that ensure information security can be attributed to the system of moral norms or ethical rules that have been formed at the enterprise, observing which it is possible to ensure the protection of information. In the information security system, organizational methods and tools should be used. An important point in information security is working with personnel, including in remote mode, ensuring the security of personal data of employees, suppliers and other agents of the enterprise by appropriate methods and means.


## 1 INTRODUCTION

One of the directions of economic security is information security, which involves the implementation of effective information and analytical support for the production and economic activities of the enterprise. In the Information Security Doctrine of the Russian Federation, the current stage of society's development is characterized by the ever-increasing role of the information environment, which defines strategic goals and main directions in the field of information security (The Doctrine of Information Security of the Russian Federation, 2016). This is due to the fact that the period of active development of information technologies contributes to the emergence of new

ways of information theft, which implies the need to protect information. Special attention should be paid to problems in the management sphere, which leads to the emergence of risks of destructive impact and requires the development of appropriate information security systems (Anisimov et al., 2019). It is no accident that many countries have started to introduce laws on the protection of information (Niyazov, 2020). Currently, such a direction as ensuring the information security of the enterprise is being updated in view of the growing number of violations in this area. To do this, it is necessary to develop new methods and means of information protection that ensure a certain level of information security of the enterprise. At the same time, it should be taken into account that in the modern period there is a new

<sup>a</sup>  <https://orcid.org/0000-0003-3160-9073>

<sup>b</sup>  <https://orcid.org/0000-0001-9179-5432>

<sup>c</sup>  <https://orcid.org/0000-0003-1729-6007>

approach to the information security system, which assumes two main trends in this area: information protection and protection from information (Malyuk).

## 2 RESEARCH METHODOLOGY

The information security system is based on certain methods that can be grouped into groups (Azhmukhamedov, 2012):

- legal, which include legal acts at different levels of management, namely: international, state, local, departmental, intra-company;
- organizational, which are related to the organization of security services, the establishment of information security regimes, licensing, certification of information aspects of activities, training and retraining of personnel dealing with information security issues;
- technical, focused on the use of software and hardware, cryptographic means to protect information, as well as the use of various types of fences and obstacles.

On the other hand, methods and means of information security can be divided into two areas, such as: hardware and software security (formal) and information security through communication channels (informal). At the same time, formal means involve the use of physical, hardware and software, and informal ones are based on the regulatory framework, local regulations and moral and ethical standards.

Without touching on the issues of software, hardware and technical means of information protection, we will focus on informal methods and means in the field of ensuring information security of the enterprise.

## 3 RESULTS

When providing information security by informal methods, the organization must comply with the laws related to information security and have its own internal regulations, which will contain internal rules and measures.

Regulatory and legal methods involve the implementation of measures to establish the procedure for working with information, tools and determining responsibility for violations of the information security of the enterprise. The system of normative legal acts in the field of information

security in the Russian Federation includes acts of federal legislation and certain normative and methodological documents.

The legal framework for information security is provided at the State level. Thus, the protection of information is regulated by the Constitution of the Russian Federation, the Presidential Decree "On approval of the list of confidential information" and the Federal Laws "On Information, Information Technologies and Information Protection" (Federal Law No. 149-FZ), "On Commercial Secrets" (Federal Law No. 98-FZ), " On personal data (Federal Law No. 152-FZ).

The regulatory framework for ensuring the information security of the enterprise should be the following local regulations:

- Regulations on the use and storage of personal data;
- General Information Security Regulations;
- Information Security Policy;
- Safety regulations;
- Information Privacy Statement;
- Regulation on the use of e-mail;
- Regulations on the use of media;
- Regulations on the use of the Internet;
- Regulations on the use of the software;
- Order on the introduction of the information security policy;
- Regulations on internal labor regulations, etc.

Means of administrative (organizational) measures are crucial in the formation of a reliable shield in the protection of information, since the possibility of unauthorized access to confidential information is largely determined not by technical issues, but by the actions of the company's personnel.

Organizational methods should be aimed primarily at solving such issues as:

- promising areas of work with personnel and their work with information of various types;
- determining the location and placement of corporate network objects;
- implementation of measures to ensure fire and physical protection;
- implementation of control measures in terms of ensuring information security in all areas of the company's activities;
- assigning personal responsibility for the implementation of protective measures.

The main means of information security when using organizational methods can be attributed to:

- organizational measures of a security and security nature;
- organizational measures implemented in terms of the use of technical means that ensure the

collection, processing, accumulation and storage of confidential information;

- organizational measures for the formation, use, accounting, storage, destruction of both documents and confidential information carriers.

In the field of organizational and administrative means of information security, an information policy should be called, which provides a list of information and documents that should be familiarized with the employees of the enterprise, it also sets out the methods and time frames for submitting information and documents. The objectives of the information policy are:

- formalization of the information sphere of the enterprise, focused on the movement of intra-company objective and reliable information;
- formation of the principles of working with information in the enterprise.
- maximum satisfaction of information requests of persons involved in the company's activities;
- protection in terms of unauthorized access to information containing confidential information.

The information policy of the enterprise should be based on the following principles:

- regular and timely submission of information, which is assumed by the current legislation;
- completeness, reliability, and objectivity of the information provided;
- immediate reflection of changes occurring in the enterprise that make previously disclosed information inaccurate or inconsistent;
- the unity of the rights of all persons involved in the company's activities to access non-confidential information;
- ensuring compliance between the transparency of the company's activities and its interests in the provision of information;
- security of confidential official or commercial information, as well as control over its use and dissemination.

The moral and ethical means that ensure information security can be attributed to the system of moral norms or ethical rules that have been formed at the enterprise, observing which it is possible to ensure the protection of information. These standards do not belong to the category of mandatory, as is typical for legally approved standards, while non-compliance with them affects the reduction of the level of authority of the employee.

The personnel plays an important role in the administrative and organizational support of the information security of the enterprise. Depending on

the level of access to confidential information, employees of the organization may have information about:

- other employees of the enterprise;
- about the organization's partners: intermediaries, suppliers, buyers, advertising agencies, etc.
- about the employees of state institutions that the organization contacts: tax authorities, municipal law enforcement agencies, etc.
- about the production process;
- about the internal regulations of the organization, etc.
- from the financial and other statements of the company;
- about internal security models;
- about development plans, forecasting;
- contained in the internal audit documents of the organization;
- about payment documents and data on economic indicators;
- about the scope of work, the size of deliveries, contractual terms;
- located in the client database;
- about the technologies used in production;
- about the information security system, etc.

Therefore, an important point in ensuring information security is working with staff, which includes: working with a potential employee during an interview, collecting information and monitoring an employee at the time of his stay in the organization and working with an employee when he is dismissed. Interaction with a potential employee when applying for a job includes conducting an interview to identify the necessary qualities of the applicant, checking skills, conducting testing, etc.

Ways to work with employees who own confidential information of the organization include:

- employee training;
- conducting training sessions;
- control over the performance of the employee's duties related to the protection of information;
- conducting research related to the degree of awareness of employees in the field of confidential work;
- conducting internal investigations in the event of a threat of information leakage and identification of violators.

An important organizational task in working with employees of the organization related to confidential information is to create the right psychological climate in the team.

It is advisable to use the following methods of work for employees who use documents that represent a trade secret:

- create instructions for using and working with protected information;
- appointment of persons responsible for office work;
- strict supervision of employees who have access to confidential documentation;
- obtaining written consent from employees for non-disclosure of commercial information;
- application of technologies for the protection of confidential information;
- administrative control over the security of the use of information in their confidential documentation.

One of the tools when working with employees who have access to confidential information should be a comprehensive work with the staff. When there is a need for a new employee for a position that involves working with confidential information, it is advisable to adhere to the following admission technology.

The most widely used way to protect the business information of an enterprise is to enter into a non-disclosure agreement on the organization's trade secrets. Such an agreement must be signed with all employees who, in the course of their work, begin to possess secret information and confidential information about the company. To regulate such relations related to the use of confidential information in the company, first of all, the main document of the organization – the Charter, which discloses the concept of commercial secrets and establishes responsibility for its violation.

A threat to the information security of an enterprise can also be the dismissal of an employee who had access to confidential data. After dismissal, the employee no longer has obligations to the organization, which may encourage him to disclose valuable information to competitors. In order to reduce the risk of such consequences, the company's management should inform employees about the prohibition of using any information obtained at the workplace in their own interests or in the interests of third parties. In order to protect the company from the possible consequences of such actions, the employee must sign a non-disclosure of confidential information (trade secrets) after his dismissal. If an employee violates this agreement, all losses incurred by the company as a result of illegal actions can be recovered in court.

Another tool aimed at maintaining a high level of the company's confidential data protection system is

the need to actively engage in training, placement, promotion, and stimulation of employees, regularly instruct them about the rules for working with confidential information, inform them about the need to comply with all these rules and about responsibility in case of violation.

An important aspect in the present time is the transition of the company's employees to remote work. In this regard, a particularly important aspect is the formation of ways of information security of employees in this mode of their work. To ensure the information security of employees when working remotely, the company must develop and prepare a document that will display brief information for employees that will help them protect themselves directly at their workplace. The list of aspects that should be specified in this document includes:

- how to protect the devices with which the employee works with antivirus software;
- pay special attention to the importance of updates to programs and the operating system on the employee's computer, since applications and operating systems are constantly finding vulnerabilities through which an attacker can steal any employee information; updates are often used to monitor and fix problems that arise;
- how to set up Wi-Fi encryption so that attackers do not intercept the data that an employee enters over the Internet, for example, about passwords in the system for remote access or corporate email credentials;
- emphasize the importance of changing the username and password from the router, since many employees may have it by default, and this can be used by attackers when compiling the code of viruses and malware;
- an explanation for the employee that in coworking areas or other public places, you should work especially carefully, so that unscrupulous people surrounding the employee in public places can not track his information through public Wi-Fi;
- pay special attention to blocking the device when an employee leaves the workplace, so that no unauthorized persons see various corporate information, or accidentally delete important data;
- the importance of using only corporate mail or corporate messengers, since all the information sent through them can be intercepted by an attacker and used for their own purposes;
- configuring the employee's firewall system to monitor incoming and outgoing traffic when

exchanging data between the local and corporate networks; when monitoring traffic, an assessment is made in accordance with the security system, as a result of which a decision is made to allow or block traffic;

- familiarizing employees with the possibility of threats via email through email phishing (you can conduct a test mailing of such messages in order to show employees what they can expect and analyze in detail the errors that occur in this case).

At the enterprise it is necessary to adhere to clear methods of information protection when performing remote work and in this case it is possible to use such methods as:

- instructing the company's employees about possible threats and the rules of protection against them, by familiarizing them with the developed document on information security in remote work;
- use of its own remote access and data storage facilities, such as internal cloud storage, to provide the company with the tools to control and protect all data;
- use of connection to workplaces to protect both employees and the company from unauthorized access by third parties as much as possible;
- development and implementation of a secure digital space for employees with built-in information security tools;
- the most optimal resource, however, and financially costly will be to provide all employees working on remote access with portable mobile computing equipment (laptops), on which antivirus and corporate software will be installed in advance; this will help to increase the protection of corporate information several times and ensure safe operation;
- for employees who interact with critical and confidential information, allocate a separate domain to monitor and respond to security threats promptly, preventing information and data from leaking to third parties.;
- ensuring continuous monitoring of the security of objects of confidential information, as well as maintaining logs of the actions of employees interacting with this information;
- ensuring the possibility of rapid response of the security service and taking measures to protect information in the event of computer threats and attacks by intruders;

- geolocation tracking to prevent unauthorized entry of an employee in time, for example, from another point of the earth;
- if an employee logs in from a personal device, then enter it in the database of trusted devices to clearly see the "alien" and unregistered machine in the system;
- tracking "simultaneous" connections under the same account; these anomalies can help the company detect unauthorized access to the system of third parties and take timely measures to eliminate them;
- tracking attempts to connect to the system from compromised hosting sites, fake addresses; timely disconnection of user data from the network will help the company protect itself from data theft and infection of the system with malicious software and viruses.

A fairly common and dangerous problem in remote work is phishing, due not only to its successful technical component, but also to its effective psychological component, since phishing allows you to bypass the most advanced defense systems, affecting the basic emotions of people thanks to social engineering. That is why it is especially important for the company not only to tell employees about the harm caused by phishing, but also to work out with them the skills of safe behavior with the help of developed systems that simulate real attacks. Responsible employees should regularly conduct training sessions with the staff to develop skills for safe work with remote connection. It is important to practice phishing situations, as many techniques have a sophisticated impact, sometimes not discernible even by experienced cybersecurity specialists. The fundamental task for the company will be to develop the skills of employees' behavior in conditions close to real phishing attacks, simulating the actions of intruders.

A necessary measure for ensuring information security at remote work in the company is to create a system for protecting not only data about the business processes of the enterprise, but also personal data of both employees and suppliers.

The company should take certain measures to ensure the security of personal data, namely:

- identify threats to the security of personal data in the process of working with them in the information systems of the enterprise;
- use technical and organizational means to ensure the security of personal data;
- evaluate the effectiveness of methods and means of ensuring information security in terms of personal data;

- keep records of all personal data carriers;
- create a system for detecting unauthorized access to personal data;
- create a system for restoring personal data that was violated as a result of unauthorized access;
- determine the mechanisms of access to personal data;
- create a system of control measures for actions to ensure the security of personal data.

## 4 DISCUSSION

All means of administrative and organizational measures are aimed at creating a well-functioning system that ensures information security and monitoring this system. Organizational methods should be used not only to ensure the protection of information, but also to be implemented at all objects of the corporate network, which gives a significant positive effect and reduces the number of external and internal threats.

The staff of the enterprise, performing their work, has to some extent confidential information. No technical and software tools will ensure the protection of information from the human factor. The level of employees' ownership of confidential information depends on the specifics of their work responsibilities and the level of access to this information. Therefore, employees of the organization are one of the sources of information leakage, which leads to financial losses of the organization, which involves the development of information security tools when working with employees. An important means of information protection is limited access to confidential information, so that only the information that they need to perform their professional activities is available to employees, as well as working with staff in the process of hiring and firing from the enterprise.

A particularly important aspect in the modern period is the transition to remote work. Ensuring the information security of employees when working remotely the company is provided with the development of a document that should reflect the main ways of working with a remote connection, as well as the main tasks of the employee to ensure personal information security at the home workplace.

When processing personal data, the company must be based on legal, technical and organizational means of protecting information from unauthorized access, from the dissemination, destruction and modification of data, as well as from other illegal actions that pose a threat to the personal data of

employees, suppliers and other agents of the company.

## 5 CONCLUSIONS

Thus, as a result of the implementation of the proposed methods and methods for ensuring information security of the enterprise, a decrease is expected:

- the probability of information theft;
- the probability of intentional and unintentional misrepresentation and damage to the company's information;
- the probability of unauthorized access to information resources;
- leaks of information to competitors;
- hardware failure and failure;
- the probability of errors by users and IT specialists that can adversely affect the information.

At the same time, it will increase:

- the level of control over information security at all levels of the enterprise hierarchy;
- level of information security risk management;
- efficiency of the employee identification process;
- the effectiveness of the use of information security tools.

## REFERENCES

- Anisimov, V.G., Anisimov, E.G., Saurenko, T.N. and Zotova, E.A. (2019). Models of forecasting destructive influence risks for information processes in management systems. *Information and control systems*, 5 (102): 18–23.
- Azhmukhamedov, I. M. (2012). *Solving problems of ensuring information security on the basis of system analysis and fuzzy cognitive modeling: monograph*, Astrakhan, 344 p.
- Decree of the President of the Russian Federation of 06.03.1997 No. 188 (ed. of 13.07.2015) «On Approval of the List of Confidential Information» [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_13532/942772dce30cfa36b671bcf19ca928e4d698a928/](http://www.consultant.ru/document/cons_doc_LAW_13532/942772dce30cfa36b671bcf19ca928e4d698a928/).
- Federal Law No. 149-FZ of 27.07.2006 (latest version) «On Information, Information Technologies and Information Protection» [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/).
- Federal Law No. 152-FZ of 27.07.2006 (latest version) «On Personal

- Data»[http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/).
- Federal Law No. 98-FZ of 29.07.2004 «On Commercial Secrets "(last revision)  
[http://www.consultant.ru/document/cons\\_doc\\_LAW\\_48699/](http://www.consultant.ru/document/cons_doc_LAW_48699/).
- Malyuk, A. A. *On the issue of the intensification of information security processes*.
- Niyazov, Kh. (2020). Legal basis of information security: comparative approach. *History questions*, 3: 107–113.
- The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993 with amendments approved during the all-Russian vote on 01.07.2020)  
[http://www.consultant.ru/document/cons\\_doc\\_LAW\\_28399/](http://www.consultant.ru/document/cons_doc_LAW_28399/).
- The Doctrine of Information Security of the Russian Federation. Approved by the Decree of the President of the Russian Federation of 5.12.2016 No. 646.  
<https://www.garant.ru/products/ipo/prime/doc/71456224/>

