



# Information Security in the System of Economic Security of Companies

Tatiana O. Grafova<sup>1,2</sup><sup>a</sup>, Irina R. Kirishchieva<sup>1</sup><sup>b</sup> and Ekaterina V. Gomeleva<sup>1</sup><sup>c</sup>

<sup>1</sup>Rostov State Transport University, Rostov-on-Don, Russia

<sup>2</sup>Rostov Branch of Russian Customs Academy, Rostov-on-Don, Russia

**Keywords:** Information Security, Economic Security, Threats, Risks, External and Internal Factors, Information Policy, Confidential Information.

**Abstract:** One of the areas of economic security is information security, which implies the implementation of effective information and analytical support for the economic activities of the enterprise. Now, more than ever, it is relevant to ensure the information security of companies, since every year the growth of information security violations is increasing exponentially. In the age of information technology and the daily development of new methods of stealing information, it is necessary to pay full attention to the issue of protecting information of commercial enterprises. To do this, it is necessary to clearly define the legal norms for the protection of secrets, as well as a system of control over the protection of commercial secrets and its nondisclosure.

## 1 INTRODUCTION


Currently, serious attention is paid to the effective provision of information security in the system of economic security of the enterprise. Since with the progress in the field of information technology and the complete informatization of all processes in the enterprise, it is more and more difficult to ensure the integrity, availability and confidentiality of information. Information technologies are being updated at a very fast pace, and similarly, there is an increase in the number of all kinds of threats aimed at information resources. Every enterprise is in an information environment and any of its areas is subject to information security threats, which always entail financial losses. That is, any threat to information security affects not only the information environment of an enterprise, but also economic security. In order to smoothly implement effective information security in the economic security system, enterprises need to regularly update and improve information security methods and tools.


The company's information security system is based on certain methods that can be combined into groups:


- legal regulation of information security in the system of economic security of the enterprise;
- factorial influence on information security at the enterprise, with the identification of external and internal threats, their prevention and suppression based on tools and methods;
- analysis of information security in the system of economic security in the company, and interpretation of the result obtained in terms of the levels of protection of the information environment in the company.

Research results.

An important element in information security (IS) of an enterprise is legal regulation. It defines the procedures and regulations for storing information on paper and electronic media in the organization, indicates the ownership of legal entities to certain data. Ensuring the safety of trade secrets is an important criterion for ensuring both information security and economic security. In order to prevent the threat of information leakage from the organization from employees, and the receipt of

<sup>a</sup> <https://orcid.org/0000-0002-4646-0155>

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

<sup>c</sup> <https://orcid.org/0000-0003-1061-7904>

information by third parties, when drawing up an employment contract, the clause "On nondisclosure of commercial secrets" is prescribed. The employment contract is drawn up in accordance with the Labor Code of the Russian Federation of December 30, 2001 No. 197-FZ (as amended on July 31, 2020) (as amended and supplemented, entered into force on August 13, 2020). The list of all norms for the lawful drafting of an employment contract is spelled out by the Labor Code of the Russian Federation, article 57 "Content of an employment contract." According to the Labor Code of the Russian Federation, article 88 "Transfer of personal data of an employee", an employer does not have the right to disclose personal data of an employee without his written consent, with the exception cases stipulated by this Code or other federal laws (Labor Code of the Russian Federation of December 30, 2001 No. 197-FZ). Protection of personal data of employees of the organization is part of ensuring information security. Personal data, including data about the private life of an employee, covers all the information necessary for an employer to formalize an employment relationship, change it and terminate it. This information includes the information contained in the documents that the employee, according to the Labor Code of the Russian Federation of 12/30/2001 No. 197-FZ (as amended on 07/31/2020) (as amended and supplemented, entered into force on 08/13/2020) when applying for a job (Labor Code of the Russian Federation of December 30, 2001 No. 197-FZ). It is also information that is generated by the employer during the entire employment of the employee and then stored by him after the termination of the employment relationship with the employee. Every employee needs to feel safe working in the organization in order to perform effectively.

Also, each organization has its own local regulations, which enshrine internal principles and rules for ensuring information security, such as: the rules for building an information protection system, which includes: rules for setting up logins, passwords on the PC of the organization's employees, the rules for identifying each employee, access control rules, etc. Each organization has its own effective ways of identifying the elimination of breakdowns and vulnerabilities of the information security system, elimination of the consequences after committed hacks, regulations for the preparation of reports and documentation on the state of it systems. Within the organization, regulations are being developed to ensure the protection of information security (Golubchikov, 2017). The organization can conduct

conversations with employees of the organization and the correct use of certain measures to protect information, the importance of this protection.

Information exists in all areas of the organization, forming an information space. It includes information about production, technical support, as well as economic, organizational information, information about the methods of carrying out professional activities that have actual or potential commercial value due to their unknown to third parties, as well as information related to banking operations and accounts. , all confidential information owned by accounting, legal, financial departments and many other information. Since this information carries a very large amount of confidential and compromising information, this information must be protected. This is the primary goal of an organization's information security.

Information security (IS) of an enterprise is the state of security of the information environment of an enterprise, which ensures its safe operation and development. Information security is part of economic security. Any enterprise is aimed at obtaining more profit, and in order to achieve economic benefits, it is necessary to ensure, among other things, the protection, integrity and completeness of information, both within the organization and externally. The goal of information security is to ensure the three most important security criteria: confidentiality, integrity and availability.

Confidentiality is a guarantee that information can be read and interpreted only by those people and processes that are authorized to do so. Confidentiality includes procedures and measures to prevent unauthorized users from disclosing information. Ensuring protection against possible threats to the information security of an enterprise requires making effective decisions related to identifying, taking into account and finding ways to prevent the identified threats. Information security threats lead to leakage of confidential information, which in turn leads to negative consequences affecting the economic security of the organization (Sannikova, 2017).

Integrity is a guarantee of the existence of information in its original form. Integrity can be static (immutability of information objects) and dynamic (concrete execution of complex actions).

Dynamic integrity is used, in particular, when analyzing the flow of financial messages in order to detect theft, reordering or duplication of individual messages. Integrity turns out to be the most important aspect of information security in cases where information serves as a "guide to action."

Availability - the ability for automated employees of an organization to quickly and easily get the information they need. Information security threats are potentially possible events, processes and actions that can harm information and computer systems.

By the location of the source of information security threats, they can be divided into internal and external.

Internal threats to information security - threats that have arisen within the organization and are detrimental to information security.

External threats to information security - threats that have arisen outside the organization, such as: information theft by competitors. Revenge for the dismissal of an employee, etc.

There are natural and artificial threats to information security at the enterprise:

- artificial threats - threats that have arisen directly from a person and are divided into intentional and unintentional. The former are created on purpose (attacks by malefactors), the latter arise directly from ignorance, negligence, inattention;

- natural threats are natural phenomena that do not depend on humans (fires, hurricanes, floods, etc.);

All possible classifications of information security threats affecting an enterprise can be divided into such subgroups as:

- unwanted content is programs and spam that can harm information, are created to destroy and steal information, as well as sites prohibited by law, unwanted sites;

- unauthorized access is the viewing of information by a person (employee) who does not have permission to use this information. This threat is aimed at information leakage, which can be organized in different ways: attacks on sites, hacking programs, intercepting data on the network;

- information leakage - the receipt of confidential information without the right, which is important for the organization and its employees. Leaks can be intentional or accidental;

- data loss - with this threat, information can be lost due to damage, deletion and loss of data. Loss of data can occur as a result of a violation of the integrity of information and equipment malfunction;

- fraud - the threat of illegal use of information technology. This threat contains many methods: carding, phishing, social engineering scamming, etc.;

- natural disasters - floods, tsunamis and any other natural disasters.

All of the above types of threats affect not only information security, but also the economic security of an organization. Since with hardware and software errors of the anti-virus system (problems associated

with the installation of the anti-virus system), unintentional actions leading to partial or complete system failure or destruction of hardware, software, information resources of the system (unintentional damage to equipment, deletion, distortion of files with important information or programs), a leak or loss of economically important information related to the activities of the organization can occur, which in the future can lead to a decrease in the organization's revenue and / or to an increase in unforeseen expenses. Such consequences can also be caused by unintentional damage to information carriers, sending data to an erroneous device address.

Much attention should be paid to the threat associated with deliberate action or inaction of a person. This threat can target the confidentiality of information, software or media. This can be: the introduction of agents into the number of system personnel, recruitment (by bribery, blackmail, etc.) of personnel or individual users with certain powers, the threat of unauthorized copying of secret data by the software user, disclosure, transfer or loss of access control attributes ( passwords, encryption keys, identification cards, passes, etc.). This type of threat can lead to the acquisition of confidential information constituting a trade secret by competing organizations and to the use of information for their own selfish purposes. This can lead to:

- to a decrease in the competitiveness of the organization, which will lead to a decrease in profits;
- to the outflow of partners and clients of the organization. If competitors have got hold of the data of customers and partners and the terms of cooperation with them, then the competing organization can offer them more favorable conditions for the transaction and entice them to themselves. In this case, the organization will lose part of the profit, which will affect economic security;

- in case of theft and disclosure of compromising data, the organization can spoil its image and lose competitiveness, which will also lead to a decrease in profits and affect economic security. Also, in case of theft or leakage of confidential compromising data, a competing organization can carry out blackmail to obtain its benefits. Information security at the enterprise is a special system that is aimed at identifying, eliminating and eliminating the consequences of information security threats. Any organization in the modern world is rapidly developing and multiplying its information environment. And it is very important to take the correct and appropriate measures to protect it, since the information environment of any organization is valuable, and its leakage or loss can lead to loss of

profit for the organization. Information security threats have a different nature of origin, they can be internal, external, passive, active, intentional and unintentional, natural and artificial.

The main task of information security at an enterprise is to ensure the information environment, first of all, confidentiality, integrity and availability (Litvintseva and Karelin, 2020). To ensure information security, organizations develop and use an information security model, which should include a set of relevant internal and external factors and their impact on the state of information security at the facility and the safety of information resources.

The information security model shows that the owner of information, in an effort to save the resource and reduce the risk of information security, applies countermeasures, vulnerabilities, which depend on the impact of threats. Information security threats are created by violators, and as a result, risks arise that incur losses for the resource. To ensure an effective information security system, methods and tools used for protection are being developed.

Information security methods and tools can be divided into two areas, such as hardware and software security (formal) and information security through communication channels (informal).

Instruments of informal methods of information protection are normative (legislative), administrative, organizational acts and moral and ethical standards, which include: documents, rules, activities enshrined in the organization (Malyuk, 2016).

In the meantime, there is no need to worry about it. In order to effectively and expediently use information security methods and tools, an organization must have the ability to make optimal organizational and management decisions in the field of information security. Also be able to apply the basic laws of creation and principles of functioning of systems of economic security and information security, be able to collect, analyze, systematize, evaluate and interpret the data necessary to solve professional problems related to information security.

One of the important manifestations of the influence of information security tools and methods on the economic security of an organization is the financial component. Any information security planning requires an expense from the organization.

Organizational costs can be divided into capital and operating costs.

Capital expenditures include: costs of network and telecommunications equipment, system and hardware, software, buildings and premises required to ensure information security.

Operating costs are current costs and include: personnel costs, telecommunications costs and other expenses.

Analysis of information security risks in an enterprise is a complex process, since it is not always possible to give an accurate cost estimate of an information asset of an enterprise and to determine the degree of vulnerability of an asset. The essence of risk management at an enterprise is to assess the size of risks, formulate effective and cost-effective measures to reduce risks, check whether the values of risks are within an acceptable framework (Chichkanov et al., 2020).

The first stage is the collection and processing of information related to risks. This stage can be called preparation for an information security risk assessment, which includes:

- definition of the area in which the risk is investigated;
- identification of valuable information assets;
- further assets are grouped by category;
- identification of all possible threats to information security that can damage the information of the enterprise and affect its economic security;
- the probability of the onset of information security threats is determined;
- determination of the level of damage.

Next, a risk assessment is carried out, which includes risk analysis and risk assessment.

At the initial stage, the risk is assigned a qualitative probability score from 1 to 5 and a score is given using the matrix. Let's consider the main risks of information security in the company and give them an assessment, including the likelihood and scale of costs using the matrix.

Risks ranging from 1 to 5 are low. With an indicator of 6-10, they have an average degree of damage. If the indicator is from 11 to 15, then the risk is already considered high, and if the indicator is more than 15, then the risk belongs to extremely high risks.

The risk of confidential information leakage is frequent, since all employees of the enterprise have confidential information to one degree or another and can pose a threat to information security, but at different scales of valuation, the classification of risk according to the degree of consequences will be different. So, in the event of a leak of information related to the salary of a full-time employee, the risk will be considered low, and in the event of a leak of information related to a business strategy or a trade secret, the risk will already be high.

Using this matrix, it is possible to correlate the impact of information security risks on economic security, since, depending on the value of the asset,

the damage caused to the enterprise increases or decreases, which can be measured in value terms. The stronger the consequences of the information security risk, the more financial costs the company will spend on risk prevention and recovery after the onset of the consequences. Further, each information asset from the compiled list is assessed according to the criteria of the enterprise. In a company, such criteria may be, for example, the initial cost of an asset, the cost of its renewal.

So the value of the asset will be determined using a qualitative assessment, which includes a gradation: low cost, average cost and high cost. Where low cost is such a cost at which the initial cost of an asset is minimal, when updating this asset, the costs will be minimal. The average cost of an asset will include: a low initial cost and the difficulty of updating or restoring it. The high value of the asset will include a medium to high level of investment for acquisition or formation and

high level of costs for restoration or renewal of an asset.

After each group of assets has been assigned a quality rating, the degree of risk vulnerability is considered.

Risks by degree of vulnerability are divided into:

- low level - risk vulnerability, in which it is possible to collect a critically low amount of information about the system;

- medium level - risk vulnerability at which you can get an average level of information, but it is probably enough to access confidential information;

- high level - risk vulnerability, in which it is possible with a high probability to gain access to confidential information. A risk assessment is compiled separately for each information asset in order to analyze the vulnerability locally at each site and assess the degree of protection of the asset.

With the help of these measures, the entire information security system is analyzed, the degree of its security is determined and reports are generated for further planning the information security concept. The assessment of the level of information security protection is determined by comparing the current strategy with the information security standards in accordance with GOST R 52069.0-2013 "Information Security. System of standards. Basic provisions" (Fundamentals of the legislation of the Russian Federation on notaries - approved by the RF Armed Forces on 11.02.1993).

After risk assessment, risk processing takes place, which includes an analysis of possible risk management measures, the selection of optimal risk

treatment measures and the implementation of these measures.

Further, after processing the risk and taking measures to manage it, the next stage takes place - monitoring and adjustment. At this stage, the results of risk management are monitored and, if the desired effect is not obtained, the control measures are adjusted (Grafova et al., 2019). After that, specialists from the information security department generate a report, which indicates the analysis and assessment of information security risks, indicates a step-by-step process for eliminating the risk and risk management tools. Based on the risk assessment, a full analysis and risk-oriented assessment of the entire information security system is carried out, which checks how information protection works, how the risk is assessed, and how appropriate is information security risk management (Kubasova, Tkach and Tsvigun, 2019). A full assessment of the entire work of the information protection department is given and a corresponding report is drawn up on the work done.

Reporting, formed on the basis of a risk-based assessment of information security, is used to develop further planning of the concept of information security, which is included in the concept of planning to ensure the economic security of an enterprise.

## 2 THE DISCUSSION OF THE RESULTS

Legal regulation is a very important aspect in ensuring information security, as part of the economic security of an organization. Laws protect information from both the employer and the employee of the organization. They regulate the external and internal relationships of the organization associated with the information space. Also, the organization's local regulations help to build the correct internal information protection, regulate the ways to identify and eliminate threats related to information security, reporting and documentation on the state of the organization's IT systems and further analysis of information security. Only a combination of legislative acts and internal regulations of the organization will contribute to ensuring the confidentiality, integrity and truthfulness of information and ensure the information security of the organization (Andreeva et al., 2017). Any security system is not ideal and you always need to work on improving it. Even using a number of effective measures, an organization cannot guarantee the complete security of its information environment and,

as a result, its economic security. Any threat to information security has a detrimental effect on the economic security of the organization: it leads to a decrease in the productivity of the organization, the outflow of customers and partners, the outflow of employees, incurs additional unforeseen costs, damages the reputation and image of the organization and leads to a decrease in profits. Over time, more and more new types of information security threats appear, but the introduction of new measures to eliminate them is also being developed continuously and uninterruptedly. Any organization, regardless of its field of activity, must pay enough attention to information security, since every organization has confidential information, disclosure, which can lead to harm for the organization itself, for its employees, customers and partners. This is a whole complex of measures that includes all aspects of information protection, the creation and maintenance of which must be approached most carefully and seriously. The principles and tools that the organization uses should be effective and appropriate. Information security measures in the enterprise must be developed, updated and implemented constantly, regardless of the role of the IT infrastructure in production processes.

### 3 CONCLUSION

Information security risks have a direct impact on the economic security of the enterprise, since costs are required to identify, analyze, prevent and eliminate them. Also, the occurrence of risk entails the likelihood of lost profits and the likelihood of unforeseen expenses. In order to determine how much the information security risk caused damage to the enterprise, it is necessary to analyze the risk assessment of the information security of the enterprise.

The stronger the consequences of the information security risk, the more financial costs the company will spend on risk prevention and recovery after the onset of the consequences. And in order to determine how appropriate the investments spent in the information security department are, it is necessary to assess the level of information security, based on the analysis and assessment of risks.

Every enterprise is in an information environment and any of its areas is subject to information security threats, which always entail financial losses. That is, any threat to information security affects not only the information security of an enterprise, but also economic security. That is why it is necessary to

develop models for analyzing information security risks, as well as create algorithms and methods for their analysis in order to create decision support systems for managing the information security of a company.

## REFERENCES

- Labor Code of the Russian Federation of December 30, 2001 No. 197-FZ (as revised on July 31, 2020) (as amended and supplemented, entered into force on August 13, 2020): Access from the legal reference system "Consultant Plus".
- Golubchikov, S.V. Novikov, V.K. and Baranova, A.V. (2017). Levels and legal model of information security (information protection).
- Sannikova, I.N. (2017). Topical issues of the economic security of the organization.
- Litvintseva, G. P. and Karelin, I. N. (2020). *Terra Economicus*, 18 (3): 53-71
- Malyuk, A.A. (2016). Information security: conceptual and methodological foundations of information security - M.: GLT, 280 p.
- Chichkanov, V.P., Belyaevskaya-Plotnik L.A. and Andreeva P.A. (2020). *Economy of the region*, 16(1): 1-13
- Fundamentals of the legislation of the Russian Federation on notaries (approved by the RF Armed Forces on 11.02.1993 No. 4462-1) (as amended on 27.12.2019) (as amended and supplemented, entered into force on 11.05.2020). Access from the reference legal system "Consultant Plus".
- Grafova, T.O., Tishchenko, I.A., Mishchenko, O., Kirishchieva, I.R., Kirishchieva, V.I. (2019). Basis of financial and management accounting formation within a concession company. *Advances in economics, business and management research. Proceedings of the Volgograd State University International Scientific Conference "Competitive, Sustainable and Safe Development of the Regional Economy" (CSSDRE 2019)*, pages 300-304.
- Kubasova, T., Tkach, V., Tsvigun, I. (2018). Priorities of the logistics risks management in the resource support of construction projects. *MATEC Web of Conferences. conference proceedings*, 08010.
- Andreeva, L.Yu., Skorev, M.M., Grafova, T.O. and Kirishchieva, I.R. (2017). Tools of financial management of reputational risks. *European Research Studies Journal*, 20(3B): 280-299