Prerequisites for Improving Information Security of the Enterprise

Mikhail Skorev[a], Nikolay Shevkunov[b] and Anna Zhigunova[c]
Rostov State Transport University, Rostovskogo Strelkovogo Polka Narodnogo Opolcheniya Sq. 2, Rostov-on-Don, Russia

Keywords: Information Security, Optimization Methods, Information Security Criteria, Information Protection, Vulnerabilities, Information Security Strategy.

Abstract: This article deals with the issues of protecting the economic interests of the enterprise, which in modern conditions are not given enough attention, which confronts organizations with the need to adopt new approaches to ensuring their own information, and, as a result, economic security. The economic security of the enterprise is considered, first of all, as a problem of information protection. That is why the information component of economic security plays a special role in organizations. The information component in the organization is the basis of the entire workflow, and the effectiveness of management, in general, depends on the collection, processing and transmission of information, as well as the quality of management decisions. The development of information technologies and the complete informatization of all processes in the enterprise determine the increasing complexity of ensuring the integrity, availability and confidentiality of information. Information technologies are being updated at a very rapid pace, and similarly, there is an increase in the number of various threats aimed at information resources, the main of which will be discussed below.

1 INTRODUCTION

Each enterprise is located in an information environment and any of its areas is subject to threats to information security, which always entail financial losses. That is, any threat to information security affects not only the information environment of the enterprise, but also economic security. In order to continuously implement effective information security in the economic security system, enterprises need to regularly update and improve information security methods and tools (Müller and Ulrich, 2013). Based on the general analysis of the level of information security in the enterprise, it can be concluded that the methods used to ensure information security provide a certain level of information protection, but require additional refinement and improvement. An improved security system should ensure the protection of information from possible threats relevant to the enterprise in question: blocking the channels of information leakage, preventing distortion or damage to information, strengthening the serviceability of the technical means on which the information is located and allowing employees to freely perform their work duties (Zhigunova, 2016). An improved information security system should provide maximum protection against threats related to information that may harm the economic security of the enterprise, while minimizing the cost of its development, implementation and maintenance.

2 RESEARCH METHODOLOGY

The practice of building information security systems has shown that an integrated approach to information protection involves the simultaneous use of legal, organizational, and software-technical measures that allow you to block all possible directions for the implementation of threats, both external and internal, when using information security tools.

As a result, when operating information security tools, they are used in practice:

[a] https://orcid.org/0000-0003-3160-9073
[b] https://orcid.org/0000-0001-9251-7442
[c] https://orcid.org/0000-0003-1729-6007

Skorev, M., Shevkunov, N. and Zhigunova, A.
Prerequisites for Improving Information Security of the Enterprise.
DOI: 10.5220/0010616900003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 29-34
ISBN: 978-989-758-531-9; ISSN: 2184-9862

- legal methods;
- organizational methods;
- engineering and technical methods;
- technical methods;
- hardware and software methods.

The methodology for ensuring information security within the framework of economic security should be provided by:

- risk reduction;
- formation of a timely and adequate response to threats of the external and internal order;
- assessment of possible consequences of external and internal threats;
- creating a system for eliminating possible negative consequences.

Building a functional system that combines a set of information security tools using different methods of ensuring information security can be used to prevent and prevent early threats that can cause both economic harm to the organization and face cybercriminals whose main goal is to gain access to the company's commercial information and confidential data of its customers.

Improving the chain of management decisions, based on the use of modern methods for evaluating the effectiveness of information resources, such as the analysis of the goal tree and expert assessment of bottlenecks, will allow the company to identify the weakest structural divisions, thereby developing measures to improve their activities.

And in the end, the improvement of the management and control system, which implies the organization of a real-time control system, as well as the tightening of the rules and regulations for the technical support of structural divisions working with information resources, will lead to an increase in the quality of the control system on the part of the management.

3 RESULTS

When analyzing the level of information security at the enterprise, a number of vulnerabilities related to administrative, organizational, software and technical support for information protection were identified.

At the administrative level, the main prerequisites for improving information security in the system of economic security of the enterprise are associated with weak control over potential and current employees of the enterprise and with outdated regulations related to information security of the enterprise.

At the administrative level of information security, the vulnerabilities presented in Figure 1 are identified.

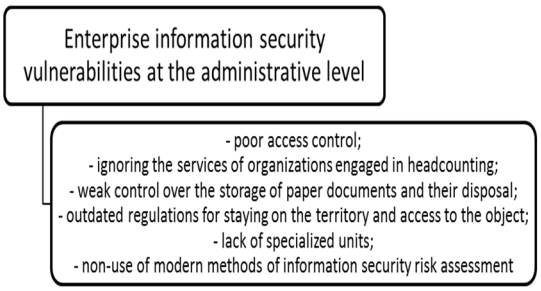

Figure 1: Enterprise information security vulnerabilities at the administrative level.

In terms of organizational protection measures, the following shortcomings were identified:

- not constant testing of employees working with confidential information for their legal awareness;
- not exercising control over the familiarization of employees with the new provisions related to information security (Sobotta, 2016);
- lack of verification of compliance with the rules of working with confidential information;
- the lack of regular training courses and testing of personnel, the purpose of which is to teach the rules of working with confidential information, means of protection (Mendling, et al., 2018).

Failure to comply with these measures at the enterprise creates an additional vulnerability of information resources. One of the most important tools of information security is the implementation of control and clear regulation of the information security system with the help of local regulations.

When analyzing software and hardware methods of information protection at the enterprise, a number of shortcomings were identified at the software level of information security. These vulnerabilities are shown in Figure 2.

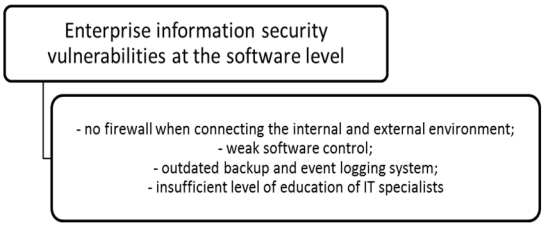

Figure 2: Enterprise information security vulnerabilities at the software level.

These vulnerabilities at the software level do not allow protecting the enterprise's information flows over the internal network. At the software level, in the presence of these shortcomings, there may be such threats as: distortion, destruction or theft of information using unwanted content, unauthorized access to information, information leaks, threats of fraud using information technologies.

When analyzing the information security at the enterprise at the technical level, the prerequisites for improving information security are identified, presented in Figure 3.

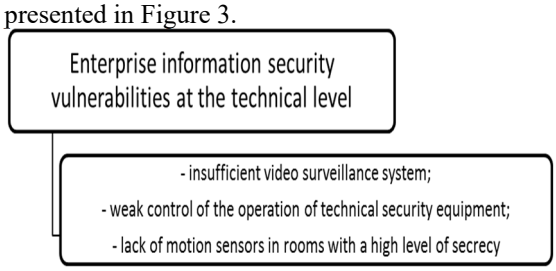

Figure 3: Enterprise information security vulnerabilities at the technical level.

These omissions in the information security system lead to the vulnerability of information resources and significantly increase the risks of information security, which can lead to the loss of financial benefits and material damage.

An improved information security system in the economic security system should be based on the information security model shown in Figure 1 and include at the administrative level:

- information confidentiality provisions;
- regulation on the use of e-mail (Krasnova et al., 2014);
- regulations on the use of media;
- regulation on the use of the Internet (He and Freeman, 2010);
- regulations on the use of the software;
- order on the introduction of the information security policy;
- regulations on the rules of internal labor regulations;
- provisions on emergency situations when ensuring information security.

At this level, compliance with all regulations in all sectors of the enterprise must be monitored.

At the organizational level, ensuring information security, the organization of an effective information security system at all levels should be established and constant security monitoring should be ensured (Scheibe and Gupta, 2017).

Information security at the technical level must have modern technical equipment in all sectors of the organization, and especially in rooms with a high level of secrecy.

Enterprise information security at the program level should include:

- control of access to confidential information;
- intrusion and anomaly detection;
- backup and archiving;
- centralized security management on all PCs;
- server-level intrusion prevention;
- audit and monitoring of security tools;
- monitoring the activities of employees on the Internet;
- analysis of the content of mail messages;
- analysis of the security of information systems;
- spam protection;
- integrity control;
- information access key infrastructure.

To ensure cost-effective information security, it is important to understand that the total cost of information protection should not be higher than the amount of possible economic damage from information security threats.

The information security strategy should be developed for the next year. But since, in the course of the current activity of the enterprise, there are continuously many changes related to the market conditions, markets for resources and services consumed by the organization, the emergence of new technologies, the strategy for ensuring information security may change during the year and be rescheduled for the next year, as well as additional adjustments may be made every year.

The main task of the enterprise in the context of the pandemic is to ensure the information security of employees working remotely. In the conditions of digitalization of all business processes, threats to information security can be destructive for the company's activities and entail unplanned losses not only of information data, but also quite real financial losses.

To ensure the safety of employees when working remotely, the company needs to develop and prepare a document that will display brief information for employees that will help them protect themselves directly at their workplace. This document should reflect the basic principles of working with a remote connection, as well as the main tasks of the employee to ensure personal information security at the home workplace.

In turn, the company must take care of information security on its part. A clear system for supporting the security system should be developed, and the main principles and measures that ensure it should be highlighted.

The company must adhere to clear rules when performing remote work in the company, such 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 two-factor authentication for VPN connection and access to corporate mail;
- use of proprietary remote access and data storage tools, such as internal cloud storage, to provide the enterprise with 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 (digital workspace) with built-in information security tools;
- the most optimal, however, resource and financial cost will be to provide all employees working on remote access with portable mobile computing equipment (laptops), on which anti-virus and corporate software will be installed in advance. This will help to increase the protection of corporate information several times and ensure safe operation (Barlow et al., 2011);
- for employees who interact with critical and confidential information, allocate a separate domain to monitor and respond quickly to security threats in the event of them and to prevent the leakage of information and data to third parties.;
- ensure continuous monitoring of the security of objects of confidential information, as well as keep logs of the actions of employees interacting with this information, and timely analysis.
- to ensure the possibility of rapid response of the security service and the adoption of measures to protect information in the event of computer threats and attacks by intruders;
- track the geolocation of the VPN connection in order to prevent unauthorized entry of an employee in time, for example, from another point of the earth;
- track information about the connected device via VPN, if an employee logs in from a personal device, then enter it into the database of trusted devices, in order to clearly see the "alien" and unregistered machine in the system;
- tracking "simultaneous" connections under the same account. These anomalies can help the company identify 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, proxy servers, or fake addresses. Timely disconnection of user data from the network will help the company to protect itself from data theft and infection of the system with malware and viruses;
- tracking the volume, duration and any anomalies of sessions in the VPN connection, which may indicate that the user is behaving unusually;
- For a VPN connection, use programs such as Cisco ASA, Cisco ISE, Cisco DUO, and Cisco AnyConnect;
- develop and implement software that allows you to detect unauthorized access through a VPN connection and quickly block it.

Since the most common and dangerous problem in remote work is phishing, thanks 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 by affecting the basic emotions of people thanks to social engineering. That is why it is especially important 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 sophisticated effects, sometimes not discernible even by experienced cybersecurity specialists. The fundamental task in this case will be to develop the skills of employees ' behavior in conditions close to real phishing attacks, simulating the actions of intruders.

4 DISCUSSION

Analysis of the theory and practice of building an information security system has shown that traditionally every organization can choose one of the ways to optimize the information security system.

According to the first way, the optimization of the information security system is carried out by the internal forces of the organization itself, by specialists working with the information structure.

As practice has shown, the first way is currently most in demand by domestic institutions, as it has a number of advantages such as:

- cost savings due to the absence of the need to invite specialists from outside, as well as the allocation of a separate item of expenses for their labor;
- the possibility of a wider use of information systems, due to unrestricted access to the commercial component.

However, the first way has a number of significant disadvantages, which are expressed in the following:

- as a rule, the level of training and professional experience of the employees of the institution itself does not sufficiently meet the requirements of optimization, which does not allow the implementation of the procedure for diagnosing the state of the system, as well as the subsequent development and implementation of the project to improve the information security system;
- as a result of the workload of the employees responsible for optimization, the latter are not able to perform the current main tasks;
- for the effective functioning of an improved information security system, highly qualified centralized strategic management of project development is required, which is also not always possible to achieve by the organization's specialists (Shevkunov and Zhigunova, 2018).

In addition to the above, it is worth noting the fact that according to statistics, the allocated 85 % of projects for optimizing information security systems implemented by the organization itself remained incomplete, or were executed with large errors, which ultimately leads to low efficiency of their execution.

The second way to optimize the information security system is to purchase a proven project for organizations with a similar organizational structure, goals and subjects of activity.

Like the above-mentioned path, the considered option of optimizing the information security system also has a number of advantages and disadvantages.

As advantages, it is worth highlighting:

- obtaining a ready-made, proven system developed by high-level professionals;
- costs are lower than when implementing an optimization project in-house from scratch.

The basic disadvantages of the second way of optimization, which is reduced to the acquisition of a proven project of the information security system, are the following:

- the need to adapt a ready-made system to the conditions of a particular organization;
- the lack of a choice of automation tools and technical support for the information security system that is most suitable for the institution or a complete rejection of automation.

As part of the third way to optimize the information security system, the delegation of functions and powers for the implementation of information technologies to external organizations (outsourcing) acts.

This modern approach, according to statistics, is still relatively rarely used by the leadership of Russian organizations. Although, with the right choice of the implementing organization, tangible results can be achieved as a result of this path of improvement:

- professional performance;
- service support;
- the possibility of developing an information security system in accordance with the complexity of the business.

Despite the presented advantages of the considered way of optimizing the information security system, it still has a number of disadvantages, among which the following deserve special attention:

- the loss of the possibility of developing the information security system;
- risk of information loss due to ignorance of the internal data structure;
- the dependence of support on the well-being of the implementing organization.

5 CONCLUSIONS

In conclusion, we note that when choosing the optimal way to optimize the information security system, the organization's management needs to pay attention to several key criteria.

The first criterion is the preservation of investment. Compliance with this criterion is determined by the fact that, regardless of the direction of modernization, the latter is always associated with certain costs that are necessary to adapt new tools and technologies to the operating conditions of each individual structural participant, as well as the costs incurred by the organization for the subsequent development of previously introduced innovations.

The second criterion is reliability, which means ensuring the availability and safety of information data in the event of problems in the information

system, accompanied in some cases by unauthorized access attempts.

The third criterion is the availability of the possibility of further growth and expansion, within the framework of which the subsequent implementation is expected in all structural divisions of the organization, including the possibility of developing additional modules by developers if such a need arises.

The fourth criterion is the level of automation of functional structural units, including automation of various types of activities, and not only the preparation and maintenance of accounting and reporting.

The fifth criterion is the clarity and accessibility of the interface, according to which any user who has access to the information system should be able to understand the specifics of its operation without describing the stages of its operation.

The sixth criterion is the possibility of integration with electronic document management. Within the framework of the presented criterion, it is assumed that there are mandatory opportunities for organizing electronic document management on the basis of a paper counterpart, not only within the organization itself, but also with external counterparties.

The seventh criterion is the adjustment to the specifics of the customer's activities, taking into account the construction of relations of its interaction with suppliers and contractors, not only within the framework of mutual settlements, but also within the framework of contractual relations in general.

The eighth criterion is a flexible pricing policy by the suppliers of the modernization implementer (Crick and Chew, 2020).

Based on all the above, it becomes obvious that in the process of choosing the path and direction of modernization of the information security system, special attention should be paid to the informatization of management, which is currently the key to ensuring the effectiveness of management decisions.

REFERENCES

Barlow, J.B., Giboney, J.S., Schuetzler, R.M., Keith, M.J., Wilson, D.W., Lowry, P.B. and Vance, A. (2011). Overview and guidance on agile development in large organizations. *Communications of the Association for Information Systems*, 29(1): 25-44. DOI: 10.17705/1CAIS. 02902

Crick, C. and Chew, E.K. (2020). Microfoundations of organizational agility: a socio-technical perspective. *Communications of the Association for Information Systems*, 46: 273-295. DOI: 10.17705/1CAIS.04612

He, J. and Freeman, L.A. (2010). Understanding the formation of general computer self-efficacy. *Communications of the Association for Information Systems*, 26(1): 225-244. DOI: 10.17705/1CAIS.02612

Krasnova, H., Veltri, N.F. and El Garah, W. (2014). Effectiveness of justice-based measures in managing trust and privacy concerns on social networking sites: an intercultural perspective. *Communications of the Association for Information Systems*, 35: 83-108. DOI: 10.17705/1CAIS.03504

Mendling, J., Decker, G., Reijers, H.A., Hull, R. and Weber, I. (2018). How do machine learning, robotic process automation, and blockchains affect the human factor in business process management? *Communications of the Association for Information Systems*, 43(1): 297-320. DOI: 10.17705/1CAIS.04319

Müller, S.D. and Ulrich, F. (2013). Creativity and information systems in a hypercompetitive environment: a literature review. *Communications of the Association for Information Systems*, 32(1): 175-200. DOI: 10.17705/1CAIS.03207

Scheibe, K.P. and Gupta, M. (2017). The effect of socializing via computer-mediated communication on the relationship between organizational culture and organizational creativity. *Communications of the Association for Information Systems,* 40(1): 294-314. DOI: 10.1111/j.1467-6486.1994.tb00640.x

Shevkunov, N. and Zhigunova, A. (2018). Methodological foundations for assessing the effectiveness of information security. *Science and Education: Economy and Economics; entrepreneurship; Law and Management,* 2(93): 33-36.

Sobotta, N. (2016). Why forwarded email threads are hard to read: the email format as an antecedent of email overload. *Communications of the Association for Information Systems,* 39(1): 16-31. DOI: 10.17705/1CAIS.03902

Zhigunova, A. (2016). Information security of business activity. *Economic and legal aspects of the development of the sovereignty of the Russian Federation at the present stage: Materials of the International Scientific and Practical Conference*, pages 25-29.