

Research of Processes for Ensuring Financial and Economic Security of Economic Entity

Karpenko K.V.

Department of Finance and Accounting
Institute of Service, Tourism and Design (branch)
North-Caucasus Federal University
Pyatigorsk, Russia

Kecherukov R.K.

Ministry of Finance of the Karachay-Cherkess Republic
Cherkessk, Russia

Novoselova N.N.

Department of Finance and Accounting
Institute of Service, Tourism and Design (branch)
North-Caucasus Federal University
Pyatigorsk, Russia

Abstract – This article is devoted to topical issues of ensuring the financial stability of market entities through the creation of an information security system as the basis of the financial and economic security of an enterprise. Based on the analysis of literary sources, the basic requirements and principles for creating an enterprise information security system are determined, since modern conditions for the functioning of the economy bring to the fore the need to create a local system of financial and economic security at any enterprise. Thus, ensuring the information security of any economic unit from a problem is transformed into a specific tactics of functioning, coupled with a survival strategy in the long-term time horizon. A number of researchers understand the economic security of enterprises not only as ensuring financial stability, but also as creating potentials for the outstripping growth of business activity and profitability. It should be noted that the competitive market, the unstable economic situation and the lack of an active position when introducing the latest digital technologies will put the company in a rather disadvantageous position, which determines the necessity and relevance of the chosen research topic. In our opinion, the main goal of the system of ensuring the financial security of the enterprise is the stable and effective functioning of the business unit in the present and building up the totality of all available development opportunities in the long term. This goal is identical to the goals of the controlling system. But the formation of a management system by achieving the diverse goals of a business unit is influenced by the need to create a security zone from external and internal threats. The presented article also discusses the most effective tools (methods) for improving the efficiency of the financial component of market entities based on the formation of an enterprise information security system.

Keywords – state, economy, private capital, finance, security

I. INTRODUCTION

Modern conditions for the economy functioning bring to the fore the need to create at any enterprise a local system of financial and economic security. Ensuring the information security of any economic unit is transformed from a problem into a specific tactics of functioning, coupled with a survival strategy in the long-term time horizon. At the same time, the

financial and economic security of the activity remains an important and very specific aspect of the general economic security of the enterprise.

The term economic security of an enterprise is interpreted by the authors in two ways: as the absence of any risks (dangers) for effective functioning, and as the formation of mechanisms to protect independence, protect their own interests from any third-party threats, even if they are potentially possible [1, 5, 18].

In recent years, economic security of an enterprise is understood not only as “ensuring stable activity” [2, 17], but also as creating potentials for the outstripping growth of business activity and profitability. Otherwise, the competitive market, the unstable economic situation and the lack of an active position when introducing the latest digital technologies will put the company in a rather disadvantageous position.

Financial security should include a number of aspects:

- the level of inviolability of financial resources and interests of the enterprise in any financial relationship;
- the effectiveness of the financial system in organizing the work of the entire economic system of the enterprise;
- the ability of the enterprise to form a safe zone in the process of financial support;
- the ability of the enterprise to provide all areas of its activities with financial resources and to develop a scheme for using them with maximum impact [1, 2, 7].

The main goal of the enterprise financial security system is the stable and effective functioning of the business unit in the present and the accumulation of all available development opportunities in the long term. This goal is identical to the goals of the controlling system. But the formation of a management system for achieving the diverse goals of a business unit is influenced by the need to create a security zone from external and internal threats.

II. MATERIALS AND METHODS

In the process of carrying out the study, the application received a systematic approach, as well as methods of observation, analysis, comparison, graphic and generalizations. In the process of writing the article, the method of comparative analysis and the method of scientific cognition were also used.

III. RESULTS

Creation of a local system of financial and economic security – a complex of material and digital resources, including all types of capital, including human, information systems and digital technologies, the latest production complexes, patent rights, licenses, subsoil use rights, etc. [3, 10, 24].

The stability of enterprises is endangered by the influence of both objective and individual factors. It is more difficult to control the effect of objective (external) factors. Individual factors depend on the efficiency of domestic economic services.

Support for information security at the enterprise is also based on internal aspects of the activity. Most often, confidential information leaves the information-analytical network through the employees of the enterprise itself, due to negligence or a deliberate desire to cause damage.

At the same time, various factors affect the structural components and features of the functioning of a secure information-analytical system.

Let us consider in more detail the methods of using tools to improve the efficiency of the enterprise information security system [1, 8, 18–21]:

1. Creation of physical obstacles – the use of material objects or directed power efforts to maintain a protective circuit against criminal or negligent actions, cutting off access to all types of controlled information carriers and hardware components.

2. Management of access to system components – the use of regulatory components for the means of an automated system of an enterprise that controls the access of each category of information users to information media and the system as a whole. The access control system includes the following functions [3, 7, 9, 10, 14, 15, 24, 25]:

- Codification of information security tools and identification of each employee of the enterprise;
- Authentication system, certifying the authenticity of the subject presented identifiers of the object or person;
- Strict prescription and operational control of the scope of authority of everyone admitted to the system, development and constant monitoring of the time, persons and means of information protection involved in security procedures;
- Strict adherence to the creation of protocols for accessing information security tools and confidential information resources;

- The use of audible alarms, mechanisms to disable or refuse to issue information upon request in case of an unauthorized attempt to obtain information.

3. System components camouflage – the use of integrated automation on the basis of a cryptographic approach to blocking access to information resources of the enterprise.

4. Regulation of admission to the system – the methodology involves minimal access to the information resources of the enterprise in case of emergency or dangerous situations.

5. Prescription of penalties – the methodology is based on the establishment of a set of strict rules when working with information resources of the enterprise, based on the application of penalties, as well as the inclusion of logging measures for administrative and criminal liability for violations.

6. Creation of incentive mechanisms – the methodology is based on a set of universal human ethical and moral norms that encourage not starting any points of the rules for using the formation resources of the enterprise.

The considered methods of protecting information flows of the enterprise will allow directing the functioning of each business unit and the entire enterprise as a whole to ensure maximum security of the entire information system of the enterprise.

Creating a secure information and analytical system of an enterprise is impossible in a single responsibility center or functional area of activity. It is necessary to develop interconnected organizational and methodological measures and procedures that form a secure not only local information network, but also its interaction with external sources of information and its consumers.

Organizational measures include: regulation of internal procedures for the preparation and movement of documentation, the procedure for working with IT services, technologies, as well as with the means of protecting information security. Technical measures for protecting the information-analytical system are understood as the use of specialized devices and software for access control, systematic monitoring of the information flow, antivirus and other types of protection

Creating a safe and relevant information-analytical system is possible in those enterprises where management understands the need for a systematic and integrated approach to its formation. This will take into account all security threats and predict the vulnerabilities of the entire system.

It is important to understand that the information security system requires a continuous process of operational control in all areas of activity, for the timely "capture" of any operation that calls into question the security of the information-analytical system. At the same time, more and more services are involved in the creation and maintenance of the system in working condition: departments of information technology, economic security, personnel management and other resources.

The system of financial and economic security of activity can be represented by a set of constantly made managerial decisions, the purpose of which is the early detection and prevention of any kinds of dangers and threats to the enterprise.

The creation of an effective information security system, as part of the financial and economic security of an enterprise, should be based on the following significant areas [7, 12–13, 25]:

1. A prospective assessment of all types of potential and previously occurring situations that have created a threat or caused damage in the past, as well as factors influencing them;
2. Analysis of the nature and possible economic consequences of emerging threats to the information and analytical system of the enterprise or its business units;
3. The selection of effective measures for early monitoring of threats and the creation of the necessary local regulations, with the distribution and consolidation of responsibility for their implementation;
4. Implementation of the selected set of measures to combat threats.

The information security system is formed by each enterprise independently, depending on its needs, but it also has blocks common to all business entities, which are shown in Figure 1.

At the same time, the information security system, forming the relevant security achievement system should ensure the implementation of the following areas [6–9]:

- creating an effective protective circuit for the entire character of the enterprise from possible illegal actions inside or outside the enterprise;
- monitoring the legality of all functions performed and individual operations;
- development of protective mechanisms against the criminal actions of competitors in the market;
- development of protective mechanisms against dishonesty of employees, especially the management team, of the enterprise itself.

The information security system of any business unit is based on three aspects:

- creating conditions for maintaining confidentiality of information and mechanisms for protecting the intellectual property of an enterprise;
- the formation of a highly qualified security service staff for each member of the staff of the enterprise;
- creation of a material and documentary basis for security and safety of all available property of the enterprise.

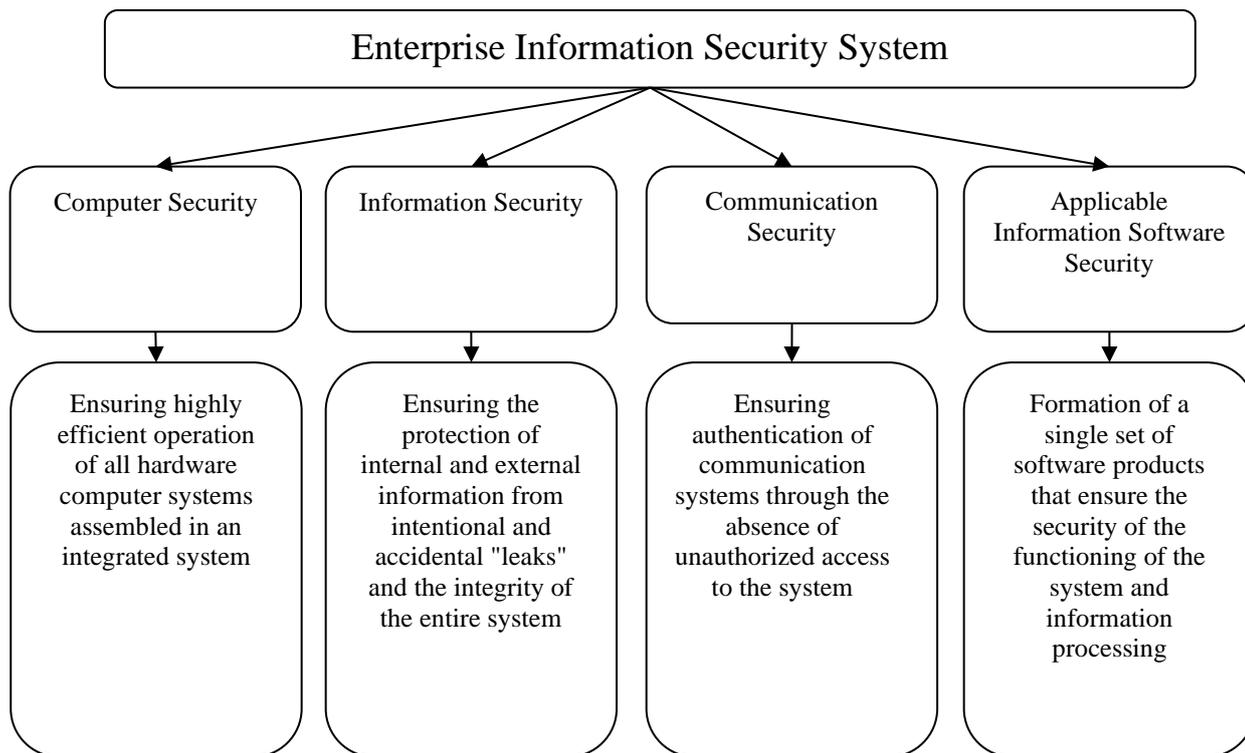


Fig. 1. The main blocks of the enterprise's information security system [Author's summary of [1, 2, 9, 17–19, 24]

IV. DISCUSSION

Most specialists in the field of information security of an enterprise focus on subjective threats (up to 80 % of all potential dangers) [4, 5, 8, 9, 11, 16, 21–25].

The management staff faces a number of issues that require the creation of a very expensive security system:

- What are the main channels of information leakage?
- What tools can help ensure early detection and elimination of threats?
- What tools will reduce the costs of operating a local information security system?

At the same time, information security enterprises is understood as the security of an information-analytical system, subject to the requirements of secrecy, relevance, analyticity, authenticity and ease of obtaining and processing all data [6, 9, 24].

The transition to a digital model of the economy and the associated increase in the number of information risks leads to the creation of a high-quality information security system subject to the following conditions [5, 9, 16, 20–24]:

1. The processes of information exchange and data storage should be focused on preventing the occurrence of the possibility of transferring to competitors or criminal structures any relevant information that affects the current situation or the strategic development of the enterprise as a whole or its business units;

2. Participation in the process of protecting and ensuring the safety and stability of the enterprise development not only of the security department, but of the entire staff of employees.

To create an effective model of the enterprise's information security system, management personnel can be recommended to observe the following rules:

1. Cash means of information protection should be understandable for use, accessible and simple when organizing maintenance.

2. Most users of information security tools have the minimum privileges necessary to perform their job functions.

3. All components of the information security system must be connected in an autonomous circuit.

4. The ability to disable information security tools if they negatively affect the functioning of business units or the enterprise as a whole.

5. Security system developers should take into account the maximum degree of hostility of the environment, should assume the worst intentions on the part of attackers and the ability to circumvent all defense mechanisms.

6. All cash means of information protection of the enterprise and their location should be kept secret.

For small and medium-sized enterprises, it is economically more profitable to hire specialized security services, rather than create and recoup internal work.

V. CONCLUSION

Thus, at the present stage of each industry economic development, characterized by the introduction of the latest digitalization technologies, the number of dangerous situations and threats to the information security of an enterprise is growing. Their analysis and prevention plays a huge role in the overall security system of the enterprise and in financial and economic security, in particular. The greatest attention to security systems should not be focused on external threats, but on dangers emanating from the internal environment of the enterprise. Any leak of confidential information, even due to the carelessness or lack of experience of the contractor or the operational control system employee, or a threat to information resources, can cause a decrease in income and / or profit, deterioration in the image of the market and even bankruptcy of the enterprise.

The most economically viable in the early stages of the implementation of security systems will be the choice of protective equipment that forms a reliable modular security system, with a closed circuit from external risks and strict regulations, with operational monitoring of internal access to enterprise information resources.

References

- [1] D.V. Shiryayev, E.I. Artemova, M.V. Zelinskaya, S.N. Novoselov, S.D. Galiullina, E.E. Pismennaya, "Knowledge economy" as a resource for the intensification of socio-economic transformation of the regional economic space", *International Review of Management and Marketing*, vol. 6, no. S1, pp. 232–237, 2016.
- [2] A.N. Bobryshev, Y.V. Golchenko, M.Y. Kazakov, "Directions of municipal territorial and economic transformation in a monopolar highly urbanized region", *Actual problems of economics*, vol. 2, no. 152, pp. 230–238, 2014.
- [3] T.V. Grechkina, E.V. Golushko, D.D. Galcheva, L.V. Krasnyuk, E.A. Kosinova, "Features of accounting organization the costs sanatorium complexes", *Indo American journal of pharmaceutical sciences*, vol. 06, no. 03, pp. 5165–5171, 2019.
- [4] N.N. Novoselova, D. Shkurkin, E.P. Kolpak, T.V. Kormiltsyna, "Regional clusters in the strategy of achieving technological leadership", *International Journal of Applied Business and Economic Research*, vol. 15, no. 13, pp. 171–177, 2017.
- [5] K.V. Shulga P.V., Mikhailushkin, E.P. Kolpak, "Study of the forms and conditions of economic crises in the regional economies of developing countries", *Revista ESPACIOS*, vol. 39, no. 31, pp. 26, 2018. ISSN 0798 1015.
- [6] S.S. Slepakov, V.V. Hubulova, "To the question of the revival and renewal of the science of political economy", *The Future of the Global Financial System: Downfall or Harmony*. Springer, 2018.
- [7] M. Kazakov, V. Gladilin, A. Mirokhina, E. Drannikova, G. Narozhnaya, "System diagnostics and monitoring of socio-economic and tourist potential of peripheral territories of the region", *Journal of Environmental Management and Tourism*, vol. 9, no. 2, pp. 283–290, 2018. Retrieved from: <https://journals.aserspublishing.eu/jemt/article/view/2097>
- [8] L. Kazakova, M. Kazakov, L. Korobeinikova, D. Shikhalieva, O. Dubskaya, "Transformation of household farms in regions of Russia: retrospective experience and modern dynamics", *Journal of Advanced Research in Law and Economics*, vol. 8, no. 6, pp. 1785–1797, 2018. Retrieved from: <https://journals.aserspublishing.eu/jarle/article/view/1830>

- [9] A.V. Dorozhkin, V.N. Yasenev, "Information security as a tool to ensure the economic security of an economic entity", *Economics and Entrepreneurship*, vol. 5-1, no. 58, pp. 812–816, 2015.
- [10] D.E. Esipov, D.V. Gavlovsky, L.Yu. Likharev, S.N. Fomina, The problem of ensuring information security. Information support and work with youth. Collection of student works. Moscow, 2012, pp. 41–45.
- [11] P.S. Ivlichev, N.A. Ivlicheva, "Information technology to ensure the security of means of payment in the light of modern trends in cybercrime", *Economics and Entrepreneurship*, vol. 2-1, no. 79, pp. 135–139, 2017.
- [12] O.V. Inshakov, Mechanisms for implementing the strategy for the formation of nanoindustry in the regions of Russia. Volgograd: VolSU Publishing House, 2009, 240 p.
- [13] M.Yu. Kazakov, A.N. Bobryshev, Yu.V. Golchenko, Directions of municipal-territorial and economic transformation in the monopolar highly urbanized region *Actual problems of economics*, vol. 2, no. 152, pp. 230–238, 2014.
- [14] E.N. Klochko, M.V. Zelinskaya, "Development of a mechanism for transforming the state economic policy of modern Russia", *Vestnik Adygey State University. Series 5: Economy*, vol. 4, no. 210, pp. 13–21, 2017.
- [15] E.N. Klochko, S.M. Reznichenko, "Characterization of the reproductive potential of the ethno-economy of the Krasnodar Territory and the Republic of Adygea", *Business. Education. Pravo*, vol. 3, no. 44, pp. 67–73, 2018.
- [16] S.S. Kovalchuk, M.A. Denisova, N.O. Kovalkovskaya, L.O. Strilling, "The place and role of computer security in ensuring information security", In the collection: *Security of the Information Space [Proceedings of the XIII All-Russian Scientific and Practical Conference of Students, Graduate Students and Young Scientists, 2015]*, pp. 104–108.
- [17] Ensuring the information security of the organization. Retrieved from: <http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/>
- [18] O.V. Orlik, "Financial and economic security of the enterprise and the principles of its maintenance", *Economics and management: theory and practice*, vol. 2, pp. 286–291, 2014.
- [19] A.S. Popova, V.V. Sorokozherdiev, S.G. Spirina, "Economic and legal aspects of the implementation of the strategy of modernization of Russia and neighboring states in the post-Soviet space", *Society and Law*, vol. 1, no. 51, pp. 346–390, 2015.
- [20] N.P. Romashkina, "Information security as part of the problem of ensuring strategic stability", *Strategic stability*, vol. 1, no. 82, pp. 8–13, 2018.
- [21] V.D. Rudolph, "Information security of the enterprise: the essence, the main problems of ensuring", *Economics and society*, vol. 4-2, no. 23, pp. 199–203, 2016.
- [22] S.S. Slepakov, V.A. Sidorov, N.L. Orlova et al., *Reproduction of Russia in the 21st Century: Dialectics of Regulated Development*. Moscow: RUSAINS, 2017.
- [23] I.V. Taranova, I.M. Podkolzina, V.V. Prokhorova, O.N. Kolomyts, E.M. Kobozeva, "Global financial and economic crisis in Russia: trends and prospects", *Research Journal of Pharmaceutical, Biological and Chemical Sciences*, no. 6, pp. 769–775, 2018.
- [24] T.N. Tuhkanen, I.I. Guryashina, "Information support of decisions and information security", *Modern development trends and prospects for the introduction of innovative technologies in mechanical engineering, education and the economy*, no. 1, pp. 129–131, 2016.
- [25] P.Yu. Filyak, V.M. Shvarev, "Ensuring the information security of the organization based on the information security management system", *Information and Security*, vol. 18, no. 4, pp. 580–583, 2015.