CZU: 004.056.53:339.137
DOI: https://doi.org/10.53486/icspm2022.57

PROTECTION OF INFORMATION AT THE ENTERPRISE IN CONDITIONS OF COMPETITION

RYBALCHENKO Lyudmyla Volodymyrivna
ORCID: 0000-0003-0413-8296
Ph.D, Ass. Prof, Dnipropetrovsk State University of Internal Affairs,
Dnipropetrovsk region, Ukraine, mail: luda_r@ukr.net
KOSYCHENKO Oleksandr Oleksandrovych
ORCID: 0000-0002-6521-0119
Ph.D, Ass. Prof, Dnipropetrovsk State University of Internal Affairs,
Dnipropetrovsk region, Ukraine, mail: kosichenko-inform@meta.ua
RYZHKOV Eduard Volodymyrovych
ORCID: 0000-0002-6661-4617
Ph.D, Professor, Dnipropetrovsk State University of Internal Affairs,
Dnipropetrovsk region, Ukraine, mail: revord924@ukr.net

ABSTRACT

The information development of society is becoming more and more attractive every year for registration and communication on social networks, as well as for working with information resources, where there is a need to place both company data and personal data. Therefore, the need for data protection in today's information life is growing.

Personal data are information about the date and place of birth, his name and surname, passport data, tax identification number, signature, profession and marital status. At the legislative level of the country, the Law of Ukraine "On Personal Data Protection" has been developed, which deals with the protection of personal data of individuals and legal entities during processing and use. Managers of personal data may be public authorities, local governments, state or municipal enterprises.

Personal data can be used by cybercriminals to commit any economic crime, both at the level of enterprises and individuals. It is to protect this data that care must be taken not to disclose it to unverified third parties or organizations of good faith or reputation. Modern information activities are essential for the use of the latest technologies and secure information protection.

KEYWORDS: *information, information field, personal data, information security, regulatory framework*

JEL CLASSIFICATION: D80; G14; M21; L86

INTRODUCTION

The activities of commercial enterprises are always accompanied by danger and risk. Most often, the risk may be from competitors, third parties or staff. They are often caused by political and legal instability, intensification of competition, illegal use of hardware and software, and more. Therefore, in the framework of enterprise management, in addition to the main functions, managers are entrusted with the issues of information security.

The economic security of the enterprise is to create such conditions for its operation, which will ensure the stability and protection of its activities from possible negative influences of both external and internal environment. It is the information component of the economic security of the enterprise occupies one of the important places. Information security is the ability to protect information resources of the enterprise from any threats of unauthorized access to them.

Analysis of the organization of the information space of the enterprise is in the field of view of economic efficiency of the enterprise. The main amount of information of the enterprise circulates within its organizational, legal and physical boundaries. Unauthorized access to the information environment of the company from various channels and sources can be used to harm the company, blackmail or corruption. These can be open publications and databases, customers, suppliers, investors, credit institutions, intermediaries, personal data of employees and other channels. These sources can give a lot of information to competitors or third parties.

The purpose of this study is to highlight the mechanisms of implementation of regulatory and legal support for information protection at the enterprise.

Presentation of the main material of the study. In recent years, the regulatory framework for information protection at the national level has improved significantly. This was expressed in the adoption by the Ukrainian leadership of a number of laws [5-8] and other regulations relating to the regulation of creation, use, transfer and storage of information and copyright, the licensing of activities in the field of information protection and more.

On the basis of these documents is built legal protection of information, which is designed to provide the state legal framework and regulatory framework for a comprehensive system of information protection at the enterprise, regardless of its ownership and category of protected information.

In addition to laws and other state regulations, the legal support of the system of protection of confidential information at the enterprise includes a set of internal regulatory and organizational documentation, which includes:

- Statute;
- Collective bargaining agreement;
- Employment contracts with employees of the enterprise;
- Rules of internal procedure of employees of the enterprise;
- Job responsibilities of managers, specialists and employees of the enterprise;
- Instructions for users of information-analytical and technical support of networks and databases;
- Instructions for administrators of information-analytical and technical support and networks, as well as databases;
- Provisions on the information protection unit;
- The concept of information protection system at the enterprise;
- Instructions of employees admitted to the protected information;
- Instructions of employees responsible for information protection;
- A reminder to the employee to keep a trade or other secret;
- Contractual obligations and more.

It should be noted that all these documents, depending on their main regulatory or legal purpose, specify the requirements, norms or rules to ensure the required level of information security at the enterprise or its structural units, aimed at staff and management.

Legal support makes it possible to resolve many controversial issues that arise in the process of information exchange at various levels: from communication to data transmission on computer networks. In addition, a legal system of administrative measures is formed, which allows to apply penalties or sanctions to violators of internal security policy of the enterprise, as well as to establish clear conditions for ensuring the confidentiality of information used or formed between economic entities, their contractual obligations, implementation of joint activities and more. In this case, the parties who do not meet these conditions are liable within the framework provided by the relevant clauses of bilateral documents (agreements, contracts, etc.) and Ukrainian law.

The economic activity of any enterprise is always associated with the flow of information. Management is an ongoing process of creating and implementing management influences to achieve the goal within the information field. In general, the information field of the enterprise can be divided into internal and external. The internal information field combines information that originates within the enterprise. It is important to note that the quality and content of the internal information field mainly depends only on the company and management. The company's own information field is formed at the expense of internal sources of information, the amount of which is limited. The economic activity of any enterprise is always associated with the flow of information. Management is an ongoing process of creating and implementing management influences to achieve the goal within the information field. In general, the information field of the enterprise can be divided into internal and external. The internal information field combines information that originates within the enterprise. It is important to note that the quality and content of the internal information field mainly depends only on the company and management. The company's own information field is formed at the expense of internal sources of information, the amount of which is limited.

Information can be divided into conditionally constant and variable. Conditionally constant information includes information that is virtually unchanged over a long period. It includes both normative and scientific information. Regulatory information is needed to make decisions and monitor their implementation. It includes various normative and reference data, basic indicators, standards. This information rarely changes. Regulatory information is the most fully systematized, presented in a form that is easy to work with and mandatory. Correction or cancellation of these documents is only on the instructions of higher authorities. Scientific reference information is information obtained from scientific and technical literature, regulatory and technical documentation, various bulletins, news releases and more.

Variable information reflects changes in the criteria of management and operation of units, as well as changes in the planned parameters. It includes summaries that change periodically in content and nomenclature. It includes groups of planning, operational, reporting information and similar types.

Planned information includes summaries of the parameters of control objects and control objects that need to be achieved and maintained, the parameters of production processes that need to be achieved and maintained for the required period. For production units and supply units, it is created in the form of specific planned tasks, indicators. For management units, it includes methods and means of achieving the objectives and is expressed in the creation of instructions, standards, the application of which regulates and normalizes the work of the management staff. This information is directive and is corrected during operational management.

Operational and production information includes summaries of costs, balances, shortages of materials and components, shortcomings of technological documentation, downtime. These summaries of deviations in the processes of achieving the goal of management are necessary for the creation and implementation of corrective actions of management. In addition, it is a set of data that characterizes qualitatively and quantitatively all types of products, as well as various reports on the movement of these types of products in the production cycle; data on the course of the technological process of production, energy, the position of vehicles and more.

Reporting information includes various reports on the state of their units, the results of production tasks, the state of supply and sales at a particular time. Given the inclusion of planned information of the enterprise in the variable, in the first place in full is the variable information.

To achieve completeness and comprehensiveness of information protection, the development and implementation of even the most complete and impeccable legal support will be insufficient. Any laws or regulations lose their effectiveness and cease to be effective normative means of regulating various kinds of relationships in the absence of the environment to which these rules apply.

In order to create a reliable legal basis for the information protection system, it is necessary to organize this system, create the preconditions for its operation, develop a set of consistent and

coordinated activities, identify its components and subsystems. The organizational system of information protection serves for these purposes.

The information protection system is a set of organizational and technical measures to ensure information security at the enterprise, the creation of a common security policy and control of its effectiveness. The development and implementation of the system must be preceded by a thorough study of information resources of the enterprise, making justifications and arguments in favor of creating a system of protection. Thus resources and labor costs for its creation and functioning are calculated and distributed in advance, the most priority ways and directions of its development are chosen. Then the possible causes, variants of manifestation and consequence of violations of information security, failures of programs, hardware and processing systems, as well as the transfer of information, its unauthorized receipt, modification and dissemination are identified.

In other words, the information-functional model of the enterprise is formed and the sketch scheme of the protection system is created. The organizational part of the system should include the following.

First, the identification of information that constitutes a trade secret of the enterprise, and compiling a list of such information with its division into groups by category of confidentiality and the required level of protection. In the future, such lists should be compiled for each unit or area of activity of the enterprise.

Secondly, planning the implementation of the information protection system (GIS), which identifies the most vulnerable areas of information exchange channels, schedules organizational and organizational and technical measures, calculates the resources expended, compiles a general list of employees (specialists, employees and managers)) involved in the implementation of the system, and units, determines the order of interaction of structural elements and parts of the enterprise at the stage of creating a system of information protection.

Third, measures to implement and implement the system. At this stage, the following can be done: compiling a list of designated premises where closed events are held or critical information is circulating; identification of officials authorized to exercise control and operational management of the GIS; training of specialists in the field of information security, supporting the functioning of information security systems, tools and devices; regulation of functional responsibilities of employees of information security departments; definition of controlled zones; establishing the procedure for periodic attestation inspections of allocated premises, etc.

Fourth, at the stage of functioning of the information protection system, the following organizational measures must be constantly carried out: registration of works with the use of information that is a trade secret; registration of all events related to the development, use, transfer of information containing confidential information, and making changes to protected information resources; keeping records of documentation and media of confidential information; responding to destabilizing factors in order to prevent or reduce the impact on information; delimitation of rights of access to protected information resources. Fourth, at the stage of functioning of the information protection system, the following organizational measures must be constantly carried out: registration of works with the use of information that is a trade secret; registration of all events related to the development, use, transfer of information containing confidential information, and making changes to protected information resources; keeping records of documentation and media of confidential information; responding to destabilizing factors in order to prevent or reduce the impact on information; delimitation of rights of access to protected information resources.

Fifth, measures are being taken to ensure control over the effectiveness of the system. For example, conducting periodic inspections, including the use of special testing programs, reviewing registration documents, monitoring the implementation of organizational measures to comply with security policy rules, analyzing the state of the protection system, making decisions on improving technical means and systems, organization and security policy.

In addition, regular preventive interviews should be conducted with company personnel to prevent security breaches. These conversations are necessary to raise the level of awareness of

employees in relation to the problem of information protection to the level of understanding of each of them the usefulness and necessity of the measures taken. These measures should be aimed at ensuring information security, which, in turn, is an integral part of the overall security of the enterprise. Only a conscious attitude of employees to this problem can make the protection system truly effective and reliable.

CONCLUSION

Thus, variable information is the main source of data about the enterprise. But not only because it contains the most important information about the current state of the organization, but because it is used by all governing bodies to perform their basic functions. Therefore, variable information in the overall structure of information will be of major interest to competitors of the enterprise. And this is not just because of its inclusion in the total amount of information of the enterprise, but because through access to it may be possible to access at least one of the management of the enterprise.

In addition, variable information is of interest to competitors for the following reasons:

- it is relatively similar in combination with the mass and common sources of its occurrence in connection with the systematization of business reporting;
- the same source data is used repeatedly to obtain information on different types of economic activities at different levels of government;
- the main part of the variable information is subject to regular processing, which retains the fundamental possibility of access to it for a certain time;
- different flows of variable information have links that allow you to confirm or deny the existence of a fact, event;
- variable information is characterized by relatively large volumes and simple processing;
- data obtained from one operation are the source for others (even in several departments). With the existing connections between the functions, it allows, having the information created during the execution of one function, to restore the information picture of the performance of many other functions.

The information interests of competitors, as a rule, are structural in nature, ie will be directed to those nodes in the administration and other services of the commercial organization, through which passes a significant array of variable information. They are likely to have a specific focus, ie will be aimed at certain units of the commercial organization and individuals from among employees who have access to variable information.

In the information space of the enterprise there are always objective opportunities for loss or leakage of information. Therefore, information protection, first of all, should be built taking into account the content of variable information and ways to work with it. This applies to all streams of variable information circulating in all communications of the enterprise from ordinary documents, local computers, cable, telephone and computer networks, mobile communications. Information security will never be fully ensured if there is no analytical component, that is, there will be no systematic work on the analysis of the information field of the enterprise.

When reorganizing enterprises, a large number of documents of various kinds appear, which regulate almost all activities. In other words, there is a large amount of variable information that can be obtained legally and used by both regular competitors and criminal organizations.

Information security of the enterprise should be provided, first of all, by legal methods of protection. At the same time, its organizational component plays an important role in improving the efficiency of the information protection system at the enterprise.

REFERENCES

1. Rybalchenko L., Kosychenko O. Features of latency of economic crimes in Ukraine / L Rybalchenko, O. Kosychenko // Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. - 2019. - Special Issue № 1 (102). – P. 264-267. DOI: 10.31733/2078-3566-2019-5-264-268

2. Дисковський А.О., Косиченко О.О., Рибальченко Л.В. Основи організації захисту об’єктів та інформації від злочинних посягань : навч. посібник для слухачів магістратури

/ О.А. Дисковський, О.О. Косиченко, Л.В. Рибальченко. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2020. - 96 с.
3. Рибальченко Л.В., Косиченко О.О. Економічна безпека України та напрями що до її підвищення. Колективна монографія: «Modern engineering and innovative technologies». Німеччина. Випуск 12, червень 2021. с.109-123.
4. Рибальченко Л.В., Косиченко О.О., Рижков Е.В. Вплив тіньової економіки на економічну безпеку України. Науковий вісник Дніпропетровського державного університету внутрішніх справ : Збірник наукових праць. – 2019. – № 2 (103) . – С. 175-183.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 681-IX від 04.06.2020
6. Закон України "Про захист персональних даних" (Відомості Верховної Заради України (ВВР), 2010, № 34, ст. 481). Нова редакція № 2297-VI від 13.02.2022.
7. Закон України «Про інформацію» від 02.10.1992 № 2657-XII у новій редакції від 01.01.2022.
8. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. Нова редакція від 15.03.2022 // https://zakon.rada.gov.ua/laws/show/3855-12#Text