Oksana Vivchar
Ternopil National Economic University
ORCID: 0000-0001-9246-2226

Inna Zaitseva-Kalaur
Ternopil National Economic University
ORCID: 0000-0001-5924-5844

Oksana Redkva
Ternopil National Technical University named after I. Puliy
ORCID: 0000-0002-8246-4305

Volodymyr Gevko
Members of the Ukrainian Parliament
ORCID: 0000-0003- 2716-8113

Organizational and legal procedures for ensuring the security and protection of an economic entity: a security knowledge approach

Target setting. Establishing and applying a "trade secret" regime to information that is commercially valuable to an entity is one of the priority issues for strengthening economic security.

Actual scientific research and issues analysis. The problems of security and protection of commercial secrecy have been studied extensively by such researchers as H. Androshchuk, Yu. Nosik, O. Slipachuk, A. Sliadnieva, S. Chikin, V. Chernenko and others. The authors analyse the current state of the legal regulations of this institute, investigate the protection of trade secrets in the countries of the European Union and consider measures of legal and organizational nature regarding its preservation, etc. However, despite the rich scientific background in this field, the issues of protection and protection of trade secrets remain relevant today. The lack of a special law on trade secrets imposes on entities the setting of objectives to establish and enforce trade secret systems for information which is important and valuable for strengthening the economic security of the enterprise. It offers both great opportunities for the latter and requires great effort and responsibility in their decision making.

The research objective – to characterize (step-by-step) the process of classifying information as a commercial secret, having studied the effective system of protection and defense of this legal institute.

In order for the information stored in the "trade secrets", an entity needs to plan and organize actions of a legal nature. First of all, this involves the introduction of relevant provisions in the constituent documents.

In the constituent documents with reference to Articles 505, 506 of the Civil Code of Ukraine[1] and Articles 36, 135, 155, 162 of the Civil Code of Ukraine[2] to provide the right of an enterprise to transfer the information belonging to it to a trade secret and the right to receive internal documents by which its composition, scope and procedure for the protection of information that is confidential or commercially confidential shall be determined.

On the basis of these documents, the company plans and organizes the development, adoption and implementation of enterprise key documents to ensure economic security[3]. These are documents that directly protect the trade secrets of an enterprise and documents that provide the trade secrets of the enterprise as a vector for ensuring economic security when hiring personnel.

Documents that directly protect the trade secrets of an enterprise include:

1. *Regulations on the organization of trade secrets* and other confidential information (Regulations on trade secrets). This regulation regulates measures for the organization of protection and protection of trade secrets, the procedure for dealing with information that is a trade secret, the obligation of employees to keep a trade secret, the procedure for disclosure of information containing a trade secret, liability for breaches of business secrecy, etc.;

2. *List of information pertaining to restricted information.*

3. *Provisions for special record-keeping for documents* containing restricted information;

4. *Provisions on information security when dealing with* proprietary and proprietary media;

5. *Instruction on the order of execution of requests received from law enforcement agencies, courts and other state institutions;*

6. *Instruction on carrying out checks on the observance of standards of information security when working with trade secret material carriers.*

Documents that ensure the protection of company trade secrets retained by staff include:

---

[1] *Tsyvilnyi kodeks Ukrayiny* (2003, January 16), Offic. Bulletin of Ukraine.

[2] *Hospodarskyi kodeks Ukrainy* (2003, January 16), Vidomosti Verkhovnoi Rady Ukrainy, Kyiv: Parlam. vyd-vo.

[3] O. Vivchar, *Management system interpreting financial and economic security business in economic processes*, "Mathematics education" (Social Sciences) vol. 11, 2016, no. 4, p. 947–959.

1. *Employment contract (contract), job descriptions* specifying issues related to trade secrets and liability for violation of the right to use a trade secret, including after dismissal of an employee;

2. *Obligation of enterprise employees to restrict access to sensitive information;*

3. *Regulations on the non-disclosure of trade secrets of the enterprise and other provisions*, rules, obligations and the signature of the employee on the basis of which the enterprise protects its interests.

4. *Description of requirements for agreements with third parties* regarding access, processing, transmission or management of enterprise information.

The procedure for assigning information to a trade secret is a complex multidimensional phenomenon that involves the application of legal and organizational measures to protect the trade secrets of an entity.

The procedure for the classification of information as a trade secret involves several clearly defined steps.

The *first stage* is the updating of information that needs protection by designating it as a trade secret. Next, a careful study of the information selected as confidential and the drafting of the regulations on the trade secret and the list of information that make up the trade secret of the enterprise are necessary. The relevant list of confidential information can be formed in the following areas: personnel policy of the enterprise, financial activity of the enterprise, pricing policy of the enterprise, sales activity of the enterprise, ensuring the security of the enterprise.

To accomplish this task, an enterprise manager appoints a person responsible for the confidentiality plan for confidential information and trade secrets and the trade secret commission. It is necessary to form a list of information of the trade secrets of an enterprise with the involvement of specialists of the profile units in each of the areas. Such a list could be used in case of disputes concerning particular information belonging to the category "trade secret" involving experts of such divisions. Such persons, even in the presence of the main features of a trade secret, can determine in each case how dangerous its disclosure is.

There are no requirements or regulations in domestic law regarding the structure and content of the Regulations on Trade Secrets. However, despite the differences in the fields of activity, structures, number of employees and management of enterprises, the researchers have formulated some general recommendations for its content:

1. General provisions.

2. Determination of the list of information constituting trade secrets and confidential information of the enterprise.

3. The procedure for the protection of trade secrets and confidential information of the enterprise.

4. The procedure for issuing employees documents, information, transfer of information that is a trade secret and confidential information of the enterprise to contractors, clients and public authorities.

5. Procedure for hiring (firing) an employee/employee of the enterprise.

6. Responsibility for the disclosure of information constituting trade secrets and confidential information of the enterprise.

7. Final provisions.

8. Supplements.

In section 2 of this provision, it is advisable to characterize the list of information with general concepts, and to define them in detail and to refer to the list of information that constitutes a commercial secret of the enterprise[4].

The Appendices may include standard documents relating to trade secrets, such as: "Business Note with a Proposal for Disclosure of Trade Secrets", "Employee's Obligation to Disclose Trade Secrets and Confidential Information", "Business Visitors Agreement", etc.

The second stage – the head of the enterprise issues an order for approval and implementation at the enterprise of the regulation on the trade secret of the enterprise and the procedure for acquaintance with it.

The next stage – the commission forms the list of information, which comprises the company secrets. At this stage, a deadline for the secrecy of information is provided. For the period of existence, a trade secret can be divided into short-term classified information and long-term classified information. Typically, the timing of classified short-term information is up to 6 months, while long-term information is from 6 months and longer.

The fourth stage involves the approval of the list of information, which is a trade secret of the enterprise and consists of two stages:

1) the assignment for each type of information of the corresponding classification mark. "Particularly confidential" means information that will be adversely affected by the whole activity of the enterprise, and "secret" means information whose possession may cause damage to a particular line of business activity;

2) approval and signature by the head of the enterprise of the list of the information, which is a trade secret. All of the information listed in the said document has been officially granted the status of a trade secret of the enterprise[5].

The list of trade secrets should be periodically adjusted. Information that has lost its value, become publicly available, or has lost commercial

---

[4] S. Chikin, V. Chernenko, *Upravlinnya komertsiynoyu tayemnytseyu na pidpryyemstvi: diyi orhanizatsiynoho, tekhnichnoho ta psykholohichnoho kharakteru*, „Teoriya i praktyka intelektualnoyi vlasnosti" 5 (2011), p. 57.

[5] O. Lokotetska, *Systema zakhystu komertsiynoyi tayemnytsi pidpryyemstva*, „Biznes Inform" 12 (2011), p. 82.

value, etc., should be removed and new items needing protection should be added.

The fifth stage is the establishment of the material storage media that comprise the company secrets. Holders of confidential information may include persons, documents, products, official media or technical means. In this case, the person is the link between all other carriers of trade secrets as he/she develops and approves the documentation, manufactures products, prepares materials for publication, announcements and displays in the media, works on computers, typewriters, with telephones, faxes and other technical means. For each type of confidential information, it must be decided in what form it will exist. A trade secret may have several media, which must be taken into account when defining the methods of its protection, as well as those who possess it.

The *sixth stage* identifies specific individuals who have, or may have, access to sensitive information.

The disclosure of a trade secret is mainly due to the fact that the head of the enterprise pays insufficient attention to the study of the identity of the person with access to trade secrets.

It should be noted that while giving the right of access to information classified as a "trade secret" the manager must:

– determine the need for access to confidential information by an employee for the performance of his/her tasks;

– verify the employee's right to access trade secrets;

– acquaint the employee with the degree of responsibility for violation of the legislation on illegal collection, dissemination and use of trade secrets;

– issue a written document on employee's obligations regarding the disclosure of trade secrets which are at his/her responsibility.

When verifying an employee for access to trade secrets, the following should be taken into account:

– age over 18;

– any convictions for crimes connected with disclosure of state or commercial secrets, as well as financial and economic secrets;

– presence of mental illness, use of alcohol and drugs;

– the fact of providing false information about himself/herself in the procedure of registration for admission ;

– presence of suspicious links with employees of competing enterprises[6].

The seventh stage is the choice of methods to protect the trade secrets of an enterprise in order to ensure economic security.

In order to develop an effective system of protecting trade secrets, it is necessary to study all possible ways of illegal possession of it.

[6] S. Chikin, V. Chernenko, *Upravlinnya komertsiynoyu tayemnytseyu na pidpryyemstvi*..., p. 61.

The most common unlawful acts that allow you to master confidential information of the company are:

– bribery of employees of the enterprise who own or have access to confidential information;
– wiretapping;
– remote audio listening;
– copying of media;
– decoding of radio radiation of computers, faxes, teletypes;
– visual and auditory control of the premises;
– placement of micro transmitters in premises and cars;
– use of professional spies;
– recruiting a competitor's employees;
– referring agents to employees or specialists of a competitor.

A low level of control over security measures, unsatisfactory working conditions, inefficient employee incentive system, savings on technical means of protection, staff turnover, imperfect work system, etc. contribute to the illegal possession of trade secrets.

Effective methods of protection in the context of safeguarding conditions are:

1. *The creation of a secret regime division with the functions of support and control over the observance of the established secrecy regime, the activity of which is determined by the corresponding instructions, regulations or orders.*

As the main functions of the secretariat, it is advisable to define the following:

– development, implementation and maintenance of the permitting system of access to information;
– development and implementation of the marking of documents and data carriers classified as commercial secrets and actions for their preservation;
– development and implementation of secret records;
– planning and organizing technical actions for the protection of information carriers and information networks;
– actions aimed at identifying information leakage, sources of such leakage and localization of negative consequences, etc.;
– planning, organization and implementation of psychological actions: staff briefings, investigations, audits, etc.;
– monitor, analyse and provide recommendations for improvement.

In justified cases the secrecy regime-division may be entrusted with the functions of providing protection of assets and personnel of the enterprise[7].

[7] Ibidem, p. 60.

2. *The company must ensure a strict regime of access to sensitive information.* This involves:

– admission to the premises where the information is kept confidential;

– careful selection of personnel working with confidential information. It is known that the fewer the people have access to such information, the more likely it is to remain secret. Therefore, a limited number of persons are required to have access to certain classified information.

In the case of dismissal of an employee who has been privy to a trade secret, he/she should sign a warning-obligation of non-disclosure of information that became available to him/her while working at the enterprise. The purpose of the choice of such a warning obligation of non-disclosure is to prevent the disclosure of a company secret by an employee and to create legal grounds for damages upon the disclosure of such information[8].

3. *For the protection of trade secrets when entering into business contracts and conducting business negotiations.*

In order to maintain the confidentiality of information transmitted to the partner, confidentiality agreements must be concluded between the parties.

The purpose of a confidentiality agreement is to protect all information for the negotiating party. The confidentiality agreement imposes on the receiving party the obligation to disclose it only to those employees who need this information to work (checks, tests, evaluations, adaptations) for the sake of which it is transmitted. In turn, these employees should be obliged not to disclose the information transmitted.

A confidentiality agreement is concluded to ensure that the party transmitting the information can be sure that the recipient of the information will keep it confidential from other parties and use it only for themselves and for certain specified purposes.

By referring to the definition of confidential information, one can obtain the necessary protection of the information transmitted.

Confidential information, which can be transmitted when concluding business agreements refers to any information or sensitive data that contains information of a technical nature, information on the development, marketing, sales, maintenance, specifications, cost, know-how of the enterprise and technological process, the availability of software of all types of media containing or disclosing such information and methods which become available in accordance with the provisions of the contract.

Any agreement involving the transfer of commercially valuable information includes two components on which negotiations should be based: 1) trust

[8] O. Vivchar, *Integrated management system of financial and economic security business under conditions of post-crisis recovery*, [w:] *National Economic Reform: experience of Poland and prospects for Ukraine. Part 3. Business management strategies*, Kielce 2016, s. 183–197.

in each other between all parties involved; 2) reasonable foresight of the information owner.

When negotiating the transfer of non-proprietary commercial information stored in the know-how mode, it is often necessary to conclude an option agreement.

The basic condition of the option agreement is the buyer's obligation to use the technical documentation and any information received from the seller only for the purpose of a thorough examination of the know-how, and to maintain confidentiality, taking necessary measures, including limiting relevant obligations. Upon any breach of this obligation, which results from the disclosure of know-how, the buyer will indemnify the seller for the losses. Equally important are the assurances of the seller to temporarily not offer the know-how to anyone else, and to enter into a know-how transfer agreement if the buyer decides to purchase after evaluating the feasibility and economic feasibility of using the know-how in his or her enterprise.

If the economic feasibility of concluding a transfer agreement is not established, the buyer will return to the seller the technical documentation and the information on the basis upon which the decision was made.

Obviously, both parties benefit from such an agreement. In particular, the seller can partially reimburse R&D expenses for a fee. As a rule, the price of the option contract is 20–30% of the value of the foreseeable future agreement and is not returned to the buyer in case of its cancellation of the license agreement. The information on the basis of which the buyer made the decision about the inappropriate acquisition of know-how helps the seller to make money, to improve its development.

The buyer also receives benefits. He has the right to evaluate his own capacity to innovate on more preferential terms than when the acquiring know-how. At the same time, the buyer receives samples of products that can be produced in the future and the necessary technical assistance of the seller. This is a valuable tool for studying the market for future goods. Such an agreement form, as an option contract, is convenient and beneficial for both parties.

4. *Introduction of appropriate labelling of media with confidential information.*

Trademark information may be differentiated by an enterprise by the degree of importance it is assigned.

Example:

1. For confidential information – the stamp "For Official Use Only" or "FOUO";

2. The enterprise, as a rule, establishes a three-level system of commercial secrecy, which is indicated by the following restrictive markings:

"Commercial Secret – Especially Important" ("CS-EI") "Commercial Se-

cret – Strictly Confidential" ("CS-SC") "Commercial Secret – confidential" ("CS-C").

The aforementioned marking shall be affixed to the information medium and, in the case of electronic storage of the information, the stamp shall precede the discovery of the information directly.

5. *Securing documents that contain business secrets.*

Documents containing a trade secret require a special storage mode. They should be stored in service rooms in cabinets (safes), securely locked and sealed storage.

Documents issued for the work of the executing staff are returned to the record-keeping service (secretary) or to the archives on the same day. In some cases, with the permission of the office manager or the person in charge of the enterprise's archives, documents may be stored with an employee for the length of time that he or she needs to complete the task, provided that they are fully supervised. In this case, the documents are not allowed to be left in the open and after work, they should be placed in a lockable cabinet or safe[9].

Documents containing trade secrets may not be taken outside the enterprise. Only when it is necessary to consult with specialists from other enterprises, which are territorially located in one settlement, the manager of the enterprise can give the workers written permission to bring these documents outside the enterprise.

Employees posted for industrial purposes to other settlements are prohibited from carrying documents containing the trade secret of the enterprise. Such documents shall be forwarded in advance for their intended purpose.

The presence of documents containing trade secrets should be reviewed annually by a commission specifically designated by the order of the head of the enterprise. The commission includes persons charged with keeping and storing these documents, as well as employees of the enterprise.

In archives and libraries where a large number of restricted documents are stored, their availability can be checked once every five years[10].

The results of inspections shall always be recorded in a protocol. If a loss of documents with the *TS* stamp or a disclosure of information containing a trade secret is detected during the check, this should immediately be reported to the management of the enterprise, the heads of the secret department and office management, as well as the security service of the company, if any.

To investigate a loss of documents or disclosure of information contained in them, a commission should be appointed by order of the head of the enterprise, regardless of the results of the commission's investigation, the order should be approved by the head of the enterprise.

---

[9] O. Zahoretska, *Osoblyvosti roboty z dokumentamy, shcho mistyat komertsiynu tayemnytsyu pidpryyemstva*, „Dovidnyk kadrovyka" 9 (2011), p. 44.

[10] Ibidem, p. 45.

6. *Application of technical means of protection of trade secrets.* Technical security measures are based on the use of various electronic devices and special programs that are part of the information processing system and perform security functions. For example, detectors, instruments securing wire communications, software, equipment for detecting recorders, acoustic and vibroacoustic noise, scanning means, detection of information leakage, installing special equipment to monitor the premises of the organization, etc.

7. *Increasing employee loyalty* includes properly organized work with company employees (personnel policy) and the use of material and moral incentives. One of the key tasks of a manager should be the properly organized selection of employees, the creation of a favourable social and psychological climate within the organization and the formation of "professional patriotism". By resolving the issues of social protection of employees, organization of recreation and leisure and medical services, the manager creates a favourable environment in a team that minimizes the likelihood of consciously causing harm to the enterprise by its employees. There is also no need to neglect the introduction of a system of material remuneration, the creation of opportunities for professional growth or staff involvement in decision making. Work conditions create guidance for their subordinates and depend on the state of the psychological atmosphere in the team, so when getting the maximum satisfaction from their work, employees are able to work most productively. The development of their interest in the success of the enterprise should be aimed at minimizing the turnover of personnel and at the same time – the loss of intellectual potential of the enterprise and the ability to disclose confidential information.

Thus, a business entity that intends to exercise its right to business secrecy must independently plan and organize all legal and organizational activities to enable the use and protection of information in commercial secrecy. The effectiveness of its protection will depend on the efforts made by the manager of such information. However, given the current realities, particular attention should be paid to issues that, according to research, have a greater impact on the protection of commercially valuable information. First, it is the continuous development of information technologies that enable the rapid copying and dissemination of valuable information. Often, such actions take place without the owner's permission. Therefore, it is important to pay particular attention to the application of trade secrets, using reliable information systems, licensed software, etc. Secondly, more attention should be paid to increasing employee loyalty by taking the right steps to improve productivity, secure footage, reduce turnover, and minimize the risk of trade secrets.

References

Chikin, S., Chernenko V., *Upravlinnya komertsiynoyu tayemnytseyu na pidpryyemstvi: diyi orhanizatsiynoho, tekhnichnoho ta psykholohichnoho kharakteru*, „*Teoriya i praktyka intelektualnoyi vlasnosti*" 5 (2011).

Lokotetska O., *Systema zakhystu komertsiynoyi tayemnytsi pidpryyemstva*, „Biznes Inform" 12 (2011).

Vivchar O., *Integrated management system of financial and economic security business under conditions of post-crisis recovery*, [w:] *National Economic Reform: Experience of Poland and prospects for Ukraine*. Part 3. *Business management strategies*, Kielce 2016.

Vivchar O., *Management system interpreting financial and economic security business in economic processes*, „Mathematics education" (Social Sciences) vol. 11 (2016), no. 4.

Zahoretska O., *Osoblyvosti roboty z dokumentamy, shcho mistyat komertsiynu tayemnytsyu pidpryyemstva*, „Dovidnyk kadrovyka" 9 (2011).

Streszczenie

Procedury organizacyjne i prawne stosowane w celu zapewnienia podmiotowi gospodarczemu bezpieczeństwa i ochrony: podejście oparte na wiedzy na temat bezpieczeństwa

Słowa kluczowe: informacja, tajemnica handlowa, ochrona tajemnicy handlowej, zabezpieczenie tajemnicy handlowej, podmiot gospodarczy, wzmocnienie bezpieczeństwa gospodarczego

W warunkach transformacji społeczeństwa ukraińskiego i tworzenia innowacyjnej gospodarki, stosowanie reżimu "tajemnicy handlowej" do informacji, które mają wartość handlową dla podmiotu gospodarczego, jest jedną z priorytetowych kwestii w zakresie wzmacniania bezpieczeństwa gospodarczego. Należy jednak zauważyć, że procedura kwalifikowania informacji jako tajemnicy handlowej jest złożonym, wielowymiarowym zjawiskiem, wymagającym zastosowania środków prawnych i organizacyjnych w celu ochrony i bezpieczeństwa tajemnicy handlowej podmiotu. Na tej podstawie artykuł jasno określa etapy procedury kwalifikowania informacji jako tajemnicy handlowej. Analizie poddano nowoczesny, skuteczny system bezpieczeństwa i ochrony informacji, który ma wysoką wartość handlową dla zwiększenia bezpieczeństwa ekonomicznego podmiotu.

Dlatego też skuteczność ochrony cennych informacji handlowych będzie zależeć od wysiłków podejmowanych przez zarząd. Jednakże, biorąc pod uwagę obecne realia, szczególną uwagę należy zwrócić na kwestie, które mają wpływ na ochronę cennych informacji handlowych: stały rozwój technologii informacyjnych oraz wzmacnianie lojalności pracowników.