UDC 330.5; 343.72
DOI 10.31733/2786-491X-2022-1-96-107

Lyudmila RYBALCHENKO©
Ph.D. (Economics),
Associate Professor
(Dnipropetrovsk State University of Internal Affairs),
Ukraine

Alexander KOSYCHENKO©
Ph.D. (Technics),
Associate Professor
(Dnipropetrovsk State University of Internal Affairs)
Ukraine

Illia KLINYTSKYI©,
Ph. D. (Law)
(*Silesian University),*
Poland

ENSURING ECONOMIC SECURITY OF ENTERPRISES TAKING INTO ACCOUNT THE PECULIARITIES OF INFORMATION SECURITY

Abstract. Protection of important interests of the population and the state from unauthorized access, protection of confidentiality and availability of information, is information security. A number of Laws of Ukraine have been created in the domestic legislation on information security, including the Law of Ukraine "On Information" and the Law of Ukraine "On Protection of Information in Information and Telecommunication Systems". These laws regulate the legal framework for information security and information activities, among which the subjects of information security are the participants in these processes, the owners of information are responsible for ensuring the interests of the population and the state. All information is generated, stored, processed and transmitted using appropriate information systems, technologies, computers, software, etc. In turn, computers and software can suffer from threats caused by threats from the Internet, network, mail, and so on. To ensure effective economic security of enterprises, it is important to control the internal mechanism of functioning, monitor economic performance indicators, and make effective management decisions.

© Rybalchenko L., 2022
ORCID iD: https://orcid.org/0000-0003-0413-8296
luda_r@ukr.net

© Kosychenko, A., 2022
ORCID iD: https://orcid.org/0000-0002-6521-0119
kosichenko-inform@meta.ua;

© Klinytskyi I., 2022
ORCID iD: https://orcid.org/0000-0002-7401-8233
illia.klinicki@gmail.com

***Keywords**: fraud, business risk, competition, information security, regulatory framework. combating fraud, national security, economic security of the state*

Introduction. Security is defined by many components, including personnel working with it, means of communication, information leaks, removal or intentional damage, and so on. An important element of information system protection is access to it, which is related to production management, finance, economics, inventions and more. One of the aspects of information security is the confidentiality of information provided by the use of protection systems of modern information systems.

Working with payment information systems, electronic money, has its own means of access through passwords, i.e. there is a check of work on user identification. It is a means of security with personal data of clients, registered in banking or financial institutions. Banking users are monitored via the Internet or information systems, which is dangerous.

Analysis of the regulatory and legal support of the information field of the enterprise offers a strategy for its information security. The main focus is on the protection of variable information as the most important for information security. There is a need to take into account the components of information security based on a systems approach.

Businesses face many threats. Most often, these are threats from competitors or criminal structures. They are often caused by political and legal instability, intensification of competition, illegal use of hardware and software, etc. Therefore, in the framework of enterprise management, in addition to the main functions, information security is assigned to managers.

Analysis of recent research and publications. As you know, the economic security of the enterprise – a complex, multi-vector concept. The information component occupies an important place in it. Information security is the ability of the company's staff to protect information resources and flows from threats of unauthorized access to them.

Analysis of the organization of the information space of the enterprise, as a rule, attention is paid in the works of various researchers, but mainly from the angle of economic efficiency of the enterprise (Rybalchenko, L., & Kosychenko, O., 2019). The main amount of information of the enterprise circulates within its organizational, legal and physical boundaries. Obtaining by criminal or other structures information necessary to harm the company, blackmail, or for corrupt practices, such as in the form of a “roof”, can be done through the objects of the information environment of the company from various channels and sources. These are 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 competitive or criminal structures.

The purpose of the work is to study the information (economic) security of enterprises in the world and the application of the mechanism of regulatory and legal support of the information protection system at the enterprise.

Formulation of the main material. In recent years, the legal framework for the information protection system at the national level has improved significantly. This was reflected in the adoption by the Ukrainian leadership of a number of laws (d’Agostino G., et al., 2019 – Bank S., et al., 2018) and by-laws

(Varnaliy, Z., et al., 2016) concerning the regulation of the creation, use, transfer and storage of information and copyrights, the procedure for licensing activities in the field of information protection, and the like.

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

At the same time, in addition to laws and other state regulations, the legal support of the system of protection of confidential information at the enterprise should include a set of internal regulatory and organizational documentation.

It should be noted that all these documents, depending on their main regulatory or legal purpose, indicate the requirements, rules or regulations to ensure the required level of information security in the enterprise or its departments, aimed primarily at staff and management.

Legal support makes it possible to resolve many controversial issues that inevitably arise in the process of information exchange at various levels – from language communication to data transmission in computer networks. In addition, a legal system of administrative measures is formed, which allows to apply penalties or sanctions to violators of the internal security policy of the enterprise, as well as to establish clear enough conditions to ensure the confidentiality of information used or formed in cooperation between economic entities. In this case, the parties who do not comply with these conditions are liable within the framework provided for 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. As you know, any management is a continuous 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 (own) 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 itself (primarily on management). The fact is that the company's own information field is formed by internal sources of information, the number of which is limited. The number of types of external information and its sources is very significant (Rybalchenko, L., & Kosychenko, O., 2019).

On the other hand, the information that provides the process of decision-making and management functions in a commercial organization, it is advisable to divide by type into conditionally constant and variable. Conditionally constant information includes information that is virtually unchanged over a long period (for an infinitely large number of control cycles). It includes both normative-reference and scientific-reference information. Regulatory information is needed to make decisions and monitor their implementation. It includes various normative and reference data, control indicators, standards.

This information rarely changes. Regulatory information is usually the most fully systematized, presented in a form that is convenient to work with and mandatory. Correction or cancellation of these documents is only at the direction of higher authorities. Scientific reference information is information

obtained from scientific and technical literature, regulatory and technical documentation, various bulletins, news releases, etc.

Variable information, first of all, reflects the change of criteria of management and work of divisions, and also the changes brought 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 must be achieved and maintained; about 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, rules, 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 a summary of costs, balances, shortages of materials and components, shortcomings of technological documentation, downtime. These reports on deviations in the processes of achieving the goal of management are necessary to create and implement corrective actions of management. In addition, it is a set of data that characterize 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, on energy, on the position of vehicles, etc.

Reporting information includes various summaries of the status of their units, the results of production tasks, the state of supply and sales at a particular time. Taking into account the inclusion of the planned information of the enterprise in the variable, in the first place in full is the variable information.

It is clear that to achieve completeness and comprehensiveness of information protection only 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 types of relationships in the absence of the environment to which these rules apply.

In other words, 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 functioning, develop a set of consistent and coordinated activities, and identify its components and subsystems. For these purposes, the organizational system of information protection.

The organizational system of information protection is a set of organizational and organizational and technical measures to ensure information security at the enterprise, the creation of a common security policy and control of its effectiveness. Implementation of the project to create a comprehensive information security system should be carried out in stages.

The development and implementation of the system must be preceded by a thorough study of information resources of the enterprise and the presentation of justifications and arguments in favor of creating a protection system. 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 information security violations, failures of programs, hardware and processing systems, as well as the transfer of information, its unauthorized receipt, modification (destruction) and dissemination are established.

In other words, the information-functional model of the enterprise is formed and the sketch scheme of system of protection 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 according to the 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 information security system (ISS), in the process of which the most vulnerable areas of information exchange channels are determined, the schedule of organizational and organizational-technical measures is made, the calculation of spent resources is made, the general list of employees (specialists, employees and heads) involved in system implementation and divisions is made. interaction of structural elements and parts of the enterprise at the stage of creating an ISS.

Third, taking measures to implement and implement the ISS. At this stage, the following can be done: compiling a list of dedicated premises where closed events are held or critical information is circulating; identification of officials authorized to exercise control and operational management of the ISS; advanced 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 ISS the following organizational measures should be carried out constantly: registration of works with the use of information constituting a trade secret; registration of all events related to the development, use, transmission of information containing confidential information, and making changes to protected information resources; keeping records of documentation and media of confidential information; responding to the manifestation of destabilizing factors in order to prevent or reduce the effect on information; delimitation of rights of access to protected information resources.

Fifth, measures are being taken to monitor 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 the rules of security policy, analysis of the protection system, making decisions to improve hardware and systems, organizational construction and security policy.

In addition, regular preventive interviews should be conducted with company personnel to prevent violations of security policy. These conversations are necessary to raise the level of awareness of employees in relation to the problem of information security to the level of understanding by each of them of 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.

The formation of the concept of economic security of the enterprise includes the following stages: analysis of the impact of internal and external factors on the state of economic security of enterprises; components and means of ensuring and principles of economic security of enterprises; assessment of the current state of the level of economic security of the enterprise; development of a set of measures and tools to ensure the economic security of the enterprise. Since the object of guaranteeing economic security is a stable economic condition of the enterprise, which, in turn, is a complex and multifaceted mechanism, the effective guarantee of its protection should be implemented through a comprehensive approach to managing this process. An integrated approach involves taking into account the management of the object of all its main aspects, and the elements of the managed system are considered only in the totality of integrity and unity.

The main content of the concept of safe operation is the formation of the foundations of the enterprise management system aimed at creating conditions for stable operation and systematic satisfaction of the enterprise's security needs at all stages of its life cycle – from birth to independent or forced liquidation (bankruptcy).

The basic principles of operation of the management system within the concept of safe operation of the enterprise are as follows:

1. Unconditional satisfaction of both the general needs of the enterprise and its employees.
2. Flexibility of the structure of economic potential, which ensures its stable functioning in the present and safe operation in the future.
3. Constant expectation of threats, both internal and external.
4. The ability of the management structure to respond quickly to threats and effectively use existing opportunities.
5. Effective information support of planning and use of enterprise strategies.
6. Public awareness of the importance of creating favorable conditions for the company to take measures to maintain its own economic security.

The main threats that hinder economic security are: divergence of economic interests of enterprises, weak motivation of employees to prevent threats and their lack of interest in the final results of the enterprise. In these conditions, the company is forced to adapt to the external environment without backlash (Rubalchenko L., & Ryzhkov E., 2019).

Therefore, its capabilities remain to control the internal mechanism of operation, monitoring of economic indicators of financial and economic activities and effective management decisions. In this situation there is a need to form a concept of economic security of enterprises for this based on the analysis and synthesis of existing scientific views systematized the main functional elements of economic security of the enterprise, which include: financial, technical, intellectual, political, legal, informational, legal and social.

Fraud is a serious problem faced by organizations of all types, sizes and industries. It manifests itself in different ways, but in general it is divided into three categories: misappropriation of assets, corruption and fraud with financial statements. For the last 20 years, economic crimes and fraud have remained one

of the world's leading economic crime issues. The processes taking place in the field of financial and economic relations lead to the fact that the state is increasingly losing control over the economy and finance.

According to the results of the World Survey of Economic Crimes and Fraud in 2018, 48 % of Ukrainian organizations suffered from cases of economic crimes and fraud (in 2016 – 43 %). For comparison, the world average for economic crime is 49 %. One of the main types of economic crimes for many years is bribery and corruption, which are negatively affected by 73 % of Ukrainian organizations that have become their victims (Rybalchenko, L., & Kosychenko, O., 2019).

We will conduct research on economic crimes and fraud and assess their impact on businesses around the world. In 99 countries, more than 5,000 respondents, the amount of losses in 2020 amounted to more than 42 billion USA dollars.

In Figure 1 cited Crimes: frequency of overall experience. It was the biggest in the world Customer Fraud (35 %), Cybercrime (34 %), Asset Misappropriation (31 %), Bribery and Corruption (30 %), Accounting/Financial Statement Fraud (28 %) and other (Figure 1).

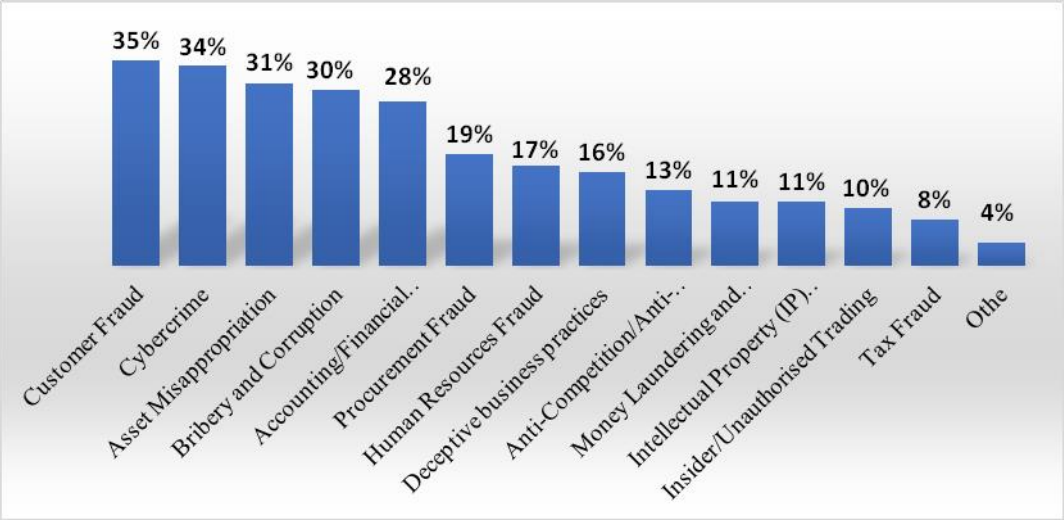

Figure 1 – Crimes: frequency of overall experience, 2020
Source: built by the authors according to the data (PWC Ukraine "World Economic Crimes and Fraud Survey 2020. Removing fraud from the shadows' ")

51 % of respondents in Ukraine suffered from fraud in 2020, this indicates that this figure is higher than the global average (47 %), and there has been an increase compared to 2019 (48 %). More than 1/3 of respondents in Ukraine suffered from 2-5 fraud incidents in 2020. Comparing the dynamics of fraud in Ukraine and the world, it should be noted that the largest and most popular types remain: misappropriation of property, corruption, customer fraud, cybercrime, and procurement fraud (Figure 2).

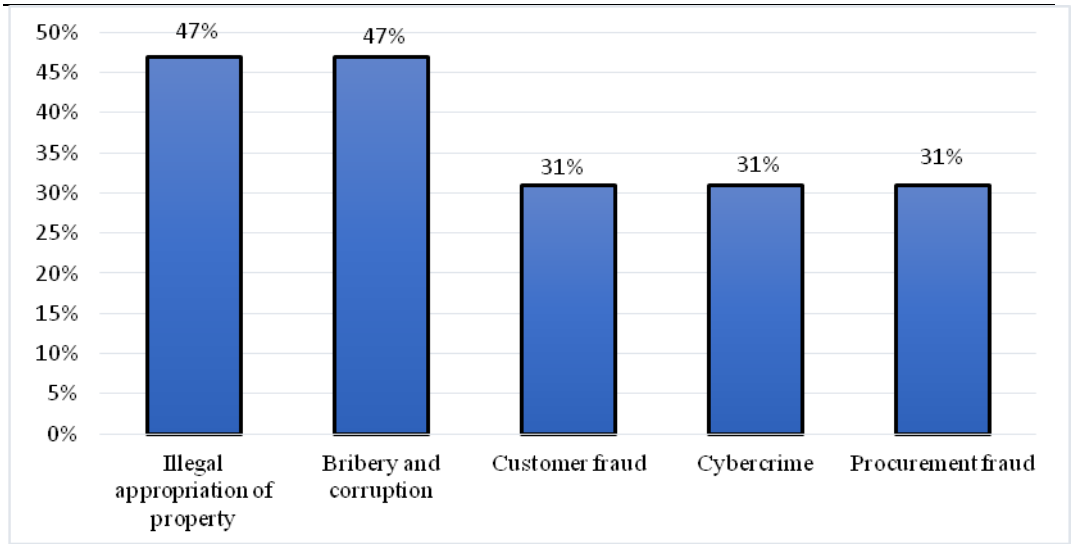

Figure 2 – The most popular types of fraud in 2020
Source: built by the authors according to the data (PWC Ukraine "World Economic Crimes and Fraud Survey 2020. Removing fraud from the shadows' ")

For the three types of property fraud, unfair competition and procurement fraud were the most significant for domestic companies in terms of financial losses (Figure 3). Of these types of fraud, the share of misappropriation of property was the most unprofitable for 19 % of companies, which is 42 % of these types of losses. Unfair competition and procurement fraud account for 29 % of losses for companies for 29 % of losses. Almost two-thirds of companies have already suffered losses from these types of fraud.

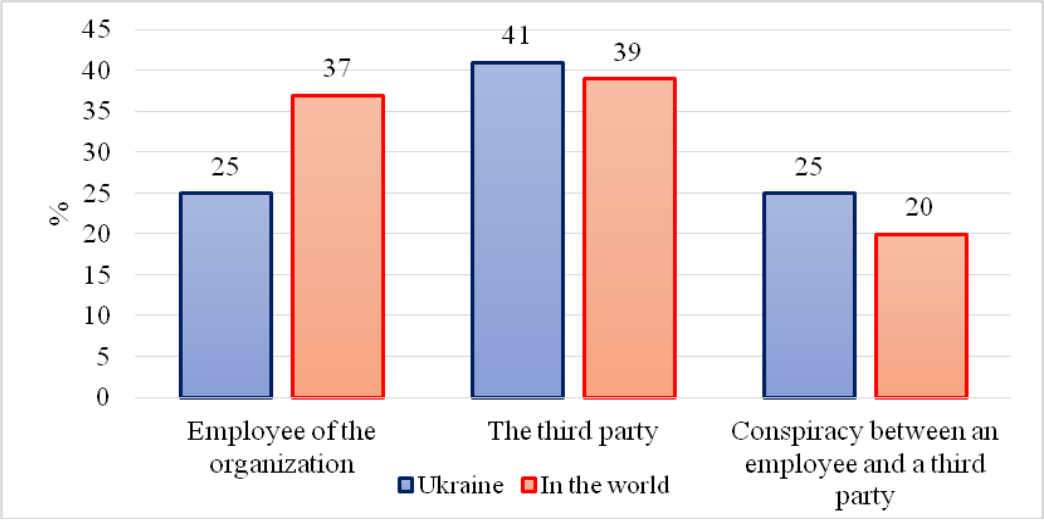

Figure 3 – The most unprofitable types of fraud in 2020
Source: built by the authors according to the data (PWC Ukraine "World Economic Crimes and Fraud Survey 2020. Removing fraud from the shadows' ")

The largest factors of fraud in enterprises (Figure 4) are the "third party", whose share in Ukraine is 51 % (41 % of enterprises), in the world 49 % (39 % of enterprises). Fraud caused by employees of domestic enterprises, their share is 40 % (25 % of enterprises), in the world 60 % (37 % of enterprises) Conspiracy between an employee and a third party in Ukraine their share is 56 % (25 % of enterprises), in the world 44 % (20 % of enterprises).

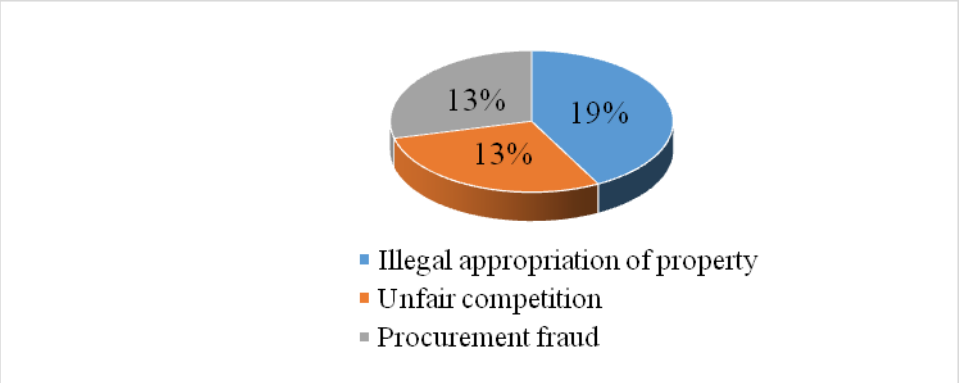

Figure 4 – Factors of enterprise fraud in 2020
Source: built by the authors according to the data (PWC Ukraine "World Economic Crimes and Fraud Survey 2020. Removing fraud from the shadows' ")

Almost half of the respondents in Ukraine do not conduct at all or only informally check and constantly monitor the integrity of their counterparties.

The cost of fraud for businesses in 2020 was as follows (Figure 5)

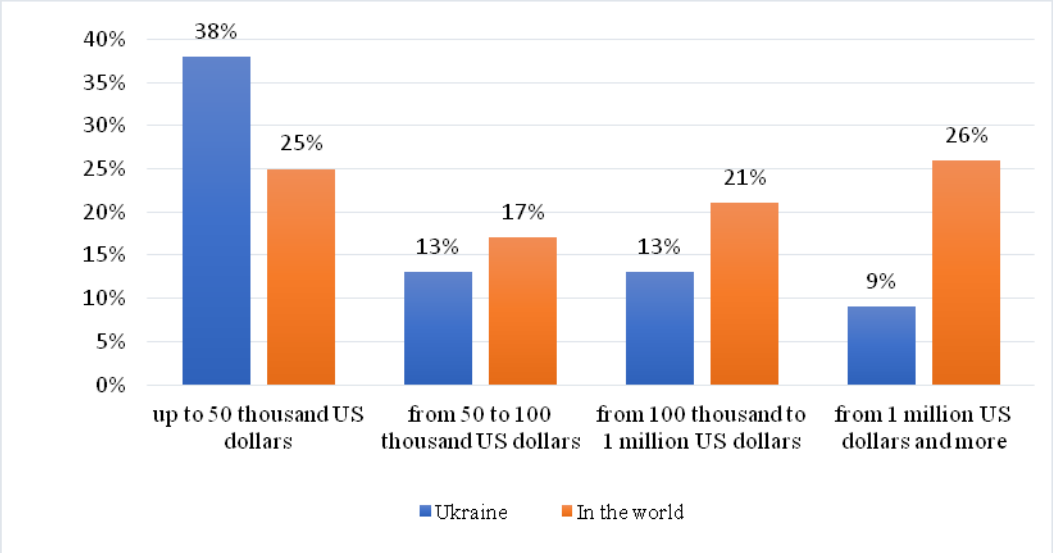

Figure 5 – The cost of losses of enterprises in 2020
Source: built by the authors according to the data (PWC Ukraine "World Economic Crimes and Fraud Survey 2020. Removing fraud from the shadows' ")

In Ukraine in 2020, 38 % of enterprises suffered losses from fraud (Figure 5), the amount of which amounted to 50 thousand US dollars, which is more than 25 % in the world. For 13 % of domestic enterprises, losses from fraud ranged from 50 to 100 thousand US dollars, in the world for 17 % of enterprises. Another 13 % of Ukrainian enterprises suffered losses ranging from 100 thousand to 1 million US dollars, in the world 21 % of enterprises suffered. The largest losses of 1 million US dollars and more fraud were caused by 9 % of Ukrainian enterprises, in the world 26 % of enterprises suffered such losses.

Of all Ukrainian companies, only 59 % investigated their worst case of fraud, and a third reported it to the supervisory board. Only 3 % of respondents in Ukraine hired an external forensic expert in response to their worst case of fraud, compared to 20 % of respondents in the world. Every fourth organization in Ukraine does not have a special risk management program, 22 % of respondents in Ukraine have not conducted any risk assessment in the last two years (PWC Ukraine "World Economic Crimes and Fraud Survey 2020. Removing fraud from the shadows' "). On average, six fraud cases were reported per company.

Conclusions. 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 entry into 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 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.

Information security of the enterprise should be provided, first of all, by legal methods of protection. At the same time, an important role in improving the efficiency of the information protection system at the enterprise is played by its organizational component, the creation of protection of corporate information from competitors and criminal organizations.

Professional fraud can lead to financial losses, court costs, which can lead to the closure of the organization. Only strategic planning can significantly reduce the risk situations in enterprises that have arisen as a result of fraud. Company policy should be aimed at the use of modern means to prevent fraud.

Thus, an important place in the process of enterprise security is the formation of the concept of economic security of the enterprise, which includes means and principles of economic security of enterprises, tools and factors influencing the economic security of enterprises, the main elements of economic security.

We offer the following steps to combat fraud:

1. Identifying risks and applying effective measures.

2. Effective management, qualified experts and monitoring of anti-fraud information technology

3. Analysis of the causes of fraud.

4. Conducting investigations into the identified consequences of fraud.

5. The need to inform law enforcement agencies about fraud at the enterprise.

6. Increasing the use of effective mechanisms for internal control of fraud prevention in the enterprise.

7. Introduction of modern advanced technologies to protect information from criminal activity.

Conflict of Interest and other Ethics Statements

The authors declare no conflict of interest.

References

Asghari, M. (2017). "National security and economic growth". *Iranian Economic Review, 21*, 4, pp. 905-924, https://ier.ut.ac.ir/article_64087.html.

Bank S., Sekerin V., Gorokhova A., Nikolaykin N., & Shcherbakov, A., (2018). "Risks and Threats Posed to a Company's Economic Security", *International Journal of Engineering &Technology* (IJET), *7*, pp. 210-215.

d'Agostino, G., Dunne J. P., & Pieroni, L. (2019). Military Expenditure, Endogeneity and Economic Growth. *Journal Defence and Peace Economics, 30*, pp. 509-524.

Levit, M. (2010). *Analyst in Public Finance, Government and Finance Division, National Security Strategy*, 34 p.

Navarro, P. (2018). *Why Economic Security is National Security, RealClear*. Politics, https://www. realclearpolitics.com/articles/2018/12/09/why_economic_security_is_national_security _13887 5.html.

PWC Ukraine "World Economic Crimes and Fraud Survey 2020. Removing fraud from the shadows' ", https://www.pwc.com/ua/gecfs/ua.

Report To The Nations. 2020 Global Study on Occupational Fraud and Abuse, https: // www.acfe.com/report-to-the-nations/2020/#download.

Rubalchenko L., & Ryzhkov E. (2019). Ensuring enterprise economic security. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. Special Issue, 1*, pp. 268-271. (in Ukrainian).

Rybalchenko, L., & Kosychenko, O. (2019). Features of latency of economic crimes in Ukraine. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. *Special Issue, 1*(102), pp. 264-267. (in Ukrainian).

S. Onyshchenko, O. Maslii, B. Ivanyuk (2019). *The Impact of External Threats to the Economic Security of the Business. 7th International Conference on Modeling, Development and Strategic Management of Economic System (MDSMES 2019).*

Tymoshenko, O. & Oleshko, A. (2018). State policy of economic security of Ukraine in conditions of global instability. *Ekonomika ta derzhava, 9*, pp. 30-33. DOI: 10.32702/2306-6806.2018.9.30.

Varnaliy, Z. & Onishchenko, S., & Masliy A. (2016). Threat prevention mechanisms of Ukraine's economic security. *Economic Annals-XXI, 159* (5-6), pp. 20-24. DOI: http://dx.doi.org/10.21003/ea.V159-04. (in Ukrainian).

Людмила РИБАЛЬЧЕНКО, Олександр КОСИЧЕНКО, Ілля КЛИНИЦЬКИЙ

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ З УРАХУВАННЯМ ОСОБЛИВОСТЕЙ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. Захист важливих інтересів населення та держави від несанкціонованого доступу, захист конфіденційності та доступності інформації, представляє собою інформаційна безпека.

У вітчизняному законодавстві щодо інформаційної безпеки створено низку законів, серед яких Закон "Про інформацію, інформатизацію і захист інформації". Цим законом регламентовано правові основи щодо інформаційної безпеки та інформаційної діяльності, серед яких суб'єктами інформаційної безпеки є самі учасники цих процесів, власники інформації несуть відповідальність за забезпечення гарантій інтересів населення та держави.

Суб'єктами інформаційної безпеки є інтереси тих, хто використовує інформаційні системи та засоби щодо захисту і збереження інформації від можливих загроз. Питання інформаційної безпеки пов'язано з інформаційними технологіями, які використовуються для забезпечення інформаційної безпеки.

Захист інформаційної безпеки полягає не лише у застосуванні несанкціонованого доступу до інформації, а й використанні відповідних методів щодо її безпеки та захисту.

Уся інформація формується, зберігається, оброблюється та передається з використанням відповідних інформаційних систем, технологій, комп'ютерів, програмного забезпечення, тощо. У свою чергу, комп'ютери, програмне забезпечення можуть потерпати від загроз, які спричинено через небезпеки, що потрапили через інтернет, мережу, пошту, тощо.

Для забезпечення ефективної економічної безпеки підприємства важливим є контроль за внутрішнім механізмом функціонування, моніторинг економічних показників діяльності, прийняття ефективних управлінських рішень.

Ключові слова: *шахрайство, підприємницький ризик, конкуренція, боротьба із шахрайством, інформаційна безпека, національна безпека, нормативно-правова база, економічна безпека держави.*

Submitted: 20.09.2021
Revised: 26.01.2022
Accepted: 21.02.2022