DOI: 10.15276/ETR.04.2021.3
DOI: 10.5281/zenodo.6536523
UDC: 330.47:004.9
JEL: F63, L86, M15

INFORMATION PROTECTION OF BUSINESS PROCESSES IN THE DIGITAL ECONOMY CONDITIONS

ІНФОРМАЦІЙНИЙ ЗАХИСТ БІЗНЕС-ПРОЦЕСІВ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Tetiana L. Budoratska
Odessa Polytechnic State University, Odesa, Ukraine
ORCID: 0000-0001-9114-295X
Email: tatyana.budoratskaya@gmail.com

Hanna O. Kovalova
Odessa Polytechnic State University, Odesa, Ukraine
ORCID: 0000-0003-0251-7946
Email: kovalyova.anna17@gmail.com

Iryna B. Trofymenko
Odessa Polytechnic State University, Odesa, Ukraine
ORCID: 0000-0001-9236-9961
Email: irina.trofimenco@gmail.com

Received 14.08.2021

Будорацька Т.Л, Ковальова Г.О., Трофименко І.Б. Інформаційний захист бізнес-процесів в умовах цифрової економіки. Оглядова стаття

Дана стаття присвячена актуальній в умовах цифрової економіки проблеми інформаційного захисту бізнес-процесів підприємства. В роботі запропоновані функціональні моделі підсистем, які формують комплексну модель захисту. Аналіз структури бізнес-процесів дозволив сформувати необхідну систему показників інформаційної безпеки, які безпосередньо впливають на організацію всієї структури захисту як від зовнішніх так і від внутрішніх загроз.

Наведено математичні формули для визначення узагальнюючого показника оцінки якості структури захисту і коефіцієнт захищеності бізнес-процесу. Подано характеристику значень комплексного показника інформаційної захищеності та їх зв'язок із загальним станом безпеки підприємства. Визначено варіанти оцінок захисту, їх взаємозв'язок з моделями на рівні комплексної оцінки.

Ключові слова: бізнес-процес, інформаційна безпека, цифрова економіка, цифровизация, шифрування/дешифрування даних

Budoratska T.L., Kovalova H.O., Trofymenko I.B. Information Protection of Business Processes in the Digital Economy Conditions. Review article.

This article is dedicated to the problem of information protection of an enterprise business processes, which is relevant in the digital economy. The research paper proposes functional models of subsystems that form an integrated protection model. The analysis of the business processes structure made it possible to form the necessary system of information security indicators that directly affect the entire structure organization for protection from both external and internal threats.

Mathematical formulae are given for determining the generalized indicator for assessing the quality of the protection structure and the security factor of the business process. The characteristics of the complex indicator values of information security and their relationship with the general status of enterprise security are presented. The options for assessing protection, their relationship with models at the level of integrated evaluation are determined.

Keywords: business process, information security, digital economy, digitalization, data encryption / decryption

The purpose of the Doctrine of Information Security of Ukraine is to clarify the formation and implementation principles of state information policy.The doctrine is based on the principles of respect for human and civil rights and freedoms, respect for a person's dignity, his/her legitimate interests protection, as well as the legitimate interests of society and the state, ensuring Ukraine's sovereignty and territorial integrity [1].

The state policy priorities in the information sphere should be to ensure Ukraine's information space protection and development. The country's enterprises and organizations are no less interested in ensuring information security. This requires the security policy development based on the information threats analysis, so that within the allocated budget were provided certain levels of confidentiality, integrity and availability of the enterprise information resources. This is in line with the trends of the fourth industrial revolution, which was called Industry 4.0. Despite the fact that Ukraine later entered the Industry 4.0 zone, but nevertheless it must determine the future growth, Ukrainian enterprises prosperity and their competitiveness, bring the country to a new economic and industrial levels [2].

The emphasis on digitization and digital transformation has been an area of intense global research, but the pandemic has accelerated efforts to make more effective strategies available to realize all the benefits of Industry 4.0. The emphasis has shifted sharply from digitization (data conversion into digital form) to digitization, which focuses on the "organizational process" or "business process" of

technological change in industries, organizations and markets [3]. Technological productions digitalization allows to create new production processes applying key technological tendencies of Industry 4.0 and its design principles. Particular attention should be paid to some key aspects, such as the business process development and optimization, effective change management protocols, processing of large data sets and their protection. The flow of huge data sets to and from the organization over the Internet makes information and computer data protection one of the main elements of Industry 4.0. From this perspective , the research conducted and described in this article relates to the information protection of the enterprise main business processes.

Analysis of recent researches and publications

Unimpaired organization of modern domestic enterprises is impossible without the active use of digital technologies. The problems of digital economy development, the need to process large data amounts, business processes optimization from the standpoint of digitalization are the object of scientific research by both foreign and domestic scientists. In their works they focus on such important key aspects of digitalization as the information technology aspect, digital maturity, when data and information serve as business assets and tools for creating digital services, expanding the use of digital platforms and transformations, expanding business processes for digital business. Digitization is considered as a stage of creating opportunities and conditions for the productive work of business using the knowledge and ideas necessary for the enterprise.This is reflected in the scientific works of S. Khan, J. Bloomberg, J. Mancini, J. Mueller, A. Frank, L. Frolova, O. Hrybinenko, D. Semylitko [3-10]. Among the domestic scientists involved in the business process development and modeling, we should mention K. Bahatska, M. Dyba, Z. Sokolovska, O. Husiev, S. Lehominova [11-14].

Issues of ensuring information security and information structure security of the enterprise business processes operation acquire special importance [15]. T. Kliebanova, V.L. Buriachok, V.B. Dudykevych, M.P. Karpinskiy, O.S. Petrov, V.O. Khoroshka, O. Stelmashonok devoted their works to the economic security, development and functioning of information protection systems. The topic of business processes security with the increased use of computer networks, the Internet is increasingly in need of attention. The status of the information protection structure of business processes characterizes the enterprise economic status , the market competitiveness status.

The aim of the article is to determine the information security system objects, to develop the proposal to create a model of information security for business processes, the system formation of information security indicators.

For this purpose it is necessary to carry out the analysis of the generalized information structure of business processes, probable dangers, to define the properties providing protection against the basic threats.

The main part

The digital connection between developers, workers and physical production facilities can and should provide significant benefits in terms of production growth. In order to ensure communication, it is extremely important to establish a clear interface between different business processes, correctly identify the necessary technologies and establish information security and protection against threats [10].

Creating a business system is impossible without a mechanism that includes protecting information resources as a part of the enterprise potential. Management system protection means supporting and protecting business processes. Well-established process work and optimization of functional components are the keys to economic and technological advantages. The protection of the information base and resources is based on the data availability, integrity and confidentiality.

Risk and threat analysis has shown that the information structure must have the data security used in business processes and the ability to provide protection against unauthorized access, using commercial, business or technological information [4]. Organization business process information protection infrastructure should be carried out in accordance with the principles of systemicity, complexity, reasonable sufficiency, flexibility of management and ease of applying protective measures and means.

The structural protection model of business process information should reflect the basic approaches to the the security system organization in the enterprise and independently represent the business process that reflects access control, data integrity, data encryption.

The information protection system objects in the designed model taking into account the responsible executors are planned:

— access control subsystem;
— registration and accounting subsystem;
— integrity subsystem;
— cryptographic subsystem.

Based on the formulated principles, taking into account the requirements for the information protection infrastructure of business processes, a conceptual model has been developed, which can be presented for clarity in the form of functional parts. The Figure 1, presents a variant of the information protection model of business processes, including these functional models-subsystems. Any objects, subjects or systems that interact with the system being modeled from the outside can be present as performers. They are called actors. Each variant of the model defines a set of actions without details to represent specific uses, actors and relationships between these elements.

The access management function model controls access to information systems, its components, to information resources, and also carries out users' identification and authentication, often in a cryptographic way. Actors are business applications,

external programme applications, staff associated with the assigned object. Due to the possibility of information being stolen and destroyed, possible violators and hackers are present as actors.

The registration and accounting function model is represented by a components list of the function and the main executor i.e. the information security system (ISS) administrator. The data integrity model involves several performers: the ISS administrator and the personnel responsible for the physical security of the information system (IS). Having one function involves performing different components by different actors.

The cryptographic function involves both data encryption and decryption. These model actors are: ISS administrator and cryptographic tools. The model provides for classification (division) by confidentiality and encryption of the required information. From the viewpoint of information protection infrastructure and the possible threats nature, the main function should contain components characterized by the following security factors: from unauthorized access (UAA) to information; from interception (theft) of information; from accidental obstacles (failures); from interference in the business process.

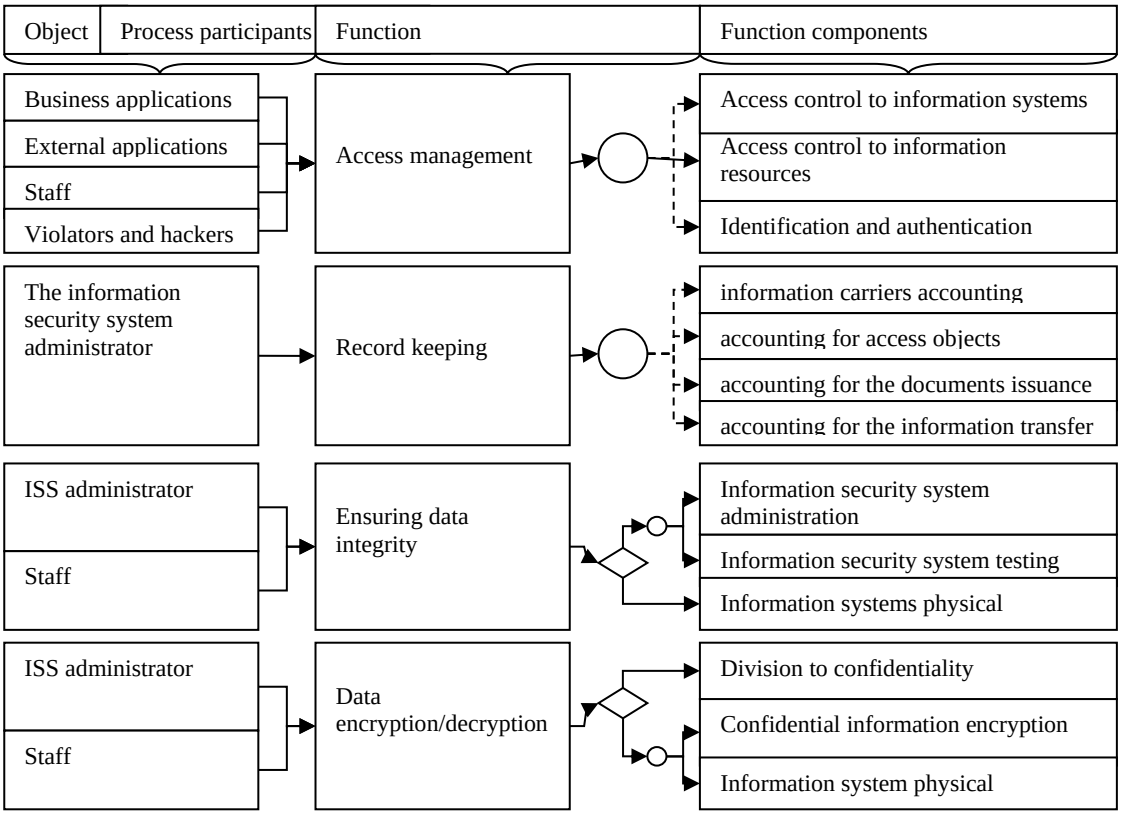

Figure 1. The Comprehensive Model of Business Process Information Protection System. Models of Functional Subsystems

Source: authors' own development

On the other hand, in order to implement the main function of providing protection taking into account possible threats, the information protection system must have certain properties. Mathematically, it can be formulated as follows:

$$R = \sum_{i \in N} K_i \times r_i, \quad (1)$$

$$\sum_{i \in N} K_i = 1, \quad (2)$$

where:

R – is the generalized indicator of quality assessment for the information protection system (generalized coefficient of security, which shows the repulsion level of attacks on the whole set of possible threats) ;

r_i – is the *i*-th private indicator of quality assessment of the information protection structure (private security factor, which shows what part of the threat attacks of the i-th type is reflected), $0 \le i \le 1$;

N – many private indicators of quality assessment are given in the generalized indicator;

K_i –is the weighting factor of the *i*-th private quality indicator in the additive convolution.

The security factor of business processes Rc can be represented by the formula:

$$R_c = 1 - \frac{\sum_{b \in B} p_b \sum_{i \in N_b} \lambda_{ib} t_b (1 - r_i)}{\sum_{b \in B} p_b \sum_{i \in N_b} \lambda_{ib} t_b}, \quad (3)$$

where:

N_b – is the number of the most probable information threats for the *b-th* business transaction;

Ri – is the protection coefficient against the *i-th* threat;

λib – is the intensity of the of attacks flow of the *i-th* type of threats to the *b*-th business transaction(i $N \in b$), for i $N \notin b$ $\lambda_{ib} = 0$;

tb – is time of the *b-th* business operations execution;

B – is the number of business transactions in the business process;

pb – is the probability of doing the *b* business in the business process.

The optimization task involves using a model to minimize the cost of information security structure (ISS) and a model to maximize the level of information assets security.

These models also have a mathematical representation. In the framework of this article, their description is omitted.

The choice of the optimal system of information protection should be based on many options. It is reasonable to assume that the increase in the cost of information protection is accompanied by an increase in the quality of protection. In the considered models of the information protection complex it is provided that along with the basic functions realization of protection, the system should have the properties providing protection against the main threats. Thus, the information security indicators system should be based on the properties assessment of the protection system [15]. The indicators system should provide an assessment of both individual properties and a joint assessment of information security, as shown in the Figure 2.

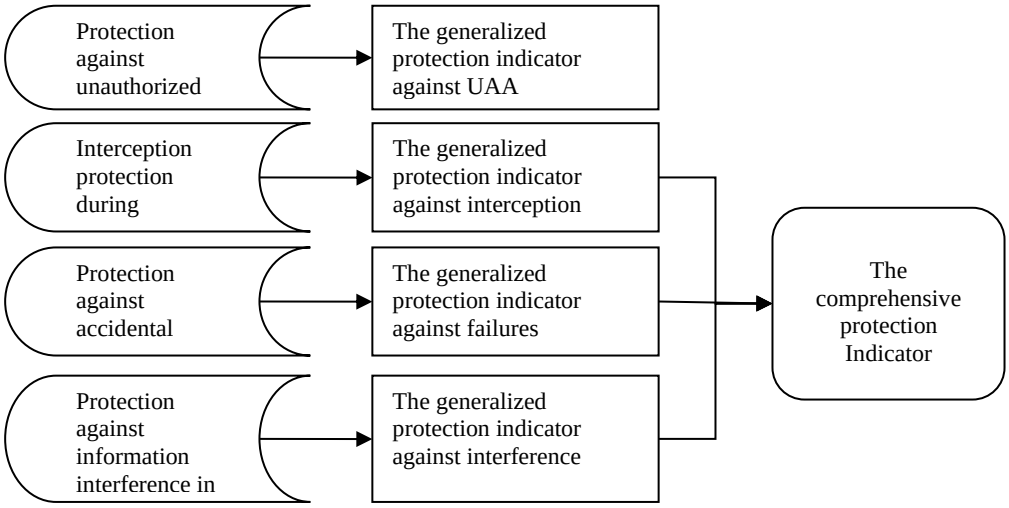

Figure 2. The Relationship between Generalized Indicators of Information Security and a Comprehensive Indicator of Business Processes Information Security
Source: compiled by authors on materials [15-16].

The information structure analysis of business processes, probable threats allowed to form a system of indicators of business processes information security of, presented in the Figure 3.

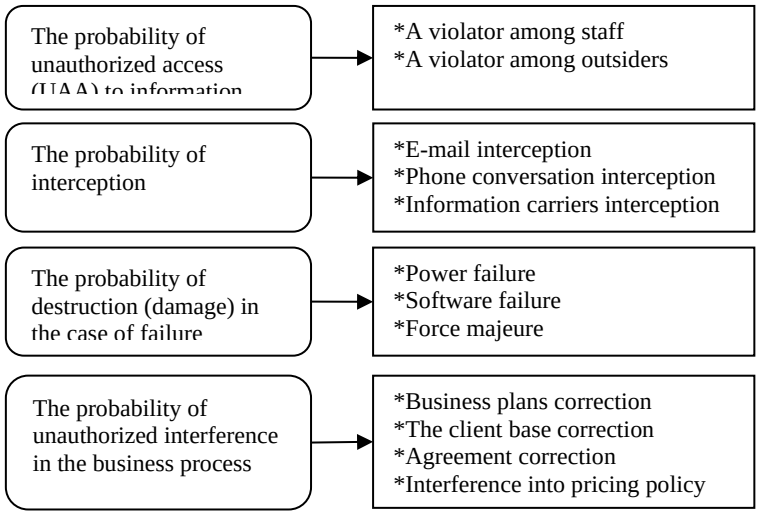

Figure 3. The Main Indicators of Business Processes Information Security
Source: compiled by authors on materials [15].

It is also necessary to take into account the value of information resources of business processes. For accounting purposes of the specifics of Ukrainian companies, it is advisable to assess the value of information assets by the cost method, which is equal to one-time and current expenses. The one-time ones include: organizational expenses and expenses for the purchase and installation of protection. Inevitable expenses are the costs of maintaining the achieved level of security of the enterprise information environment.

Total expenditure form the expenses of preventive measures, the control expenses and losses (external and internal) replenishment. Depending on the security level of information resources, the components of total expenditure change, as well as the total expenditure of security [8]. One-time expenses for forming the enterprise information security policy may be included, if such a policy is provided. When estimating the expenses of a security system at any enterprise, it is necessary to take into account the percentage of total security expenses and total sales.

The main indicator of economic costs efficiency for the information protection structure is the net present value (NPV) in a given period of time T:

$$NPV = \sum_{t=1}^{T} \frac{\Delta if_t(R) - \Delta of_t(R)}{(1+E)^t} - K_R, \quad (4)$$

where:

$\Delta if_t(R)$ – is the change in incoming cash flow in the *t-th* subperiod, taking into account the measures implementation to protect information;

$\Delta of_t(R)$ – is the change in the initial cash flow taking into account the measures implementation to protect information;

K_R – are non-current and current information assets of the information security infrastructure;

E – is the annual rate of return on capital.

The organization of information protection at the enterprise affects the results of its economic activity. In order to set the formation of the business process protection structure , it is necessary to add the marginal conditions for the effectiveness of information protection costs. The main indicators of the enterprise economic activity , on which we impose conditions, include: annual profit, the enterprise cost , profitability.

The qualitative level of the formed system of information protection at the enterprise is determined by the complex indicator of information security, built on the basis of indicators optimization of information security, which correspond to the indicators in the Figure 4.

According to the subsystems models (listed earlier and correspond to those shown in the Figure 1), which form a conceptual model, the fundamental task of forming an information security system in the enterprise can be formulated by two formulations of the issue:

$$R \geq R_{tr};\ S \rightarrow min, \quad (5)$$

$$R \rightarrow max;\ S \leq S_{dop}, \quad (6)$$

where

R – is the comprehensive indicator of information security,

R_{tr} – is the information security indicator of the required level,

S – are resources for information protection in value terms,

S_{dop} – is allowable cost of information protection system.

The essence of these expressions is that the complex indicator should be not less than the required level and at the same time should be taken into account from the company funds that can be spent on information security.

Obviously, the goals of creating a reliable information security infrastructure meet the formula 5 formulation, as it provides the required level of business processes information security. It is assumed that the allocated resources will be minimized, if possible. In any case, they will be sufficient to ensure the condition R ≥ Rtr.

Considering that the funds allocation for the creation of a complex structure for the protection of information, often in limited quantities, then, of course, will suffer and the security of the complex. Thus training and creation of protection can be organized based on the possibilities of the summary options presented in the formulae 5 and 6 and their sequential implementation.

In each individual case (enterprise-specific), the pricing (value) of information assets, and therefore the loss from the information threats realization, may differ in absolute terms, but this does not mean that the relative value of information assets to each individual enterprise is different. Therefore, a comprehensive indicator of information security, the meaning of which is the weighted average probability of information threats reflection may have some significance.

The protection status of the enterprise business processes is characterized by the information security indicator, which is calculated by the weighted average probability of elimination. The data are given in the Table 1.

Table 1. The Characteristics of Comprehensive Indicator Values of Information Security

The comprehensive indicator value of information security(R)	Characteristics of the status of the information security system
1	2
Less than 0,50	Weak protection. A small part of the threats is blocked. The losses are very significant. It is necessary to increase the financial impact of remedies.

Continuation of Table 1.

1	2
0,51–0,75	Medium protection. Unreflected information threats lead to significant losses, making the company vulnerable a lot of measures.
0,76–0,87	Increased protection. A significant part of the threats is blocked. Market conditions and the number of customers change slightly.
0,88–0,95	Strong protection. Most threats do not affect information resources. Losses are minimized
0,96–1	Very strong protection. Disclosure will bring minor economic damage to the company.

Source: compiled by authors on materials[15-16].

Assessing the indicators of the enterprise information security is realized by models of level of protection indicators of BP [8]. Based on the conceptual model of the structure of business process information protection, models of evaluation and optimization of business processes are developed, the Figure 4 shows their relationship.

Models of the complex assessment level and optimization are designed to form the security comprehensive indicator, simulate functioning of the information security structure, optimization and selection of protection options. The data of the models of the indicators level, as shown in the Figure 4, are the sources for the model of the structure of information security, which along with the model of formation of a complex indicator is central at the level of integrated assessment and optimization .

Changes in one of the system indicators are consistently reflected in each other and in the generalized indicator. Its growth can occur with the growth of a single indicator or the growth of all the system indicators. Reducing at least one indicator can be critical for the generalized. The influence of one component on the overall performance of the system is determined by exponential functions that have a saturation area.

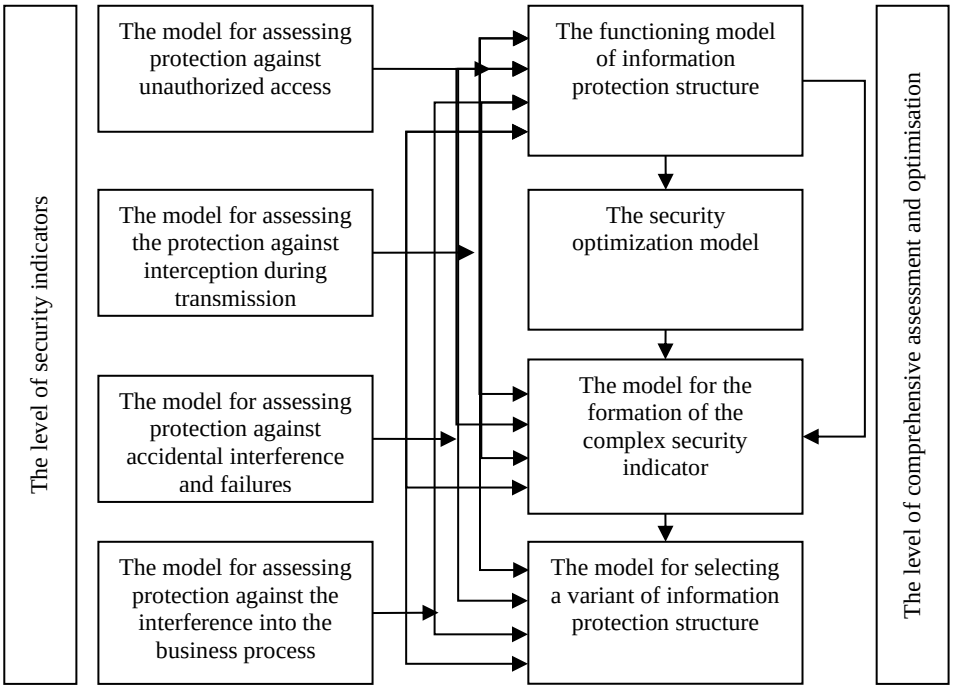

Figure 4. The Models Interrelation of Assessment and Optimization of the BP Protection System
Source: compiled by authors on materials [15].

In view of the abovementioned, calculating the compatible total indicator *Ro* of information security can be represented by the formula 7.

$$R_o = \frac{R_o}{K} = \frac{1}{N_k}\sum_{i=1}^{N_k} 2^{N_k \sqrt[-1]{\prod_{i=1}^{N_k} r_i^{2p}}}, \qquad (7)$$

where

N – is the number of indicators that are at the level of security indicators;

r_i – is the weight coefficient of the i-th property indicator.

A distinctive feature of the developed method is that the weights are not considered as constant values.In fact, the more difficult it is to ensure a given value of the indicator, the more important its role. The closer the indicator is to its limit value, the less its weight.

The formulated optimization problem is aimed at solving the issue of determining the order of private indicators optimization of protection against potential threats, i.e. what indicators and how much should be

improved, how these changes in general will affect the level of information security of business processes.

Conclusions

In order to achieve a certain economic level, Ukraine, along with other countries, is moving to the Industry 4.0 system, where one of the key technological trends are modeling methods and data protection, as well as the principle of business process management (BPM). In turn, business processes are important for successful business and require information and computer protection.

The article proposes a variant of the information protection model, which includes separate functional subsystems, considered protection indicators and a generalized complex indicator, reflects the dependence of a complex indicator on its components, determines the protection degree depending on the complex indicator, defined models of indicators assessment. The system analysis of information security indicators has allowed to determine the relationship between the models of indicators assessment and optimization of the information protection structure of business processes. In order to ensure a high level of comprehensive performance, it is necessary to try to make the maximum possible indicator of protection against interception, the indicator of protection against failures, the rate of unauthorized access. It should be noted that the success of the company business is determined by the level of resources invested in information security.

Abstract

At the present stage, digitalization and using the information technology (IT) are being actively implemented in all the spheres of economy. At the same time, one has to determine and make decisions about what information is needed, how relevant, reliable and confidential. Now more and more computer equipment is involved in enterprises, the means and methods of information processing are becoming more and more complicated. This increases the dependence of enterprises on the degree of security of the IT they use, while the quality of information management support directly depends on the organization of the information protection system.

The information security analysis of IT shows that currently not enough attention is paid to the security system. To a greater extent, this concerns information protection of business processes, which, in the light of modern trends in business organization, play a decisive role in the success of an enterprise. In order to block and prevent the most probable information threats, an economically justified protection system should function, which is focused on supporting business processes, taking into account the information and the enterprise financial resources. It should be said that investments in security generate significant returns through improving business processes.

The aim of the study is to develop a functional model for protecting business processes, to determine a comprehensive security indicator. To do this, it is necessary to solve the following tasks: to identify potentially dangerous situations and threats, to define subsystems of protection against threats to form a general model, to determine security indicators for subsystems that form a generalized indicator.

In the course of the research, the main promising processes have been identified. This served as the basis for the protection concepts development. Taking into account the components of business processes and possible threats with a low level of information security made it possible to determine which threats could become the most dangerous. These include violators' unauthorized access to information, interception of information during its transmission through communication channels, destruction or distortion of information due to random interference, violators' unauthorized influence on the business process from among the participants in the process. The listed set of dangerous situations made it possible to develop a version of a generalized model of information protection of business processes, to formulate a system of security indicators. A system of models for assessing security, a model for forming a complex security indicator is proposed.

An important factor for information security is the enterprise economic policy and the interest degree of the management and staff. This will allow the company to systematically and harmoniously approach the successful organization of transformations in the process approach, isolate its confidential data and achieve business success.

Список літератури:

1. Доктрина інформаційної безпеки України: Рішення РНБО від 29 грудня 2016 року // Офіційний вісник України. – 2017. – № 20. – ст. 8. [Електроний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0016525-16#Text.
2. Трофименко І.Б. Концептуальна основа підтримки цифрової трансформації з використанням підходу інтегрованого управління бізнес-процесами / І. Б. Трофименко // Конкурентоспроможність економіки: показники, фактори впливу та шляхи підвищення: матеріали науково-практичної конференції (м. Дніпро, 28 серпня 2021 р.). – Дніпро: НО «Перспектива». – 2021. – С. 51-55.
3. Khan S. Leadership in the Digital Age: A Study on the Effects of Digitalisation on Top Management Leadership. / S. Khan. Master's Thesis. Stockholm University. Stockholm, Sweden. – 2016. [Електроний ресурс] – Режим доступу: https://www.semanticscholar.org/paper/%E2%80%9C-LEADERSHIP-IN-THE-DIGITAL-AGE-%E2%80%9D-Wilson-Goethals.
4. Bloomberg J. Digitization, Digitalization, and Digital Transformation: Confuse Them At Your Peril. / J. Bloomberg // Forbes. – 2018. [Електроний ресурс] – Режим доступу: https://www.forbes.com/sites/

jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformationconfuse-them-at-your-peril/#9e41a532f2c7.

5. Mancini J. Digitalizing Core Business Processes. True Transformation is more than Digitization. / J. Mancini // AIIM. – Part 1 of 3. – 2018. [Електроний ресурс] – Режим доступу: https://info.aiim.org /aiim-blog/digitalizing–core–business–processespart-1–of-3-true-transformation-is-morethan-digitizati on.
6. Müller J.M. Business model innovation of industry 4.0 solution providers towards customer process innovation. / J. M. Müller, S. Däschle // Researchgate. – 2018. – 6. – 260. [Електроний ресурс] – Режим доступу: https://www.researchgate.net/publication/329554607_Business_Model_Innovatio n_of_Industry_40_Solution_Providers_Towards_Customer_Process_Innovation.
7. Frank A.G. Servitization and Industry 4.0 convergence in the digital transformation of product firms: A business model innovation perspective. Technol. Forecast. Soc. Chang. / A. G. Frank, G. H. Mendes, N. F. Ayala, A. Ghezzi – 2019. – 141. – 341-351. [Електроний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0040 162518311156?via%3Dihub.
8. Фролова Л.В. Трансформація підприємництва в умовах цифрової економіки / Л. В. Фролова, І. М. Бойко // Економіка: реалії часу. Науковий журнал. – 2021. – № 2 (54). – С. 47-56. [Електроний ресурс] – Режим доступу: https://economics.net.ua/files/archive/2021/No2/47.pdf. DOI: 10.15276/ETR.02.2021.6. DOI: 10.5281/zenodo.5115832.
9. Грибіненко О.М. Диджиталізація економіки в новій парадигмі цифрової трансформації. / О. М. Грибіненко // Міжнародні відносини. Серія: Економічні науки. – 2018. – №16. [Електроний ресурс] – Режим доступу: http://journals.iir.kiev.ua/index.php/ec_n/article/view/3523/3197.
10. Семилітко Д. Диджиталізація в дії: як цифрова трансформація бізнесу впливає на успіх компанії. /Д. Семилітко // Аудитор України. – 2019. – № 5. – С. 76-79. [Електроний ресурс] – Режим доступу: http://kumr.edu.ua/wp-content/uploads/2021/03/DIDZHYTALIZATSIYA-BIZNESU-OGODENNYA-TA-MAJBUTNYE.pdf.
11. Багацька К. Бізнес-процеси в умовах диджиталізації економіки. / К. Багацька, А. Гейдор // Науковий журнал «Вісник КНТЕУ». – 2019. – №5(127). – с. 23-32. [Електроний ресурс] – Режим доступу: http://visnik.knute.edu.ua/index.php?option=com_content&view=article&id=2532&atid=264 &lang=ua.
12. Диба М.І., Гернего Ю.О. Диджиталізація економіки: світовий досвід та можливості розвитку в Україні. / М. І. Диба, Ю. О. Гернего // Фінанси України. – 2018. – № 7. – С. 50-63. [Електроний ресурс] – Режим доступу: http://finukr.org.ua/?page_id=340&lang=ru&hid=3107.
13. Соколовська З.М. Моделі ринкової економіки на сучасних технологічних платформах / З. М. Соколовська // Бізнес Інформ. – 2017. – № 11. – С. 430-440. [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/binf_2017_11_64.
14. Гусєва О.Ю., Легомінова С.В. Диджиталізація – як інструмент удосконалення бізнес-процесів, їх оптимізація. / О. Ю. Гусєва, С. В. Легомінова // Економіка. Менеджмент. Бізнес. – 2018. – № 1 (23). – С. 33-39. [Електроний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/ecmebi_20 18_1_7.
15. Stelmashonok E.V. Object-oriented approach to the information protection system modeling / E. V. Stelmashonok, V. L. Stelmashonok// Petersburg economic journal. – 2018. – №2. – С.30-41 DOI: 10.25631/PEJ.2018.2.4/. [Електроний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/ obektno-orientirovannyy-podhod-k-modelirovaniyu-sistemy-zaschity-informatsii.
16. Андрианов В.В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев [Електроний ресурс] – Режим доступу: http://www.pqm-online.com/assets/fles/lib/books/andrianov.pdf.

References:

1. The Doctrine of Information Security of Ukraine: CNSDU Decision of December 29, 2016. (2017). Official Bulletin of Ukraine, 20, 8. Retrieved from https://zakon.rada.gov.ua/laws/show/n0016525-16#Text.
2. Trofymenko, I.B. (2021). Kontseptualna osnova pidtrymky tsyfrovoi transformatsii z vykorystanniam pidkhodu intehrovanoho upravlinnia biznes-protsesamy. (pp. 51-55). Konkurentospromozhnist ekonomiky: pokaznyky, faktory vplyvu ta shliakhy pidvyshchennia: materialy naukovo-praktychnoi konferentsii (m. Dnipro, 28 serpnia 2021 r.). Dnipro: NO "Perspektyva" [in Ukrainian].
3. Khan, S. (2016). Leadership in the Digital Age: A Study on the Effects of Digitalisation on Top Management Leadership. Master's Thesis, Stockholm University, Stockholm, Sweden. Retrieved from https://www.semanticscholar.org/paper/%E2%80%9C-LEADERSHIP-IN-THE-DIGITAL-AGE-%E2 %80 %9D-Wilson-Goethals.
4. Bloomberg J. (2018). Digitization, Digitalization, and Digital Transformation: Confuse Them At Your Peril. Forbes. Retrieved from https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformationconfuse-them-at-your-peril/#9e41a532f2c7.

5. Mancini J. (2018). Digitalizing Core Business Processes. True Transformation is more than Digitization, Part 1 of 3. AIIM. Retrieved from https://info.aiim.org/aiim-blog/ digitalizing-core-business-processes-part-1-of-3-true-transformation-is-morethan-digitization.
6. Müller, J.M. & Däschle, S. (2018). Business model innovation of industry 4.0 solution providers towards customer process innovation. Researchgate, 6, 260. – Retrieved from https://www.researchgate.net/publication/329554607_Business_Model_Innovation_of_Industry_40_Solution_Providers_Towards_Customer_Process_Innovation.
7. Frank, A.G., Mendes, G.H., Ayala, N.F. et al. (2019). Servitization and Industry 4.0 convergence in the digital transformation of product firms: A business model innovation perspective. Technol. Forecast. Soc. Chang., 141, 341-351. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0040162518311156?via%3Dihub.
8. Frolova, L.V. & Boyko, I.M. (2021). Transformation of entrepreneurship in the digital economy. Economics: time realities. Scientific journal, 2 (54), 47-56. Retrieved from https://economics.net.ua/files/archive/2021/No2/47.pdf. DOI: 10.15276/ETR.02.2021.6. DOI: 10.5281/zenodo.5115832 (accessed 17.10.2021) [in Ukrainian].
9. Hrybinenko, O.M. (2018). Didzhytalizatsiia ekonomiky v novii paradyhmi tsyfrovoi transformatsii [Digitizing the economy in the new paradigm of digital transformation]. Mizhnarodni vidnosyny, 16. Seriia. Ekonomichni nauky. Retrieved from http://journals.iir.kiev.ua/index.php/ec_n/article/view/3523/3197 [in Ukrainian].
10. Semylitko, D. (2019). Didzhytalizatsiia v dii: yak tsyfrova transformatsiia biznesu vplyvaie na uspikh kompanii [Digitization in action: how digital business transformation affects company success]. Audytor Ukrainy, 5, 76-79 [in Ukrainian].
11. Bahatska, K., Heidor, A. (2019) Biznes-protsesy v umovakh didzhytalizatsiyi ekonomiky [Business processes in the context of digitalization of the economy]. Visnyk KNTEU, 5, 23-32 [in Ukrainian].
12. Dyba, M.I. & Herneho, Yu.O. (2018). Didzhytalizatsiia ekonomiky: svitovyi dosvid ta mozhlyvosti rozvytku v Ukraini [Digitizing the economy: world experience and development opportunities in Ukraine]. Finansy Ukrainy, 7, 50-63 [in Ukrainian].
13. Sokolovska, Z.M. (2017). Modeli rynkovoi ekonomiky na suchasnykh tekhnolohichnykh platformakh. Biznes Inform, 11, 430-440. Retrieved from http://nbuv.gov.ua/UJRN/binf_2017_11_64 [in Ukrainian].
14. Husieva, O.Iu., & Lehominova, S.V. (2018). Didzhytalizatsiia – yak instrument udoskonalennia biznes-protsesiv, yikh optymizatsiia [Digitization – as a tool for improving business processes, optimizing them]. Ekonomika. Menedzhment. Biznes, 1 (23), 33-39. Retrieved from http://nbuv.gov.ua/UJRN/ecmebi_2018_1_7 [in Ukrainian].
15. Stelmashonok, E.V. (2018). Object-oriented approach to the information protection system modeling economic journal, 2, 30-41 DOI: 10.25631/PEJ.2018.2.4/ Retrieved from https://cyberleninka.ru/article/n/obektno-orientirovannyy-podhod-k-modelirovaniyu-sistemy-zaschity-informatsii.
16. Andryanov V.V., Zefyrov S.L., Holovanov V.B., et al. Obespechenye ynformatsyonnoi bezopasnosty byznesa. Retrieved from http://www.pqm-online.com/assets/fles/lib/books/andrianov.pdf [in Ukrainian].

Посилання на статтю:
Budoratska T.L. Information Protection of Business Processes in the Digital Economy Conditions / T. L. Budoratska, H. O. Kovalova, I. B. Trofymenko // Економіка: реалії часу. Науковий журнал. – 2021. – № 4 (56). – С. 22-30. – Режим доступу до журн.: https://economics.net.ua/files/archive/2021/No4/22.pdf.
DOI: 10.15276/ETR.04.2021.3. DOI: 10.5281/zenodo.6536523.

Reference a Journal Article:
Budoratska T.L. Information Protection of Business Processes in the Digital Economy Conditions / T. L. Budoratska, H. O. Kovalova, I. B. Trofymenko // Economics: time realities. Scientific journal. – 2021. – № 4 (56). – P. 22-30. – Retrieved from https://economics.net.ua/files/archive/2021/No4/22.pdf.
DOI: 10.15276/ETR.04.2021.3. DOI: 10.5281/zenodo.6536523.