DOI: 10.15276/ETR.02.2021.5
DOI: 10.5281/zenodo.5115824
UDC: 339.9
JEL: F61, F62

MANAGEMENT OF INFORMATION SECURITY OF PRODUCTION

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ВИРОБНИЦТВА

Mariia A. Nesen
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: 0000-0002-4610-3895
Email: nesenmaria5@gmail.com

Viktoriia I. Liashevska, PhD in Economics, Associate Professor
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: 0000-0001-6520-3632
Email: v.i.liashevska@karazin.ua

Yelizaveta V. Fomina, PhD in Economics, Associate Professor
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: 0000-0003-4431-1460
Email: e.v.fomina@karazin.ua

Received 30.01.2021

Несен М.А., Ляшевська В.І., Фоміна Є.В. Управління інформаційною безпекою виробництва. Оглядова стаття.

У статті актуалізовано проблему надійності інформації підприємства. Розглянуто методологічні основи побудови та впровадження системи управління інформаційною безпекою діяльності компанії. Згідно з встановленою метою цієї роботи визначено підходи для забезпечення безпечного управління механізмами інформаційної системи. Виявлені рішення, завдяки яким є можливість захищати інформацію, що передається на внутрішньому та зовнішніх ринках. Розглянуті системи, що допомагають автоматизувати функціонування процесів організації..

На основі міжнародних стандартів та проведеного аналізу сучасних підходів до визначення сутності моделі менеджменту інформаційної системи, запропоновано ключові етапи створення ефективної системи управління інформаційною безпекою бізнес-процесів.

Ключові слова: бізнес-процеси, інформаційна безпека, система управління, управління підприємством, інформаційна система, ризик

Nesen M.A., Liashevska V.I., Fomina Y.V. Management of information security of production. Review article.

The article actualizes the problem of reliability of enterprise information. The methodological bases of construction and implementation of the information security management system of the company are considered. In accordance with the established purpose of this work, approaches to ensure safe management of information system mechanisms are identified. Solutions have been identified that make it possible to protect information transmitted in domestic and foreign markets. The systems that help automate the functioning of the organization's processes are considered.

Based on international standards and the analysis of modern approaches to defining the essence of the information system management model, the key stages of creating an effective information security management system for business processes are proposed.

Keywords: business processes, information security, information security, enterprise management, information system, risk

Information policy plays a very important role in the company's activities and covers almost all its parts. Rapid development in the information sphere is the reason for the emergence of fundamentally new threats to businesses.

In order to resolve and generally avoid possible conflicts related to the theft of valuable data, it is necessary to pursue a successful information policy. However, this relationship, which is related to information security, requires effective regulation.

Every company must take care of its information security in order to protect information interests.

Analysis of recent research and publications

Some aspects of this issue have been found in the works of modern scientists Mytko A.M. (2012), Bobrov Ye.A. (2012), Vasyltsiv T.H. (2014), Bondarenko O.O. (2014), Maślanka-Wieczorek B. (2014), Bodnar, I.R. (2013), Marushchak A.I. (2011), Leyli Ali Allakhverdieva (2020), Skrynnyk, O. (2020) and others. But the question of forming an effective information management system of the firm requires further research and comparison.

Unsolved aspects of the problem

Collection and analysis of economic data on making adequate management decisions is a decisive factor in the system of business processes. Information systems help to correctly assess the most used software packages and prevent possible errors that occur due to inattention and inaccuracy of measurements, etc. [1]. Therefore, the proposed topic is relevant.

The aim of the article is to determine the theoretical and methodological basis for the formation of a comprehensive mechanism for managing information security of the enterprise, the importance of information systems in enterprise management and analysis of the most common systems for automation.

The purpose and objectives of this article are to study the features of information security of production in Ukraine as an important issue of efficient work in the company.

The main part

Contact details, licenses, certificates and other documents of the company are constantly transmitted through various channels for verification and communication with market participants. In cases where information systems do not have a sufficient level of protection, there is a risk of losing corporate confidential data. Which in turn can be a serious threat to the operation of the enterprise, because competitors will be able to access all the documentation and use it to their advantage.

The quality of functioning of each enterprise directly depends on the efficiency and reliability of information support of its activities.

Having a customer base, the composition of the enterprise, the base of suppliers, prices for products and other materials, you can conduct a detailed analysis of the enterprise, and identify the strengths and weaknesses of the company. If this information is received by outsiders, the company may find itself in a very bad position.

After all, if you take into account all the shortcomings of the company's competitors and exclude them from the activities of your company, you can significantly improve the level in the overall market. In addition, after the analysis, you can determine the unique trade offer of the company's competitors and adapt it to your style [2].

If errors or violations are found in the documents, the company may face a significant deterioration of its reputation. This will lead to a loss of trust of customers, partners and suppliers, and thus – a decrease in sales. In such a situation, the organization may be in complete danger of forced exit from the market.

Many actions can now be taken to secure information, but it is important to take a comprehensive approach to this problem. That is, to use several approaches to information security management: process, organizational, optimization, cybernetic, etc. With these control systems, you can solve both specific and complex problems.

Information security management should include certain actions that will be aimed at maintaining and creating a stable operation of the enterprise, should provide access and storage of important company data, in addition to keep records of operations. To improve the quality of the management system, it is necessary to conduct an audit and timely develop a strategy for the company's development. And first of all – to analyze the internal state of the organization, to identify its mechanism of operation and opportunities for improvement.

To date, there are 5 main types of resources owned by the company: labor, material, financial, knowledge and information support. They play an important role in the efficient operation of the enterprise and require constant improvement [3].

In order to maintain the proper condition of the enterprise, it is necessary to adhere to a defined action plan. Thanks to these measures, the cycle will be in constant motion, and all information resources of any corporate level are under control.

Thus, it is necessary to make a list of sales and operations in advance, ie to consider each aspect of the operation of enterprise processes and to establish the volume of production of finished products. Next, you need to develop a table of data on the characteristics of the required resources. Last, no less important. The step is to manage the created system, because to get started you need to settle everything and analyze the possible risks and dangers in the course of further activities of the company.

Information security of the enterprise is the foundation of stable work of the organization, and for its maintenance it is necessary to consider three important components (fig. 1).

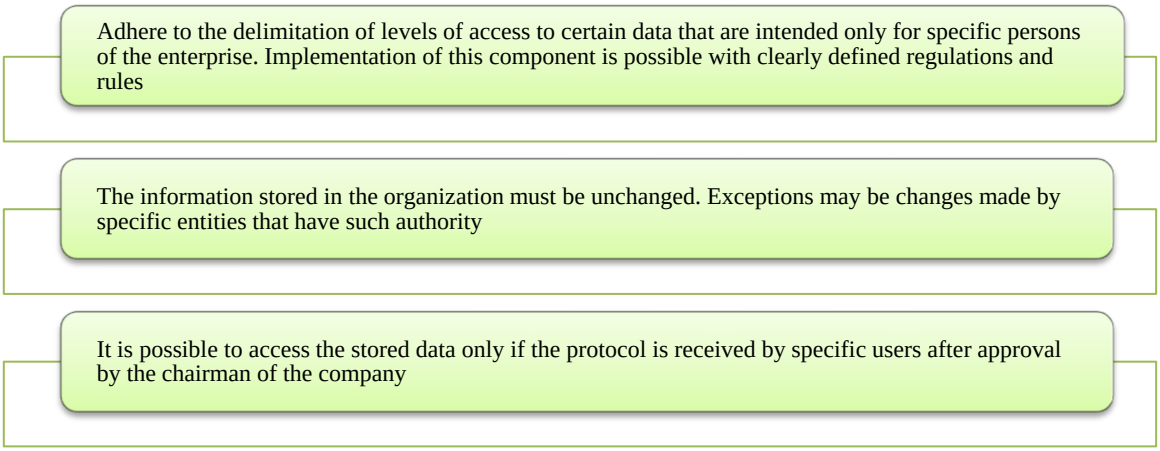

Figure 1. Information security components
Source: compiled by authors on materials [3].

Each organization must create a model of protection solely taking into account the conditions of its internal environment and business interests. The most effective schemes are those that ensure the security of each commercial process.

Mandatory elements of information security management of the enterprise should be the following (Fig. 2).

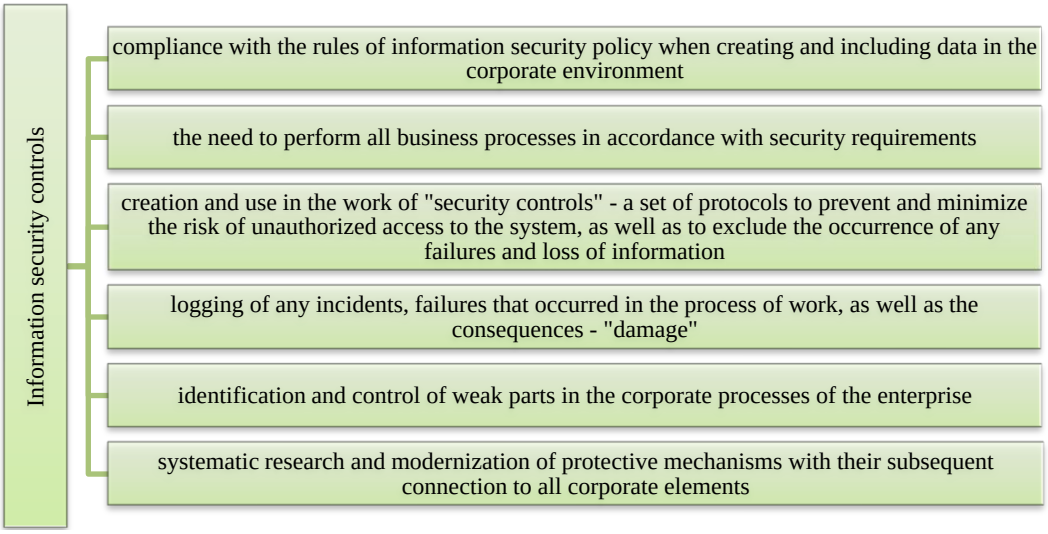

Figure 2. Elements of information security management of the enterprise
Source: compiled by authors on materials [3].

The process management configuration system includes a database, a graphical visualization subsystem, a monitoring and scheduling level, a management component, a system analysis level, and many other important elements that are part of information security.

Thanks to configuration management, rapid adaptation to the environment can be achieved.

This technique involves the proper implementation of the necessary actions for each level of information security. In addition, it is possible to identify which management approach is needed for each level.

Information system - certain structures of elements that collect, process, transmit, store and provide data. Each system has a certain structure, the elements of which reflect the functioning of the object of management and influence it through management [4].

Information security management is a cyclical process and includes several important elements (Fig. 3)

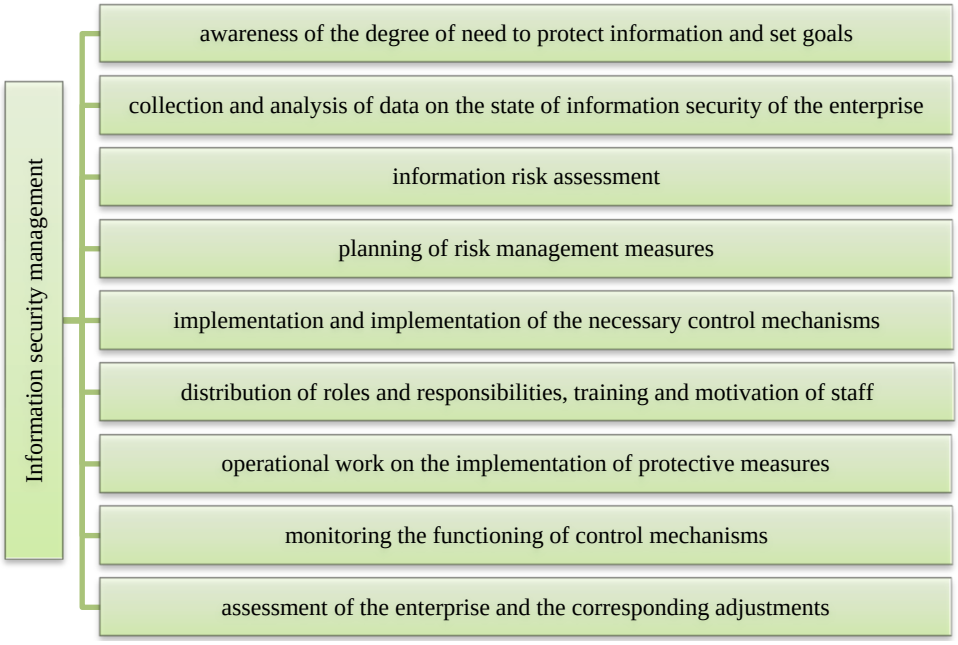

Figure 3. Components of information security management of the enterprise
Source: compiled by authors on materials [4].

Unity and orderliness ensure effective implementation of management decisions, support for business goals, management of enterprise resources and product data, document management, accounting automation and flexible response to external and internal changes in the firm.

According to statistics, automation improves the overall performance of the firm and reduces the amount of analytical work. Productivity increases by more than 15 percent, and the turnover of working capital decreases to 12 percent. It should be noted that the term of execution of orders is reduced by 20-50% and costs up to 15% of annual turnover [5].

If we consider information security from the system approach, we can identify four main factors of information technology hazards for the activities of organizations, due to the results of scientific and technological progress.

The first such group includes the intensive development of psychological influence on people through information flows.

The second group is based on the use of the results of modern information technology for illegal actions, namely – social crimes. These include computer hooliganism, fraud with any transaction, illegal copying of data, etc. Leading researchers in this field believe that computers are increasingly the cause of many data thefts from the system.

The third group can be represented as electronic control over life, goals, mood, political activity, and so on.

Thanks to high information technology, it is possible to store and use large arrays of data relating to each part of the organization.

The fourth group includes the use of information technology in political conflicts. This is especially important now, because every year the influence of the media on the content and direction of the political system grows.

There is also another key element of information security – protection against data theft on computers. For some time, there has been a tendency to increase theft in cases such as attempts to tamper with telecommunications and information structures, as well as the introduction of new techniques and tools for these illegal actions.

All these factors pose a threat to the national information space, so if no action is taken on these crimes, many organizations will lose control of the information space of their database, which in a broader sense will make it impossible to ensure the rights of all citizens in this area [6].

There are various methods of unauthorized access to the database. However, there is no single security measure to protect a company from criminals. Reliable protection can only be achieved by providing a comprehensive security mechanism.

The main components of such a complex should be technical, regulatory and organizational tools (Fig. 4).

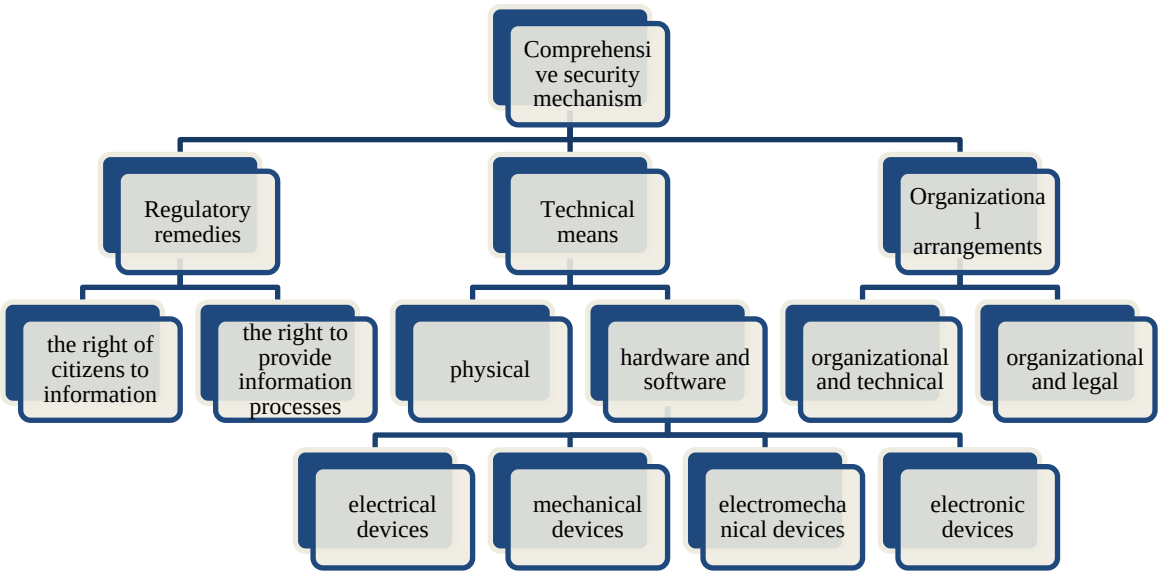

Figure 4. Comprehensive security mechanism
Source: compiled by authors on materials [6].

The main components of the security mechanism complex should be technical, regulatory and organizational means. They, in turn, include several elements that increase the likelihood of secure storage of information in space.

Today, the personal computer, tablet, telephone and other mobile means of communication are the main devices for data processing, protection, storage and transmission. Due to the fact that the information is in electronic means, the risk of its capture increases.

After all, technical devices are often accompanied by electromagnetic radiation, through which you can access the flow of information.

According to research by Ernst & Young

services [8], the most valuable information for cybercriminals in today's information security market for 19 % of respondents is customer information, 13 % of financial information, 13 % of strategic plans, 12 % of board member information, 12 % of customer passwords, 10 % of R&D information, 9 % of M&A information, 7 % of intellectual property and 5 % of non-patented IP (Fig.5).

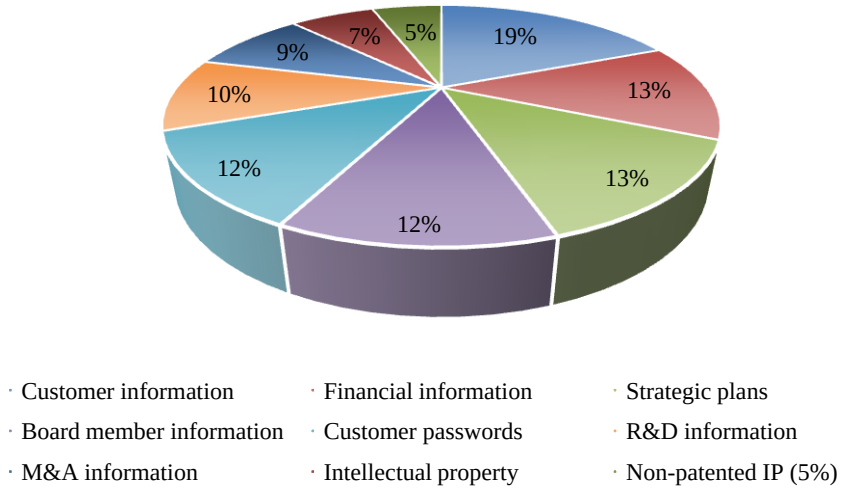

Figure 5. Top 10 most valuable information to cyber criminals
Source: compiled by authors on materials [8].

An integrated information security system should operate on the basis of regulations and only according to a clearly defined and agreed action plan. The availability of hardware and software will allow you to effectively manage, especially given the emergency conditions of crime.

Proper organization of the workspace helps to increase productivity and get the best results after the experiments. Keeping order provides a guaranteed opportunity to scale, thanks to a global approach to solving problems.

The information security management system is based on the analysis of risks that arise at the external and internal levels. In order to prevent these risks, it is necessary to constantly monitor and evaluate the current system of the enterprise. This will reveal the shortcomings of the system, which can be corrected in the future [9].

Such inspections should be performed regularly to ensure the efficient operation of all system processes. All actions to regulate the information security of the enterprise must be noted at the stages of planning and implementation. The clarity of the tasks and their implementation will allow to identify problems in time and solve them.

In some cases, it is necessary to conduct extraordinary inspections, this should also be quickly identified during the analysis of the system. With immediate implementation and response to the possible risk and vulnerability of information processes, the likelihood of incidents is significantly reduce [10].

There are also possible threats of intentional errors that occur outside the company's activities, they can include many types (Fig. 6).

It is possible to provide fast response to any threats thanks to the automated processes built in system. Today there is a wide range of tools for automation of production management: work with Internet environments, software packages (for example, "BEST-5", "SAP Business One"), logistics management, stimulation of business ideas and more [11].

However, it is important to understand how to use these techniques to maximum advantage. Setting up business operations and preparing for the launch of the program are crucial, because it depends on the economic benefits for the company. Therefore it is necessary:

— to optimize the chain of processes by developing the necessary procedures for implementing change;
— to develop a full-featured information system and create secure conditions for storing data on it;
— to expand the functional reserves of the enterprise for effective accounting and making verified management decisions in all areas of activity;
— to collect, store and quickly access the company's accounting information;
— to ensure timely and complete provision of data to managers of all levels of government from a single information fund;
— to increase the degree of validity and timeliness of decisions made through the prompt collection, transmission and processing of information;
— to ensure the continuous operation of equipment to preserve the integrity of any operational data of the organization, in the first place – confidential;
— to identify promising areas of development of the organization.

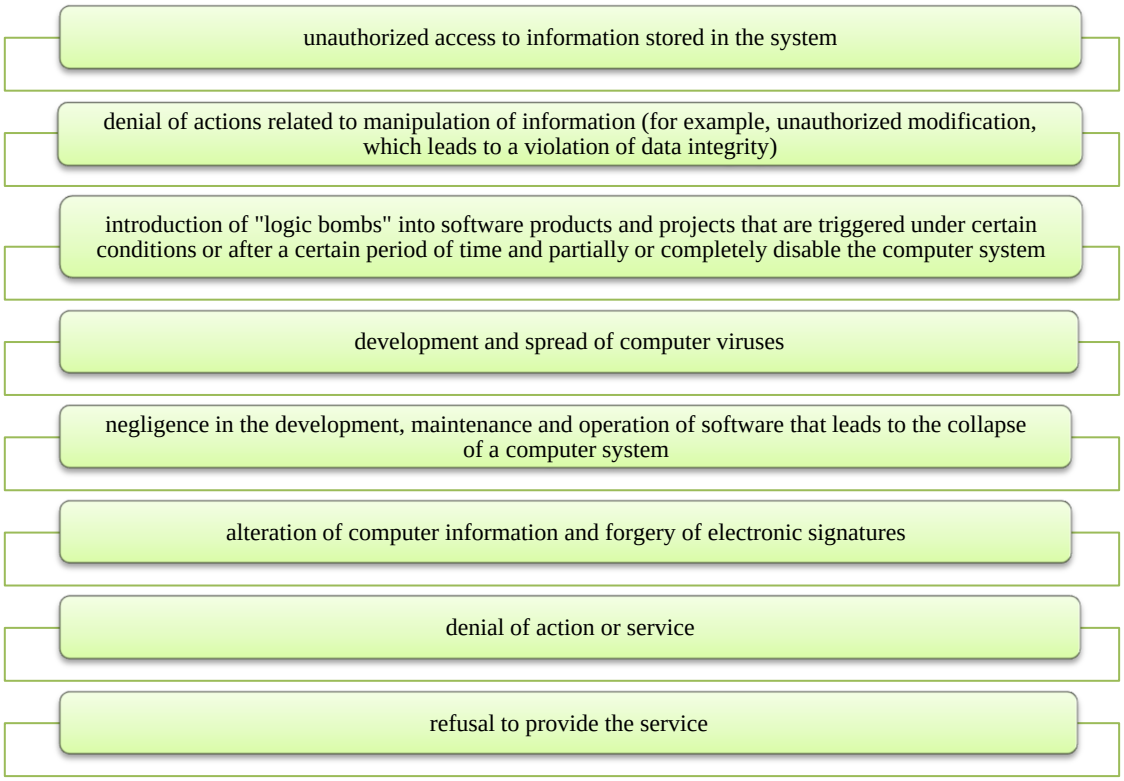

Figure 6. Types of threats related to intentional errors that occur outside the business
Source: compiled by authors on materials [10].

Conclusion

Thus, in today's world, information technology is developing very rapidly, which directly affects people's lives. The use of information systems to automate production management is the key to safe and, consequently, successful business.

When choosing an information system should focus on the level in the system of public administration, the area of functioning of the economic object, the types of management processes and the degree of automation of information processes. It is the optimization of the components of the process allows you to reach the top in any case, which in the future will only improve the activities of the enterprise. Therefore, the study of information security management of the enterprise is now very important and requires detailed analysis, especially in the digital age.

Abstract

The quality of functioning of each enterprise directly depends on the efficiency and reliability of information support of its activities. Collection and analysis of economic data on making adequate management decisions is a decisive factor in the system of business processes. Information systems help to correctly assess the most used software packages and prevent possible errors that occur due to inattention and inaccuracy of measurements, etc. Therefore, the proposed topic is relevant.

The aim of the article is to determine the theoretical and methodological basis for the formation of a comprehensive mechanism for managing information security of the enterprise, the importance of information systems in enterprise management and analysis of the most common systems for automation.

The purpose and objectives of this article are to study the features of information security of production in Ukraine as an important issue of efficient work in the company.

Setting up business operations and preparing for the launch of the program are crucial, because it depends on the economic benefits for the company. Therefore it is necessary:

— to optimize the chain of processes by developing the necessary procedures for implementing change;
— to develop a full-featured information system and create secure conditions for storing data on it;
— to expand the functional reserves of the enterprise for effective accounting and making verified management decisions in all areas of activity;
— to collect, store and quickly access the company's accounting information;
— to ensure timely and complete provision of data to managers of all levels of government from a single information fund;

— to increase the degree of validity and timeliness of decisions made through the prompt collection, transmission and processing of information;
— to ensure the continuous operation of equipment to preserve the integrity of any operational data of the organization, in the first place - confidential;
— to identify promising areas of development of the organization.

Thus, in today's world, information technology is developing very rapidly, which directly affects people's lives. The use of information. When choosing an information system should focus on the level in the system of public administration, the area of functioning of the economic object, the types of management processes and the degree of automation of information processes. It is the optimization of the components of the process allows you to reach the top in any case, which in the future will only improve the activities of the enterprise. Therefore, the study of information security management of the enterprise is now very important and requires detailed analysis, especially in the digital age.

Список літератури:

1. Митько А.М. Інформаційна безпека як основа становлення інформаційної демократії в Україні / А. М. Митько // Актуальні проблеми міжнародних відносин. – 2012. – Вип. 108(1). – С. 85-89.
2. Бобров Є.А. Сучасні підходи до дослідження економічної безпеки / Є. А. Бобров // Економіка України. – 2012. – No 4. – С. 80-85.
3. Is cybersecurity about more than protection? [Електроний ресурс] – Режим доступу: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf.
4. Васильців Т.Г. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення / Т. Г. Васильців. – Львів: Арал. – 2012. – 386 с.
5. Бондаренко О.О. Фінансово-економічна безпека підприємства: теоретичний та практичний аспекти / О. О. Бондаренко, В. А. Сухецький // Ефективна економіка. – 2014. – No 10. – С. 23-30.
6. Maślanka-Wieczorek B. Talent management and high performance work system / B. Maślanka-Wieczorek // Journal of international studies. – 2014. – Vol. 7, No 10. – P. 23-30. [Електроний ресурс] – Режим доступу: https://www.jois.eu/?156,en_talent-management-and-high-performance-work-system.
7. Боднар І.Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку / І. Р. Боднар. – Львів: Видавництво Львівської комерційної академії. – 2013. – 320 с.
8. Cybersecurity, strategy, risk, compliance and resilience. [Електроний ресурс] – Режим доступу: https://www.ey.com/en_gl/consulting/cybersecurity-strategy-risk-compliance-resilience.
9. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. – 2011. – No 21. – С. 92-95.
10. Leyli Ali Allakhverdieva. The information services sector: defining the extent of public regulation ensuring its development / Leyli Ali Allakhverdieva // Economic Annals-XXI. – Vol. 181, No 1-2. – P. 57-67. [Електроний ресурс] – Режим доступу: http://soskin.info/en/ea/2020/181-1-2/Economic-Annals-V181-05.
11. Скринник О. Забезпечення інформаційної безпеки в цифрових організаційних системах управління / О. Скринник // Маркетинг і менеджмент інновацій. – 2011. – No 4. – С. 279–289. [Електроний ресурс] – Режим доступу: https://mmi.fem.sumdu.edu.ua/journals/2020/4/279-289.

References:

1. Mytko A.M. (2012). Informatsiina bezpeka yak osnova stanovlennia informatsiinoi demokratii v Ukraini. Aktualni problemy mizhnarodnykh vidnosyn, 108(1), 85-89 [in Ukrainian].
2. Bobrov Ye.A. (2012). Suchasni pidkhody do doslidzhennia ekonomichnoi bezpeky. Ekonomika Ukrainy, No 4, 80-85 [in Ukrainian].
3. Is cybersecurity about more than protection? Retrieved from: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf.
4. Vasyltsiv T.H. (2014). Finansovo-ekonomichna bezpeka pidpryiemstv Ukrainy: stratehiia ta mekhanizmy zabezpechennia. Lviv: Aral [in Ukrainian].
5. Bondarenko O.O. (2014). Finansovo-ekonomichna bezpeka pidpryiemstva: teoretychnyi ta praktychnyi aspekty. Efektyvna ekonomika, No 10, 23-30 [in Ukrainian].
6. Maślanka-Wieczorek B. (2014). Talent management and high performance work system. Journal of international studies, Vol. 7, No 10, 23-30. Retrieved from https://www.jois.eu/?156,en_talent-management-and-high-performance-work-system.
7. Bodnar, I.R. (2013). Suchasni realii informatsiinoho suspilstva: problemy stanovlennia ta perspektyvy rozvytku. Lviv: Vydavnytstvo Lvivskoi komertsiinoi akademii [in Ukrainian].
8. Cybersecurity, strategy, risk, compliance and resilience. Retrieved from https://www.ey.com/en_gl/consulting/cybersecurity-strategy-risk-compliance-resilience.

9. Marushchak, A.I. (2011). Informatsiino-pravovi napriamy doslidzhennia problem informatsiinoi bezpeky. Derzhavna bezpeka Ukrainy, No 21, 92-95 [in Ukrainian].
10. Leyli Ali Allakhverdieva (2020). The information services sector: defining the extent of public regulation ensuring its development. Economic Annals-XXI, Vol. 181, No 1-2, 57-67. Retrieved from http://soskin.info/en/ea/2020/181-1-2/Economic-Annals-V181-05.
11. Skrynnyk, O. (2020). Some Aspects of Information Security in Digital Organizational Management System. Marketing and Management of Innovations, 4, 279-289. Retrieved from https://mmi.fem.sumdu.edu.ua/journals/2020/4/279-289.

Посилання на статтю:
Nesen M.A. Management of information security of production / M. A. Nesen, V. I. Liashevska, Y. V. Fomina // Економіка: реалії часу. Науковий журнал. – 2021. – № 2 (54). – С. 39-46. – Режим доступу до журн.: https://economics.net.ua/files/archive/2021/No2/39.pdf.
DOI: 10.15276/ETR.02.2021.5. DOI: 10.5281/zenodo.5115824.

Reference a Journal Article:
Nesen M.A. Management of information security of production / M. A. Nesen, V. I. Liashevska, Y. V. Fomina // Economics: time realities. Scientific journal. – 2021. – № 2 (54). – P. 39-46. – Retrieved from https://economics.net.ua/files/archive/2021/No2/39.pdf.
DOI: 10.15276/ETR.02.2021.5. DOI: 10.5281/zenodo.5115824.