UDC 004.056.5JEL M 15 DOI 10.26906/EiR.2020.1(76).1924

MANAGEMENT OF INFORMATION SECURITY OF THE ENTERPRISE IN THE CONDITIONS OF DYNAMIC BUSINESS ENVIRONMENT

Iryna Chernysh*, Doctor of Sciences (Economics), Associate Professor
Viktoriia Makhovka, PhD, Associate Professor**
Liliia Lobach, Master student,
National University «Yuri Kondratyuk Poltava Polytechnic»

** ORCID 0000-0001-6565-5292*
*** ORCID 0000-0001-7985-7792*

Стаття отримана редакцією 05.02.2020 р.
The article was received by editorial board on 05.02.2020

Introduction. The significant progress and spread of information technologies, the global nature of mass communication systems have led to the creation of a global information space that forces the global community, every state, every enterprise to quickly navigate and adapt in the modern information environment. Information technology has dramatically increased online business opportunities. However, these opportunities also pose serious risks and threats to information security. Previously, information security issues have been studied in a technological context, but security needs have expanded the attention of researchers to improve the enterprise information security management process. Numerous management measures, including the development and implementation of information security policies, awareness raising, training, development of effective enterprise information architecture, IT infrastructure management, business and IT alignment, human resource management, have been found to have a significant impact on the quality of information security management.

Latest research papers and publications review. The works by famous scientists, in particular: M. Huzaliuk, O. Danilian, R. Kaliuzhnyi, S. Kovtun and others are devoted to the etymological issues of the concept of "information security", in some subject areas of study. Marushchak A., Morozov A., Kormich B. mentioned about a qualitatively new possibility of application of information security systems, along with other methods of protection of business processes in their writings.

Problem statement. The information resource of any company is the subject of increased attention from competing firms. Competition ideally is a fair competition for leadership in the market for goods and services, but examples of unfair competition are more than enough. And the main method of combating unfair competition is to access in any way a competitor's information resource. Therefore, the focus is on effective management of information security at the enterprise.

Main material and investigation results. Dynamic conditions of business environment development are characterized by instability of internal and external factors, which necessitates the expansion of the directions of application of information technologies to build a strategy of adaptation and survival in market conditions. The use of information technology can be one of the ways of forming the competitive advantages of the enterprise, expanding its range of opportunities by improving the process of information exchange, establishing ways of cooperation between partners and clients, improving the effectiveness of management methods. But, at the same time, modern information technologies also create conditions for threats to the economic and financial security of the enterprise.

Consequently, information has evolved from a factor in ensuring effective economic activity to an effective means of competition, the rational use of which will increase the profitability of the enterprise and ensure its sustainable development in the future. Proof of the above is the famous saying of Winston Churchill: "Who owns the information, he owns the world." Thus acquires relevance of information security.

Information security refers to the processes and methodologies that are designed and implemented to protect printed, electronic, or any other form of classified, private and confidential information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or breach.

Information security covers different spheres of activity and aims to form the necessary conditions to support the interests of the enterprise, region, state in the information sphere.

Fig. 1. presents the varieties of security and the levels at which information security is managed.

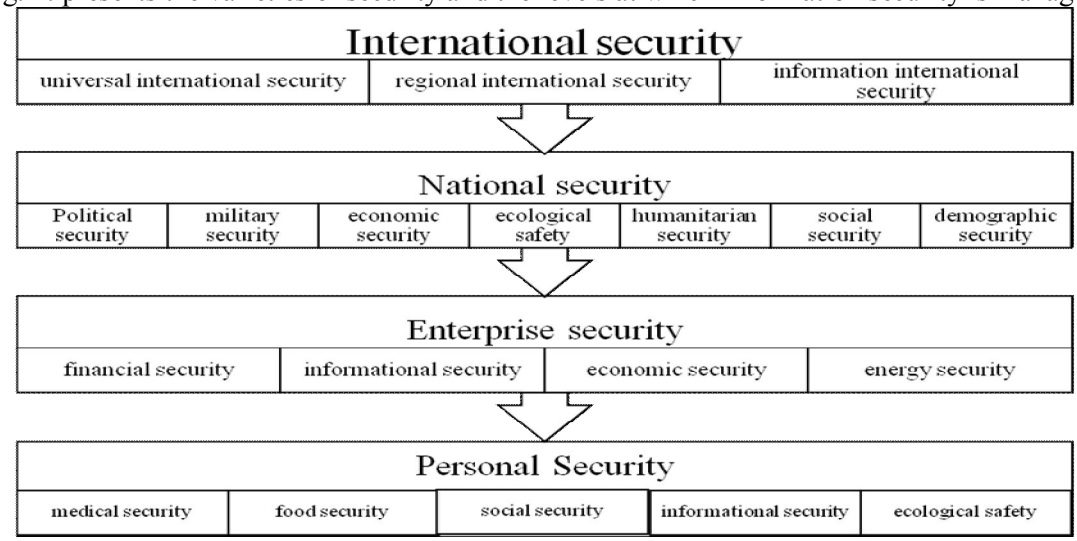

Fig. 1. Security varieties and levels at which information security is managed

From an objective point of view, information security arose from the emergence of modern means of communicative interconnection between people, as well as through the awareness that the interests of society and the individual may be harmed by influencing, or unlawful action on, the media of communication and the development of which provides information exchange between all elements of society.

In the Table 1 we will characterize the essence of the concept of "information security".

Table 1

Etymology of the term "information security"

Characteristics	Author, reference
Information security - the state of security of the norms and parameters of information processes and relations established by the legislation, which provides the necessary conditions for the existence of the state, human and society as subjects of these processes and relations	Kormych B. [11]
Information security (infosec) is a set of strategies for managing processes, tools and policies necessary to prevent, detect, document and counteract threats to digital and non-digital information. Information security responsibilities include creating a set of business processes that will protect information assets, regardless of how the information is formatted, in transit, processed, or dormant.	Managing information security amid new threat [13]
Information Security (IS) is designed to protect the confidentiality, integrity and accessibility of computer system data from persons with malicious intent.	Techopedia electronic resource [4]
Information security is a state of protection of vital interests of the individual, society and the state, minimizing the damage caused by incompleteness, untimely information, unreliability of information or negative information influence, due to the negative consequences of the functioning of information technologies, as well as through unauthorized dissemination of information technology.	Marushchak A.I. [14]
Information security is the protection of the statutory rules by which information processes occur in the country. ensuring the conditions of existence and development of society and the state guaranteed by the Constitution	Kormych B.A. [12]
Information security is a state of security of the person of the society and the state in which information development is achieved.	Petryk V. [15]
Information security is the protection of personal information about senders and recipients, protection of information from unauthorized access, creation of a reliable source of supply of information of information services and necessary equipment protection of information directly related to all aspects of national security, including the military potential of the state.	Developments in the Field of Information and Telecommunication in the Context of International Security [3]
information security as a state of information, information systems and resources, in which information is protected against leakage, destruction, forgery, theft, etc. To ensure security, a set of legal, technical and organizational measures are needed to prevent misuse of information.	Rusina Yu. O. [16]

Therefore, information security is a set of practices designed to protect data from unauthorized access or alteration, both when stored or transmitted from one machine or physical location to another. This can sometimes be called data security. As knowledge has become one of the most important assets of the 21st century, efforts to preserve information have become increasingly important.

Historically, information security management has largely relied on technical controls, however, studies have shown that most information security failures occur because of a breach of control by trusted employees. This suggests that information security management can only be properly ensured if the focus goes beyond technical control and involves business process and organizational issues. Information security management is primarily about strategic, tactical and operational issues related to the planning, analysis, design, implementation and support of an organization's information security program.

Information security management is the process of administering people, policies and programs to ensure the continuity of operations while maintaining strategic alignment with the organizational mission [2].

Information security management should be based on principles (Fig. 2).

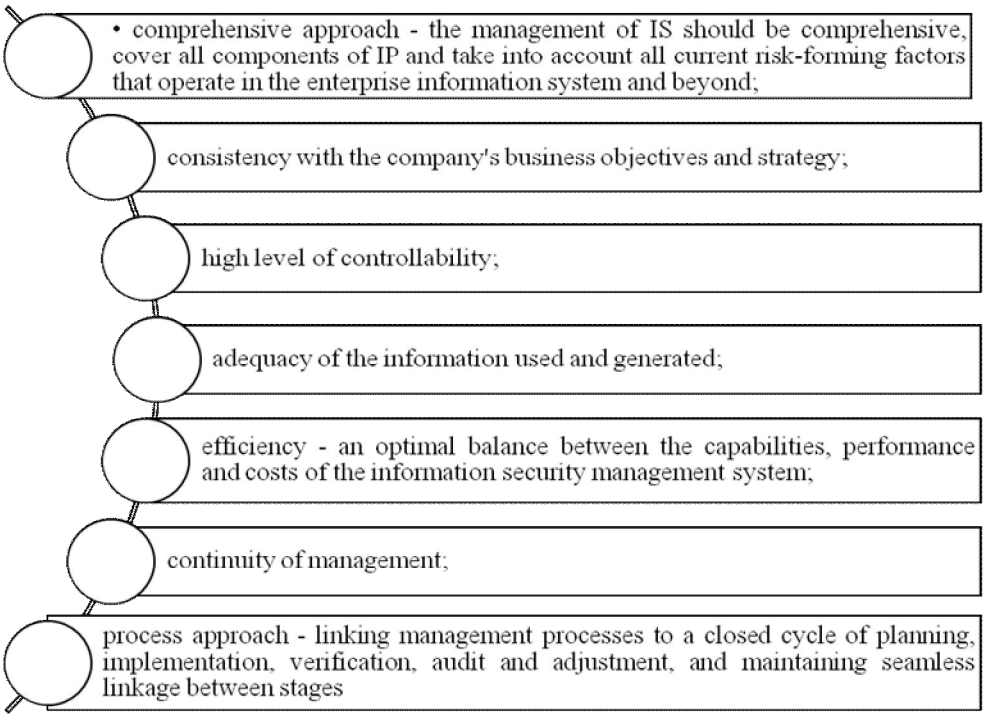

Fig. 2. Principles of information security management

The modern business environment is characterized by a number of problems that arise before the management of the enterprise in the field of information security (Fig. 3). The emergence of certain problems is caused by the threats of internal and external origin, which are presented in Fig. 4.

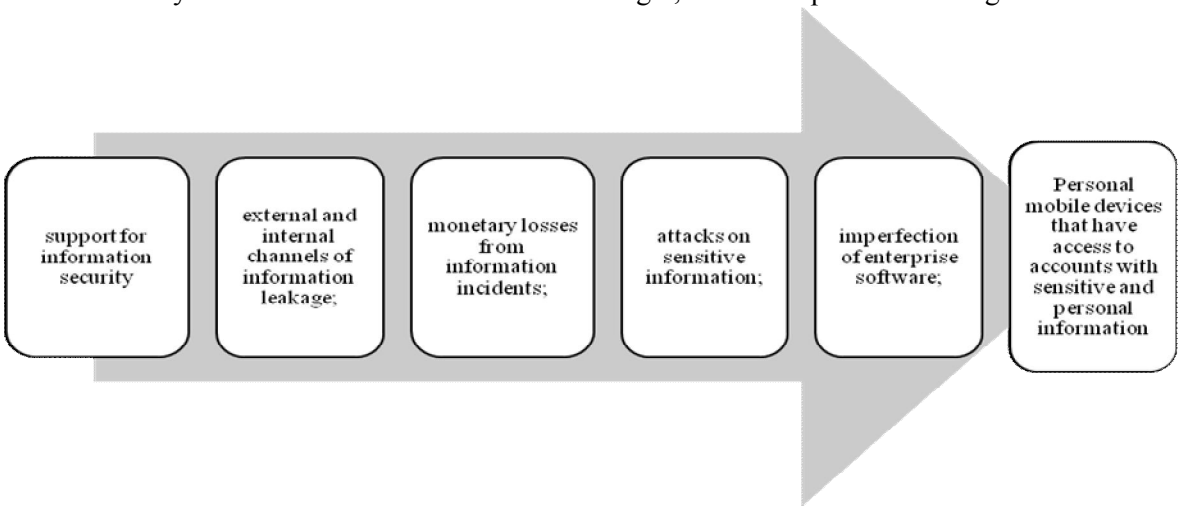

Fig. 3. Problems that arise for the management of the enterprise in the field of information security

Information security is usually understood as the state of the most efficient use of corporate resources to prevent threats and ensure the stable functioning of the business entity.

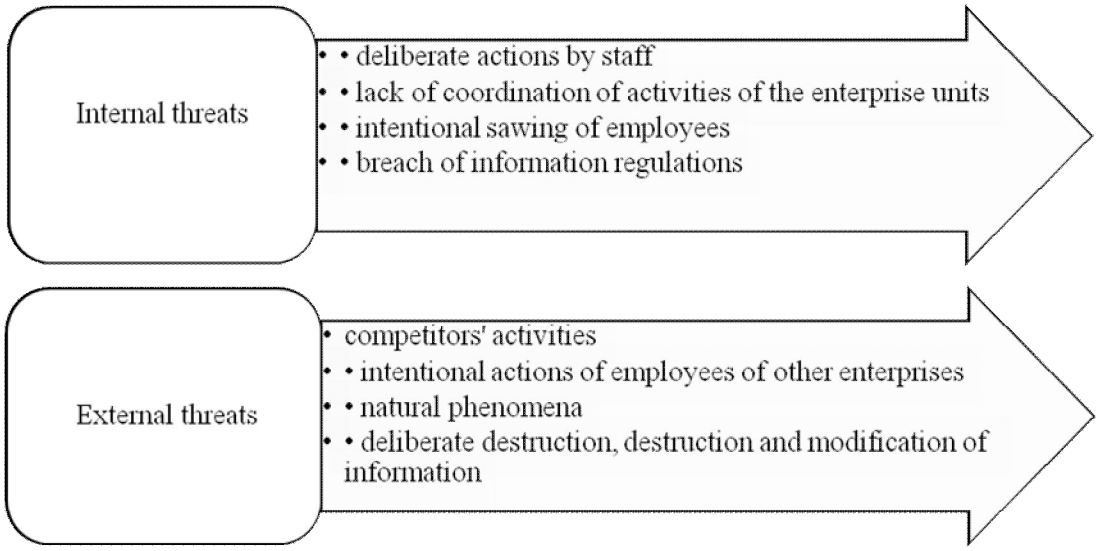

Fig. 4. External and internal threats to information security of the enterprise

Information security is one of the components of the enterprise security formation, and to ensure its stable development and competitiveness it is necessary to create an effective information security management system.

Countering and neutralizing the negative impact of certain threats and ensuring information security of the enterprise form a management system in the field of information security, which directs its activities in the following areas:

formation and practical implementation of a comprehensive multilevel enterprise information security policy and system of internal requirements, norms and rules;

organization of information security service;

development of a system of measures and actions in case of occurrence of unforeseen situations;

carrying out audits of the state of information security at the enterprise.

The system of information security management is understood as part of the general management system, the basis of which is risk analysis, and the purpose is to create, implement, control and improve measures in the field of information security [18].

An information security management system involves applying a systematic approach to managing enterprise sensitive information so that it remains secure. This system covers people, processes and IT systems.

An information security management system is a management system based on a systematic approach to business risks to create, implement, operate, control, review, maintain and improve information security.

Other scholars [1] define the information security management system as a documented system that ensures the security of information and data in an organization. Each enterprise is tasked with providing a comprehensive information security plan. Modern information systems are complex sets of technologies (i.e., hardware, software, and firmware), processes, and people working together to enable organizations to process, store, and transmit information in a timely manner to support business and business processes. The information should be accessible, accurate and up-to-date so that the management of the enterprise can make effective business decisions.

It should be noted that information security of the enterprise is a systematic, purposeful activity of management bodies of the enterprise, certain officials, whose competence is to ensure information security, using the allowed forces and means to achieve the state of security of the information environment of the enterprise, which ensures its normal functioning and dynamic development. [14]. Based on the above, we can conclude that the protection of information security of the enterprise should be comprehensive and systematic:

analysis of possible threats to information security of the enterprise;

planning and development of information security measures;

prompt implementation of the planned actions.

The enterprise information security management system performs diagnostics of possible weaknesses and threats at the head pressures (Fig. 5): evaluation of software and technical security of information; assessment of information reliability of personnel; evaluation of information provided to decision makers by the enterprise information service [5-9].

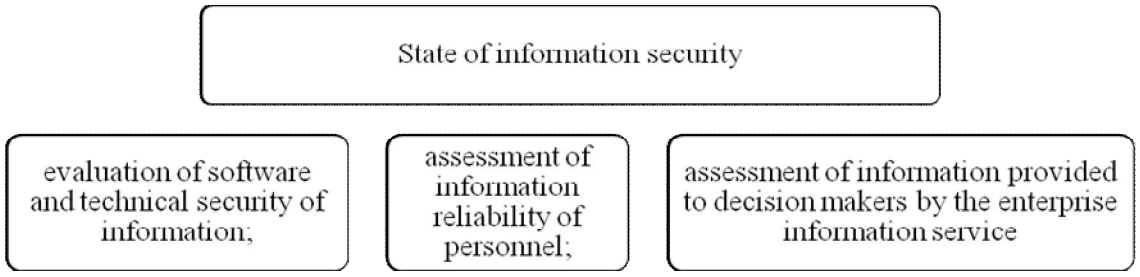

Fig. 5. Determining the state of information security of the enterprise

Accordingly, the main ways to ensure information security at the enterprise can be roughly divided into two groups – organizational and technical. Organizational security measures are limited to limiting the potential for unauthorized physical access to information systems. Technical means of protection involve the use of software and technical means, aimed primarily at limiting the access of the user, who works with the information systems of the enterprise, to the information to which he has no right [10].

The directions of technical protection of the information environment of the enterprise are [17]:

protection of automated systems against computer viruses and illegal modification – immunity programs and software modification mechanisms apply;

protection against leakage through secondary channels of electromagnetic radiation and guidance – by means of shielding of equipment, premises, the use of masking noise generators, additional checking of equipment for the presence of compromising radiation;

protection of information in communication channels and switching nodes - procedures are used for subscriber and message authentication, encryption and special communication protocols;

protection of information resources from unauthorized access and use – means of control of power-on and download of software, as well as methods of password protection at login are used;

protection of legal significance of electronic documents – in case of trust relations between two business entities and when there is a need to transfer documents (payment orders, contracts) over computer networks – to determine the truth of the addressee, the document is supplemented with a "digital signature" – a special label, inextricably logically linked to text and formatted using a secret cryptographic key.

Conclusions. Therefore, information security management is a subsystem of the overall enterprise security management system, which provides continuous risk monitoring and is focused on the formation, implementation, control, support and improvement of information security measures. The enterprise information security subsystem consists of organizational structures, policies, planning actions, responsibilities, procedures, processes and resources. The main purpose of information security of the enterprise is to protect the business interests and resources of the enterprise from liquidation and loss of confidentiality.

REFERENCES:

1. Caralli, R. A. & Wilson, W. R. (2004). The Challenges of Security Management (p. 1). Retrieved from ESM White Paper v1.0 Final-2.doc.

2. Cazemier, J. A., P. L. Overbeek & L. M. Peters. (2000) Security Management (IT Infrastructure Library Series), Stationery Office, UK.

3. Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012, ICT4Peace Publishing, Geneva.

4. Elektronnyi resurs. Rezhym dostupu: https://www.techopedia.com/definition/10282/information-security-is. Zaholovok z tytulu ekranu.

5. ISO GUIDE 72:2001, Guidelines for the justification and development of management system standards.

6. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.

7. ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance..
8. ISO/IEC 38500:2008, Corporate governance of information technology.
9. ISO/TC 176/SC 2/N 544R2, ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems, 13 May 2004.
10. Kazakevych O. Yu. Predprinimatel v opasnosti: sposoby zashchity. Praktycheskoe rukovodstvo dlya predprynymateley i biznesmenov / O.Yu. Kazakevich, N.V. Konev. – M.: Yurfak MHU, 2011. – 152 s.
11. Kormych B. A. Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy : avtoref. dys. na zdobuttia nauk. stupenia dokt. yuryd. nauk : spets. 12.00.07 «Administratyvne pravo i protses; finansove pravo; informatsiine pravo» / B. A. Kormych ; Nats. un-t vnutr. sprav. – Kh., 2004. – 42 c.
12. Kormych B.A. Informatsiina bezpeka: orhanizatsiino-pravovi osnovy : Navch. posibn. / B. A. Kormych. K. : Kondor, 2008. 382 s.
13. Managing information security amid new threat.https://searchsecurity.techtarget.com/definition/information-security-infosec.
14. Marushchak A. I. Informatsiino-pravovi napriamy doslidzhennia problem informatsiinoi bezpeky / A. I. Marushchak // Derzhavna bezpeka Ukrainy. – 2011. – № 21. – S. 92–95.
15. Petryk V. Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby / V. Petryk // Yurydychnyi zhurnal. 2009. № 5. S. 122-125.
16. Rusina Yu. O., Ostriakova V. Yu. Udoskonalennia systemy upravlinnia informatsiinoiu bezpekoiu na pidpryiemstvi // Mizhnarodnyi naukovyi zhurnal "Internauka". – 2017. – №14.
17. Stepanov E. M. «Kroty» na firme (personal i konfidentsialnaya informatsiya) // Predprinimatelskoe pravo / E.M. Stepanov. – 1999. – №4. – S. 53-56.
18. Zhuravel M.M. Problemy zakhystu informatsii [Elektronnyi resurs] / M.M. Zhuravel, S.V. Parshukov. – Rezhym dostupu: http://informatika.udpu.org.ua/?page_id=1173.

UDC 004.056.5JEL M 15

Черниш Ірина Володимирівна, доктор економічних наук, доцент. **Маховка Вікторія Михайлівна**, кандидат економічних наук, доцент. **Лобач Лілія Володимирівна**, магістрант Національний університет «Полтавська політехніка імені Юрія Кондратюка». **Управління інформаційною безпекою підприємства в умовах динамічного бізнес-середовища.** Мета статті полягає у дослідженні особливостей управління інформаційною безпекою підприємства. Визначено, що інформаційна безпека охоплює різні сфери діяльності й має на меті формування необхідних умов для підтримки інтересів підприємства, регіону, держави в інформаційній сфері. Виокремлено основні різновиди безпеки та рівні на яких здійснюється управління інформаційною безпекою: міжнародна, національна, безпека на підприємстві й безпека особистості. Визначено сутність поняття «інформаційна безпека» як певний набір стратегій управління процесами, інструментами та політикою, необхідними для запобігання, виявлення, документування й протидії загрозам цифровій і нецифровій інформації. Обов'язки інформаційної безпеки включають створення набору бізнес-процесів, котрі захищатимуть інформаційні активи незалежно від того, як форматується інформація, чи вона перебуває в транзиті, обробляється або знаходиться в стані спокою. У результаті дослідження було визначено, що система управління інформаційною безпекою складова загальної системи управління, базою якої є аналіз ризиків, а призначенням – створення, реалізація, контроль та вдосконалення заходів у сфері інформаційної безпеки. Система управління інформаційною безпекою передбачає застосування системного підходу до управління конфіденційною інформацією підприємства, щоб воно залишалося у безпеці. Така система охоплює людей, процеси й IT-системи. Результати проведених досліджень дозволяють дійти висновку, що кожне підприємство стоїть перед завданням забезпечити комплексний план захисту інформації. Сучасні інформаційні системи – це складні набори технологій (тобто апаратного, програмного та мікропрограмного забезпечення), процесів і людей, котрі працюють разом, щоб надати організаціям можливість своєчасно обробляти, зберігати й передавати інформацію для підтримки господарської діяльності та бізнес-процесів. Перспективами подальших досліджень є визначення потенційних напрямів мінімізації ризиків і загроз інформаційній безпеці, що забезпечить не тільки відповідний рівень конкурентоспроможності підприємства, але і його подальший розвиток.

***Ключові слова**:* інформація, безпека, інформаційна безпека, система управління інформаційною безпекою, захист.

UDC 004.056.5JEL M 15

Iryna Chernysh, Doctor of Sciences (Economics), Associate Professor. **Viktoriia Makhovka,** PhD, Associate Professor. **Liliia Lobach,** Master student. National University «Yuri Kondratyuk Poltava Polytechnic». **Management of information security Of the enterprise in the conditions of dynamic business environment.** The purpose of the article is to investigate the features of enterprise information security management. The authors determined that information security covers different spheres of activity and aims to form the necessary conditions to support the interests of the enterprise, region, state in the information sphere. The article defines the main varieties of security and the levels at which information security is managed: international, national, enterprise security and personal security. The essence of the concept of information security is defined as a set of strategies for managing processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security responsibilities include creating a suite of business processes that will protect information assets, whether formatted, in transit, processed, or dormant. As a result of the research it was determined that the information security management system is a component of the general management system, the basis of which is risk analysis, and the purpose is to create, implement, control and improve measures in the field of information security. An information security management system involves applying a systematic approach to managing enterprise sensitive information so that it remains secure. This system covers people, processes and IT systems. The results of the conducted researches make it possible to conclude that each enterprise is faced with the task of providing a comprehensive plan for information security. Modern information systems are complex sets of technologies (i.e., hardware, software, and firmware), processes, and people working together to enable organizations to process, store, and transmit information in a timely manner to support business and business processes. Prospects for further research are to identify potential areas for minimizing risks and threats to information security, which will ensure not only an appropriate level of competitiveness of the enterprise, but also its further development.

Keywords: information, security, information security, information security management system, business.

UDC 004.056.5JEL M 15

Черныш Ирина Владимировна, доктор экономических наук, доцент. **Маховка Виктория Михайловна**, кандидат экономических наук, доцент. **Лобач Лилия Владимировна**, магистрантка. Национальный университет «Полтавская политехника имени Юрия Кондратюка». **Управление информационной безопасностью предприятия в условиях динамической бизнес-среды**. Цель статьи заключается в исследовании особенностей управления информационной безопасностью предприятия. Установлено, что информационная безопасность охватывает различные сферы деятельности и имеет целью формирование необходимых условий для поддержки интересов предприятия, региона, государства в информационной сфере. Выделены основные разновидности безопасности и уровни, на которых осуществляется управление информационной безопасностью: международный, национальный, безопасность на предприятии и безопасность личности. Определена сущность понятия «информационная безопасность» как некий набор стратегий управления процессами, инструментами и политикой, необходимыми для предотвращения, выявления, документирования и противодействия угрозам цифровой и нецифровой информации. Обязанности информационной безопасности включают создание набора бизнес-процессов, которые будут защищать информационные активы независимо от того, как форматируется информация, обрабатывается или хранится. В результате исследования было определено, что система управления информационной безопасностью составная часть общей системы управления, базой которой является анализ рисков, а назначением – создание, реализация и совершенствование мероприятий в сфере информационной безопасности. Система управления информационной безопасностью предполагает применение системного подхода к управлению конфиденциальной информацией предприятия, чтобы оно оставалось в безопасности. Данная система охватывает людей, процессы и информационные системы. Результаты проведенных исследований позволяют сделать вывод, что каждое предприятие стоит перед задачей обеспечить комплексный план защиты информации. Современные информационные системы – это сложные наборы технологий (то есть аппаратного, программного и микропрограммного обеспечения), процессов и людей, которые работают вместе, чтобы предоставить организациям возможность своевременно обрабатывать, хранить и передавать информацию для поддержки хозяйственной деятельности и бизнес-процессов. Перспективами дальнейших исследований является определение потенциальных направлений минимизации рисков и угроз информационной безопасности, что обеспечит не только соответствующий уровень конкурентоспособности предприятия, но и его дальнейшее развитие.

Ключевые слова: информация, безопасность, информационная безопасность, система управления информационной безопасностью, защита.