JEL code classification: C10, M41; DOI: 10.31388/2519-884X-2020-42-226-231

***Illiashenko K.V.**, PhD in Economics, Associate Professor*
Dmytro Motornyi Tavria State Agrotechnological University
katerina.illyashenko@tsatu.edu.ua

ACCOUNTING AND ANALYTICAL SYSTEM OF THE ENTERPRISE IN THE ASPECT OF INFORMATION SECURITY

Abstract. *The article deals with the impact of Information Technologies on the security of accounting and analytical activities of the enterprise in modern economic conditions. The most common approaches to determining the economic security of an enterprise are studied. The concepts of "information threats" and "information security" are highlighted as separate categories that are most characteristic of automated production and accounting and analytical processes. Types of information risk are defined, both in specific cases and in the broad context of Information Security. The level of Information threat risks and ways to assess them are analyzed. The expediency of information security in accounting using computer technologies is justified. Measures to prevent possible information hazards for accounting and analytical activities are proposed.*

Keywords: *information, information technology, security, enterprise, risks, activities, accounting, analysis*

УДК: 657:358

***Ілляшенко К.В.**, к.е.н., доцент,*
Таврійський державний агротехнологічний університет імені Дмитра Моторного
katerina.illyashenko@tsatu.edu.ua

ОБЛІКОВО-АНАЛІТИЧНА СИСТЕМА ПІДПРИЄМСТВА В АСПЕКТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Метою дослідження є розгляд впливу інформаційних технологій на економічну безпеку підприємства, аналіз інформаційних ризиків для бухгалтерського обліку та пошук заходів щодо запобігання можливим інформаційним небезпекам. Формування інформаційного суспільства концептуально і практично означає створення нового світогляду, в якому захист від інформаційних загроз матиме дуже важливе значення. У статті розглядається вплив інформаційних технологій на економічну безпеку підприємства в сучасних економічних умовах. Досліджено найбільш поширені підходи до визначення економічної безпеки підприємства. Виділено поняття» інформаційні загрози «та» інформаційна безпека" як окремі категорії, найбільш характерні для автоматизованих виробничих та обліково-аналітичних процесів. Визначено види інформаційного ризику, як у конкретних випадках, так і в широкому контексті інформаційної безпеки. Проаналізовано рівень ризиків інформаційної загрози та способи їх оцінки. Обґрунтовано доцільність забезпечення інформаційної безпеки в бухгалтерському обліку з використанням комп'ютерних технологій. Було вирішено, що питання інформаційної безпеки в бухгалтерському обліку з використанням комп'ютерних технологій слід розглядати в двох аспектах: запобігання зловживань або ненавмисних порушень з боку працівників підприємства (внутрішній аспект) та створення відповідної інформаційної безпеки для запобігання несанкціонованого доступу, пошкодження комп'ютерних програм або даних вірусами, комп'ютерного саботажу (зовнішній аспект). Запропоновано заходи щодо запобігання ймовірній небезпеці для інформації, що служить для обліково-аналітичної діяльності, а також можливі методи зниження інформаційного ризику, формування нового підходу до управління підприємством, захист внутрішньої інформації від зовнішнього втручання, аналіз інформаційних ризиків при прийнятті управлінських рішень. Зроблено висновок про те, що формування нового підходу до інформаційної безпеки бухгалтерського обліку потребує перегляду кадрових питань, нових форм контролю та обов'язкового обліку факторів, характерних для нової цифрової економіки.*

Ключові слова: *інформація, інформаційні технології, безпека, підприємство, ризики, діяльність, бухгалтерський облік, аналіз*

Problem statement. The rapid digitalization of all spheres of life of society and the state has caused, in addition to undoubted advantages, a number of significant problems. One of them was the need to protect accounting and analytical systems and other important data of enter-

prises from possible information hazards. While the economic potential is increasingly determined by the level of development of the information structure, the potential vulnerability of the economy to information impacts is also growing proportionally. So, hacker attacks, ransomware viruses, industrial espionage, theft of personal information-all this has become an integral part of business risks. And a fully automated form of accounting with a network connection is becoming one of the main sources of such vulnerability.

Analysis of recent research and publications. The research on economic security issues was based on the works of Shevchenko I., Lokhanov N., Bosner Yu. and others. The solution of the problem of information security and information risks was started in the works of Tsaregordtsev O. V., Tsigichko V. M., Yasenev V. M. and others. Problems of information security of accounting were considered in the research Muravsky V., Shishkova N. L., Ignatenko M. M.

Despite the large number of publications on the problem under consideration, there is still no comprehensive analysis of potential information threats to accounting at enterprises.

Formulation of the goals of the article. The purpose of the study is to consider the impact of Information Technologies on the economic security of accounting and analytical activities of the enterprise, analyze information risks for accounting and search for measures to prevent possible information hazards.

The content of the main material. The formation of the information society is based on the latest information, telecommunications and communication technologies. It is new technologies that have led to the rapid spread of global information networks, which open up fundamentally new opportunities for International Information Exchange. The formation of the information society conceptually and practically means the formation of a new worldview, in which security against Information threats will be very important.

Informatization of the economy began not so long ago with the introduction of computer technology and the spread of the Internet. It raised a number of new questions for researchers of economic activity of enterprises, including on issues of economic security.

When carrying out commercial activities, there is information that, as other market participants know, can significantly reduce the profitability of this activity. The company's activities generate information, the disclosure of which may reduce the effectiveness of the policy. Such information is private, and the established mode of its use is designed to prevent unauthorized access to it. In this case, the object of protection is the mode of access to information, and information security consists in the impossibility of violating this mode. An example is information and telecommunications systems and communication facilities designed to process and transmit information that is part of the system. The main object of security in them is the mode of access to classified information. Information security of such systems consists in protecting this information from unauthorized access, destruction, modification, and other actions. The information security system includes subsystems:

- computer security;
- data security;
- secure software;
- security of communications [1].

At the moment, there are several common approaches to determining the economic security of an enterprise:

- protection against economic crimes – ensuring the security of an enterprise is reduced to protection against various types of economic crimes (theft, fraud, falsification, industrial espionage, etc.). Of course, these threats are very important and must be constantly analyzed and taken into account, but it is impossible to reduce the concept of economic security only to this [2, p.179];

- the state of effective use of resources or potential – an approach that tries to avoid the use of the concept of threat in the definition of economic security, is based on the economic concepts of achieving the goal, functioning of the enterprise, that is, it is a resource-functional approach;

- the presence of competitive advantages – an approach whose followers believe that the presence of competitive advantages due to the compliance of material, financial, personnel, technological potentials and organizational structure of the enterprise with its strategic goals and objectives will provide it with a certain level of economic security [3, p.54]. But the very fact of

having advantages and potential without their use and implementation does not guarantee the company Economic Security;

- implementation and protection of economic interests – a relatively new approach based on the implementation and protection of economic interests of the enterprise, defines economic security as the protection of its vital interests from internal and external threats, that is, the protection of the enterprise, its personnel and intellectual potential, information, technology, capital and profit, which is provided by a system of measures of a special legal, economic, organizational, information-technical and social nature [4, p.37].

In our opinion, the latter approach is the most correct, since it specifies a system of information technology measures at the same level as others. But information threats are not yet classified as a separate category.

Ensuring information security should begin with identifying the subjects of relations related to the use of information systems. The range of their interests can be divided into the following main categories: accessibility (the ability to get the required information service in a reasonable time), integrity (relevance and consistency of information, its protection from destruction and unauthorized changes), confidentiality (protection from unauthorized access) [5].

Based on the above, in the most General form, information security can be defined as the impossibility of harming the properties of a security object caused by information and information infrastructure (Fig. 1).

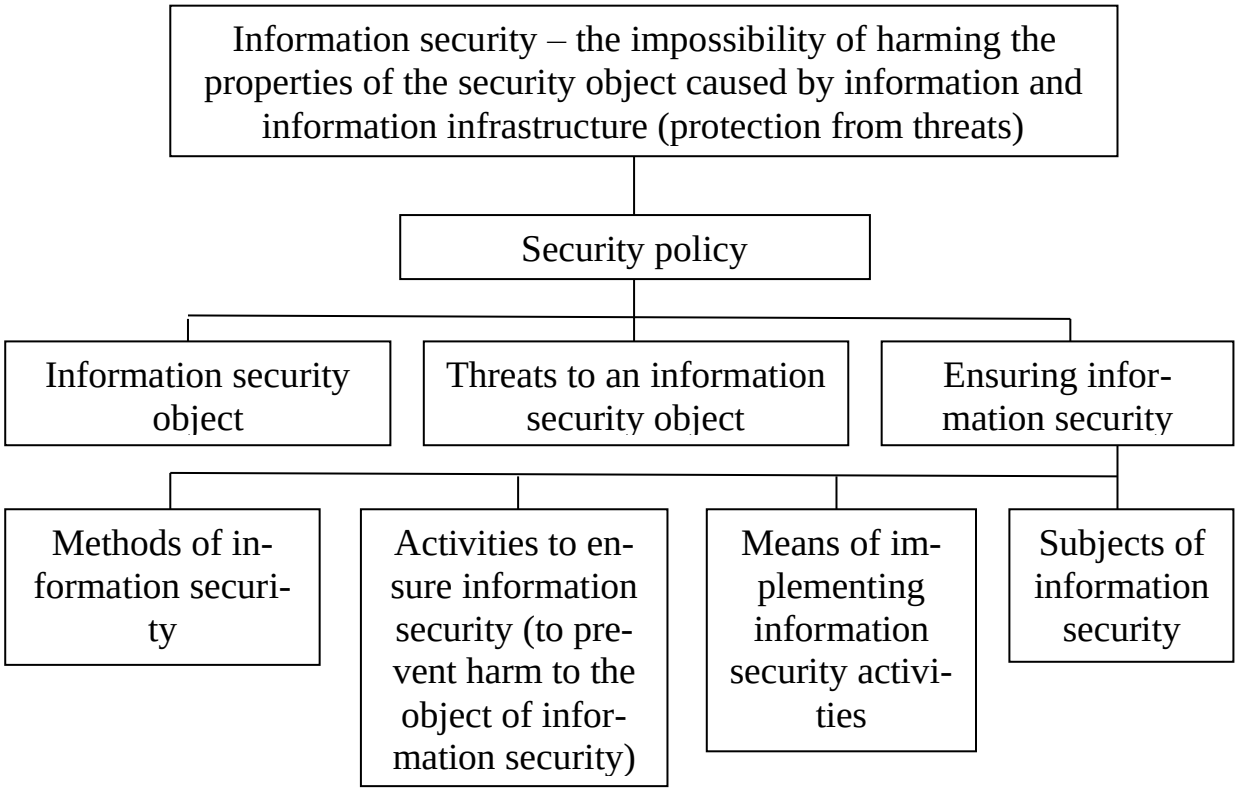

Fig. 1. General view on enterprise information security

Since the object of Information Security is an enterprise, the content of the concept of «Information Security» will consist in protecting the interests of the owner of this enterprise, satisfying with the help of information, or related to the protection against unauthorized access of those information that are quite important to the owner. Interests manifest themselves through objects that can serve to satisfy them, and actions taken to own these objects. Accordingly, interests, as an object of security, can be represented by a set of information that can satisfy the interest of the owner, and his actions aimed at mastering information or concealing information. These components of the information security object are protected from external and internal threats [6, p.188].

It should be noted that the use of Information Technologies is one of the important factors determining the competitiveness of enterprises.

However, along with the obvious advantages, such as automation of production and accounting and analytical processes, availability of electronic calculations, speed of information processing for making managerial decisions, the use of Information Technologies brings new significant risks [7, p. 20].

You can give many definitions of information risks, the application of each of which will be justified by the tasks being solved. The narrowest definition of information risks is the risks of loss from unauthorized changes in information due to failures in the functioning of information systems or their failure, leading to losses [8, p.251].

Options for processing information risks can be divided into the following stages [9]:

– risk reduction – the level of risk should be reduced by implementing measures and controls so that the residual risk can be re-evaluated as acceptable (implementation of information security tools);

– risk keeping - the decision to save risk without taking further action;

– risk avoidance – abandonment of an activity or condition that causes a specific risk. this can also include exposure to the source of the threat, which can change the conditions that cause the risk;

– transfer (delegation) of risk – the risk is transferred to the party that can most effectively manage it.

In the process of risk analysis, the following activities are carried out:

– identification of all assets within the selected area of activity;

– determining the value of identified assets;

– identification of threats and vulnerabilities for the identified assets;

– risk assessment for possible cases of successful implementation of information security threats against identified assets;

– selection of risk acceptance criteria;

– preparing a risk management plan.

Schematically, this can be depicted as follows (Fig. 2).

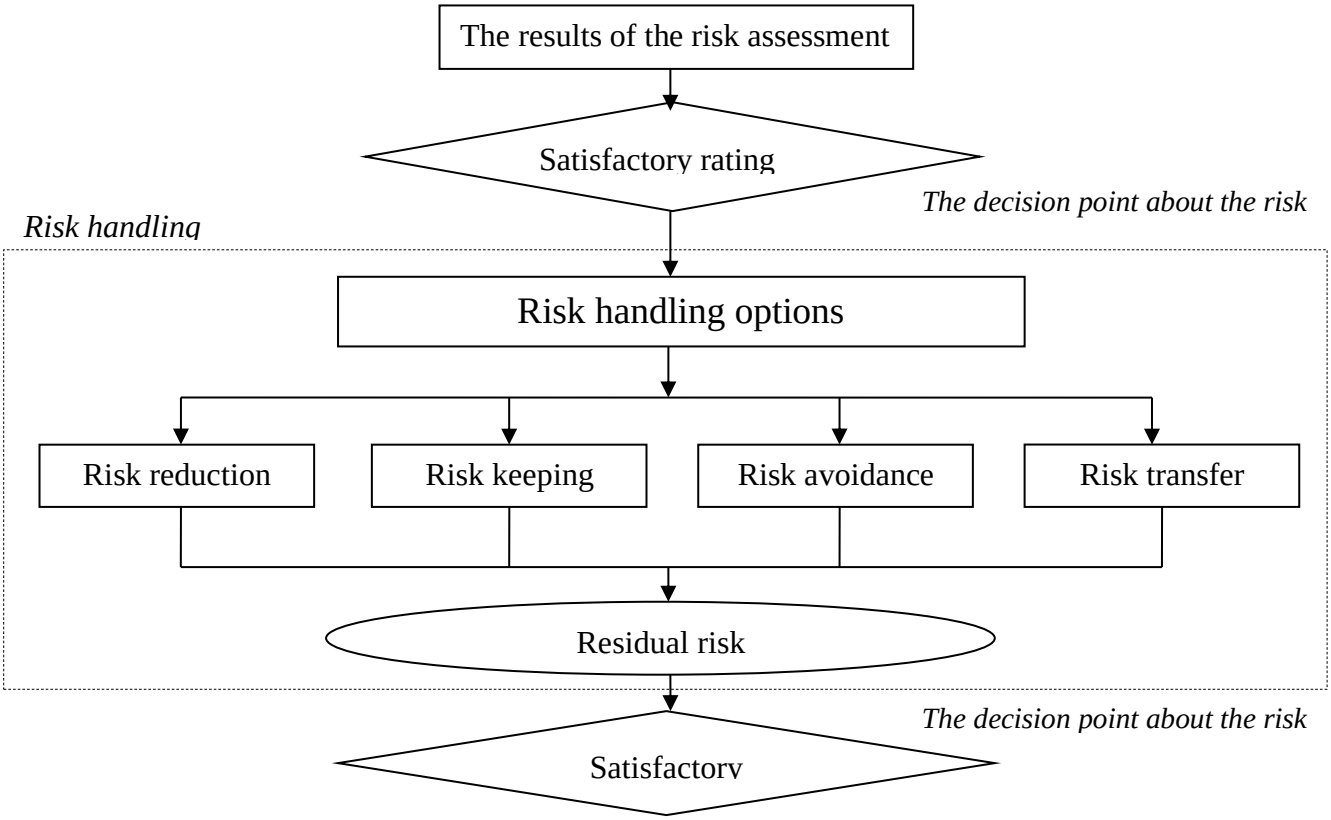

Fig. 2. Options for handling information security risks*

- author's development

Information technologies help in managing and optimizing the company's activities, and prevent many economic risks. For example, they reduce the probability of bankruptcy [10, p.

197]. But at the same time, they also act as a risk factor.

The issue of information security in accounting using computer technologies should be considered in two aspects: prevention of abuse or unintentional violations by employees of the enterprise (internal aspect) and creation of proper information security to prevent unauthorized access, damage to computer programs or data by viruses, computer sabotage (external aspect) [11, p.232].

Preventive mechanisms for preventing losses and distortions of accounting information should be based on complex, interrelated methods and procedures for identifying and analyzing risks for the enterprise's accounting information system, developing control technologies for managing the security of Accounting Information [12, p.126].

Currently, the largest share in this group of activities in accounting and Reporting Information Processing Systems is made up of special software packages or individual programs that are included in the software in order to implement information protection tasks. Technological means of information security are a set of measures that are organically integrated into the technological processes of data transformation [13, p. 87].

Possible methods of reducing information risk for each unit are standard and can be used in accounting and analytical activities [14, p.121]:

- risk acceptance-recognition of potential losses as acceptable;
- risk prevention - making decisions aimed at removing the risk factor, in particular, eliminating the causes of the corresponding threat (for example, refusing to use installed software that significantly violates information security requirements);
- risk limitation – introduction of special controls that reduce the probability of implementing an information threat and (or) its consequences;
- risk transfer-creating conditions to compensate for potential losses by transferring risk to a third party, for example, using insurance or outsourcing certain functions.

These methods are not mutually exclusive and can be used in a comprehensive manner.

But preventing information hazards should not be limited to reducing risks alone. Since the onset of crisis situations is almost impossible to predict, it is necessary to create a number of measures, and above all, control systems for rapid response and making the right management decisions.

For an automated accounting form, it is very important to have reliable protection and daily backup of data on secure media. Printing out the most important financial documents on paper should not be considered outdated, so that the work of the accounting service does not stop, for example, due to power outages.

In our opinion, an equally important factor in accounting security is the use of only licensed software that has a technical support service, updates to vulnerable components, and so on.

Also, the problem deserves more attention from business leaders who still use outdated management models. The formation of a new approach requires a review of personnel issues, new forms of control and mandatory consideration of factors characteristic of the new digital economy.

Conclusion. In the course of our research, we concluded that at this stage, information threats are underestimated and insufficiently studied in the context of accounting and analytical activities of enterprises. While the economic potential is increasingly determined by the level of development of the information structure, the potential vulnerability of the economy to information impacts is growing proportionally. That is why it is so important to thoroughly study the types of information threats and develop measures to avoid them. This is primarily the formation of a new approach to enterprise management, protection of internal information from external interference, analysis of information risks in making managerial decisions, and so on.

The rapid development of technology progress has led to the fact that the information environment is growing exponentially and information technologies are penetrating all spheres of life. Information aspects of the security of accounting and analytical activities of enterprises are becoming an increasing priority. Thus, the topic of information threats and accounting security remains quite relevant, and the issues considered deserve further in-depth research.

References:

1. Understanding the Fundamentals of Information Security. Available at: https://imagexmedia.com/blog/2017/05/understanding-fundamentals-information-security (accessed 3 November 2020).
2. Shevchenko I. (2010) Osoblyvosti formuvannia ekonomichnoi bezpeky pidpryiemstva [Features of formation of economic security of the enterprise]. *Nauka moloda*. no. 10, pp. 178-181.
3. Lokhanova N. (2005) Systema upravlinnia stanom ekonomichnoi bezpeky pidpryiemstva: problemni pytannia, kontseptsiia rozvytku [Management system of the state of economic security of the enterprise: problematic issues, the concept of development]. *Ekonomist*. no. 2, pp. 52-56.
4. Bosner Yu. (2010) Strategicheskie podhodyi k ekonomicheskoy bezopasnosti predpriyatiy [Strategic approaches to economic security of enterprises]. *Institutsionalnaya ekonomika.* no. 1, pp. 34-48.
5. How to ensure information security is at the heart of the business. Available at: https://www.computerweekly.com/opinion/How-to-ensure-infosec-is-at-the-heart-of-any-business (accessed 5 November 2020).
6. Ovsiannikov V.V., Dekhtiar S.V., Palamarchuk S.A., Chernysh Yu.O., Shemendiuk O.V. (2015) Analiz normatyvno-pravovykh ta orhanizatsiino-tekhnichnykh aspektiv zabezpechennia informatsiinoi bezpeky [Analysis of legal, organizational and technical aspects of information security]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. no. 3(24), pp. 187-193.
7. Tkachuk T. (2009) Formuvannia systemy informatsiinoi bezpeky biznesu [Formation of business information security system]. *Biznes i bezpeka.* no. 4, pp. 19-23.
8. Mishchenko S. P. (2012) Informatsiina skladova ekonomichnoi bezpeky pidpryiemstva [Information component of economic security of the enterprise]. *Visnyk ekonomiky transportu i promyslovosti.* no. 39, pp. 250-254.
9. International Convergence of Capital Measurement and Capital Standards A Revised Framework, Basel, Switzerland, November 2005.
10. Tereshchenko M. A. (2012) Informatsiini tekhnolohii v systemi upravlinnia pidpryiemstvom pidpryiemstva ta zapobihannia yoho bankrutstva [Information technologies in the enterprise management system of the enterprise and prevention of its bankruptcy]. *Zbirnyk naukovykh prats Tavriiskoho derzhavnoho ahrotekhnolohichnoho universytetu (ekonomichni nauky)*. no. 1 (17), pp. 193-200.
11. Muravskyi V. (2013) Zabezpechennia informatsiinoi bezpeky v avtomatyzovanykh systemakh bukhhalterskoho obliku [Information security in automated accounting systems]. *Ekonomichnyi analiz.* Vol.4. no. 12, pp. 232-235.
12. Shyshkova N. L. (2016) Zasoby pidvyshchennia kerovanosti bezpekoiu oblikovoi informatsii [Tools to improve security manageability of accounting information]. *Ekonomichnyi visnyk.* no. 3, pp. 119-127.
13. Ignatenko M. M. (2017) Formuvannia informatsiinoi bezpeky pidpryiemstv i orhanizatsii v umovakh avtomatyzatsii obliku ta finansovoi zvitnosti [Formation of information security of enterprises and organizations in the conditions of authorization of accounting and financial statements]. *Visnyk Berdianskoho universytetu menedzhmentu i biznesu.* no. 4 (40), pp. 84-88.
14. Illiashenko K. V. (2012) Informatsiinyi vzaiemozviazok analizu ta bukhhalterskoi zvitnosti [The information relationship analysis and financial statements]. *Visnyk KhNTUSH: ekonomichni nauky*. no. №127, pp. 118-123.

Список літератури:

1. Understanding the Fundamentals of Information Security. URL: https://imagexmedia.com/blog/2017/05/understanding-fundamentals-information-security (дата звернення: 03.11.2020)
2. Шевченко І. Особливості формування економічної безпеки підприємства. *Наука молода.* 2010. №10. С. 178-181.
3. Лоханова Н. Система управління станом економічної безпеки підприємства: проблемні питання, концепція розвитку. *Економіст*. 2005. №2. С. 52-56.
4. Боснер Ю. Стратегические подходы к экономической безопасности предприятий. *Институциональная экономика.* 2010. №1. С. 34-48.
5. How to ensure information security is at the heart of the business. URL: https://www.computerweekly.com/opinion/How-to-ensure-infosec-is-at-the-heart-of-any-business (дата звернення: 05.11.2020)
6. Овсянніков В.В., Дехтяр С.В., Паламарчук С.А., Черниш Ю.О., Шемендюк О.В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2015. № 3(24). С. 187-193.
7. Ткачук Т. Формування системи інформаційної безпеки бізнесу. *Бізнес і безпека.* 2009. №4. С. 19-23.
8. Міщенко С. П. Інформаційна складова економічної безпеки підприємства. *Вісник економіки транспорту і промисловості.* 2012. №39. С. 250-254.
9. International Convergence of Capital Measurement and Capital Standards A Revised Framework, Basel, Switzerland, 2005.
10. Терещенко М.А. Інформаційні технології в системі управління підприємством підприємства та запобігання його банкрутства. *Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки).* 2012. №1 (17). С. 193-200.
11. Муравський В. Забезпечення інформаційної безпеки в автоматизованих системах бухгалтерського обліку. *Економічний аналіз.* 2013. Вип. 12. Ч. 4. С. 232-235.
12. Шишкова Н.Л. Засоби підвищення керованості безпекою облікової інформації. *Економічний вісник.* 2016.№3.С.119-127.
13. Ігнатенко М.М. Формування інформаційної безпеки підприємств і організацій в умовах автоматизації обліку та фінансової звітності. *Вісник Бердянського університету менеджменту і бізнесу.* 2017. № 4 (40). С. 84–88.
14. Ілляшенко К.В. Інформаційний взаємозв'язок аналізу та бухгалтерської звітності. *Вісник ХНТУСГ: економічні науки.* 2012. №127. С. 118-123.