УДК: 330.131.7
JEL: D89

В. І. Скіцько
Київський національний економічний університет імені Вадима Гетьмана

ІНФОРМАЦІЙНІ РИЗИКИ ЛОГІСТИЧНИХ СИСТЕМ

Використання новітніх інформаційних та телекомунікаційних технологій в логістичних системах, а також навмисні чи випадкові дії людей можуть зумовити виникнення низки інформаційних ризиків. У роботі розкрито сутність інформаційних ризиків логістичних систем. Запропоновано бачення автора щодо визначення поняття інформаційних ризиків логістичних систем, їх об'єкта, суб'єкта, джерел, а також класифікації. Проаналізовано різні підходи щодо управління та моделювання таких ризиків та окреслено подальші напрями досліджень.

Ключові слова: логістична система, інформаційний ризик, моделювання, оцінювання, ризик-менеджмент, класифікація інформаційних ризиків.

INFORMATION RISKS OF LOGISTICS SYSTEMS

The use of new information and communication technologies in logistics systems and intentional or random actions of people can lead to occurrence of information risks. In this paper, the essence of information risks logistics systems is revealed. The paper presents the author's vision of the definition of information risks in logistics systems, their objects, subjects, sources and classification. Existing approaches to modelling and control of such risks was performed. Outlines, future directions of research were put forward.

Key words: logistics systems, information risk, modelling, evaluation, risk management, information risk classification.

Problem statement. Today it is not enough to make a high quality product or provide a service. It is necessary that this product or service is really needed by the consumer, moreover – needed in the required quantity and good quality, for the attractive price and delivered to the agreed place and at the agreed time. This can be achieved by building the effective company's logistics system in which information occupies one of the main places.

Information stream always accompanies the material stream which is considered the main one. And although it is hard to talk about the existing of the notion logistics itself without the material stream, its existence would be problematic without accompanying streams (information, financial and service). At the moment there have been no considerable changes in material streams flow lately. The goods are delivered by various means of transport just it was done before. At production facilities the products are still made of raw materials and definite constituents which still requires the definite number of operations. Although the production is constantly modernized, the modernization usually presupposes automation of the number of production operations, i.e. replacement of men with machines (computer, robot, etc.). Besides, in order to increase the effectiveness of the company's functioning the automated systems of management, the systems of support of decisions making and other software means of processing, storing and transfer of information may be used. However, their use stipulates the occurrence of the corresponding information risks and IT-risks.

In context of logistics systems any actions with information stream also condition the occurrence of the corresponding risks. At the moment one of the main problems is also the protection of information from competitors or other parties which may damage the company having acquired the information. In this case we may talk about the risks of information security. Wide use of up-to-date information and telecommunication means and technologies in logistics may be considered innovative, as there is no enough experience of their use. This also brings about the risks. With the help of such means information is represented in electronic form. That is why we can talk about electronic information risks. There are also other situations in logistics systems in which occur the risks that may be considered information ones.

Contemporary conditions of business activity require the responsible attitude to information risks, in particular, due to the fact that information constituent of business plays the increasingly more important role in strengthening the company's competitive ability. Therefore, there is a need to identify the potential information risks of logistics systems, make their classification; to determine the factors (sources) of risks, their objects and subjects; to conduct the quantitative evaluation of the risks level with the help of the number of economical and mathematical models; to develop the effective system of information risks management etc.

Analysis of latest researches and publications. A great number of works of Ukrainian and foreign scientists and specialists are devoted to various aspects of the problem of modelling and management of economic risks. In part of these works logistics risks are investigated. In particular, Goncharov V. M., Larina P. P., Baluyeva O. V., Ovechkina O. A., Morgachov I. V. investigate the logistics risks using the traditional approach which presupposes the determination of essence of risk in logistics, conduction of system analysis of risks, development of backgrounds, directions and methods of risks management [1]. These authors point out that logistics activity is usually carried out under the conditions of asymmetry of information which stipulates the occurrence of the corresponding risks which considerably effect the result of the company activity. Brodetskiy G. L., Gusev D. A., Yelin E. A. investigate first of all the problem of decision making in logistics under the conditions of risk [2] pointing out among the logistics risks the risks of material, financial and information streams. Yenchenko Ye. V. investigated the system risks in logistics, proposed the corresponding mathematical models of risks evaluation in the processes of supply, distribution and service maintenance [3]. Rovenskikh M. V. proposes in the works [4] the recommendations of determining the risks of logistics systems of the production facility, methodical approach as for evaluation of the forecast level of such risks and corresponding model and system of risks management. The number of authors, for example Volynets L. M. and Gamelyak I. P. [5], Korolenko N. V. [6], Kondratenko N. O. and Lobashov O. O. [7], Koretsku M. [8], regard the conceptual principles of risk management in logistics, provide practical recommendations as for developing the system of logistics risk management.

On the other side, there are a number of investigations on information risks of the companies, in particular [9–11]. The analysis of these and other works has shown that at the moment there is no unanimous definition of the notion "information risk". Some authors consider that information risk is connected with any undesired situations which may affect the completeness, truthfulness, actuality of information used in taking managing decisions. Others think that information risks are conditioned by the application of informational means and technologies in company's activity. Besides, the risks of information safety are often taken as information risks.

However, at the moment the problem of analysis, modelling and managing information risks in logistics is still not investigated enough. In the number of works there are some aspects of this problem, but there are no systematic investigations which predetermined the choice of the topic and goal of the given work.

The goal of investigation is to analyze the existing principles of analysis, modelling and management of information risks in logistics, specify the existing and develop the new ones.

Main results of investigation.

The essence of information risks in logistics systems. In major cases it is not of economic benefit to avoid the risks, it is necessary to be able to take it into account in making managing decisions applying the modern instruments of modelling. At the same time there are risks that are practically impossible to avoid. Information risks may be referred to them. We can make such conclusion, in particular, due to the fact that without complete, correct and latest information it is almost impossible to take a valid decision.

The absence of unambiguous generalized explanation of the notion of information risk predetermines the necessity of its definition in scientific investigations.

Under logistics system we will understand a specially organized integration of logistics elements (chain items) within the frames of a definite economic system for optimization of the processes of transformation of material stream [12]. Logistic elements (components) are people, transport, warehouses, means of communication, information, structures, tasks, technologies etc. [12, 13].

Basing on the existing conceptual approaches to risks definition, in particular [14], we can state the following: *information risk of the logistics system* is the economical category which reflects the peculiarities of perception by the persons taking decisions in the logistics system of fuzziness and conflict in situations connected with potential losses and other problems in organization of transfer and storing of the necessary information of the appropriate quality, necessary contents in the required place and at the required time to the necessary person who takes decisions. In other words, information risk is connected with potential undesired situations which interfere with achieving the goal of the company's information logistics and stipulate the corresponding potential losses.

The object of information risk of the logistics system is a logistics system as a complex of various logistic components that need complete, trustworthy and latest information for effective functioning which may be difficult to transfer and store.

The subject of information risk of the logistics system are the people (as elements of the logistics system) who facilitate the achieving of aim of the risk object functioning, have the corresponding competences for taking decisions as for the object of the risk and bear the responsibility for the consequences of realization of these decisions.

The sources of information risk of the logistics system are the factors (processes, phenomena) the occurrence of which makes it difficult to receive the complete, trustworthy and latest information for taking the corresponding decisions in logistics system.

Classification of information risks of logistics systems. One of the important aspects in investigation of any type of risk is its classification. However, there is no generally accepted concept of risk classification, each of the scientists and specialists put forward their own vision of the problem. Besides, among the researched scientific works we didn't find any systemic classification of information risks of logistics systems. That is why basing on the most widely used approaches and principles of risks classification enlisted, in particular, in [14, 15], we will propose our own classification of information risks of logistics systems.

Conceptually the following groups of information risks of logistics system may be pointed out: 1) risks of functioning of the company's information system; 2) risks if information security of the company; 3) information risks of logistic elements; 4) risk of logistic streams.

Risks of functioning of the company's information system. One of the main constituents of modern company's functioning is its information system through which automation of business processes is carried out and on the basis of built into it system of reports the management can take managing decisions. "Information system in logistics is in a certain way organized complex of personnel, interrelated means of computer equipment, various guides, necessary software which provide the opportunity to plan, regulate, control and analyze the functioning of the logistics system" [16].

However, in the work of such system a number of undesired situations may occur which stipulate the occurrence of the corresponding information risks. The factors of such situations may be: intentional or unintentional actions of employees which condition misrepresentation of information in the system and/or incorrect work of information system; unauthorized access to the system from outside (in particular, there is a probability of hacker attacks on the sites of Internet shops not connected with information system); there may also be bugs in software code which may not show not on the stage of system testing, but in its complete version; changes of software code, adding of new modules to information system with the aim of improving the automation of the existing business processes or automation of the new ones; probable errors in database structure; problems in functioning of information system hardware (computers, laptops, smartphones, scanners, computer and telecommunication networks etc.).

In general case in the structure of the logistic information system we can distinguish the subsystem of managing the order procedures; subsystem of support of taking logistic decisions; subsystem of scientific research and communication; subsystem of generating outgoing forms and reports [17, 18] and corresponding information risks. Information risks of the subsystem of managing the order procedures will be connected with the probable distortion of information as a result of information exchange among the contractors – participants of the logistics system (logistics supply chain), in particular, due to electronic data exchange. The basis of the automated subsystem of support of taking logistic decisions is a number of economic and mathematical methods and models, and the correctness of their work depends on the "quality" of the used in them incoming information. Therefore, distortion of such information, its incompleteness, incorrectness etc. stipulates the occurrence of the corresponding information risks that may fundamentally affect the decisions of the company management. In the subsystem of scientific research and communication the interrelation among the elements of the logistics system and managing functions is realized with application of various instruments, predictive estimation of the influence of the external and internal environment of the company on the logistics system functioning is carried out [18]. In this subsystem various source of information are used which condition the corresponding information risks. The subsystem of generating the outgoing forms and reports represents the outgoing interface where the results of functioning of other subsystems are shown in convenient for the person shape and, in our opinion, restricted risks to the full are typical of it.

Information system in logistics consists of functional and supplying subsystems [16]. Supplying subsystem includes [16]: technical supply – means with the help of which generation, transfer, reception and processing of information streams in logistics system are carried out; information supply – various guides, classifiers, means of formalized description of data etc.; mathematical supply – the complex of economical and mathematical methods and models with the help of which logistic tasks are completed (which form the functional subsystem). Undesired situations in functioning of these subsystems condition the occurrence of the corresponding information risks.

Risks of information security of the company can be considered one of the main information risks, as the competitor side, having acquired some information, may bring considerable damage to the company. "Risks of information security are the risks which information assets of the organization are subject to" [19]. Information assets are the information represented in paper, electronic or oral form and is of considerable value for the company [19].

Using the classification of information risks of the company put forward in [20], to the risks of information security in logistics we may refer the following ones: the risk of potential leak of confidential, commercial information (which may diminish the competitive advantages of the company, harm the reputation of the company, derail some agreements etc.), connected with performing logistic operation; risk of loss of valuable data or their probable inaccessibility due to, in particular, failures in the functioning of information and telecommunication network and system caused by the actions of the hackers; the risk of the probable distortion or deletion of information (which is used in functioning of the logistics system) by hackers or the company employees (intentional or unintentional).

Information risks of logistic elements. In general to logistic elements may be referred people, material values, structures, tasks, technologies etc., which within the frames of the logistics system are oriented on achieving definite goals in conditions of the ever changing external environment [12, 13]. For achieving the goals of functioning of the logistics system such elements should own definite information the acquiring of which may be connected with corresponding risks. The signs of errors that such information may include, and other undesired situations connected with its transfer and processing by the logistics elements can be considered operational information risks of the logistics elements. In particular, operators entering data in the computer system may make a mechanical mistake (misprint) which will be revealed in some time, but on the basis of the entered data some decisions may be taken by that moment. For example, in commerce the situations are possible (usually when staff is not qualified enough or doesn't perform its obligations in the appropriate way) in which there is one name of the item, but different types of packing (for food products), different sizes (for clothes, shoes) etc. and incorrect entering of data (which do not correspond the real availability) conditions the number of the future misunderstandings (in

information system there is the size of the chosen shoes model and there is no such size in stock etc.). Besides, in this case incorrect decision may be taken as for the purchase of the necessary products.

Information risks of the logistic streams. This type of risks is first of all connected with information streams. However, in a certain way this type of risks is indirectly typical of other streams due to the fact that any logistic stream may not exist and flow without the accompanying and present inn it information. Information stream may be characterized by the following factors [16]: the source of occurrence; direction of the stream movement; the speed of reception and transfer; the intensity of stream; the volume of stream etc. Thus, under information risks of logistic streams we will understand the potential negative changes in the indicators of the information stream and other streams that are conditioned by changes in the accompanying information stream. For example, one of such risks is the risk of reduction of speed of information stream due to the use of information and telecommunication networks and systems by bigger number of users and their transfer of the increased volume of information. Let us recall how the speed of the home Internet may fall in the evening or at the weekend when all the people are home in comparison with day time on week days. The reason for this is the use of the same channel of information by a bigger number of people and transfer of the bigger volume of information is performed. The same may happen in the logistics systems. This is why actual is the task of choice of hardware and software which would allow working quickly and effectively in case of the increased information loads on the system.

Depending on the type of information carrier we may distinguish *the electronic information risks and "traditional" information risks.* Electronic information risks are connected with probable undesired situations in functioning of the logistics system which are stipulated by incomplete, untimely or incorrect information represented in digital form with the help of various modern means that may be used for generation, transfer, reception or storing of such information. For example, there is a risk that transferred in electronic form invoice from the supplier will be incorrectly uploaded in information system of the researched company without additional control by personnel which will further condition the number of inefficient decisions. Automatic transfer of the price-lists by the suppliers to their contractors or by various Internet shops to the sites that are the accumulated catalogues of goods may also not always be successful. In particular, during generation of the price-lists file not all the cells may be filled which may condition some errors during import of the file in the contractors' system; during the transfer of such file breakdowns in the functioning of information and telecommunication networks may occur etc.

"Traditional" information risks are connected with probable undesired situations that may occur in functioning of the logistics system and are conditioned by incomplete, untimely or incorrect information represented in "traditional" form, i.e. on paper or oral form. For example, when a manager shares the information with subordinates, there may not be full understanding. Information about the product on its packing may be damaged while transporting which may bring about further problems in its movement to the consumer within the logistics system. For example, the damaged bar code will be impossible to identify automatically.

However, now information may very quickly change the type of its carrier, so it is quite hard to unambiguously talk about manifestation of electronic or traditional information risks. For example, the printed from the information system information (invoice, report etc.) may contain some mistakes – will it be the manifestation of electronic or traditional information risks? In this case, in our opinion, we need to mention *mixed information risks.*

Management of the logistics systems information risks. The aim of developing the system of management of information risks of the logistics systems is to minimize the potential negative influence of manifestations of such risks on functioning of the logistics system in general and its elements. The system of information risk management constitutes of such elements [1]:

– subject of management – a person or a group of people having the corresponding competences for taking managing decisions and bearing responsibility for the consequences of realization and taking such decisions;

– principles of risk management – rules and statements which should be observed in the process of managing the information risks of the logistics system;

– methods of risk management – means of actions aimed at achieving the goal (or goals) of information risk management. They are the basis of tactics of information risks management;

– means of risk management – various instruments (material, intellectual, technical, information resources; innovative technologies; mathematical models of evaluation and forecasting of risks etc.);

– strategy of information risk management – general plan as for managing information risks for a long period of time which is based, in particular, on the forecast evaluations of the levels of information risks and ways of their elimination.

At the moment there is no generally accepted approach as for developing the system of information risk management of the logistics system. However, various state and field standards and methodologies may the guides, for example:

– ISO/IEC 27001:2013 “Information technologies. Methods of security protection. The system of management of information security. Requirements” [21], ISO/IEC 27002:2013 “Information technologies. Methods of security protection. Collection of rules of information protection management” [22];

– NIST (National Institute of Standards and Technology 800-30 “A guide on managing risks for information and technological systems” [23];

– CRAMM (CCTA Risk Analysis and Management Method), Central Computer and Telecommunications Agency (CCTA) [24, 25];

– OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation [26];

– COBIT 5 for Risk [27];

– DSTU 3396.0-96 “Protection of information. Technical protection of information. Major statements” [28], DSTU 3396.1-96 “Protection of information. Technical protection of information. Procedure for the conduct of works” [29], DSTU 3396.2-97 “Protection of information. Technical protection of information. Terms and definitions” [30].

A thorough analysis of methodologies NIST 800-30, CRAMM, OCTAVE was performed, in particular, in investigations [19, 31].

The managing of information risks of the logistics systems should be performed in the context of general risk management and may consist of stages enlisted, in particular, in [32, 33]:

1) Evaluation of the environment. At this stage strategic, tactical and operational goals of information risk management of the logistics system are determined;

2) Evaluation of risk. This stage includes identification, analysis and calculation (evaluation) of risk;

3) Decrease of the risk level. At this stage the results of information risk management and decisions as for the frames of the allowed level of the corresponding risks, the effectiveness and level of the allowed information risks are evaluated.

Besides, for managing information risks one may use the generalized schematic diagram of risk management which is represented in [34] and adapted to logistic risks in [33].

One of the main stages of information risks management is qualitative and quantitative analysis of risks. Qualitative analysis of information risks presupposes identification of factors of information risks, the number of situations in which the corresponding threats may occur – in particular, the threat to information security. Qualitative evaluation of information risks may be performed, for example, with the help of expert evaluations method [1]. For performing the quantitative analysis of information risks one may use the number of methods [1, 14, 33, 35], among which are the method of analogies, the analysis of vulnerability, methods of imitational modeling, analysis of the market of potential losses, statistical method, scenario method etc. To quantitative indexes of the risk level are referred [1, 14, 35]: the expected potential losses; the risk coefficient; mean-square deviation; dispersion; the coefficient of variation; semi-variation; semi-square deviation; the coefficient of semi-variation; the coefficient of asymmetry; the coefficient of excess.

Qualitative and quantitative analysis of information risks, their quantitative evaluation may be a good ground for taking the corresponding managing decisions the aim of which is achieving the goals of functioning of the logistics system with the help of appropriate economic and mathematical models.

Modeling of information risks of logistics system. Today risks of information security are the most researched, and for them various models exist. Now the models may be divided into models of detection of threats and vulnerabilities and models of information streams [36]. In the work [37] the following models are enlisted: the model of evaluation of information security risks; imitational model of processing information security risks on the basis of the painted Petri net; model of detecting the vulnerabilities in the process of exploitation the information system of the company with the use of business games (the method of brainstorm is taken as basis for the game); incremental model of development of information security system which allows, in particular, speeding up the creation of such system. The constituent parts of one of the possible models of information streams can be found in [36], where the process of information security risks evaluation by threats of maintenance failure, confidentiality and integrity is described. Such models have the corresponding software realization.

However, few works are devoted to modeling of other types of information risks, and it is necessary to fill this gap. There are various instruments of mathematical modeling that can be used for information risks modeling. The concept of the game theory [14] is one of the progressive concepts that can be used for solving the problems of taking decisions in logistics which are burdened, in particular, by information risks. Within the frames of this concept a number of information situations are distinguished which are characterized by the level of uncertainty as for the economic environment being in one of its possible states at the moment of the subject of management taking decision [38]. Depending on information situation various criteria of decisions taking may be used in managing the process of functioning of the logistics system which are set forth in [14, 38].

We regard as prospective the use of the basic instruments of artificial intellect in modeling of information risks of the logistics systems: expert systems, artificial neuron nets, fuzzy sets and fuzzy logic, population methods and optimization models (genetic algorithm and coevolution). These instruments have their advantages and disadvantages which require separate investigations as for the development of the corresponding economic and mathematical models of evaluation of information risks of the logistics systems.

Conclusions. Information if competently used has always been one of the means due to which the companies could increase their competitiveness. Information carriers have been changing throughout the existence of the mankind – usually new carriers appear. In particular, the development of the up-to-date information and telecommunication technologies allowed to more widely use information in electronic form for both household and business needs. Such use conditioned the widening of spectrum of information risks. Information risks of the logistics systems acquire the ever bigger part among other risks. That is why it is necessary to be able to determine their sources, to evaluate, model and manage them. Some aspects of this problem were considered in this article.

By this work we wanted to widen the understanding of information risks, in particular, of logistics systems. We made a definition of information risks of the logistics systems, described their object, subject, sources. We offered classification of such risks and showed conceptual approaches to modeling and managing information risks of logistics systems and prospects for further investigations. In particular, it is appropriate to develop the theory and modeling of information risk of logistics systems in the following directions: qualitative and quantitative analysis; indexes of the qualitative evaluation of the risk level; economical and mathematical modeling; risk management.

1. Управління ризиками в логістиці: [навч. посіб.] / В. М. Гончаров, Р. Р. Ларіна, О. В. Балуєва та ін.]; за заг. ред. В. М. Гончарова. – Львів: Магнолія 2006, Луганськ – 2013. – 253 с. 2. Управление рисками в логистике: учеб. пособие для студ. учреждений высш. проф. образования / Г. Л. Бродецкий, Д. А. Гусев, Е. А. Елин. – М.: Издательский центр «Академия», 2010. – 192 с. – (Непрерывное профессиональное образование: Логистика). 3. Єнченко Є. В. Моделювання і управління системними ризиками в логістиці [Текст] : дис... канд. екон. наук : 08.03.02 «Економіко-математичне моделювання» / Є. В. Єнченко. – К., 2006. – 229 с. 4. Ровенских М. В. Управление рисками логистической системы промышленного предприятия: дис… канд. экон. наук : 08.00.05 «Экономика и управление народным хозяйством: логистика» / М. В. Ровенских. — Санкт-

Петербург, 2008. — 261 с. 5. Волинець Л. М. Обґрунтування необхідності управління ризиками в логістичній системі підприємства / Л. М. Волинець, І. П. Гамеляк // Управління проектами, системний аналіз і логістика. – К.:НТУ – 2012. – Вип. 10. – С. 382–386. 6. Короленко Н. В. Управление рисками логистической системы предприятия: теоретические аспекты [Електронний ресурс] / Н. В. Короленко // Ефективна економіка. – 2013. – № 10. – Режим доступу: http://www. economy.nayka.com.ua/?op=1&z=2428 7. Кондратенко Н. О. Інструменти управління та методи оцінки ризиків у логістичних системах [Електронний ресурс] / Н. О. Кондратенко, О. О. Лобашов // Науково-технічний збірник «Комунальне господарство міст». Серія «Економічні науки». – 2012. – Вип. 102. – С. 343–350. – Режим доступу: http://eprints.kname.edu.ua/25233/1/343-350%20Кондратенко%20НО.pdf 8. Korecký M. Risk management in logistics [Електронний ресурс] / M. Korecký // Carpathian Logistics Congress 7. – 9. 11. 2012, Jeseník, Czech Republic, EU. – Режим доступу: http://konsys2.tanger.cz/files/proceedings/09/reports/837.pdf 9. Селюченко Н. Є. Інформаційний ризик в антикризовому управлінні / Н. Є. Селюченко, В. П. Кічор // Вісник Національного університету «Львівська політехніка» «Проблеми економіки та управління». – 2008. – № 611. – С. 197–202. 10. Замула О. А. Система управління інформаційними ризиками компаній / О. А. Замула, В. І. Черниш, К. І. Іванов, Б. В. Волобуєв // Радіолектронні і комп'ютерні системи, 2011. – № 4 (52). – С. 134–139. 11. Мельник Г. В. Моделювання системи управління інформаційними ризиками в корпоративній інформаційній системі / Г.В. Мельник // Бізнес-Інформ, 2013. – № 9. – С. 95–99. 12. Крикавський Є. В. Логістичні системи: навч. посіб. / Є. В. Крикавський, Н. В. Чорнописька. – Львів: Видавництво Національного університету «Львівська політехніка», 2009. – 264 с. 13. Бажин И. И. Логистика: компакт-учебник. – Харьков: Консум, 2003. – 181 с. 14. Вітлінський В. В. Ризикологія в економіці та підприємництві: монографія / В. В. Вітлінський., Г. І. Великоіваненко – К.: КНЕУ, 2004. – 480 с. 15. Рогов М. А. Риск-менеджмент [монография] / М. А. Рогов. – М.: Финансы и статистика, 2001. – 120 с. 16. Гаджинский А. М. Логистика: учебник / А. М. Гаджинский. – 16-е изд., перераб. и доп. – М.: Издательско-торговая корпорация «Дашков и Ко», 2008. – 484 с. 17. Денисенко М. П. Організація та проектування логістичних систем: підручник / за ред. проф. М. П. Денисенка, проф. П. Р. Левковця, проф. Л. І. Михайлової. – К.: Центр учбової літератури, 2010. – 336 с. 18. Балабанова Л. В. Логістика: підручник / Л. В. Балабанова, А. М. Германчук. – Львів: Магнолія 2006, 2013. – 368 с. 19. Ромака В. А. Менеджмент у сфері захисту інформації: підручник / В. А. Ромака, Р. О. Корж, Ю. Р. Гарасим. – Львів, ЗУКЦ, 2013. – 462 с. 20. Риски информационной безопасности [Електронний ресурс] на сайті компанії «ARinteg». – Режим доступу: http://www.arinteg.ru/articles/riski-informatsionnoy-bezopasnosti-26222.html 21. ISO/IEC 27001:2013 «Information technology. Security techniques. Information security management systems. Requirements» [Електронний ресурс]. – Режим доступу: https://www.iso.org/obp/ui/ #iso:std:iso-iec:27001:ed-2:v1:en 22. ISO/IEC 27002:2013 «Information technology. Security techniques. Code of practice for information security controls» [Електронний ресурс]. – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en 23. NIST Special Publication 800-30 «Risk Management Guide for Information Technology Systems» [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/ nistpubs/800-30/sp800-30.pdf 24. 10 Steps to Do It Yourself CRAMM [Електронний ресурс]. – Режим доступу: http://itsmsolutions.com/wp-content/uploads/2013/01/ DITYvol4iss50.pdf 25. A Qualitative Risk Analysis and Management Tool – CRAMM [Електронний ресурс]. – Режим доступу: http://www. sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 26. Parthajit Panda. The OCTAVE® Approach to Information Security Risk Assessment [Електронний ресурс] / ISACA Journal, vol. 4, 2009. – Режим доступу: http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Documents/jpdf094-the-OCTAVE.pdf 27. COBIT 5 for Risk [Електронний ресурс] / ISACA. – Режим доступу: http://www.isaca.org/ COBIT/Pages/Risk-product-page.aspx 28. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення» [Електронний ресурс]. – Режим доступу: http://info-stand.com/downloads/dstu/dstu-3396.0-96/dstu-3396.0-96.pdf 29. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт» [Електроний ресурс]. – Режим доступу: http://info-stand.com/ downloads/dstu/dstu-3396.1-96/dstu-3396.1-96.pdf 30. ДСТУ 3396.2-97 «Захист інформації. Технічний

захист інформації. Терміни та визначення» [Електронний ресурс]. – Режим доступу: http://info-stand.com/downloads/dstu/dstu-3396.2-97/dstu-3396.2-97.pdf 31. Гарасим Ю. Р. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем [Електронний ресурс] / Ю. Р. Гарасим, В. А. Ромака, М. М. Рибій // Вісник Національного університету "Львівська політехніка". "Автоматика, вимірювання та керування". – 2013. – № 753. – С. 90–99. – Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/23330/1/16-90-99.pdf 32. ISO. Risk Management – Principles and guidelines ISO 31000. Switzerland: ISO, 2009. – 24 p. 33. Вітлінський В. В. Концептуальні засади моделювання та управління логістичним ризиком підприємства [Електронний ресурс] / В. В. Вітлінський, В. І. Скіцько // Проблеми економіки. – Науково-дослідний центр індустріальних проблем розвитку НАН України, 2013. – № 4. – С. 246–253. – Режим доступу: http://www.problecon.com/_inc/kachka_pdf.php?year=2013&volume=4_0&pages=246_253 &abstract=2013_04_0'))%20{return%20false} 34. Вітлінський В. В. Основні засади управління ризиком в бізнесі / В. В. Вітлінський // Машинна обробка інформації. – 1995. – Вип. 57. – С. 12–23. 35. Вітлінський В. В. Аналіз, оцінка і моделювання економічного ризику. – К.: ДЕМІУР, 1996. – 212 с. 36. Куканова Н. Методика оценки риска ГРИФ 2006 из состава Digital Security Office [Електронний ресурс] / Н. Куканова. – Режим доступу: http://www.dsec.ru/ipm-research-center/article/risk_ assessment_method_ vulture_2006_from_the_composition_of_the_digital_security_office/?sphrase_id=1695 37. Кононович В. Г. Моделювання процесів управління ризиками інформаційної безпеки [Електронний ресурс] / В. Г. Кононович, Ю. В. Копитін // Збірник наукових праць «Управління розвитком складних систем». – 2013. – № 16. – С. 100–109. – Режим доступу: http://urss.knuba.edu.ua/files/zbirnyk-16/21.pdf 38. Економічний ризик: ігрові моделі: навч. посіб. / В. В. Вітлінський, П. І. Верченко, А. В. Сігал, Я. С. Наконечний; за ред.. д-ра екон. наук., проф. В. В. Вітлінського. – К.КНЕУ, 2002. – 446 с.

1. Goncharov V. M., & Larina R. R., & Baluyeva O. V. (2006). Upravlinnia ryzykamy v lohistytsi. Lviv, Lugansk: «Magnoliia 2006». 2. Brodetskiy G. L., & Gusev D. A., & Yelin E. A. (2010). Upravlenie riskami v logistike. Moskva: Izdatelskiy centr «Akademiya». 3. Yenchenko, Ye. V. (2006). Modeliuvannia i upravlinnia systemnymy ryzykamy v lohistytsi: dysertatsiia kandydata ekonomichnikh nauk: 08.03.02 «Ekonomiko-matematychne modeliuvannia». Kyiv. 4. Rovenskikh M. V. (2008). Upravlenie riskami logisticheskoy sistemy promyshlennogo predpriyatiya: disertatsiya kandidata ekonomicheskikh nauk : 08.00.05 «Ekonomika i upravlenie narodnym khozyaistvom: logistika». Sankt-Peterburg. 5. Volynets L. M., & Gamelyak, I. P. (2012). Obgruntuvannia neobkhidnosti upravlinnia ryzykamy v lohistychnii systemi pidpryiemstva. Upravlinnia proektamy, systemnyi analiz i logistyka, 10, 382-386. 6. Korolenko N. V. (2013). Upravlenie riskami logisticheskoy sistemy predpriyatiya: teoreticheskie aspekty. Efektivna ekonomika, 10, from http://www.economy.nayka.com.ua/?op=1&z=2428 7. Kondratenko N. O., & Lobashov O. O. (2012). Instrumenty upravlinnia ta metody ocinky ryzykiv u lohistychnykh systemakh. Naukovo-tehnichnyi zbirnyk «Komunalne gospodarstvo mist». Seriia «Ekonomichni nauky», 102, 343-350, from http://eprints.kname.edu.ua/25233/1/343-350%20Kondratenko%20NO.pdf 8. Korecký M. (2012). Risk management in logistics. Carpathian Logistics Congress 7–9. 11. 2012, Jeseník, Czech Republic, EU. from: http://konsys2.tanger.cz/files/proceedings/09/reports/837.pdf 9. Seljuchenko N. Ye., & Kichor V. P. (2008). Informaciinyi ryzyk v antykryzovomu upravlinni. Visnyk Nacionalnogo universytetu «Lvivska politekhnika». Seriia «Problemy ekonomiky ta upravlinnia», 611, 197–202. 10. Zamula O. A., & Chernysh V. I., & Ivanov K. I., & Volobuiev B. V. (2011). Systema upravlinnia informaciinymy ryzykamy kompanii. Radiolektronni i kompiuterni systemy, 4(52), 134–139. 11. Melnyk G. V. (2013). Modeliuvannia systemy upravlinnia informaciinymy ryzykamy v korporatyvnii informaciinii systemi. Biznes-Inform, 9, 95–99. 12. Krykavskyy Ye. V., & Chornopyska N. V. Logistychni systemy. Lviv: Vydavnytsvo Nacionalnogo universytetu «Lvivska politekhnika». 13. Bazhin I. I. (2003). Logistika. Xarkov: Konsum. 14. Vitlinskyy V. V., & Velykoivanenko, G. I. (2004). Ryzykologiia v ekonomici ta pidpryiemnytsvi: Monografiia. Kyiv: KNEU. 15. Rogov, M. A. (2001). Risk-menedzhment [monografiya]. Moskva: Finansy i statistika. 16. Gadzhinskiy A. M. (2008). Logistika. Moskva: Izdatelsko-torgovaia korporaciia «Dashkov i Ko». 17. Denysenko M. P., & Levkovets P. R., & Mykhailova L. I. (2010). Organizaciia ta proektuvannia logistychnykh system. Kyiv:

Tsentr uchbovoi literatury. 18. Balabanova L. V., Germanchuk A. M. (2013). Logistyka. Lviv: «Magnoliia 2006». 19. Romaka V. A., & Garasym Yu. R. (2013). Menedzhment u sferi zahystu informacii. Lviv, ZUKC. 20. Riski informacionnoi bezopasnosti, from: http://www.arinteg.ru/articles/riski-informatsionnoy-bezopasnosti-26222.html 21. ISO/IEC 27001:2013 «Information technology. Security techniques. Information security management systems. Requirements», from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en 22. ISO/IEC 27002:2013 «Information technology. Security techniques. Code of practice for information security controls», from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en 23. NIST Special Publication 800-30 «Risk Management Guide for Information Technology Systems», from: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf 24. 10 Steps to Do It Yourself CRAMM, from: http://itsmsolutions.com/wp-content/uploads/2013/01/DITYvol4iss50.pdf 25. A Qualitative Risk Analysis and Management Tool – CRAMM, from: http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 26. Parthajit Panda. (2009). The OCTAVE® Approach to Information Security Risk Assessment. ISACA Journal, 4, from: http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Documents/jpdf094-the-OCTAVE.pdf 27. COBIT 5 for Risk. ISACA, from: http://www.isaca.org/COBIT/Pages/Risk-product-page.aspx 28. DSTU 3396.0-96 «Zakhyst informacii. Tekhnichnyi zakhyst informacii. Osnovni polozhennia», from: http://info-stand.com/downloads/dstu/dstu-3396.0-96/dstu-3396.0-96.pdf 29. DSTU 3396.1-96 «Zakhyst informacii. Tekhnichnyi zakhyst informacii. Poriadok provedennia robit», from: http://info-stand.com/downloads/dstu/dstu-3396.1-96/dstu-3396.1-96.pdf 30. DSTU 3396.2-97 «Zakhyst informacii. Tekhnichnyj zakhyst informacii. Terminy ta vyznachennia», from: http://info-stand.com/downloads/dstu/dstu-3396.2-97/dstu-3396.2-97.pdf 31. Garasym, Yu.R., & Romaka, V.A., & Rybiy, M.M. (2013). Analiz procesu upravlinnia ryzykamy informaciinoi bezpeky v procesi zabezpechennia vlastyvosti zhyvuchosti system. Visnyk Nacionalnogo universytetu «Lvivska politekhnika». Seriia «Avtomatyka, vymiriuvannia ta keruvannia», 753, 90-99. from: http://ena.lp.edu.ua:8080/bitstream/ntb/23330/1/16-90-99.pdf 32. ISO. Risk Management – Principles and guidelines. ISO 31000. (2009). Switzerland: ISO. 33. Vitlinskyy, V.V., Skitsko, V.I. (2013). Konceptualni zasady modeliuvannia ta upravlinnia logistychnym ryzykom pidpryiemstva. Problemy ekonomiky, 4, 246–253, from: http://www.problecon.com/_inc/kachka_pdf.php?year=2013&volume=4_0&pages=246_253&abstract=2013_04_0'))%20{return%20false} 34. Vitlinskyy, V.V. (1995). Osnovni zasady upravlinnia ryzykom v biznesi. Mashynna obrobka informacii, 57, 12–23. 35. Vitlinskyy, V.V. (1996). Analiz, otsinka i modeliuvannia ekonomichnogo ryzyku. Kyiv: DEMIUR. 36. Kukanova, N. Metodika otsenki riska GRIF 2006 iz sostava Digital Security Office, from: http://www.dsec.ru/ipm-research-center/article/risk_assessment_method_vulture_2006_from_the_composition_of_the_digital_security_office/?sphrase_id=1695 37. Kononovych, V. G., Kopytin, Yu. V. (2013). Modeliuvannia procesiv upravlinnia ryzykamy informaciinoi bezpeky. Upravlinnia rozvytkom skladnykh system, 16, 100–109, from: http://urss.knuba.edu.ua/files/zbirnyk-16/21.pdf 38. Vitlinskyy V. V., & Verchenko P. I., & Sigal A. V., & Nakonechnyi Ya. S. (2002). Ekonomichnyi ryzyk: igrovi modeli. Kyiv, KNEU.